MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DESPACHO Nº 147.2021.DOF - ORÇAMENTO.0745808.2021.015252

Em atenção ao Decreto nº 44.751 de 27/10/2021 que dispõe sobre os procedimentos a serem adotados para o encerramento da execução orçamentária, financeira e contábil do exercício de 2021, sobrestam-se os autos, aos quais se dará prossseguimento com a reabertura do sistema de execução orçamentária para o exercício de 2022.

Atenciosamente,

FRANCISCO EDINALDO LIRA DE CARVALHO
Diretor de Orçamento e Finanças

Documento assinado eletronicamente por **Francisco Edinaldo Lira de Carvalho**, **Diretor(a) de Orçamento e Finanças - DOF**, em 27/12/2021, às 09:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0745808** e o código CRC **5CBBF4F3**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

QUADRO - RESUMO DO PROCESSO DE COMPRA Nº 345.2021.SCOMS.0731246.2021.015252

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS	PI nº: 2021.015252
PROCURADORIA-GERAL DE JUSTIÇA	PC Nº 170/2021
SETOR DE COMPRAS E SERVIÇOS	DATA: 24/11/2021

IDENTIFICAÇÃO DO FORNECEDOR

RAZÃO SOCIAL	INDEFINIDO – A LICITAR
CNPJ	-

DETALHAMENTO DO OBJETO

Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
1	Serviço de Firewall em Alta Disponibilidade	Meses	48	R$ 68.580,67	R$ 3.291.872,16
2	Serviço de Monitoramento da Solução	Meses	48	R$ 50.919,00	R$ 2.444.112,00
3	Serviço de Migração do Ambiente Atual	Unidade	1	R$ 30.553,33	R$ 30.553,33
4	Serviço de Treinamento da Solução	Pessoas	5	R$ 12.377,67	R$ 61.888,35

TOTAL		R$ 5.828.425,84
MODALIDADE DA CONTRATAÇÃO		**FUNDAMENTO LEGAL**
	DISPENSA DE LICITAÇÃO	
	INEXIGIBILIDADE DE LICITAÇÃO	
	SISTEMA DE REGISTRO DE PREÇOS	
	PRORROGAÇÃO DE CONTRATO	
X	**A LICITAR**	**Lei 8.666/93**
INFORMAÇÕES COMPLEMENTARES		
Encaminhe-se à DOF para providências.		

Documento assinado eletronicamente por **Edjane de Pinho Oliveira**, **Chefe do Setor de Compras e Serviços - SCOMS**, em 24/11/2021, às 16:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Adryne Pinheiro Benones**, **Estagiário(a)**, em 24/11/2021, às 16:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0731246** e o código CRC **11802D80**.

MAPA DEMONSTRATIVO DE PREÇOS Nº 130.2021.SCOMS.0731238.2021.015252

Procedimento Interno: 2021.015252
Processo de Compras: 170/2021

MAPA DEMONSTRATIVO DE PREÇOS

Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE	VALOR ESTIMADO UNITÁRIO	VALOR ESTIMADO TOTAL
A		Serviço de Firewall em Alta Disponibilidade	**48**	**R$ 68.580,67**	**R$ 3.291.872,16**
		Fontes Consultadas	**UNIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
	1	Network Secure Seguranca da Informacao LTDA CNPJ: 05.250.796/0001-54	Meses	R$ 80.824,00	R$ 3.879.552,00
		Servix Informática LTDA – BA CNPJ: 01.134.191/0003-09	Meses	R$ 45.418,00	R$ 2.180.064,00
		NTSec Soluções em Teleinformática LTDA CNPJ: 09.137.728/0002-15	Meses	R$ 79.500,00	R$ 3.816.000,00
	ITEM	**DESCRIÇÃO**	**QUANTIDADE**	**VALOR ESTIMADO UNITÁRIO**	**VALOR ESTIMADO TOTAL**
		Serviço de Monitoramento da Solução	**48**	**R$ 50.919,00**	**R$ 2.444.112,00**
		Fontes Consultadas	**UNIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
	2	Network Secure Seguranca da Informacao LTDA CNPJ: 05.250.796/0001-54	Meses	R$ 42.408,00	R$ 2.035.584,00
		Servix Informática LTDA – BA CNPJ: 01.134.191/0003-09	Meses	R$ 70.349,00	R$ 3.376.752,00
		NTSec Soluções em Teleinformática LTDA CNPJ: 09.137.728/0002-15	Meses	R$ 40.000,00	R$ 1.920.000,00
	ITEM	**DESCRIÇÃO**	**QUANTIDADE**	**VALOR ESTIMADO UNITÁRIO**	**VALOR ESTIMADO TOTAL**
		Serviço de Migração do Ambiente Atual	**1**	**R$ 30.553,33**	**R$ 30.553,33**

	3	**Fontes Consultadas**	**UNIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
		Network Secure Seguranca da Informacao LTDA CNPJ: 05.250.796/0001-54	Unidade	R$ 30.000,00	R$ 30.000,00
		Servix Informática LTDA – BA CNPJ: 01.134.191/0003-09	Unidade	R$ 23.660,00	R$ 23.660,00
		NTSec Soluções em Teleinformática LTDA CNPJ: 09.137.728/0002-15	Unidade	R$ 38.000,00	R$ 38.000,00
	ITEM	**DESCRIÇÃO**	**QUANTIDADE**	**VALOR ESTIMADO UNITÁRIO**	**VALOR ESTIMADO TOTAL**
	4	Serviço de Treinamento da Solução	**5**	**R$ 12.377,67**	**R$ 61.888,35**
		Fontes Consultadas	**UNIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
		Network Secure Seguranca da Informacao LTDA CNPJ: 05.250.796/0001-54	Pessoas	R$ 10.000,00	R$ 50.000,00
		Servix Informática LTDA – BA CNPJ: 01.134.191/0003-09	Pessoas	R$ 12.133,00	R$ 60.665,00
		NTSec Soluções em Teleinformática LTDA CNPJ: 09.137.728/0002-15	Pessoas	R$ 15.000,00	R$ 75.000,00
TOTAL					**R$ 5.828.425,84**

INFORMAÇÕES COMPLEMENTARES

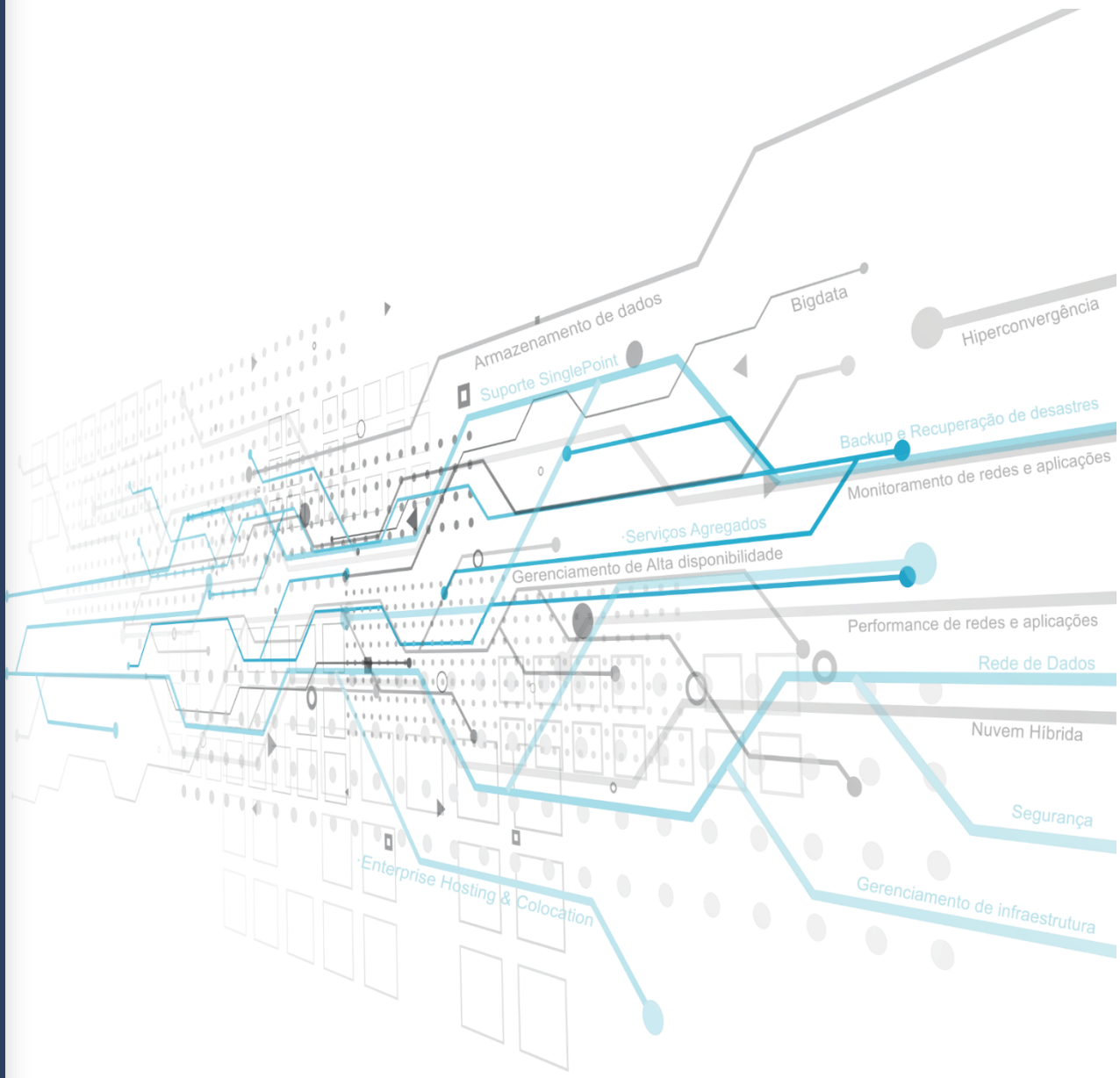
- Período de Cotação de Preços: 08/11/2021 a 24/11/2021. Considerando o tempo decorrido para a tentativa de recebimento de, no mínimo, 3 (três) propostas válidas, justifica-se que, somente nesta data foi possível finalizar a etapa de pesquisa de preços visando à aquisição pretendida, não sendo possível cumprir o prazo de 5 (cinco) dias úteis, disposto no Ato PGJ N°0112/2012.
- Responsável pela Cotação: Adryne Benones, sob supervisão de Edjane Oliveira.
- Método matemático aplicado para a definição do valor estimado: (X) Média.
-Justificativa: O preço médio é adotado quando a frequência de um conjunto de preços é simétrica, ou seja, quando a média e a mediana coincidem.
- Este Setor de Compras e Serviços realizou pesquisa de mercado junto aos fornecedores: : Actar <mg@actar.com.br>; Algartele <editais@algartelecom.com.br>; Altasnet <compras@altasnet.com.br>; Approachtec <daniels@approachtec.com.br>; Arper <comercial@arper.com.br>; Arvvo <andre.oliveira@arvvo.com.br>; BFF Companybsb <bffcompanybsb@gmail.com>; Blueeye <comercial@blueeye.com.br>; Via Contabil<registro.viacontabil@gmail.com>; Comdados BA <sac@comdados-ba.com.br>; Compwire <joao.wagnitz@compwire.com.br>; Core Tecnologia <vendas.core@coretecnologia.net.br>;Callebe Araujo <callebearaujo@gmail.com>; Cyberone <fernando@cyberone.com.br>; Dask <comercial@dask.com.br>; Everco <contato@everco.com.br>; Fasthelp <contato@fasthelp.com.br>;Contelb <contelb@contelb.com.br>; Future <rafael.sampaio@future.com.br>

Documento assinado eletronicamente por **Edjane de Pinho Oliveira**, **Chefe do Setor de Compras e Serviços - SCOMS**, em 24/11/2021, às 16:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Adryne Pinheiro Benones**, **Estagiário(a)**, em 24/11/2021, às 16:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0731238** e o código CRC **CDFA9D99**.

SERVIX



PROPOSTA TÉCNICA E COMERCIAL

www.servix.com

Proposta: SVX210597

São Paulo, 4 de novembro de 2021.

À

Ministério Público do Estado do Amazonas - MPAM,

Ref.: Solução de Segurança NGFW.

Prezado (a),

Conforme sua solicitação, estamos encaminhando nossa **Proposta Técnica e Comercial** para fornecimento de solução completa conforme referência acima citada. Nós da Servix Informática, agradecemos a oportunidade e colocamo-nos a sua disposição para esclarecimento de qualquer dúvida.

Atenciosamente,

Eduardo Fidelis

Gerente de Contas

eduardo.fidelis@servix.com

(+55 11) 3525-3400 / +55 11 99249-1761

Wesley Magalhães

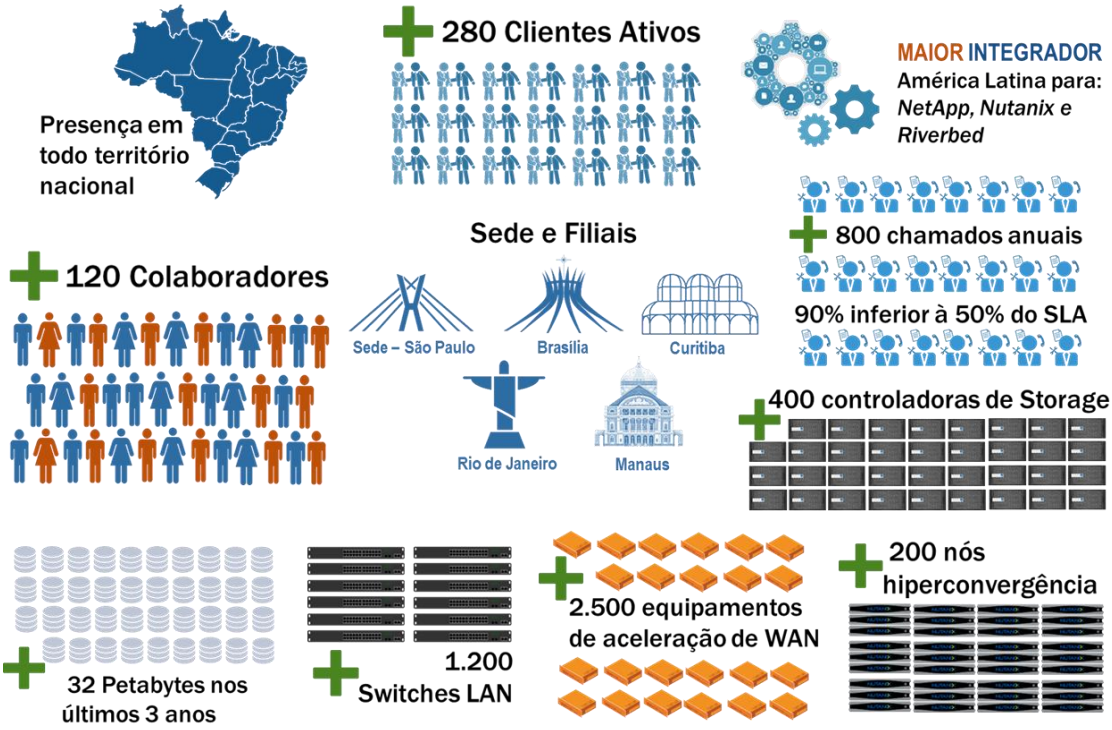
System Engineer

wesley.magalhaes@servix.com

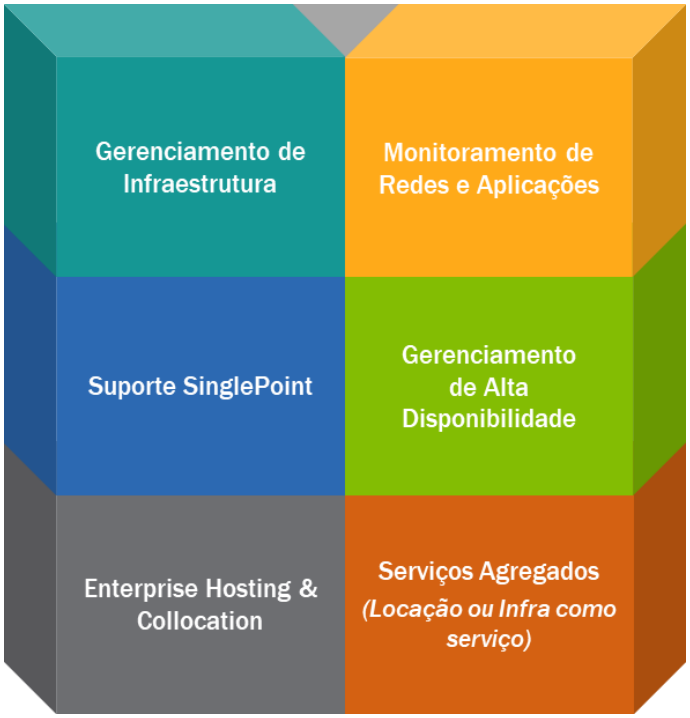
+55 11 9 7109-9226

Sobre a Servix

É integradora de soluções de tecnologia de informação para Datacenters, preparada para atender as necessidades tecnológicas de todos os segmentos de mercado. Temos um portfólio completo assim prestar atendimento de ponta a ponta.



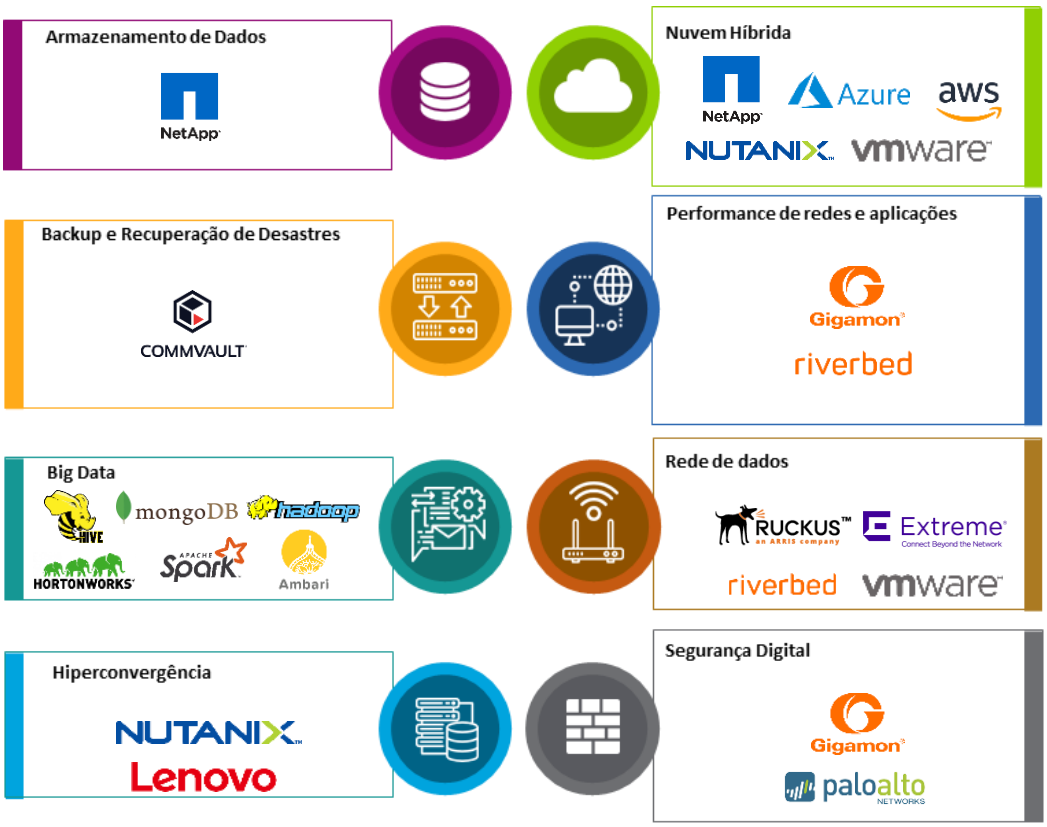
Nossos Serviços



SERVIX TEAM

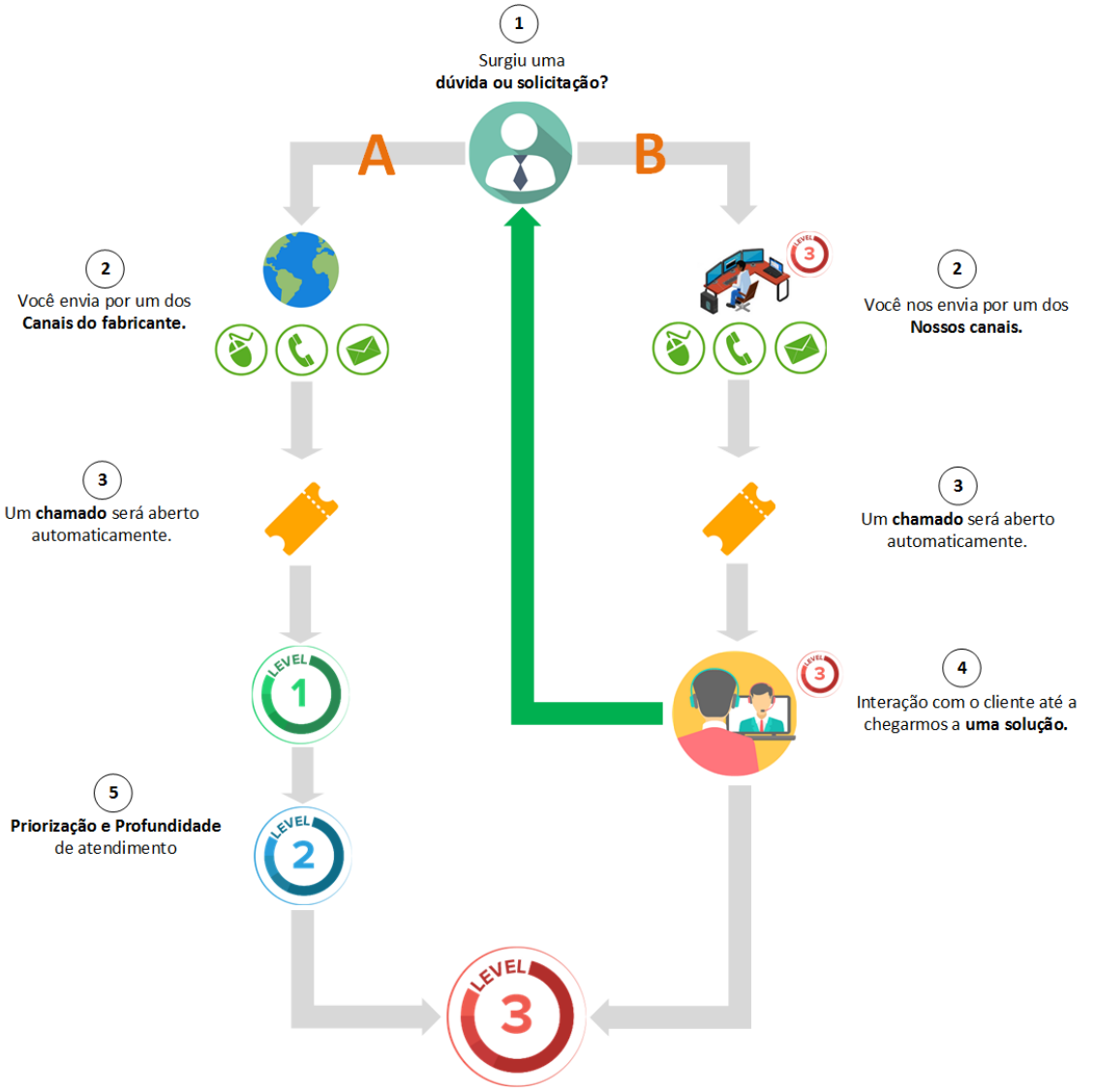
Nossas Soluções

Nossos Parceiros



Nós somos a diferença!

A Servix segue as melhores práticas de mercado, porém enxerga que apenas seguir as melhores práticas não basta para o mundo da corporativo e de Tecnologia dos dias de hoje. Devido ao seu know-how, a Servix personaliza o suporte, focando e auxiliando o cliente em melhoria contínua, eficiência técnica, priorização e acompanhamento de ocorrências. Conheça nosso fluxo e particularidades do atendimento:



Ao realizar o atendimento via Servix, na maioria das vezes, os chamados relacionados as dúvidas ou problemas são sanados no Especialista Servix de forma muito mais rápida, não havendo a necessidade de ter um escalonamento seguindo o SLA contratado no Fabricante. Em casos que a solução se dá somente pelo Fabricante, a Servix acompanha o atendimento, além de disponibilizar informações do ambiente ou execução de troubleshooting.

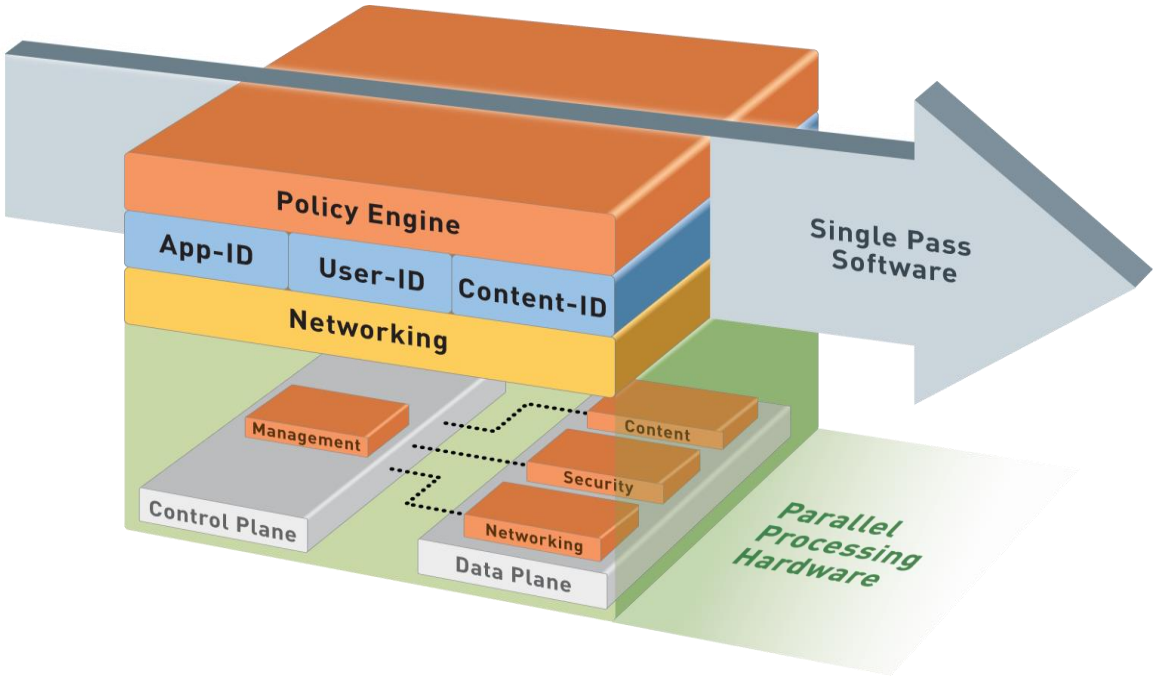
SUMÁRIO

DIFERENCIAIS PALO ALTO

A Palo Alto Networks é uma empresa de segurança de rede. Sua plataforma inovadora permite que as empresas, provedores de serviços e entidades governamentais protejam suas redes e permitam com segurança que um número cada vez mais complexo e crescente de aplicações rodem em suas redes.

O núcleo da plataforma da Palo Alto Networks é o nosso firewall de próxima geração (next-generation firewall), que oferece controle e visibilidade de aplicações, usuários e conteúdo integrados dentro do firewall por meio de sua arquitetura proprietária de hardware e software. Produtos e serviços Palo Alto Networks podem resolver uma ampla gama de requisitos de segurança de rede, a partir do datacenter para o perímetro de rede, bem como empresas distribuídas que incluem filiais e um número crescente de dispositivos móveis.

Single Pass Plataform



Passe único

- Operações únicas por pacote
    - Classificação de tráfego (identificação de Apps)
    - Mapeamento de usuário/grupo
    - Inspeção de conteúdo – ameaças, URLs, dados confidenciais
- Uma única política

Processamento Paralelo

- Hardware dedicado FPGA para funções específicas que funcionam em paralelo
- Hardware de gerência e dados separados

WildFire

Análises são realizadas em um ambiente Sandbox para arquivos desconhecido e, é apenas o primeiro passo para parar de forma eficaz ameaças avançadas. O serviço de análise baseada em cloud WildFire ™ analisa arquivos e links globalmente e designa itens nunca antes visto para uma investigação mais aprofundada por meio de análise estática e dinâmica ao longo de vários sistemas operacionais e versões de aplicativos. Se uma amostra é classificada como malicioso, o WildFire irá gerar automaticamente e preencher um conjunto holístico de novas prevenções para nossa Plataforma de Segurança de Próxima Geração e parceiros de integração, minimizando o risco de infecção a partir de ameaças conhecidas e desconhecidas, sem qualquer ação manual.

Thereat Prevention

No cenário de ameaças atual, os malwares tradicionais tornaram-se altamente segmentados e evasivos, e, especificamente projetado para ser completamente indetectável. O objetivo é violar o perímetro da rede, fornecendo malware que pode mover-se lateralmente em uma organização, extraindo dados valiosos como ele se espalha - tudo isso enquanto permanece invisível para firewalls tradicionais.

Palo Alto Networks protege sua rede contra essas ameaças, proporcionando múltiplas camadas de prevenção, enfrentando ameaças em cada fase do ataque. Nossa assinatura de prevenção de

ameaças protege a rede contra ameaças avançadas através da identificação e digitalização de todo o tráfego - aplicações, usuários e conteúdo em todas as portas e protocolos.

URL Filtering

Inteligência de ameaça global constantemente atualizada. Incluídos em nossa lista de categorias da web alguns são de alto risco, como malware, phishing e proxy-avoidance, que permitem controlar de forma granular o acesso a sites que se enquadram nestas categorias perigosas, impedir downloads, automatizar uma mensagem de aviso para Usuários, ou restringir o acesso completamente.

Nosso banco de dados global de filtragem de URLs é sincronizado com a inteligência de ameaças do WildFire e proteções geradas automaticamente a cada 15 minutos, o que significa que as categorias de URL, incluindo malware e phishing, estão sempre atualizadas para que seus usuários e dados estejam sempre protegidos.

Palo Alto Networks PA-3260 – Next-Generation Firewall

PA-3260

- Alta disponibilidade (H.A.) com modos ativo/ativo ou ativo/standby;
- Instalação simplificada;
- Identificação de aplicações independente da porta, da encriptação SSL/SSH ou técnicas de evasões aplicadas;
- Políticas de segurança para todos os usuários em todos os locais;
- Proteções extendidas para todos os vetores de ataques com as subscrições de segurança: *Threat Prevention, WildFire® malware prevention, URL Filtering, DNS Security e IoT Security;*
- Possibilidade de ativar a funcionalidade de SD-Wan simplesmente ativando a subscrição no equipamento existente.

	PA-3260
Taxa de transferência de firewall (HTTP/appmix)*	8,3/9,2 Gbps
Taxa de transferência do Threat Prevention (HTTP/appmix)†	4,1/5,0 Gbps
Taxa de transferência da VPN IPsec‡	5,0 Gbps
Máximo de sessões	3 M
Novas sessões por segundo§	105.000
Sistemas virtuais (base/máx)‖	1/6

Observação: os resultados foram medidos no PAN-OS 10.0.

SOLUÇÃO PROPOSTA

Com o objetivo de atender as necessidades do Ministério Público do Estado do Amazonas - MPAM, propomos a seguinte solução.

Cenário #01: Solução de NGFW – HA – Suporte de 48 meses.

Part #	Description	QTY
PA-PAN-PA-3260	Palo Alto Networks PA-3260	2
PA-PAN-PA-3260-TP-4YR-HA2	Threat prevention subscription 3-year prepaid, PA-3260	2
PA-PAN-PA-3260-URL4-4YR-HA2	PANDB URL filtering subscription 3-year prepaid, PA-3260	2
PA-PAN-PA-3260-WF-4YR-HA2	WildFire subscription 3-year prepaid, PA-3260	2
PA-PAN-SVC-PREM-3260-4YR	Partner enabled premium support 3-year prepaid, PA-3260	2
PA-PAN-SFP-PLUS-CU-5M	SFP+ to SFP+ PASSIVE TWINAX	2

Serviços Servix		
Serviço Servix	• Planejamento e Pós instalação • Implementação Lógica • Implementação Física • Serviço de Migração	1
Serviço Servix	Serviço de Monitoramento da Solução	1
Treinamento	40h para 5 pessoas	1

INVESTIMENTO

Nosso compromisso é o de propor soluções com qualidade e eficiência, agregando valor ao seu negócio. Razão pela qual nos empenhamos para propor valores que acreditamos ser competitivos com o mercado. O valor da solução proposta é de:

CENÁRIO 48 meses + Serviços

PLANILHA MODELO PARA PROPOSTA					
CONTRATAÇÃO DE SERVIÇO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO EM ALTA DISPONIBILIDADE, COM MONITORAMENTO, PELO PERÍODO DE 48 (QUARENTA E OITO) MESES, INCLUINDO TREINAMENTO E SERVIÇO DE MIGRAÇÃO DA PLATAFORMA ATUAL.					
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTD**	**VALOR MENSAL**	**VALOR TOTAL**
1	SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE.	MÊS	48	R$ 45.418,00	R$ 2.180.064,00
2	SERVIÇO DE MONITORAMENTO DA SOLUÇÃO.	MÊS	48	R$ 70.349,00	R$ 3.376.752,00
3	SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL.	UNIDADE	1	R$ 23.660,00	R$ 23.660,00
4	SERVIÇO DE TREINAMENTO DA SOLUÇÃO.	PESSOA	5	R$ 12.133,00	R$ 60.665,00
TOTAIS				**R$ 151.560,00**	**R$ 5.641.141,00**

PACOTE DE SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DE SOLUÇÃO

PREMISSAS

- ✓ Todos os itens descritos nesta proposta estão sujeitos à execução pela Servix somente quando licenças e suporte ativos e vigentes junto ao Fabricante da solução;
- ✓ As tarefas de "Pré-instalação" serão executadas em horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Instalação" podem ser executadas em horário comercial ou de expediente da Contratante, contudo a Servix indica que tais tarefas sejam executadas fora do horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Configuração" podem ser executadas em horário comercial ou de expediente da Contratante, contudo a Servix indica que tais tarefas sejam executadas fora do horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Migração", quando contempladas em proposta, podem ser executadas em horário comercial ou de expediente da Contratante, contudo a Servix indica que tais tarefas sejam executadas fora do horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Pós-instalação" serão executadas em horário comercial ou de expediente da Contratante;

PRÉ-INSTALAÇÃO

- ✓ Reunião de Kickoff com a Contratante;
  - Apresentar o projeto aprovado e contratado;
  - Obter os contatos e definir os times e horário dos trabalhos;
  - Apresentar equipe de gerentes e analistas da Servix;
  - Apresentar o cronograma preliminar do projeto;
  - Definir datas e restrições para o início da instalação;
- ✓ Análise da topologia, arquitetura da rede e desenho do ambiente, considerando todos equipamentos já existentes instalados que serão envolvidos no projeto;
  - Enviar o Guia de Requisitos Físicos (espaço em rack, quantidade de pontos elétricos e etc.) e lógicos (VLANs, IPs, DNS, GATEWAY, NTP e etc.) da solução;
  - Coletar as informações e preencher o Guia de Configuração do Ambiente;
  - Verificar os equipamentos entregues de acordo com a solução desenhada;
  - Verificar itens extras que precisaremos prover para a instalação;
  - Revisar e discutir os desenhos e o plano de instalação do projeto com o cliente.
  - Cadastrar equipamentos no sistema de chamados Servix;

INSTALAÇÃO

- ✓ Instalação física do(s) equipamento(s) adquirido(s) e/ou contemplado(s) no escopo da proposta no local determinado pela equipe de tecnologia da Contratante;
- ✓ Posicionar rack(s) no(s) locai(s) designado(s) pela Contratante;
- ✓ Realizar e verificar a energização dos equipamentos no(s) rack(s);
- ✓ Identificar (etiquetar) todo o cabeamento apropriadamente (provisória ou definitivamente);
- ✓ Cabear a gerência do(s) equipamento(s) adquirido(s) ou contemplado(s) no escopo da proposta;
- ✓ Revisar todo o cabeamento após a conexão;

CONFIGURAÇÃO

- ✓ Configuração do sistema de administração e gerenciamento;
- ✓ Configuração de usuários de diferentes níveis de administração;
- ✓ Configuração seguindo as melhores práticas do Fabricante;
- ✓ Configuração seguindo as regras, diretivas e normas internas da Contratante;
- ✓ Configuração de parâmetros de rede;
- ✓ Configuração com Active Directory;
- ✓ Configuração das portas;
- ✓ Configurações de NAT (Network Address Translation);
- ✓ Configurações de PAT (Protocol Address Translation);
- ✓ Configuração configurações de DNS para MGMT;
- ✓ Configuração de Balanceamento/Failover de links nos equipamentos;
- ✓ Configurar e testar o autosupport ou ferramenta disponibilizada que automatize o envio de informações para facilitar o atendimento do suporte;
- ✓ **Itens com quantidade limitada de aplicação/configuração, de acordo com a proposta:**
    - Configuração Grupos e perfis de Acesso;
    - Configuração interfaces VLAN;
    - Configuração Zonas de segurança:
    - Configuração de políticas de segurança de saída de Internet;
    - Configuração nas configurações de VPN;

- Configuração de Assinaturas de tráfego;
- Configuração de rotas estáticas;

MIGRAÇÃO

- ✓ Backup das regras e políticas do ambiente atual (caso possível);
- ✓ Backup das configurações de rede do ambiente atual (caso possível);
- ✓ Migração de configuração de rede para o(s) novo(s) equipamento(s) contemplado(s) nesta proposta;
- ✓ Migração de regras para o(s) novo(s) equipamento(s) contemplado(s) nesta proposta;
- ✓ Migração de políticas para o(s) novo(s) equipamento(s) contemplado(s) nesta proposta;

PÓS-INSTALAÇÃO

- ✓ Esclarecimento de dúvidas e/ou instruções “Best Practices” para o ambiente;
- ✓ Entrega do documento de implementação final com o resumo do ambiente (AsBuilt);
- ✓ Obter termo de aceite e encerrar o projeto;
- ✓ Obter termo de capacidade técnica;
- ✓ Treinar a equipe da Contratante na abertura de chamados no Fabricante;
- ✓ Treinar a equipe da Contratante na abertura de chamados no Servix;

- Atestado de capacidade técnica:

A Servix, ao final da implementação da solução, poderá solicitar a emissão de um atestado de capacidade técnica, informando que a compras e/ou a prestação de serviços foi concluída satisfatoriamente de acordo com o proposto.

CONDIÇÕES COMERCIAIS

Pagamento

30 dias do faturamento.

Garantia e suporte

48 meses para todo o conjunto de software, hardware e licenças.

Impostos

Já estão inclusos nos valores apresentados comercialmente todos os impostos que incidem. Quaisquer tributos, encargos sociais e/ou obrigações legais que venham a ser criados, ou alterados, após a data da proposta, e que repercutam direta ou indiretamente nos preços, implicarão na revisão dos valores descritos nesta proposta.

Validade

O Conteúdo dessa proposta é válida por 60 dias.

Prazo de Entrega

Em até 45 dias úteis após o faturamento.

Frete

Incluso na proposta.

Moeda

Valores expressos em Reais do Brasil.

Dados Cadastrais

Empresa: Servix Informática LTDA - BA

CNPJ: 01.134.191/0003-09

Inscrição Estadual: 125.903.956

Endereço: Rua Santos Dumond, 57 – Sala 202, CEP: 45.653-380– Ilhéus – BA.

Telefone/FAX: (073) 3084-3970

Dados Bancários: Banco: Itaú / Agência: 0383 / Conta Corrente: 14835-0

TERMO DE ACEITE DA PROPOSTA

Proponente: Servix Informática Ltda., inscrita no CNPJ sob n. 01.134.191/0003-09, endereço na Rua Santos Dumond, 57 - Sala 202, CEP: 45.653-380– Ilhéus – BA**.**

Cliente: Neste ato, o **Ministério Público do Estado do Amazonas - MPAM** DECLARA, para todos os fins e efeitos legais e jurídicos, ter conhecimento de todos os termos, valores, condições e peculiaridades desta Proposta Comercial **SVX210597** ao qual já pactua e autoriza a Proponente a executar suas obrigações contidas no objeto da referida proposta e, consequentemente, emitir fatura (s) e nota (s) fiscal (is) contra o **Ministério Público do Estado do Amazonas - MPAM**. Na hipótese de as partes não formalizarem o futuro contrato de compra e venda, as partes declaram e acordam, que a presente proposta, possui força e natureza contratual, produzindo todos os efeitos legais e jurídicos.

São Paulo, _____de_____de_____.

Aceite:

_____

Nome:

Cargo:

CPF:

Carimbo da Empresa:

Testemunhas:

_____ _____

Nome: Nome:

Cargo: Cargo:

CPF: CPF:

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Ministério Público do Estado do Amazonas

Proposta Comercial - VENDA [PGJ/AM] Serviço de Firewall em Alta Disponibilidade
Versão 1

Wheyla Silva
NTSec | Network Security | Regional Nordeste
Telefone: (85) 3055-3540/ (85) 9 99266-5656

Fortaleza, 23 de novembro de 2021

Always there.

+55 85 30353540
contato@ntsec.com.br | www.ntsec.com

Avenida Dom Luis, nº 906, sala 601
Aldeota – Fortaleza/CE CEP: 60.160-196

1. CARTA DE APRESENTAÇÃO

A **NTSec** é uma empresa focada em prover serviços técnicos especializados e integrar soluções em tecnologia da informação, reconhecida por proteger com eficácia negócios empresariais há mais de 10 anos.

Possuímos NOC (*Network Operation Center*) e uma equipe técnica especializada, permitindo o monitoramento e gestão dos eventos de TI, atuando de forma preventiva e proativa com o objetivo de manter o ambiente dos nossos clientes o mais estável possível.

É com grande satisfação que encaminhamos à(ao) **Ministério Público do Estado do Amazonas** proposta comercial referente a fornecimento de **[PGJ/AM] Serviço de Firewall em Alta Disponibilidade**.

Agradecemos a oportunidade e a confiança depositada na **NTSec** e esperamos poder estreitar ainda mais o nosso relacionamento e em caso de dúvida ou questionamento, entre em contato conosco.

1.1. NOSSOS PARCEIROS

1.2. ALGUMAS DAS NOSSAS CERTIFICAÇÕES

Check Point Certified Administrator (CCSA)

Check Point Certified Expert (CCSE)

Check Point Certified Master (CCSM)

Certified Information Systems Security Professional

GIAC Certified Incident Handler (GCIH)

1.3 PRINCIPAIS CLIENTES

CEARÁ

CEARÁ

2 INVESTIMENTO

LOTE	ITEM	SKU E PRODUTOS	MESES	TOTAL MENSAL R$	TOTAL 48 MESES R$
01	01	**Serviço de Firewall em Alta Disponibilidade** **2 unid.** CPAP-SG66XX-PLUS-INV 6600 Plus appliance- Inventory Unit **+ 2 unid** UPG-CPAP-SG6600-PLUS-SNBT Software Upgrade for 6600 Plus appliance with SandBlast subscription package for 1 year **+ 2 unid** CPSB-SNBT-6600-PLUS-3Y Next Generation Threat Prevention and Sandblast for additional 3 years for 6600 PLUS Appliance **+** **2 unid** CPSB-MOB-U Mobile Access Blade unlimited	48	R$ 79.500,00	R$ 3.816.000,00
	02	**Serviço de Monitoramento da Solução** **1 unid** CPSM-NGSM5 ext Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year) **+ 1 unid** CPSB-EVS-COMP-5-3Y SmartEvent, SmartReporter and Compliance for 5 gateways (Smart-1 & open server) 3 years **+ 1 unid** CPES-SS-PREMIUM-3 Enterprise Software Subscription Premium	48	R$ 40.000,00	R$ 1.920.000,00
	03	**Serviço de Migração do Ambiente Atual** **1 unid** Serviço de Migração do Ambiente Atual	01	R$ 38.000,00	R$ 38.000,00
	04	**Serviço de Treinamento da Solução** **5 unid** Serviço de Treinamento da Solução	05	R$ 15.000,00	R$ 75.000,00
				TOTAL GERAL R$	**R$ 5.849.000,00**

a. Da validade da proposta

A presente proposta tem validade de 60 (sessenta) dias corridos, a contar da data de sua emissão. Decorrido esse prazo a NTSEC – NETWORK SECURITY® reserva-se o direito de alterar, corrigir e/ou reajustar valores, bem como todas as demais condições técnicas e/ou comerciais apresentadas nesta proposta comercial.

b. Forma de Pagamento

Com preços expressos em Reais, para pagamento mensal em 30 dias corridos após o faturamento.

+55 85 30353540
contato@ntsec.com.br | www.ntsec.com

Avenida Dom Luis, nº 906, sala 601
Aldeota – Fortaleza/CE CEP: 60.160-196

c. Prazo de Entrega

Os produtos ofertados serão entregues em até 60 (sessenta) dias contados após o processamento do pedido.

d. Dados da Contratada

Razão Social: NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA
CNPJ: 09.137.728/0002-15
Endereço.: Av. Dom Luís, 906 - Bairro: Meireles - CEP: 60.160-196 | Fortaleza-CE
Tel.: (85) 3055.3540 | (85) 9 99266-5656

3 TERMO DE CONFIDENCIALIDADE

O conteúdo desta proposta destina-se exclusivamente à solicitante. As partes concordam que todas as informações contidas na mesma são confidenciais e devem ser tratadas como tais, isto é, mantidas em local seguro e disponibilizadas apenas para os colaboradores que necessitem conhecê-las.

4 DE ACORDO COMERCIAL

E por estarem acordadas sobre o conteúdo deste, as partes envolvidas manifestam seu aceite formal. A data de início dos serviços, quando aplicável, será negociada posteriormente pela equipe de projetos da **NTSEC | NETWORK SECURITY®** e a equipe designada pela(o) **Ministério Público do Estado do Amazonas**, em conformidade com as expectativas e disponibilidade dos recursos envolvidos.

A NTSEC limita sua responsabilidade civil e jurídica ao valor estipulado neste instrumento. Eventuais mudanças realizadas em qualquer um dos itens, após a assinatura deste documento, poderá invalidá-lo e originar uma nova proposta.

Fortaleza, ___de _____de 2021

_____
Ministério Público do Estado do Amazonas
Felipe Beiragrande da Costa

NETWORK SECURE

@networksecure
/networksecureTI
/networksecure

www.networksecure.com.br

NETWORK SECURE

Quem somos?
Fundada em 2002, a Network Secure é uma empresa especializada em segurança da informação e cyber security, e vem se aprimorando na utilização de técnicas e metodologias de segurança com profissionais certificados para garantir sucesso aos projetos.

O método e a organização de trabalho, no atendimento aos clientes, são personalizados para garantir a satisfação, qualidade dos serviços e resultados esperados.

Missão
Promover soluções inovadoras e confiáveis em tecnologia e segurança da informação, para os setores público e privado, potencializando suas atividades, buscando valorização, desenvolvimento pessoal e profissional de colaboradores e clientes.

Agora que já conhece um pouco sobre nosso histórico, te convidamos a conhecer os nossos serviços e nossas soluções.

SERVIÇOS

CyberSecurity
- Application Security
- Incidente Response
- Red Team
- Security Architecture

Managed Security Services
- Device Management
- On-Site Team
- Security Monitoring
- Threat Inteligence
- Vulnerability Management

Security Consulting
- Compliance LGPD/GDPR
- Risk Assessment
- Security Information Policy

Security Integration
- Application Security
- Cloud Security
- Data Security
- Endpoint Security
- Network Security
- Security Automation
- Security Awareness
- Security Operation

SOLUÇÕES

- SIEM
- Antispam
- NGFW/UTM
- Antimalware/Endpoint
- Cofre de senhas
- WAF Web Application Firewall
- DLP – Data Loss Prevention
- Balanceamento de carga
- Visibilidade / Monitoramento
- Controle de dispositivos (pendrive, modem, 3G, wifi, etc.)
- NAC / EVAS
- MDM/Gerenciamento de endpoint
- Otimização de Wan (SDWAN)
- Segurança de auditoria de banco de dados
- Wirelless
- Solução para detecção de fraude
- IPS Intrusion Prevention System/ Sistema de Prevenção de Intrusão
- Análise de código fonte
- Gerenciamento de PATCH
- Endpoint Privilege Management
- Privileged Remote Access
- Remote Support
- Autenticação Forte
- Controle de Conteúdo
- Gerenciamento de vulnerabilidade

kaspersky FORTINET IBM Security HCL
A10 PRTG NETWORK MONITOR Check Point SOFTWARE TECHNOLOGIES LTD tenable
BeyondTrust FORCEPOINT Symantec aruba a Hewlett Packard Enterprise company

www.networksecure.com.br

CLIENTE: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS - MPAM
Aos cuidados: Sr. Edjane Oliveira

Check Point
SOFTWARE TECHNOLOGIES LTD.

A Check Point Software Tecnologies foi fundada em 1993 e é uma empresa que atuaem diversos países na área de segurança para internet com diversos produtos voltados para empresas de pequeno, médio e grande porte que inclui Firewall, proteção contra ataques à redes e aplicações e gerenciamento centralizado de vários firewalls.

A Check Point Software Technologies, líder mundial em segurança da Internet, é o único fabricante que contempla Total Segurança de Rede, Dados e Endpoints, unificada sob uma Estrutura baseada em Gerenciamento Simples e Completo.

A Check Point protege seus clientes contra todos os tipos de ameaças, diminui a complexidade da segurança da informação e reduz o custo total de propriedade.

A Check Point foi a pioneira na indústria de segurança através da solução Firewall-1 e sua patente na tecnologia "Stateful Inspection". Hoje, continua inovando como pode ser visto com o desenvolvimento da Arquitetura Software Blade.

O dinamismo da Arquitetura Software Blade entrega segurança, flexibilidade e soluções simples que podem ser totalmente customizadas visando atender a exata necessidade de Segurança de uma organização ou ambiente.

A Check Point possui dentro de seu roll de clientes, milhares de negócios e organizações de todos os tamanhos, incluindo todas as companhias da "Fortune 100".

Além de trabalhar com soluções "PREMIADAS" ao proteger milhões de clientes contra Hachers, Spywares e Roubo de informações, atua hoje no melhor direcionamento de suas proteções, trazendo características relacionadas às melhores premissas de ações como, por exemplo: Gerenciamento de Identidade e Controle de Mudanças (nas políticas de Firewall).

Firewall de última geração (NGFW)

Os gateways da Check Point fornecem segurança superior além de qualquer firewall de última geração (NGFW). Projetados para a melhor proteção do Sandblast Network, esses gateways são os melhores na prevenção da quinta geração de ataques cibernéticos com mais de 60

serviços de segurança inovadores. Baseada na Arquitetura Infinity, a nova linha Quantum Security Gateway™ de 15 modelos pode fornecer até 1,5 Tbps de desempenho de prevenção de ameaças e escalar sob demanda

Segurança inflexível

Oferece prevenção contra ameaças de alto calibre com a premiada proteção SandBlast Network Zero Day pronta para uso

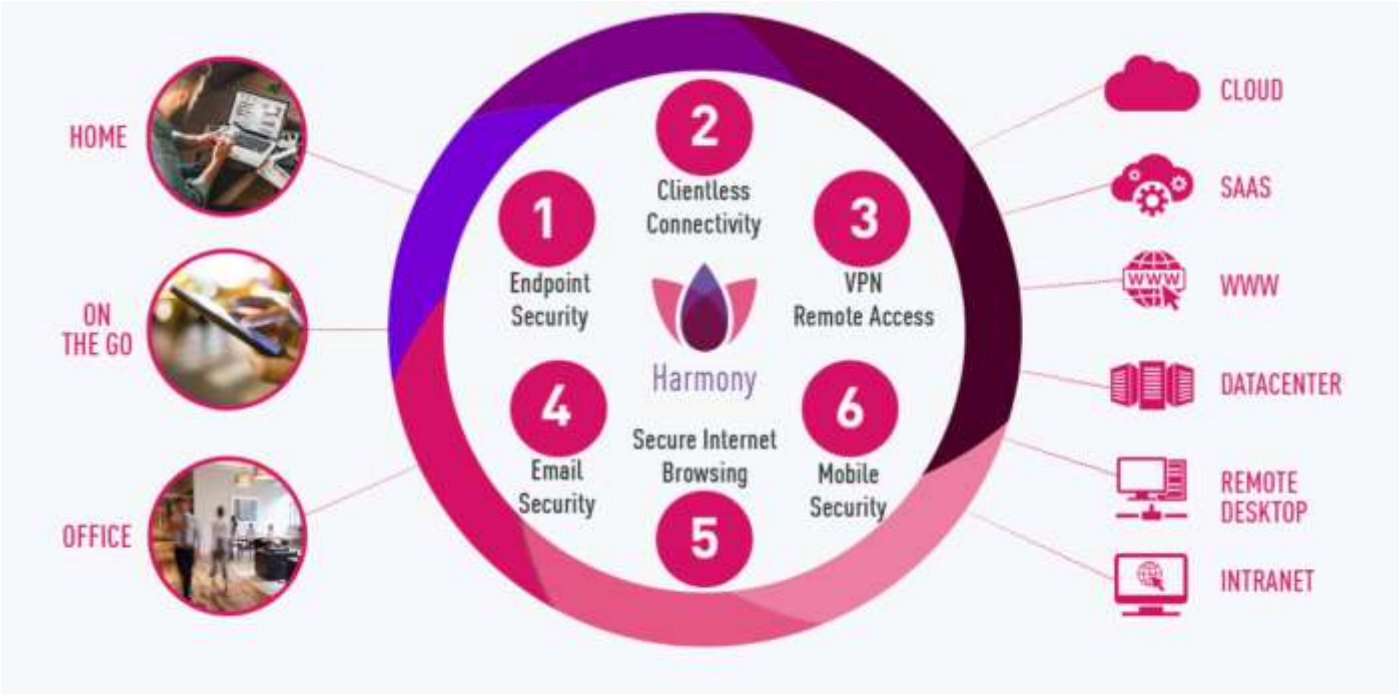
Segurança em hiperescala

Desempenho de prevenção de ameaças em hiperescala sob demanda, fornecendo às empresas expansão do nível de nuvem e resiliência no local

Segurança unificada

O controle de gerenciamento de segurança unificado R80.40 em redes, nuvens e IoT aumenta a eficiência, reduzindo as operações de segurança em até 80%

Nossos firewalls de última geração focam no bloqueio de malware e ataques de camada de aplicativo Com mais de 60 serviços de segurança alimentados pelo ThreatCloud, o serviço de nuvem de inteligência compartilhada mais poderoso do mundo, nossos gateways de segurança Quantum são capazes de reagir de forma rápida e contínua para evitar ataques cibernéticos conhecidos e desconhecidos em toda a rede. Nossos gateways aplicam políticas para melhor defender sua rede e realizam avaliações rápidas para evitar atividades invasivas ou suspeitas, como malware desconhecido, e desligá-lo.



PROPOSTA COMERCIAL:

Lote	Item	Descrição	Qde itens	Partnumber	Descrição produtos	Total mensal R$	Qde	Total R$
	01	Serviço de Firewall em Alta Disponibilidade	02	CPAP-SG66XX-PLUS-INV	6600 Plus appliance-Inventory Unit	R$ 80.824,00	48 meses	R$ 3.879.552,00
			02	UPG-CPAP-SG6600-PLUS-SNBT	Software Upgrade for 6600 Plus appliance with SandBlast subscription package for 1 year			
			02	CPSB-SNBT-6600-PLUS-3Y	Next Generation Threat Prevention and Sandblast for additional 3 years for 6600 PLUS Appliance			
			02	CPSB-MOB-U	Mobile Access Blade unlimited			
	02	Serviço de Monitoramento da Solução	01	CPSM-NGSM5	Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year)	R$ 42.408,00	48 meses	R$ 2.035.584,00
			01	CPSB-EVS-COMP-5-3Y	SmartEvent, SmartReporter and Compliance for 5 gateways (Smart-1 & open server) 3 years			

01			01	CPES-SS-PREMIUM-3	Enterprise Software Subscription Premium			
	03	Serviço de Migração do Ambiente Atual	01	Serviço de Migração do Ambiente Atual	Serviço de Migração do Ambiente Atual	R$ 30.000,00	01 Unid	R$ 30.000,00
	04	Serviço de Treinamento da Solução	05	Serviço de Treinamento da Solução	Serviço de Treinamento da Solução	R$ 10.000,00	05 Pessoas	R$ 50.000,00
TOTAL GERAL R$								**R$ 5.995.136,00**

CONDIÇÕES GERAIS

- Condições de pagamento: Mensal, mediante empenho;
- Condições Instalação: Mediante empenho;
- Valores expressos em reais incluso todos os impostos
- Prazo de entrega: Conforme TR
- Faturamento: **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ n°05.250.796/0001-54 | IM: 176407-1 | IE: 06.180.540-8**

PRAZO DA PROPOSTA

O prazo desta proposta é de 60 dias a contar da data abaixo informada, após este prazo deveser feita uma nova verificação.

Recife-PE, 24 de Novembro de 2021.

NETWORK SECURE SEGURANÇA DA INFORMAÇAO LTDA.
Juliana Viana dos Santos
Consultora Comercial
juliana.santos@networksecure.com.br
Fone: 81 99418-0534 / 81 3224-2267 Ramal: 8104

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 563.2021.SCOMS.0731261.2021.015252

Manaus, 24 de Novembro de 2021.

Ao Senhor

FRANCISCO EDINALDO DE LIRA CARVALHO

Diretor de Orçamento e Finanças – DOF

Assunto: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

Senhor Diretor,

Em atenção ao Despacho **Nº 484.2021.01AJ-SUBADM (0711354)**, encaminhamos os presentes autos tendo em vista o processo de licitação para a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, de acordo com o TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252.

Informamos que este Setor de Compras e Serviços – SCOMS realizou pesquisa de mercado em empresas nacionais em anexo (0731427, 0731208 e 0731209), conforme Mapa Demonstrativo de Preços (0731238), servindo de base para a elaboração do Quadro Resumo do Processo de Compra nº. 345/2021 (0731246), com valor total de **R$ 5.828.425,84 (cinco milhões, oitocentos e vinte e oito mil, quatrocentos e vinte e cinco reais e oitenta e quatro centavos).**

Dessa forma, encaminhamos os autos para as providências dessa Diretoria de Orçamento e Finanças – DOF, sendo que, posteriormente, deverão ser enviados à Comissão Permanente de Licitação – CPL, a fim de que se dê prosseguimento regular ao feito.

Atenciosamente,

(Assinado eletronicamente)
EDJANE DE PINHO OLIVEIRA
Chefe do Setor de Compras e Serviços

Documento assinado eletronicamente por **Edjane de Pinho Oliveira**, **Chefe do Setor de Compras e Serviços - SCOMS**, em 24/11/2021, às 16:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?

E-mail - 0729038

Data de Envio:
19/11/2021 15:41:32

De:
MPAM/Setor de Compras e Serviços <compras@mpam.mp.br>

Para:
comercial@comdados-ba.com.br

Assunto:
[PGJ/AM} Serviço de Firewall em Alta Disponibilidade

Mensagem:
Prezada Empresa Fornecedora,

Solicitamos proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

É importante ressaltar que a proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como Razão Social; CNPJ; endereço completo; contatos telefônicos; e-mail; dados bancários; entre outros.

2 - A proposta deverá ter validade mínima de 60 dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência 20.2021.DTIC.0720733.2021.015252, de forma que a proposta atenda aos requisitos exigidos. Enviamos, também em anexo, uma planilha modelo para elaboração da proposta, indicando cada item que precisará ser cotado individualmente.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.

Atenciosamente,

Edjane Oliveira
Setor de Compras e Serviços - SCOMS
Telefone: (92) 3655-0748 / 0749 / 0763
Whatsapp: (92) 3655-0763
(https://whats.link/mpam)

Anexos:
Termo_de_Referencia_0720733.html

E-mail - 0725211

Data de Envio:
12/11/2021 14:30:12

De:
MPAM/Setor de Compras e Serviços <compras@mpam.mp.br>

Para:
juliana.santos@networksecure.com.br

Assunto:
[PGJ/AM} Serviço de Firewall em Alta Disponibilidade

Mensagem:
Prezada Empresa Fornecedora,

Solicitamos proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

É importante ressaltar que a proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como Razão Social; CNPJ; endereço completo; contatos telefônicos; e-mail; dados bancários; entre outros.

2 - A proposta deverá ter validade mínima de 60 dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência 13.2021.DTIC.0691989.2021.015252, de forma que a proposta atenda aos requisitos exigidos. Enviamos, também em anexo, uma planilha modelo para elaboração da proposta, indicando cada item que precisará ser cotado individualmente.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.

Atenciosamente,

Edjane Oliveira
Setor de Compras e Serviços - SCOMS
Telefone: (92) 3655-0748 / 0749 / 0763
Whatsapp: (92) 3655-0763
(https://whats.link/mpam)

Anexos:
Termo_de_Referencia_0720733.html

[PGJ/AM] Serviço de Firewall em Alta Disponibilidade (retificação)

Setor de Compras e Servicos <compras@mpam.mp.br>

Qua, 10/11/2021 13:21

Cco: mg@actar.com.br <mg@actar.com.br>; editais@algartelecom.com.br <editais@algartelecom.com.br>; compras@altasnet.com.br <compras@altasnet.com.br>; daniels@approachtec.com.br <daniels@approachtec.com.br>; comercial@arper.com.br <comercial@arper.com.br>; arpsist@arpsist.com.br <arpsist@arpsist.com.br>; andre.oliveira@arvvo.com.br <andre.oliveira@arvvo.com.br>; bffcompanybsb@gmail.com <bffcompanybsb@gmail.com>; comercial@blueeye.com.br <comercial@blueeye.com.br>; sac@comdados-ba.com.br <sac@comdados-ba.com.br>; joao.wagnitz@compwire.com.br <joao.wagnitz@compwire.com.br>; vendas.core@coretecnologia.net.br <vendas.core@coretecnologia.net.br>; callebearaujo@gmail.com <callebearaujo@gmail.com>; fernando@cyberone.com.br <fernando@cyberone.com.br>; comercial@dask.com.br <comercial@dask.com.br>; contato@everco.com.br <contato@everco.com.br>; contato@fasthelp.com.br <contato@fasthelp.com.br>; contelb@contelb.com.br <contelb@contelb.com.br>; ronaldo@globalip.com.br <ronaldo@globalip.com.br>; fernando.jaco@aptum.com.br <fernando.jaco@aptum.com.br>

3 anexos (534 KB)

Modelo de Planilha para Proposta de Preços (Firewall).ods; Modelo de Planilha para Proposta de Preços (Firewall).xlsx; TR 020.2021.DTIC (atualizado).pdf;

Prezada Empresa Fornecedora,

No dia 22 de outubro, encaminhamos pedido de proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

Entretanto, a Diretoria de Tecnologia de Informação e Comunicação desta Procuradoria-Geral de Justiça informou, no dia 08 de novembro, a necessidade de ajuste de alguns critérios técnicos referentes aos itens "5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE" e "5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA".

Desta forma, encaminhamos o Termo de Referência 20.2021.DTIC.0720733.2021.015252, a fim de embasar a elaboração do novo orçamento. É importante ressaltar que a proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como Razão Social; CNPJ; endereço completo; contatos telefônicos; e-mail; dados bancários; marca e modelo; entre outros.

2 - A proposta deverá ter validade mínima de 60 dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência 20.2021.DTIC.0720733.2021.015252, substituto do documento anterior, de forma que a proposta atenda aos novos requisitos exigidos. Enviamos, também em anexo, uma planilha modelo para elaboração da proposta, indicando cada item que precisará ser cotado individualmente.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.
Atenciosamente,

Felipe Beiragrande da Costa
Setor de Compras e Serviços
Procuradoria-Geral de Justiça
Ministério Público do Estado do Amazonas
CNPJ: 04.153.748/0001-85
Fones: (92) 3655-0748 / 0749 / 763

Re: [PGJ/AM] Alteração nas especificações do Serviço de Firewall em Alta Disponibilidade

Eduardo Bourdot Fidelis <eduardo.fidelis@servix.com>

Qui, 11/11/2021 10:21

Para: Setor de Compras e Servicos <compras@mpam.mp.br>

Cc: marcelo.acursi@servix.com <marcelo.acursi@servix.com>

Prezado Felipe bom dia!

Ja repassei o novo documento ao time responsável e assim que tiver um retorno com alteração de valores ou não, te retorno com as novas informações.

Mais uma vez obrigado pela oportunidade.

Servix Informática Ltda.
Rua Pequetita, 215 | 7º andar
Vila Olímpia | São Paulo - SP

Eduardo Fidelis
N/NE
+55 11 9 92491761

Abertura de chamados técnicos? Acesse **http://servix.sistema.adm.br** ou ligue para **0800-940-1420**

On 11/10/21 1:09 PM, Setor de Compras e Servicos wrote:

> Prezada Empresa Fornecedora
> **SERVIX INFORMATICA LTDA**
>
> Sr. Eduardo, boa tarde.
>
> Informamos que recebemos sua proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.
>
> Entretanto, a Diretoria de Tecnologia de Informação e Comunicação informou, no dia 08 de novembro, a necessidade de ajuste de alguns critérios técnicos referentes aos itens "5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE" e "5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA".
>
> Desta forma, encaminhamos o Termo de Referência 20.2021.DTIC.0720733.2021.015252, substituto do documento enviado originalmente, para que a empresa possa verificar se os valores orçados na proposta comercial SVX210597, do dia 04 de novembro, serão mantidos ou atualizados.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.
Atenciosamente,

Felipe Beiragrande da Costa
Setor de Compras e Serviços
Procuradoria-Geral de Justiça
Ministério Público do Estado do Amazonas
CNPJ: 04.153.748/0001-85
Fones: (92) 3655-0748 / 0749 / 763

[PGJ/AM] Alteração nas especificações do Serviço de Firewall em Alta Disponibilidade

Setor de Compras e Servicos <compras@mpam.mp.br>

Qua, 10/11/2021 13:10

Para: eduardo.fidelis@servix.com <eduardo.fidelis@servix.com>

Cc: marcelo.acursi@servix.com <marcelo.acursi@servix.com>

1 anexos (510 KB)

TR 020.2021.DTIC (atualizado).pdf;

Prezada Empresa Fornecedora
SERVIX INFORMATICA LTDA

Sr. Eduardo, boa tarde.

Informamos que recebemos sua proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

Entretanto, a Diretoria de Tecnologia de Informação e Comunicação informou, no dia 08 de novembro, a necessidade de ajuste de alguns critérios técnicos referentes aos itens "5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE" e "5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA".

Desta forma, encaminhamos o Termo de Referência 20.2021.DTIC.0720733.2021.015252, substituto do documento enviado originalmente, para que a empresa possa verificar se os valores orçados na proposta comercial SVX210597, do dia 04 de novembro, serão mantidos ou atualizados.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.
Atenciosamente,

Felipe Beiragrande da Costa
Setor de Compras e Serviços
Procuradoria-Geral de Justiça
Ministério Público do Estado do Amazonas
CNPJ: 04.153.748/0001-85
Fones: (92) 3655-0748 / 0749 / 763

TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252

1. OBJETO

1.1 Contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual.

2. JUSTIFICATIVA

2.1 A presença digital pervasiva é essencial a todos os ramos de atuação na sociedade, especialmente aos órgãos públicos que prestam serviço direto à população, como é o caso do Ministério Público do Estado do Amazonas (MPAM). Isto exige que os sistemas institucionais estejam ininterruptamente conectados à Internet e disponíveis para acesso.

2.2 Intrinsecamente, todo sistema, equipamento e rede conectados à Internet estão sujeitos aos mais diversos tipos de ameaças virtuais. O fluxo constante de complexas e evoluídas ameaças como worms, spywares, cavalos de tróia, hackers, ladrões de identidade e diversos outros tipos de ataques, advindos tanto do ambiente externo quanto do ambiente interno, ameaçam os dispositivos conectados. Os danos causados pelas pragas virtuais podem comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações, serviços e operações de rede, atingindo recursos essenciais para o funcionamento do MPAM, o que inclui seus bens tangíveis e intangíveis, como a reputação da instituição perante a sociedade.

2.3 A Segurança da Informação é o processo que define os artefatos e políticas necessários para a proteção e manutenção da disponibilidade, integridade, confidencialidade e autenticidade de estações, servidores, usuários e informações corporativas. Atualmente, este processo, em nenhuma circunstância, pode ser composto apenas de um software antivírus instalado nas estações de trabalho e um firewall simples de bloqueio de portas. As ameaças, que podem ser internas ou externas, seguem aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas, com múltiplas camadas de proteção, de forma a reduzir os riscos, minimizando a probabilidade e os impactos de um eventual ataque cibernético.

2.4 Dessa forma, o MPAM necessita manter permanentemente, sob pena de interrupção de suas atividades e prejuízos irreparáveis, uma solução corporativa de Segurança da Informação avançada e à altura dos desafios impostos pelas ameaças. A solução precisa permitir a identificação das tentativas de invasão aos sistemas informatizados do MPAM, impedir e mitigar as vulnerabilidades existentes, além de intervir tempestivamente quando necessário, protegendo a Instituição da maior gama de ataques internos e externos existentes. Um item crucial e imprescindível em qualquer solução de Segurança da Informação é conhecido como firewall de próxima geração (NGFW).

2.5 O MPAM dispõe atualmente de equipamento do tipo NGFW em operação, da marca Palo Alto. Entretanto, trata-se de um único equipamento, sem qualquer tipo de redundância para caso de falhas, que já está obsoleto quanto ao hardware e ao software, ou seja, já foi descontinuado pelo fabricante, não dispondo das tecnologias de segurança mais atuais e avançadas. Além disto, com o crescimento do MPAM e da necessidade de conexões cada vez mais rápidas, a performance do equipamento está muito aquém do necessário, impondo diminuição da eficiência das atividades da instituição. Por fim, as licenças de atualização das definições de detecção de ameaças e de suporte técnico expiram no mês de agosto do corrente ano. A expiração das licenças não impede totalmente o funcionamento do equipamento, mas diminui sua eficácia conforme o tempo passa e novas ameaças surgem, sem que seja possível atualizar o equipamento com as respectivas definições de detecção e bloqueio. Fica inequivocadamente estabelecido que a substituição deste equipamento por sistema superior é urgente.

2.6 O sistema em questão, além das funcionalidades direta e especificamente relacionadas a segurança da informação, provê diversas outras funcionalidades necessárias ao funcionamento do MPAM, como o uso de VPN, por exemplo, sendo indispensável ao funcionamento do órgão como um todo. É ele que permite a conexão segura, fidedigna e unificada de todas as localidades de funcionamento do MPAM, em todo o estado do Amazonas, que inclui mais de 10 unidades descentralizadas na capital e de 54 comarcas do interior, perrmitindo o uso de todos os recursos informatizados utilizados pelos membros e servidors para consecução de suas atividades com a eficiência exigida para atingir os objetivos de atendimento à sociedade com a qualidade esperada.

2.7 A solução proposta visa elevar o patamar da proteção do ambiente computacional do MPAM e permitir a contínua mensuração do nível de segurança em que as redes do MPAM se encontram, bem como identificar as ações que devem ser tomadas para mantê-las em nível de segurança aceitável.

2.8 A contratação desta solução também se justifica pelos resultados que podem ser obtidos, quais sejam:

2.8.1 Operações digitais mais seguras, incluindo o bloqueio de acessos indevidos, roubos e sequestros de informações sensíveis do MPAM.

2.8.2 Ambiente tecnológico mais confiável.

2.8.3 Fornecimento de serviços de tecnologia mais estáveis.

2.8.4 Menor tempo de indisponibilidade do ambiente e dos serviços informatizados.

2.8.5 Parque tecnológico mais seguro contra ataques ou invasões.

2.8.6 Capacidade de planejamento, priorização e alocação de recursos melhorados.

2.8.7 Desempenho institucional e profissional incrementado.

2.8.8 Maior qualificação da mão de obra técnica na execução dos serviços de Segurança da Informação.

2.8.9 Adoção das melhores práticas de mercado, com inovação e assertividade.

2.9 A presente demanda está alinhada com o plano estratégico 2017-2027 do MPAM, objetivo 3.02 - Aprimorar a infraestrutura, gestão e governança de tecnologia da informação, por meio da iniciativa estratégica 3.02.2.03 - "Elaborar e implementar projeto de modernização do datacenter", além de dar suporte ao objetivo 2.11 - "Ampliar e integrar soluções em tecnologias da informação e comunicacão".

3. DESCRIÇÃO DO OBJETO

3.1 O objeto deste Termo compreende a contratação de serviço de firewall de próxima geração em alta disponibilidade, pelo **período de 48 (quarenta e oito) meses**, para instalação na sede do Ministério Público do Estado do Amazonas (MPAM), doravante denominado como CONTRATANTE, compreendendo os serviços de instalação, configuração, migração e ativação de equipamentos de segurança; de sistema de monitoramento dos serviços providos e de treinamento para a equipe do CONTRATANTE, por empresa especializada nestes tipos de serviço, doravante denominada CONTRATADA, conforme condições e especificações detalhadas neste Termo de Referência.

3.2 A contratação terá um único lote, organizado conforme tabela a seguir:

LOTE	ITEM	DESCRIÇÃO	UND	QTDE
A	01	Serviço de Firewall em Alta Disponibilidade	Meses	48
	02	Serviço de Monitoramento da Solução	Meses	48
	03	Serviço de Migração do Ambiente Atual	Unidades	01
	04	Serviço de Treinamento da Solução	Pessoas	05

3.3 O Lote deverá possuir vencedor único, ou seja, ser arrematado por um mesmo fornecedor, uma vez que os bens e serviços pretendidos estão intrinsecamente relacionados. A adjudicação dos itens, dentro do mesmo lote, para empresas diferentes pode resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo ao CONTRATANTE.

4. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO

4.1 A licitante deve apresentar, juntamente com os demais documentos de habilitação, atestado(s) de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem já ter prestado serviços de firewall (Next Generation Firewall), de forma satisfatória, com capacidade de tráfego (*troughput*) de, no mínimo, 10 (dez) Gbps, incluindo fornecimento de equipamento(s), serviço de instalação, treinamento, monitoramento e garantia de, no mínimo, 12 (doze) meses, similares ao objeto deste Termo.

4.2 Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.

5. DETALHAMENTO DO OBJETO

5.1 ESPECIFICAÇÕES GERAIS - PARA TODOS OS ITENS

5.1.1 São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

5.1.2 Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de end-of-sale, end-of-

support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

5.1.3 Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a CONTRATANTE seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA);

5.1.4 O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 5.4.10, ou na exposição de ativos a riscos de segurança.

5.1.5 Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional MPAM.

5.1.6 A CONTRATADA deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

5.1.7 Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. Qualquer dano eventual de manuseio/transporte a CONTRATADA será obrigada a reparo imediato.

5.1.8 Quaisquer recursos materiais que tenham sido instalados nas dependências do CONTRATANTE pela CONTRATADA durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a CONTRATADA arcar com todos os custos referentes ao envio e transporte desses materiais.

5.1.9 Após o encerramento do contrato, caso haja a necessidade expressa pelo CONTRATANTE, a CONTRATADA deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada a prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do CONTRATANTE durante uma eventual transição para os serviços de outra contradada.

5.1.10 Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço será de propriedade do CONTRATANTE, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do CONTRATANTE.

5.1.11 A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

5.1.12 A CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE

5.2.1 O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de “Firewall” provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do CONTRATANTE e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

5.2.2 Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

5.2.3 Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

5.2.4 O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web.

5.2.5 Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela CONTRATADA.

5.2.6 Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

5.2.7 Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

5.2.8 Os serviços de instalação e implantação da solução serão de responsabilidade da CONTRATADA, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos serviços especificados.

5.2.9 Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

5.2.10 Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

5.2.11 O CONTRATANTE entregará à CONTRATADA, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do CONTRATANTE e configurados pela CONTRATADA quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o CONTRATANTE.

5.2.12 O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos *appliances* que compõem a solução, operando em alta disponibilidade.

5.2.13 Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo *appliance*, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 deste Termo, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

5.2.14 Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

5.2.15 A solução deve ser capaz de atender às seguintes especificações mínimas dos serviços, a serem ofertados em uma única plataforma:

5.2.15.1 VPN

5.2.15.1.1 Suportar VPN Site-to-Site e Client-To-Site.

5.2.15.1.2 Suportar IPSec VPN.

5.2.15.1.3 Suportar SSL VPN.

5.2.15.1.4 A VPN IPSEc deve suportar 3DES.

5.2.15.1.5 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

5.2.15.1.6 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.2.15.1.7 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

5.2.15.1.8 A VPN IPSEc deve suportar AES 128 e 256 (Advanced Encryption Standard).

5.2.15.1.9 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

5.2.15.1.10 Deverá ser suportado o uso de CA interna e CA externa de terceiros.

5.2.15.1.11 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

5.2.15.1.12 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

5.2.15.1.13 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

5.2.15.1.14 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

5.2.15.1.15 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

5.2.15.1.16 Atribuição de DNS nos clientes remotos de VPN.

5.2.15.1.17 Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

5.2.15.1.18 Suportar autenticação via AD/LDAP, certificado e base de usuários local.

5.2.15.1.19 Suportar leitura e verificação de CRL (certificate revocation list).

5.2.15.1.20 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

5.2.15.1.21 Deverá manter uma conexão segura com o portal durante a sessão.

5.2.15.1.22 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 ou superior (64 bits) e Mac OS X (v10.14 ou superior).

5.2.15.2 GEOLOCALIZAÇÃO

5.2.15.2.1 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.2.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.2.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas que as utilizem.

5.2.15.3 QOS E TRAFFIC SHAPPING

5.2.15.3.1 Suportar a criação de políticas de QoS por endereço de origem, por endereço de destino e por porta.

5.2.15.3.2 QoS deve possibilitar a definição de classes por banda garantida, banda máxima e fila de prioridade.

5.2.15.3.3 Disponibilizar estatísticas RealTime para classes de QoS.

5.2.15.3.4 Deve fazer controle de banda por aplicação, por usuário e por IP.

5.2.15.4 IDENTIFICAÇÃO DE USUÁRIOS

5.2.15.4.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.

5.2.15.4.2 A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários.

5.2.15.4.3 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites de usuários ou qualquer tipo de restrição de uso, como a utilização de sistemas virtuais ou segmentos de rede, mas não se limitando a estes.

5.2.15.4.4 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.2.15.4.5 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.7 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular.

5.2.15.4.8 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de

segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.

5.2.15.5 CONTROLE DE APLICAÇÃO E FILTRO URL

5.2.15.5.1 Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

5.2.15.5.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.5.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.

5.2.15.5.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

5.2.15.5.5 Possuir pelo menos 60 categorias de URLs.

5.2.15.5.6 Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

5.2.15.5.7 Permitir a customização de página de bloqueio.

5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).

5.2.15.5.9 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

5.2.15.5.10 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

5.2.15.5.11 Reconhecer pelo menos 2700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, e-mail e compartilhamento de arquivos.

5.2.15.5.12 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.

5.2.15.5.13 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

5.2.15.5.14 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a, Bittorrent e aplicações VOIP que utilizam criptografia proprietária.

5.2.15.5.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

5.2.15.5.16 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.

5.2.15.5.17 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.2.15.5.18 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação.

5.2.15.5.19 Identificar o uso de táticas evasivas via comunicações criptografadas.

5.2.15.5.20 Atualizar a base de assinaturas de aplicações automaticamente.

5.2.15.5.21 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

5.2.15.5.22 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

5.2.15.5.23 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo.

5.2.15.5.24 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

5.2.15.5.25 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

5.2.15.5.26 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

5.2.15.5.27 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, Emule, etc), possuindo granularidade de controle/políticas para cada um deles.

5.2.15.5.28 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (WhatsApp, AIM, Hangouts, Facebook Chat, etc), possuindo granularidade de controle/políticas para cada um deles.

5.2.15.5.29 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.

5.2.15.5.30 Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para cada uma delas.

5.2.15.5.31 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como a tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc).

5.2.15.5.32 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como o nível de risco da aplicação.

5.2.15.5.33 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como a categoria da aplicação.

5.2.15.5.34 Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto.

5.2.15.5.35 Deve possuir categoria específica para classificar domínios recém registrados, com menos de 32 (trinta e dois) dias.

5.2.15.6.36 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução.

5.2.15.6 PREVENÇÃO DE AMEAÇAS COM IPS, ANTIVÍRUS E ANTI-BOT

5.2.15.6.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

5.2.15.6.2 Deve incluir assinaturas de prevenção de intrusão (IPS).

5.2.15.6.3 Deve incluir assinaturas de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

5.2.15.6.4 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por toda a vigência do contrato.

5.2.15.6.5 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

5.2.15.6.6 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU ou memória do dispositivo.

5.2.15.6.7 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear.

5.2.15.6.8 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

5.2.15.6.9 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.6.10 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

5.2.15.6.11 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

5.2.15.6.12 Deve permitir o bloqueio de vulnerabilidades.

5.2.15.6.13 Deve permitir o bloqueio de exploits conhecidos.

5.2.15.6.14 Deve incluir proteção contra-ataques de negação de serviços.

5.2.15.6.15 Deverá possuir os seguintes mecanismos de inspeção de IPS: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para

detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

5.2.15.6.16 Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

5.2.15.6.17 Detectar e bloquear a origem de port scans.

5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos.

5.2.15.6.19 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

5.2.15.6.20 Possuir assinaturas para bloqueio de ataques de buffer overflow.

5.2.15.6.21 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.

5.2.15.6.23 Suportar bloqueio de arquivos por tipo.

5.2.15.6.24 Identificar e bloquear comunicação com botnets.

5.2.15.6.25 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.

5.2.15.6.27 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação através da console de gerência centralizada.

5.2.15.6.28 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

5.2.15.6.29 Os eventos devem identificar o país de onde partiu a ameaça.

5.2.15.6.30 A solução deve ter um mecanismo centralizado de correlação e relatório de evento para IPS, Antivírus e Anti-bot.

5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

5.2.15.6.33 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança.

5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox.

5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY

5.2.15.7.1 O relatório das emulações deve apresentar a listagem dos arquivos emulados.

5.2.15.7.2 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks.

5.2.15.7.3 Caso a Prevenção de Ameaças 0-Day seja ofertada no modelo de appliance, o hardware e software fornecido não podem constar, em momento algum durante a vigência do contrato, em listas de end-of-sale, end-of-support, end-of engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2.15.7.4 Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS.

5.2.15.7.5 A solução deve ser capaz de inspecionar o tráfego criptografado SSL.

5.2.15.7.6 A solução de Emulação, deve possuir engine onde remove os conteúdos ativos e exploits a partir do documento inspecionado.

5.2.15.7.7 A solução deve possuir engine onde faça Mitigação DNS, sendo ela

possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso.

5.2.15.7.8 Implementar e identificar existência de malware em anexos de e-mail e URLs conhecidas.

5.2.15.7.9 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

5.2.15.7.10 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF.

5.2.15.7.11 A solução deve fornecer a capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, incluindo, no mínimo, as versões de Windows suportadas pela Microsoft.

5.2.15.7.12 A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

5.2.15.7.13 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.

5.2.15.7.14 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

5.2.15.7.15 Implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle).

5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

5.2.15.7.17 A solução de emulação, deverá suportar a inspeção/bloqueio de malwares em tempo real para determinar o veredito e bloqueio de um malware.

5.2.15.7.18 Implementar atualização a base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização.

5.2.15.7.19 Deve realizar bloqueio de ameaças avançadas de dia zero independente do sistema operacional.

5.2.15.7.20 O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regra individualmente visando otimizar a performance do equipamento.

5.2.15.7.21 A solução deve apresentar informações comportamental incluindo listagem de módulos e processos utilizados pelo malware e/ou código malicioso de forma sequencial.

5.2.15.7.22 Toda análise poderá ser realizada em nuvem, desde que do mesmo fabricante da solução.

5.2.15.7.23 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador para solicitar a análise.

5.2.15.7.24 Todas as máquinas virtuais utilizadas na nuvem do fabricante devem estar integralmente instaladas e licenciadas pelo período do contrato, sem a necessidade de intervenções por parte do administrador do sistema, e, as atualizações deverão ser providas pelo fabricante.

5.2.15.7.25 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.

5.2.15.7.26 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

5.2.15.7.27 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede, endereço IP.

5.2.15.7.28 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado. A solução deve suportar a inspeção de, no mínimo, os seguintes tipos de arquivos: CAB, DOC, DOCX, DOCM, DOT, DOTM, DOTX, EXE, HWP, JAR, PDF, PIF, PPAM, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, RAR, RTF, Seven-Z, SLDM, SLDX, SWF, TAR, TGZ, XLA, XLAM, XLL, XLW, XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, ZIP.

5.2.15.7.29 Implementar sincronização de hora através de protocolo NTP.

5.2.15.7.30 A solução, deve emular e eliminar malwares contidos em anexos de e-mail e documentos baixados da web.

5.2.15.7.31 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções e gráfico da taxa de transferência de tráfego monitorado.

5.2.15.7.32 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro.

5.2.15.7.33 A solução deve permitir visualizar a quantidade de arquivos emulados pela solução.

5.2.15.7.34 A solução deve permitir a visualização da fila de arquivos que serão emulados.

5.2.15.7.35 O relatório das emulações deve conter todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos.

5.2.15.7.36 A solução de sandboxing deve possuir mecanismo independente onde sua ação não depende de engines externas como antivírus, anti-malware.

5.2.15.7.37 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados.

5.2.15.7.38 O sistema de emulação deve exibir percentual de arquivos escaneados.

5.2.15.7.39 A solução deve permitir a criação de White list baseado em hash de arquivo.

5.2.15.7.40 A solução deve possuir serviço web online para categorização atualizada de sites e para definições de Widget atualizadas. As respostas recebidas pelo gateway de segurança são armazenadas localmente para otimizar o desempenho. Quando um acesso não puder ser categorizado com os dados armazenados localmente, a solução deve possuir funcionalidade que bloqueia ou permite o tráfego até que a mesma seja classificada.

5.2.15.8 NEXT GENERATION FIREWALL

5.2.15.8.1 Deverá possuir certificação ICSA para Firewall.

5.2.15.8.2 Deve permitir controle de acesso à internet por períodos do dia, mês e ano, permitindo a aplicação de políticas por horários e por dia da semana.

5.2.15.8.3 Deve permitir realizar checagem de regras para conformidade e sombreamento de regras prioritárias top-down.

5.2.15.8.4 Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado.

5.2.15.8.5 O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance.

5.2.15.8.6 Deve suportar atuação como cliente NTP (Network Time Protocol) versões 1, 2, 3 e 4.

5.2.15.8.7 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.

5.2.15.8.8 Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-interfaces lógicas associadas a VLANs.

5.2.15.8.9 A comunicação entre a solução de gerência e os appliances de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada;

5.2.15.8.10 Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos.

5.2.15.8.11 A solução deve permitir que em caso de falha de comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do appliance de segurança.

5.2.15.8.12 Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas e degradação.

5.2.15.8.13 Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário.

5.2.15.8.14 Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP.

5.2.15.8.15 A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: TACACS, RADIUS e certificados digitais.

5.2.15.8.16 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora.

5.2.15.8.17 Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário, roteamento com base em prioridades.

5.2.15.8.18 Deve implementar roteamento multicast (PIM-SM e PIM-DM).

5.2.15.8.19 Possuir funcionalidade de DHCP Relay e DHCP Server.

5.2.15.8.20 Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras.

5.2.15.8.21 Possuir base de regras singular sem separação de regras orientadas à versão de endereço IP utilizada.

5.2.15.8.22 Implementar sub-interfaces ethernet lógicas.

5.2.15.8.23 Deve suportar os seguintes tipos de NAT:

5.2.15.8.23.1 Dinâmico Many-to-1.

5.2.15.8.23.2 Dinâmico Many-to-Many.

5.2.15.8.23.3 Estático 1-to-1.

5.2.15.8.23.4 Estático Many-to-Many.

5.2.15.8.23.5 Estático bidirecional 1-to-1.

5.2.15.8.23.6 NAT de Origem.

5.2.15.8.23.7 NAT de Destino.

5.2.15.8.24 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

5.2.15.8.25 Deve implementar roteamento estático IPv4 e IPV6.

5.2.15.8.26 Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4.

5.2.15.8.27 Deve permitir a importação , criação e edição de regras SNORT.

5.2.15.8.28 Deve suportar aplicações multimídia como H.323 e SIP.

5.2.15.8.29 Deve permitir o funcionamento em modo transparente tipo “bridge”.

5.2.15.8.30 Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing).

5.2.15.8.31 Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.

5.2.15.8.32 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.

5.2.15.8.33 Deve ter a capacidade de inspecionar e bloquear tráfego operando nos modos de camada 2 (L2) e de camada 3 (L3).

5.2.15.8.34 Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações.

5.2.15.8.35 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações.

5.2.15.8.36 Promover a integração com LDAP e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações.

5.2.15.8.37 Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS.

5.2.15.8.38 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.

5.2.15.8.39 A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports".

5.2.15.8.40 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria.

5.2.15.8.41 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora.

5.2.15.8.42 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando

alterações simultaneamente.

5.2.15.8.43 Habilidade de realizar upgrade via SCP ou https via interface WEB.

5.2.15.8.44 A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços.

5.2.15.8.45 A solução deverá possuir uma ferramenta onde o fabricante disponibilize HotFixes de segurança e upgrades de versão para instalação simples e com downtime apenas no curto espaço de tempo de reinicialização.

5.2.15.8.46 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.8.47 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.8.48 Deverá suportar controle de política de firewall:

5.2.15.8.48.1 Por zona de segurança.

5.2.15.8.48.2 Por porta e protocolo.

5.2.15.8.48.3 Por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

5.2.15.8.48.4 Por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.2.15.8.49 Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo, em modo transparente, tanto em Layer 2, como em Layer 3.

5.2.15.8.50 O serviço de alta disponibilidade (HA) deve sincronizar todas as sessões, certificados de-criptografados, todas as Associações de Segurança das VPNs e todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS.

5.2.15.8.51 Deve possuir monitoração de falha de link.

5.2.15.8.52 A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces.

5.2.15.8.53 Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante.

5.2.15.8.54 Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). O fluxo mínimo de análise de regras legadas devem trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

5.2.15.8.55 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

5.2.15.8.56 Deve suportar NAT64 e NAT46.

5.2.15.9 GERÊNCIA

5.2.15.9.1 Deve possuir solução de gerenciamento e administração centralizado possibilitando o gerenciamento de diversos equipamentos de proteção de rede.

5.2.15.9.2 Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a licença de maior capacidade do portfólio ou de capacidade ilimitada.

5.2.15.9.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

5.2.15.9.4 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

5.2.15.9.5 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

5.2.15.9.6 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS).

5.2.15.9.7 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

5.2.15.9.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

5.2.15.9.9 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração.

5.2.15.9.10 Suportar backup das configurações e rollback de configuração para a última configuração salva.

5.2.15.9.11 Suportar validação de regras antes de serem aplicadas.

5.2.15.9.12 Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing).

5.2.15.9.13 Deve permitir a visualização dos logs de uma regra específica em tempo real.

5.2.15.9.14 Deve possibilitar a integração com outras soluções de Gerencamento e Correlação de Eventos de Segurança (SIEM) de mercado desde que não sejam software livre.

5.2.15.9.15 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

5.2.15.9.16 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti- Malware) e similares.

5.2.15.9.17 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.

5.2.15.9.18 Deve ser possível exportar os logs em CSV.

5.2.15.9.19 Deve possibilitar a geração de relatórios de eventos no formato PDF.

5.2.15.9.20 Deve possibilitar rotação do log.

5.2.15.9.21 Deve suportar geração de relatórios com resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego.

5.2.15.9.22 Deve permitir a criação de relatórios personalizados.

5.2.15.9.23 Suportar enviar os relatórios de forma automática via arquivo em formato PDF.

5.2.15.9.24 A solução de gerência centralizada poderá ser entregue como *appliance* virtual, devendo ser compatível/homologado para o Acropolis Hypervisor Virtualization and Software - Nutanix. Caso não haja compatibilidade/homologação a CONTRATADA deverá entregar uma infraestrutura de virtualização adequada ou entregar este item da solução na forma de *appliance* físico.

5.2.15.9.25 Deve consolidar logs e relatórios de todos os dispositivos administrados.

5.2.15.9.26 Deve possuir capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

5.2.15.9.27 Deverá possuir mecanismo de detalhamento (Drill-Down) para navegação e análise dos logs em tempo real.

5.2.15.9.28 Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso.

5.2.15.9.29 Permitir a customização do padrão regulatório da própria instituição.

5.2.15.9.30 Permitir notificação instantânea ou emissão de relatório sobre mudanças de política de segurança que impactam negativamente a segurança.

5.2.15.9.31 Monitorar constantemente ou realizar emissão de relatório sobre o status de conformidade da solução aos padrões regulatórios informados.

5.2.15.9.32 Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade estabelecidas pelo CONTRATANTE ou de acordo com o padrão estabelecido pelo fabricante.

5.2.15.9.33 Gerar alertas ou emitir relatório de conformidade sobre o impacto de suas decisões na política de segurança trazendo as considerações regulatórias na gestão de segurança estabelecidas pelo CONTRATANTE ou de acordo com o padrão pré-determinado pelo fabricante.

5.2.15.9.34 Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.

5.2.15.9.35 Possuir alertas ou emitir relatório de políticas e as potenciais violações de conformidade.

5.2.15.9.36 Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.

5.2.15.9.37 Gerar relatórios diários com base nas configurações de segurança em tempo real.

5.2.15.9.38 Permitir que os relatórios possam ser salvos, enviados e impressos.

5.2.15.9.39 Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados.

5.2.15.9.40 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

5.2.15.9.41 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

5.2.15.9.41.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação com principais eventos de segurança de acordo com a funcionalidade selecionada.

5.2.15.9.41.2 A solução deve possuir mecanismo para detectar login de administradores em horários irregulares.

5.2.15.9.41.3 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais.

5.2.15.9.41.4 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.

5.2.15.9.41.5 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius.

5.2.15.9.41.6 Permitir criações de políticas de acesso de usuários autenticada no Active Directory, que reconheçam os usuários de forma transparente.

5.2.15.9.41.7 Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados à solução.

5.2.15.9.41.8 Permitir a visualização de gráficos e mapa de ameaças.

5.2.15.9.41.9 Possuir mecanismo para que logs antigos sejam removidos automaticamente.

5.2.15.9.41.10 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.

5.2.15.9.41.11 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.

5.2.15.9.41.12 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real.

5.2.15.9.41.13 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria.

5.2.15.9.41.14 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

5.2.15.9.41.15 Caso necessite de licenciamento, a solução deverá vir totalmente licenciada para o nível mais alto de uso.

5.2.15.10 CAPACIDADES

5.2.15.10.1 Os valores mínimos e máximos a seguir servirão como margem para a CONTRATADA ofertar equipamentos que tenham capacidade compatível com os requisitos do CONTRATANTE durante o período de vigência do contrato.

5.2.15.10.2 A solução deve ser fornecida com kit para instalação em rack de 19”.

5.2.15.10.3 Os equipamentos ofertados na solução deverão ser capazes de operar com todos os recursos habilitados, mantendo os níveis de operação descritos na seção 5.9 - ACORDO DE NÍVEL DE SERVIÇO (SLA), deste Termo de Referência.

5.2.15.10.4 A CONTRATADA deverá fornecer todos os transceivers de 10G SFP+ tanto para a solução de firewall, como para os switchs do CONTRATANTE, bem como os cordões de fibra óptica. Ou seja, todas as portas de comunicação, interfaces e afins, deverão estar habilitadas e operacionais, sem custos adicionais.

5.2.15.10.5 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de

descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2.15.10.6 Para dimensionamento adequado da solução, a CONTRATADA deve levar em consideração a “Tabela de Capacidades” a seguir, que demonstra a demanda de recursos atual do CONTRATANTE, na coluna entitulada como "MÍNIMO", e a projeção de crescimento da demanda do CONTRATANTE, na coluna entitulada como "MÁXIMO". Cada conjunto da solução poderá ser entregue contemplando as capacidades mínimas da “Tabela de Capacidades”, podendo ser expandida durante toda a vigência do contrato de forma que atenda às demandas dos limites máximos especificados.

Tabela de Capacidades

	DESCRIÇÃO DO REQUISITO	MÍNIMO	MÁXIMO
5.2.15.10.7	Interface 10/100/1000 Mbit Ethernet	08	16
5.2.15.10.8	Interface 10Gbase-F SFP+	02	04
5.2.15.10.9	Interface de gerenciamento dedicada	01	01
5.2.15.10.10	Interface 10/100/1000 Mbit Ethernet BaseT dedicada para alta disponibilidade	01	01
5.2.15.10.11	Interface Console Serial	01	01
5.2.15.10.12	Fonte de alimentação redundante bivolt 100-240 VAC Hot-Swappable	02	02
5.2.15.10.13	Disco de armazenamento de 500GB HDD e/ou 240GB SSD RAID 1	01	02
5.2.15.10.14	Firewalls virtuais	10	20
5.2.15.10.15	Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps)	05	10
5.2.15.10.16	Throughput de AES-128 VPN (em Gbps)	04	08
5.2.15.10.17	Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps)	2,5	05
5.2.15.10.18	Conexões simultâneas (em milhões)	02	04
5.2.15.10.19	Novas conexões por segundo (em milhares)	100	180
5.2.15.10.20	Suportar e estar licenciado para acesso remoto Client-to-site (VPN SSL)	200	400

* Baseado em amostras reais, ou seja, não serão aceitos testes usando UDP, HTTP 1M ou testes em laboratório.

5.3 ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO

5.3.1 Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

5.3.2 Deverá ser baseado em Dashboard, para fácil visualização.

5.3.3 Deve ser entregue com regras genéricas criadas pela CONTRATADA, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

5.3.4 O serviço da CONTRATADA deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo CONTRATANTE.

5.3.5 Deve possuir acesso WEB (HTTPS).

5.3.6 Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

5.3.7 Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

5.4 ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

5.4.1 O CONTRATANTE possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser

totalmente migradas para a solução ofertada.

5.4.2 O CONTRATANTE possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links “full-route” BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.3 A CONTRATADA deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

5.4.4 O CONTRATANTE possui infraestrutura hiper convergente, e para tanto usa o Acropolis Hypervisor Virtualization and Software - Nutanix. Assim, caso a CONTRATADA necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do CONTRATANTE.

5.4.5 A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

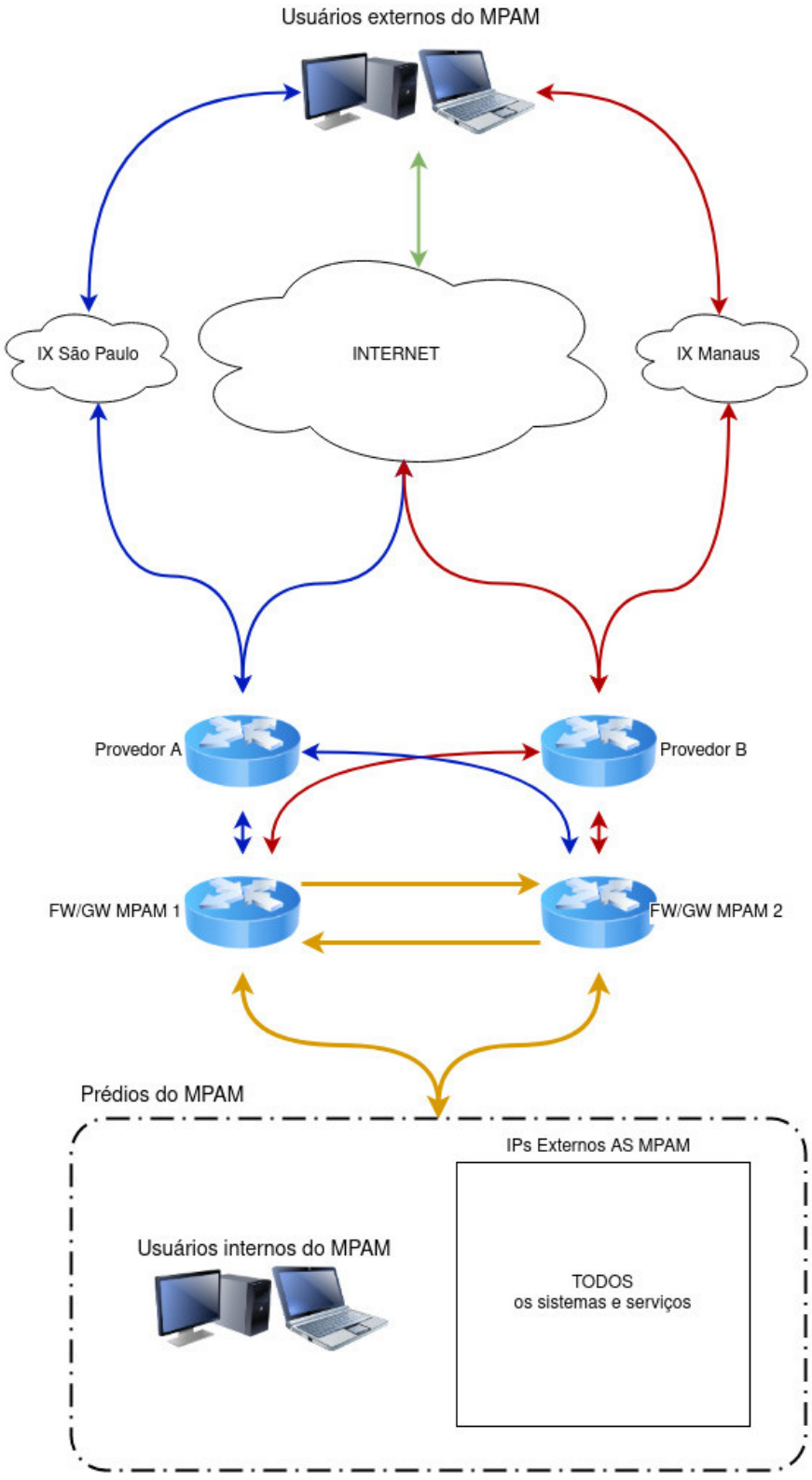
5.4.6 A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

5.4.7 A CONTRATADA deverá evitar, durante o processo de migração, interromper os serviços de rede do CONTRATANTE, nos horários das 8hs às 18hs, em dias de expediente do CONTRATANTE.

5.4.8 É de responsabilidade da CONTRATADA a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do CONTRATANTE fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

5.4.9 A CONTRATADA deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CONTRATANTE, sendo vedada sua cessão, locação ou venda a terceiros.

5.4.10 A topologia da solução deve seguir conforme imagem a seguir:



5.5 ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO

5.5.1 A CONTRATADA deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.5.2 A carga horária total para o treinamento deve ser de, no mínimo, 40 horas.

5.5.3 A CONTRATADA deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela FISCALIZAÇÂO.

5.5.4 O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como

atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fonecido em português do Brasil ou inglês.

5.5.5 O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do CONTRATANTE.

5.5.6 O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a CONTRATADA deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o CONTRATANTE. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.5.7 A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.5.8 A CONTRATADA deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.5.9 Caso o treinamento seja ofertado de forma presencial, o CONTRATANTE irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do CONTRATANTE.

5.5.10 O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a CONTRATADA deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do CONTRATANTE.

5.5.11 Será de responsabilidade da CONTRATADA prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.5.12 A CONTRATADA deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.5.13 Os instrutores designados pela CONTRATADA deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.5.14 A CONTRATADA deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.5.15 A CONTRATADA deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do CONTRATANTE e com finalidade de uso exclusivamente interno do CONTRATANTE, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela CONTRATADA.

5.6 SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS

5.6.1 A CONTRATADA deverá disponibilizar ao CONTRATANTE um número telefônico único, um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entende-se por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS.

5.6.2 No atendimento por meio de telefone a CONTRATADA fica obrigada a permitir o

recebimento de ligações de terminais fixos e móveis.

5.6.3 O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

5.6.4 Cada chamado deverá conter, no mínimo, as seguintes informações:

5.6.4.1 Número único do registro/ocorrência - a ser fornecido pela CONTRATADA.

5.6.4.2 Identificação do atendente.

5.6.4.3 Identificação do solicitante.

5.6.4.4 Data e hora de abertura do chamado/início da interrupção.

5.6.4.5 Descrição da ocorrência.

5.6.4.6 Designação do equipamento, quando for o caso.

5.6.4.7 Ações corretivas tomadas.

5.6.4.8 Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

5.6.5 O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

5.6.6 O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA.

5.6.7 Não deverá haver qualquer limitação para o número de solicitações de reparo.

5.6.8 O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a CONTRATADA deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

5.7 GARANTIA TÉCNICA

5.7.1 A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

5.7.2 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.

5.7.3 Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.

5.7.4 A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao CONTRATANTE.

5.7.5 Caso sejam detectadas falhas ou bugs nos produtos, a CONTRATADA deverá realizar as atualizações necessárias à correção do problema.

5.7.6 A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

5.7.7 A CONTRATADA é a única responsável pelos produtos fornecidos ao CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

5.7.8 A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo CONTRATANTE, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

5.7.9 Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à CONTRATADA apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.

5.7.10 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

5.7.11 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o

CONTRATANTE.

5.7.12 No que se refere a software, durante a vigência do Contrato, a CONTRATADA deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o CONTRATANTE. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

5.7.12.1 Patches, fixes, correções, updates e service packs.

5.7.12.2 Novas releases, builds e funcionalidades.

5.7.12.3 O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.

5.7.12.4 O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.

5.7.12.5 Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.

5.7.12.6 A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

5.7.12.7 A CONTRATADA deverá fornecer tais atualizações independentemente de solicitação expressa do CONTRATANTE.

5.7.12.8 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

5.7.12.9 As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA

5.8.1 Os serviços de manutenção *on-site*, serão prestados nas dependências do CONTRATANTE na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

5.8.2 O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do CONTRATANTE, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

5.8.3 A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

5.8.4 A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

5.8.5 Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

5.8.6 A CONTRATADA deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo CONTRATANTE ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser realizada nas dependências do CONTRATANTE, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

5.8.7 O CONTRATANTE poderá determinar à CONTRATADA a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da CONTRATADA.

5.8.8 Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional ao CONTRATANTE.

5.8.9 A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e

corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do CONTRATANTE.

5.8.10 O serviço de suporte deverá ser efetuado *on-site* sempre que se fizer necessário ou quando for solicitado pelo CONTRATANTE, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o CONTRATANTE.

5.8.11 Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do CONTRATANTE, a CONTRATADA deverá desinstalar, embalar e transportar o item defeituoso, instalar item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

5.8.12 Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar o CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

5.8.13 A CONTRATADA encaminhará mensagem de e-mail para o CONTRATANTE, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

5.8.14 Todos os custos diretos e indiretos para realização do atendimento presencial (*on-site*) serão de responsabilidade exclusiva da CONTRATADA.

5.8.15 Dentro do mesmo endereço, a ser executada pela CONTRATADA, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o CONTRATANTE.

5.8.16 Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

5.8.17 O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do CONTRATANTE, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

5.8.18 Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas.

5.9 ACORDO DE NÍVEL DE SERVIÇO (SLA)

5.9.1 Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos nesse Termo de Referência.

5.9.2 A CONTRATADA deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

5.9.3 A CONTRATADA deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

5.9.4 A realização de assistência técnica preventiva, caso não seja solicitada pelo CONTRATANTE, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do CONTRATANTE.

5.9.5 Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.6 Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.7 Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do CONTRATANTE, a solução será considerada como operando em Modo de Contingência.

5.9.8 Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

5.9.9 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual. Este checkup faz parte da manutenção preventiva.

5.9.10 Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.

5.9.11 O Modo de Contingência se caracteriza por:

5.9.11.1 Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.

5.9.11.2 Funcionamento acima dos limiares de desempenho, conforme estabelecido nas cláusulas 5.9.5 e 5.9.6 acima.

5.9.11.3 Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante ou fora de garantia.

5.9.11.4 Operação com funcionalidade ou performance abaixo dos mínimos exigidos neste Termo.

5.9.12 Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.

5.9.13 O estado de Inoperância Total se caracteriza por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do CONTRATANTE.

5.9.14 O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela CONTRATADA.

6. VISTORIA TÉCNICA

6.1 As empresas licitantes PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades do CONTRATANTE, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

6.2 Nos casos em que houver vistoria, os locais envolvidos pelos trabalhos deverão ser cuidadosamente inspecionados pelos licitantes, observando, entre outros aspectos, o grau de dificuldade para a consecução dos serviços e procederão à rigorosa conferência das medidas e de outros aspectos julgados de interesse.

6.3 A vistoria deverá ser realizada, preferencialmente, por profissional(is) qualificado(s) e detentor(es) de conhecimento técnico relacionado ao objeto, devidamente credenciados.

6.4 Para que as pretensas licitantes possam participar da vistoria, será necessária que a mesma credencie um representante, através da apresentação, no ato da visita, de documento devidamente assinado, indicando o nome de seu colaborador, número da cédula de identidade e CPF e delegação de poderes para representá-la na visita. A falta deste documento impossibilitará que o representante e a empresa participem da vistoria.

6.5 Para a realização da vistoria, as empresas interessadas deverão apresentar duas cópias da Declaração de Vistoria, já preenchida com os dados da empresa e assinada pelo representante, sendo que uma cópia será assinada por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO do CONTRATANTE, e devolvida para empresa, e a outra será juntada ao processo de contratação, onde a empresa declara ter realizado a vistoria técnica.

6.6 A referida Declaração deverá ser apresentada posteriormente, na fase licitatória, nos termos definidos no edital do certame.

6.7 Caso opte por não realizar a vistoria, a licitante apresentará na fase licitatória, declaração de opção pela dispensa de vistoria.

6.8 Não serão admitidas quaisquer alegações de desconhecimento ou erro orçamentário por parte da futura contratada, quando do cumprimento as obrigações.

6.9 A licitante poderá vistoriar o local onde serão executados os serviços até o último dia útil anterior à data fixada para a abertura da sessão pública.

6.10 As visitas deverão ser previamente agendadas, com pelo menos 5 (cinco) dias úteis de antecedência, pelo telefone (92) 3655-0660/3655-0666 — DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período de segunda a sexta-feira, das 8 às 14hs, excluídos feriados e pontos facultativos.

6.11 A vistoria será realizada no endereço do Edifício-Sede do MPAM, Avenida Coronel Teixeira, 7.995, bairro Nova Esperança, CEP 69037-473, Manaus/AM.

6.12 Todos os custos associados com a visita e a inspeção serão de inteira responsabilidade da licitante.

7. PRAZOS PARA A PRESTAÇÃO DO SERVIÇO

7.1 A CONTRATADA deverá em, no máximo, 65 (sessenta e cinco) dias corridos, contados a partir da assinatura do contrato, finalizar a implantação, ativação e entrega dos sistemas e equipamentos que compõem os itens 01, 02 e 03, especificados neste Termo de Referência.

7.2 A CONTRATADA deverá em comum acordo com o CONTRATANTE, no prazo máximo de 120 (cento e vinte) dias corridos, contados a partir da assinatura do contrato, finalizar o treinamento indicado no item 04 deste Termo de Referência.

7.3 Antes de findar os prazos fixados nos itens anteriores, a CONTRATADA poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pelo CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, 410 da lei n. 8.666/93.

7.4 O prazo da prestação dos serviços objeto deste Termo de Referência deverá contar da assinatura do contrato, prorrogáveis de comum acordo, até o limite estabelecido na Lei n. 8.666/93, e suas alterações.

8. RECEBIMENTO

8.1 O recebimento será feito nas seguintes etapas:

8.1.1 Será emitido Termo Individual de ACEITE para cada item do Lote.

8.1.2 Será emitido Termo de Recebimento Definitivo para todo o Lote.

8.2 O recebimento dos serviços será realizado pela FISCALIZAÇÃO do CONTRATANTE.

8.3 Para fins de aceite a CONTRATADA deverá comunicar formalmente a efetiva disponibilização dos serviços para cada item do Lote.

8.4 Para a emissão do Termo Individual de ACEITE para o Item 01:

8.4.1 Será emitido após Período de Funcionamento Experimental de até 15 (quinze) dias, que se iniciará após comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.4.2 Durante Período de Funcionamento Experimental a FISCALIZAÇÃO deverá concluir os testes necessários para constatar o funcionamento regular dos serviços disponibilizados.

8.4.3 A FISCALIZAÇÃO realizará avaliação qualitativa das especificações dos equipamentos e funcionalidades que compõem a solução conforme exigências deste Termo.

8.5 Para a emissão do Termo Individual de ACEITE para o Item 02:

8.5.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.5.2 A FISCALIZAÇÃO realizará testes com as credenciais fornecidas, teste de uso da ferramenta e teste de disponibilidade necessários para constatar o funcionamento regular dos serviços disponibilizados.

8.6 Para a emissão do Termo Individual de ACEITE para o Item 03:

8.6.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito, por parte da CONTRATADA, incluindo evidencias que demonstrem inequivocadamente que todas os critérios estabelecidos na seção 5.4 deste Termo foram atendidos, atestando a efetiva disponibilização dos serviços.

8.6.2 A FISCALIZAÇÃO realizará avaliação qualitativa das evidências apresentadas considerando a disponibilidade dos serviços do CONTRATANTE.

8.7 Para a emissão do Termo Individual de ACEITE para o Item 04:

8.7.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.7.2 A FISCALIZAÇÃO observará os critérios estabelecidos neção 5.5 deste Termo.

8.8 Somente depois de realizados e aprovados os testes definidos, o CONTRATANTE, por meio da FISCALIZAÇÃO, emitirá o Termo de Aceite, atestando a conformidade com as especificações neste Termo de Referência, liberando o início de faturamento.

8.9 A contagem do prazo para a efetiva entrega e prestação de cada item de serviço especificado no lote será suspenso quando a CONTRATADA comunicar a efetiva disponibilização do serviço, e, se for o caso, será retomado no dia seguinte a partir da emissão de comunicado por escrito do CONTRATANTE indicando NÃO ACEITE do serviço em virtude de não conformidade com algum dos requisitos presentes nesse termo de referência.

9. PAGAMENTO

9.1 Para os Itens 01 e 02:

9.1.1 Mensalmente, a CONTRATADA deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das

comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

9.1.2 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada dia de funcionamento da solução em Modo de Contingênica além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

9.1.3 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada hora de funcionamento da solução em estado de Inoperância Total além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

9.1.4 A data de início de cobrança dos serviços deverá observar a data de emissão do Termo de Aceite, sendo que a primeira fatura corresponderá à prestação de serviços desde a data de emissão do Termo de Aceite, para cada item do Lote, até o último dia do respectivo mês, de forma pro rata.

9.1.5 As demais faturas deverão abranger o período do primeiro ao último dia do mês.

9.1.6 Os valores a serem faturados concernentes aos serviços objeto desta contratação estarão sujeitos a descontos nas situações de descumprimento das metas estabelecidas para os indicadores elencados na especificação do serviço, item Acordo de Nível de Serviço (SLA).

9.1.7 Os descontos aplicados nas faturas mensais não isentam a CONTRATADA de quaisquer sanções legais ou das sanções dispostas na seção 12 - SANÇÕES ADMINISTRATIVAS.

9.1.8 Os descontos aplicados nas faturas mensais, conforme dispostos acima, oriundos do descumprimento dos níveis mínimos de serviço estipulados no item Acordo de Nível de Serviço (SLA), não se configuram como penalidades ou multas.

9.1.9 No primeiro dia útil do mês subsequente, antes da emissão na nota fiscal, a CONTRATADA deverá enviar à FISCALIZAÇÃO relatório referente aos períodos, destacando eventuais descontos e as causas da(s) indisponibilidade(s) ocorridas na prestação dos serviços para a devida aprovação.

9.1.10 As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da CONTRATADA no que diz respeito ao atendimento dos níveis de serviços especificados no acordo de nível de serviço, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

9.2 Para os Itens 03 e 04:

9.2.1 A CONTRATADA deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

9.2.2 Os pagamentos relativos aos Itens serão realizados de uma única vez, no mês seguinte a emissão do Termo de Aceite.

9.3 Ao CONTRATANTE fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas neste Termo de Referência.

10. OBRIGAÇÕES DA CONTRATADA

10.1 Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo, observando as prescrições e as recomendações do fabricante/fornecedor, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

10.2 Comunicar imediatamente ao CONTRATANTE, por escrito, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto desta contratação, e prestar os esclarecimentos julgados necessários.

10.3 Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que o CONTRATANTE julgar necessário.

10.4 Manter contato e realizar o planejamento dos serviços com o CONTRATANTE de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

10.5 Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, o objeto deste Termo de Referência que não atenda às especificações exigidas, em que se verifiquem imperfeições, vícios, defeitos ou incorreções ou rejeitados pela fiscalização.

10.6 Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pelo CONTRATANTE em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste Termo de Referência.

10.7 Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.

10.8 Acatar as observações feitas pelo Fiscal do CONTRATANTE quanto à execução dos serviços.

10.9 Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

10.10 A inobservância das especificações constantes deste Termo de Referência implicará a não aceitação parcial ou total dos serviços, devendo a CONTRATADA refazer as partes recusadas sem direito a indenização.

10.11 Seguir as orientações da Lei n. 9.472/97, do Termo de Concessão ou autorização emitido pela ANATEL, e demais disposições regulamentares pertinentes aos serviços a serem prestados.

10.12 Todos os equipamentos fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área, tais como: ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações).

10.13 Credenciar junto ao CONTRATANTE um representante, denominado preposto, aceito pelo CONTRATANTE, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, indicando as formas de contato no mínimo telefone, para comunicação rápida e email para comunicação formal;

10.14 Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação.

10.15 Implantar a supervisão permanente dos serviços, de modo adequado e de forma a obter uma operação correta e eficaz.

10.16 A CONTRATADA se responsabilizará por todos os serviços não explícitos nestas especificações, mas necessários à execução dos serviços programados e ao perfeito funcionamento das instalações.

10.17 Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.

10.18 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

10.19 Acatar que o CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

10.20 São expressamente vedadas à CONTRATADA:

10.20.1 A veiculação de publicidade acerca do CONTRATANTE, salvo prévia e expressa autorização deste;

10.20.2 A subcontratação total/parcial é permitida apenas para o Item 04 mantendo os critérios estabelecidos na seção 5.5 deste Termo.

11. OBRIGAÇÕES DO CONTRATANTE

11.1 Fornecer à CONTRATADA as informações necessárias à fiel execução do objeto deste Termo de Referência.

11.2 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA durante o prazo de vigência deste Contrato.

11.3 Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n. 8.666/93, o exato cumprimento das obrigações previstas neste Termo.

11.4 Designar, e informar à CONTRATADA, fiscal do contrato e seu substituto, mantendo tais dados atualizados.

11.5 Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos materiais, de forma a assegurar o perfeito cumprimento do contrato.

11.6 Anotar em registro próprio e notificar a CONTRATADA, por escrito, a ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.

11.7 Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este Termo de Referência.

11.8 Fazer uso adequado dos equipamentos fornecidos pela CONTRATADA, seguindo as instruções constantes de seus manuais de uso.

11.9 Efetuar o pagamento devido pelos serviços prestados, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas.

12. SANÇÕES ADMINISTRATIVAS

12.1 Se a CONTRATADA, sem justa causa e/ou sem justificativa apresentada e aceita pelo CONTRATANTE, não cumprir as obrigações descritas neste Termo ou infringir preceitos legais, serão

aplicadas, segundo a gravidade da falta, as seguintes penalidades:

12.1.1 Advertência por escrito - Será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem corno, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do MPAM.

12.1.2 Multa de 2% (dois por cento) sobre o valor global contratado, a cada reincidência na penalidade de advertência. Na hipótese de reincidência por 5 (cinco) vezes na penalidade de advertência, será considerado descumprimento total da obrigação, punível com as sanções previstas em lei.

12.1.3 Multa de 2% (dois por cento) sobre o valor global contratado, por dia de atraso, no caso de descumprimento do tempo máximo, conforme seção 7 - PRAZOS PARA A PRESTAÇÃO DO SERVIÇOS, limitado a 10 (dez) dias. O atraso superior a 10 (dez) dias será considerado como descumprimento total da obrigação, punível com as sanções previstas em lei.

12.1.4 Multa de 10% (dez por cento) sobre o valor global contratado, no caso de, sem justificativa aceita pelo CONTRATANTE, o vencedor não retirar a Nota de Empenho, a Autorização de Fornecimento de Materiais/Serviço ou não assinar o contrato deixando, assim, de cumprir os prazos fixados, sem prejuízo das demais sanções previstas.

12.1.5 Multa de até 20% (vinte por cento) sobre o valor global contratado, nos casos de INEXECUÇÃO PARCIAL do objeto contratado.

12.1.6 Multa de até 30% (trinta por cento) sobre o valor global contratado, nos casos de INEXECUÇÃO TOTAL do objeto contratado.

12.1.7 Multa de até 30% (trinta por cento) sobre o valor global contratado, na hipótese de rescisão do contrato por culpa da CONTRATADA.

13. ELABORAÇÃO

13.1 O presente Termo de Referência foi elaborado pela DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO, em conformidade com as atribuições legais e regimentais, estando em consonância com as disposições legais e normativas aplicáveis, com a necessidade, interesse e conveniência da Administração, sendo parte integrante do procedimento interno respectivo.

14. DECLARAÇÃO DO SOLICITANTE

14.1 Declaro que este Termo de Referência está de acordo com a Lei n. 8.666/93 e Lei n. 10.520/2002 e alterações.

THEO FERREIRA PARÁ
Agente de apoio - Manutenção/Informática

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

15. APROVAÇÃO

TADEU AZEVEDO DE MEDEIROS
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Theo Ferreira Pará**, **Agente de Apoio - Manutenção - Suporte Informática**, em 08/11/2021, às 10:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 08/11/2021, às 10:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Tadeu Azevedo de Medeiros**, **Diretor(a) de Tecnologia de Informação e Comunicação - DTIC**, em 08/11/2021, às 10:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0720733** e o código CRC **45D07F75**.

MEMORANDO Nº 148.2021.DTIC.0720865.2021.015252

A Senhora

EDJANE DE PINHO OLIVEIRA

Chefe do Setor de Compras e Serviços

Assunto: Encaminha Termo de Referência Nº 020.2021.DTIC, revisado.

Senhora Chefe,

Honrado em lhe cumprimentar, oportunidade em que encaminho termo de referência Nº 020.2021.DTIC, revisado, de modo a ajustar alguns subitens técnicos dos itens "**5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE"** e **"5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA"**, abaixo listados, que foram identificados recentemente.

Uma vez que os ajustes recaem apenas sobre partes essencialmente técnicas do Termo de Referência, este signatário não vê a necessidade de encaminhar o processo para aprovação da SUBADM.

Lista de subitens ajustados:

1. Foi adicionado o item 5.2.15.4.9;
2. No item 5.2.15.6.34, foram retirados a opção de suporte para arquivos do tipo Android APKs e Linux (ELF);
3. Foi alterado o item 5.2.15.8.27, passando a vigorar o texto "Deve permitir a importação, criação e edição de regras SNORT";
4. Foi alterado o item 5.2.15.8.31, passando a vigorar o texto "Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.";
5. Foi alterado o item 5.2.15.8.55, passando a vigorar o texto "Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.";
6. Foi alterado o item 5.2.15.8.56, passando a vigorar o texto "Deve suportar NAT64 e NAT46";
7. Foi alterado o item 5.2.15.9.2, passando a vigorar o texto "Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a licença de maior capacidade do portfólio ou de capacidade ilimitada";
8. Foi alterado o item 5.2.15.9.41, passando a vigorar o texto "A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:"
9. Foi removido o item 5.2.15.9.42;
10. Os subitens de 5.2.15.9.**42**.1 a 5.2.15.9.**42**.15 tiver sua numeração ajustada para 5.2.15.9.**41**.1 a 5.2.15.9.**41**.15, respectivamente;

11. Foram adicionadas informações ao item 5.2.15.10.6;
12. Foram alterados valores na "Tabela de Capacidades" relativa ao item 5.2.15.10.6;
13. Foi adicionado o item 5.8.19;

Atenciosamente,

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 08/11/2021, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0720865** e o código CRC **FC581449**.

Re: Fwd: Fwd: [PGJ/AM] Serviço de Firewall em Alta Disponibilidade

Eduardo Bourdot Fidelis <eduardo.fidelis@servix.com>
Qui, 04/11/2021 20:05
Para: Setor de Compras e Servicos <compras@mpam.mp.br>
Cc: Marcelo Acursi <marcelo.acursi@servix.com>

1 anexos (3 MB)
SVX210597 - Proposta Técnica e Comercial - Solução de Segurança Palo Alto.pdf;

Prezado Felipe, boa noite.

Segue Proposta Comercial conforme solicitado.

At.te

Eduardo Fidelis
N/NE
+55 11 9 92491761

Rua Pequetita, 215 | 7º andar
Vila Olímpia | São Paulo - SP

On 25/10/2021 09:33, Eduardo Bourdot Fidelis wrote:

> Prezado Felipe, bom dia.
>
> Recebi sua mensagem e já estamos trabalhando na Proposta conforme solicitada.
>
> At.te
>
> **Eduardo Fidelis**
> N/NE
> +55 11 9 92491761
>
> Rua Pequetita, 215 | 7º andar
> Vila Olímpia | São Paulo - SP
>
>

--------- Forwarded message ---------
De: **Setor de Compras e Servicos** <compras@mpam.mp.br>
Date: sex., 22 de out. de 2021 às 11:37
Subject: [PGJ/AM] Serviço de Firewall em Alta Disponibilidade
To:

Prezada Empresa Fornecedora,

Solicitamos proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

É importante ressaltar que a proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como Razão Social; CNPJ; endereço completo; contatos telefônicos; e-mail; dados bancários; entre outros.

2 - A proposta deverá ter validade mínima de 60 dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência 13.2021.DTIC.0691989.2021.015252, de forma que a proposta atenda aos requisitos exigidos. Enviamos, também em anexo, uma planilha modelo para elaboração da proposta, indicando cada item que precisará ser cotado individualmente.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.

Atenciosamente,

Felipe Beiragrande da Costa

Setor de Compras e Serviços

Procuradoria-Geral de Justiça

Ministério Público do Estado do Amazonas

CNPJ: 04.153.748/0001-85

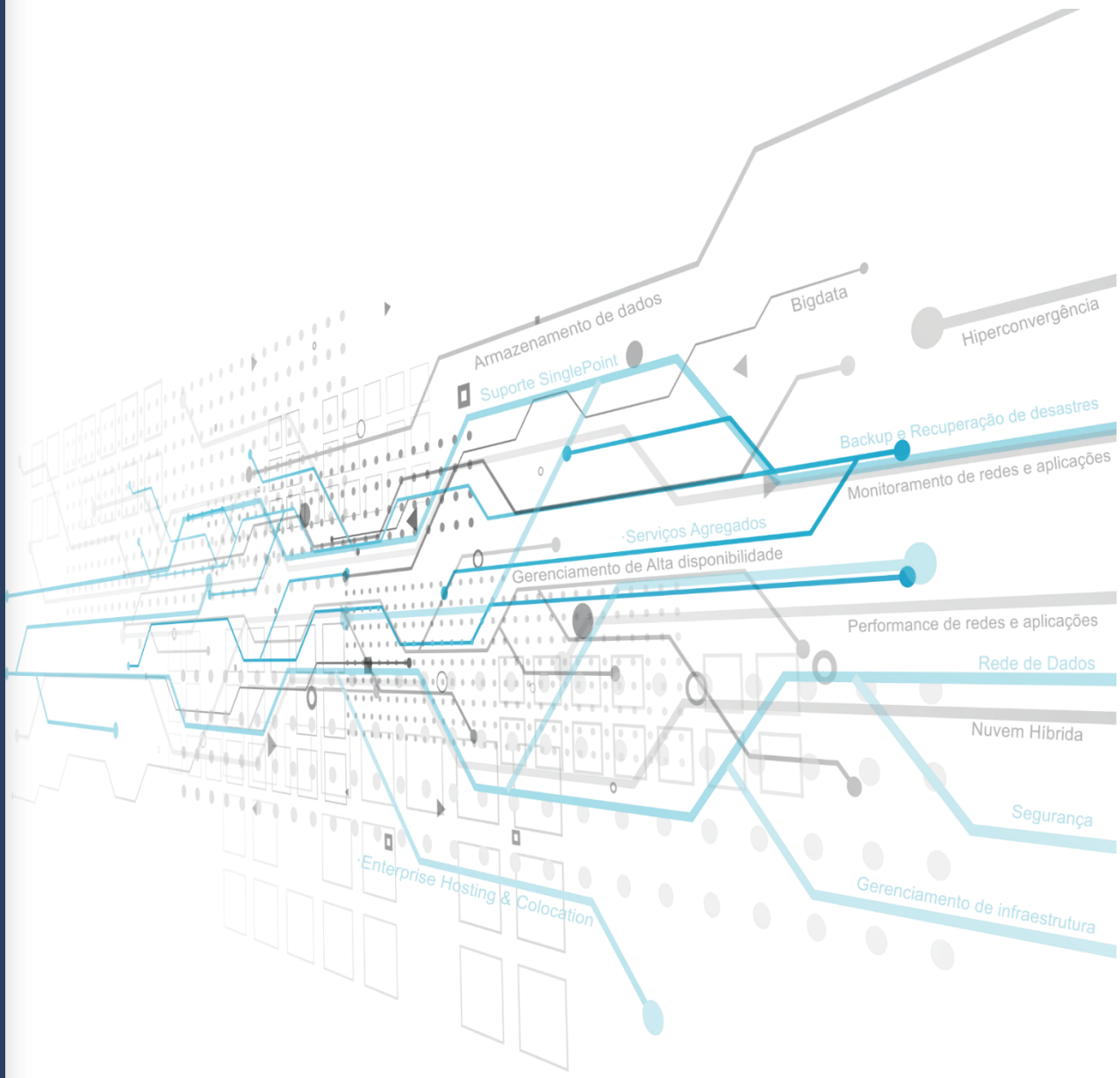
Fones: (92) 3655-0748 / 0749 / 763

--

Servix Informática Ltda
Rua Pequetita, 215 | 7º andar
Vila Olímpia | São Paulo - SP

Marcelo Acursi
Vendas N/NE
(011) 99160-1974

SERVIX



PROPOSTA TÉCNICA E COMERCIAL

www.servix.com

Proposta: SVX210597

São Paulo, 4 de novembro de 2021.

À

Ministério Público do Estado do Amazonas - MPAM,

Ref.: Solução de Segurança NGFW.

Prezado (a),

Conforme sua solicitação, estamos encaminhando nossa **Proposta Técnica e Comercial** para fornecimento de solução completa conforme referência acima citada. Nós da Servix Informática, agradecemos a oportunidade e colocamo-nos a sua disposição para esclarecimento de qualquer dúvida.

Atenciosamente,

Eduardo Fidelis

Gerente de Contas

eduardo.fidelis@servix.com

(+55 11) 3525-3400 / +55 11 99249-1761

Wesley Magalhães

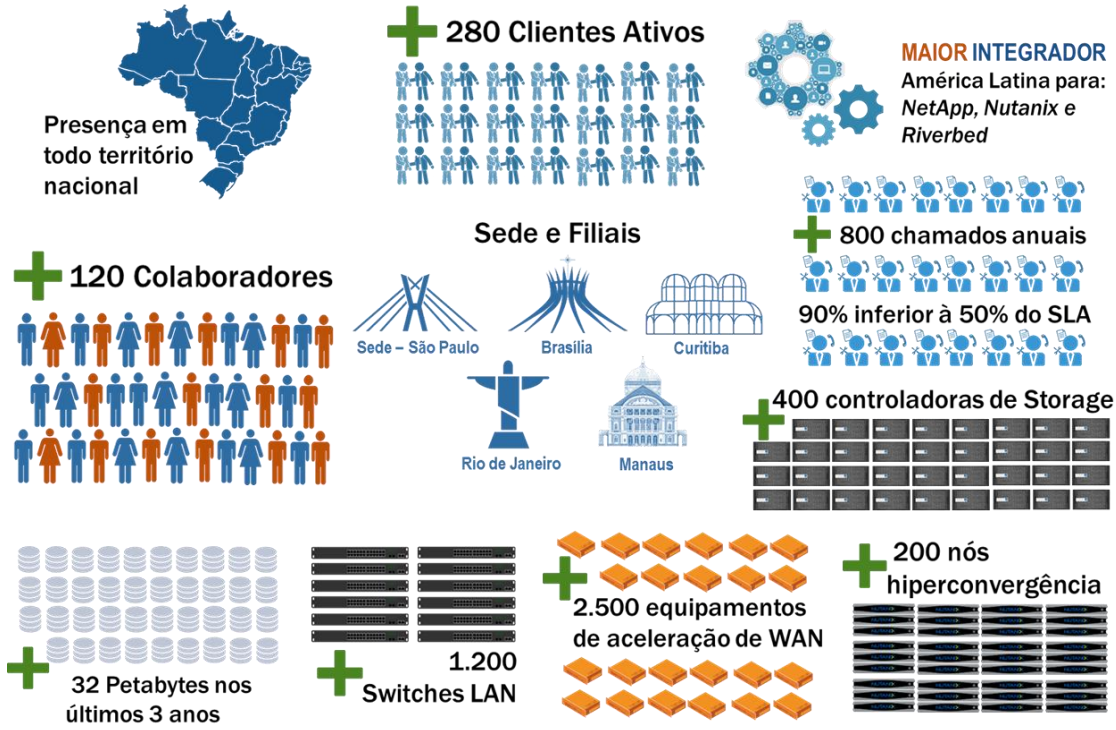
System Engineer

wesley.magalhaes@servix.com

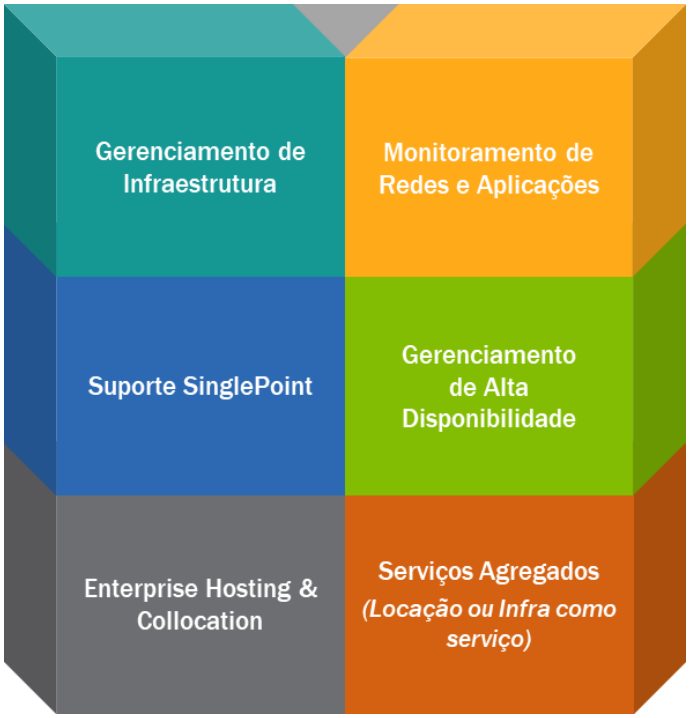
+55 11 9 7109-9226

Sobre a Servix

É integradora de soluções de tecnologia de informação para Datacenters, preparada para atender as necessidades tecnológicas de todos os segmentos de mercado. Temos um portfólio completo assim prestar atendimento de ponta a ponta.



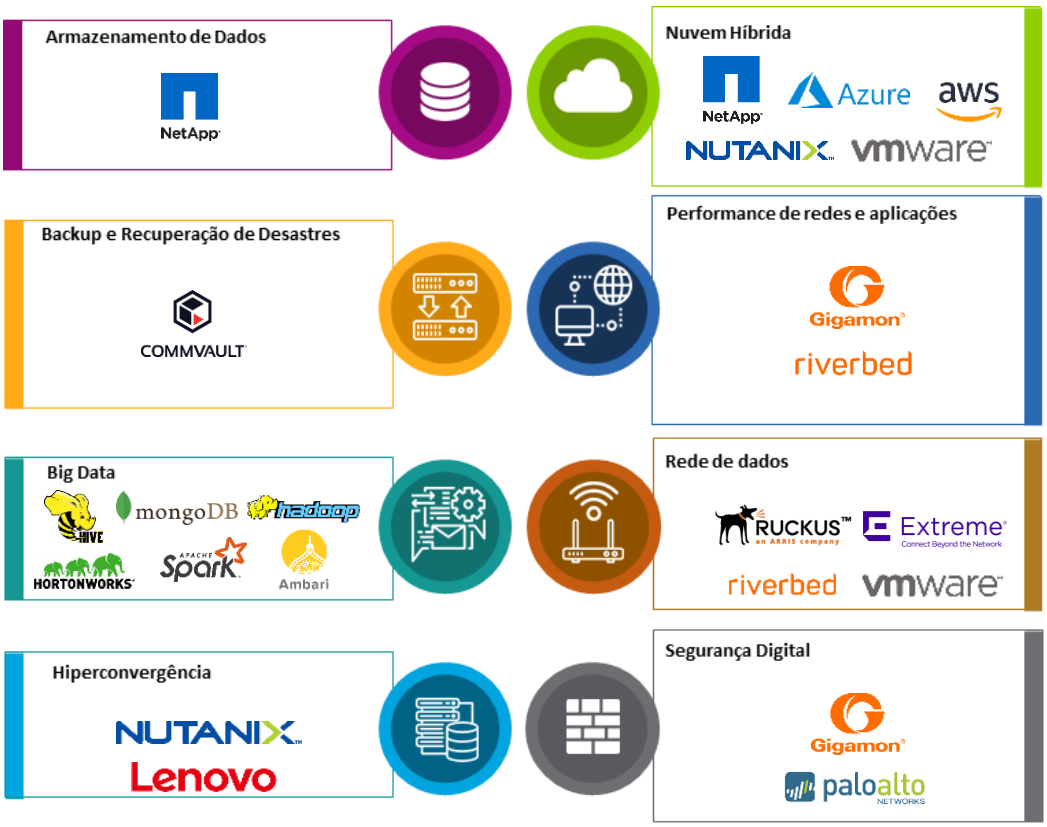
Nossos Serviços



SERVIX TEAM

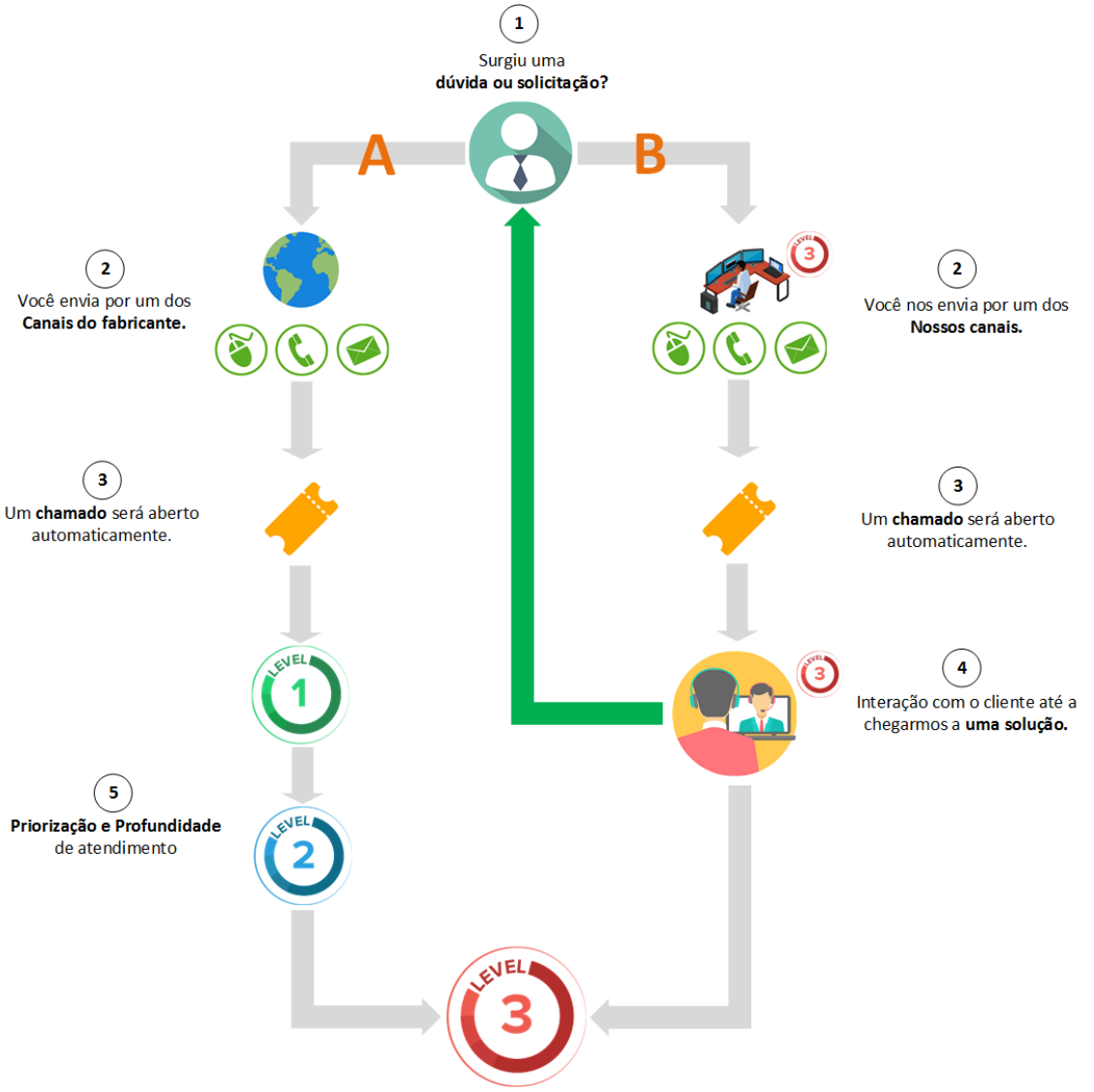
Nossas Soluções

Nossos Parceiros



Nós somos a diferença!

A Servix segue as melhores práticas de mercado, porém enxerga que apenas seguir as melhores práticas não basta para o mundo da corporativo e de Tecnologia dos dias de hoje. Devido ao seu know-how, a Servix personaliza o suporte, focando e auxiliando o cliente em melhoria contínua, eficiência técnica, priorização e acompanhamento de ocorrências. Conheça nosso fluxo e particularidades do atendimento:



Ao realizar o atendimento via Servix, na maioria das vezes, os chamados relacionados as dúvidas ou problemas são sanados no Especialista Servix de forma muito mais rápida, não havendo a necessidade de ter um escalonamento seguindo o SLA contratado no Fabricante. Em casos que a solução se dá somente pelo Fabricante, a Servix acompanha o atendimento, além de disponibilizar informações do ambiente ou execução de troubleshooting.

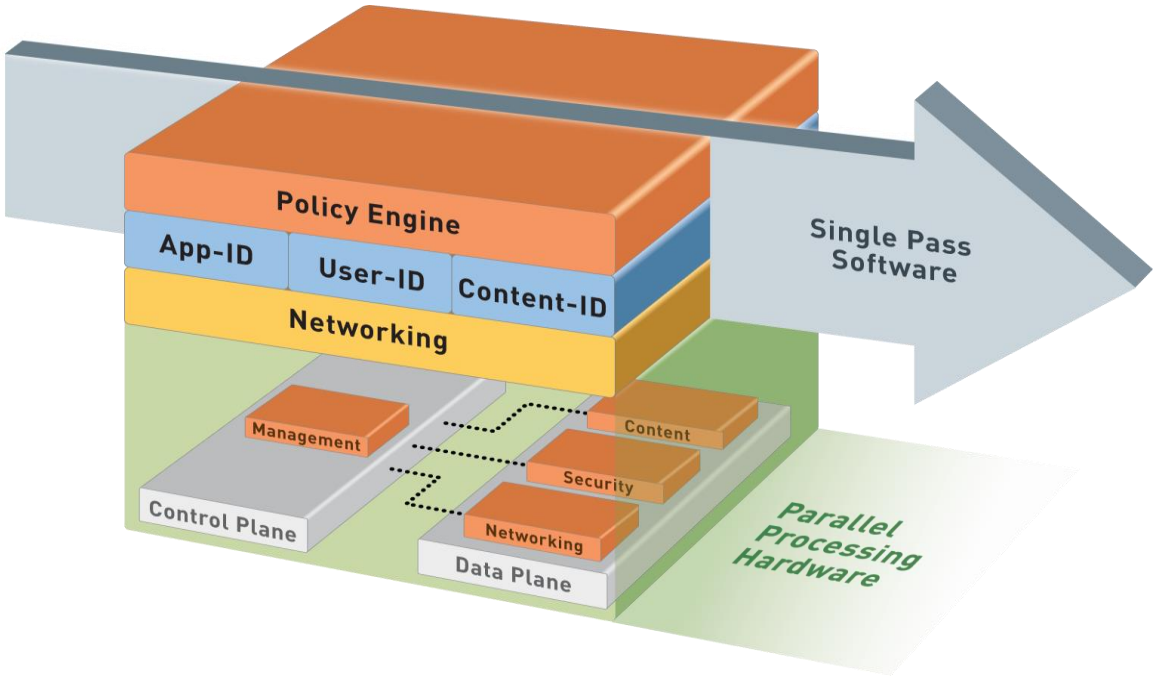
SUMÁRIO

DIFERENCIAIS PALO ALTO

A Palo Alto Networks é uma empresa de segurança de rede. Sua plataforma inovadora permite que as empresas, provedores de serviços e entidades governamentais protejam suas redes e permitam com segurança que um número cada vez mais complexo e crescente de aplicações rodem em suas redes.

O núcleo da plataforma da Palo Alto Networks é o nosso firewall de próxima geração (next-generation firewall), que oferece controle e visibilidade de aplicações, usuários e conteúdo integrados dentro do firewall por meio de sua arquitetura proprietária de hardware e software. Produtos e serviços Palo Alto Networks podem resolver uma ampla gama de requisitos de segurança de rede, a partir do datacenter para o perímetro de rede, bem como empresas distribuídas que incluem filiais e um número crescente de dispositivos móveis.

Single Pass Plataform



Passe único

- Operações únicas por pacote
    - Classificação de tráfego (identificação de Apps)
    - Mapeamento de usuário/grupo
    - Inspeção de conteúdo – ameaças, URLs, dados confidenciais
- Uma única política

Processamento Paralelo

- Hardware dedicado FPGA para funções específicas que funcionam em paralelo
- Hardware de gerência e dados separados

WildFire

Análises são realizadas em um ambiente Sandbox para arquivos desconhecido e, é apenas o primeiro passo para parar de forma eficaz ameaças avançadas. O serviço de análise baseada em cloud WildFire ™ analisa arquivos e links globalmente e designa itens nunca antes visto para uma investigação mais aprofundada por meio de análise estática e dinâmica ao longo de vários sistemas operacionais e versões de aplicativos. Se uma amostra é classificada como malicioso, o WildFire irá gerar automaticamente e preencher um conjunto holístico de novas prevenções para nossa Plataforma de Segurança de Próxima Geração e parceiros de integração, minimizando o risco de infecção a partir de ameaças conhecidas e desconhecidas, sem qualquer ação manual.

Thereat Prevention

No cenário de ameaças atual, os malwares tradicionais tornaram-se altamente segmentados e evasivos, e, especificamente projetado para ser completamente indetectável. O objetivo é violar o perímetro da rede, fornecendo malware que pode mover-se lateralmente em uma organização, extraindo dados valiosos como ele se espalha - tudo isso enquanto permanece invisível para firewalls tradicionais.

Palo Alto Networks protege sua rede contra essas ameaças, proporcionando múltiplas camadas de prevenção, enfrentando ameaças em cada fase do ataque. Nossa assinatura de prevenção de

ameaças protege a rede contra ameaças avançadas através da identificação e digitalização de todo o tráfego - aplicações, usuários e conteúdo em todas as portas e protocolos.

URL Filtering

Inteligência de ameaça global constantemente atualizada. Incluídos em nossa lista de categorias da web alguns são de alto risco, como malware, phishing e proxy-avoidance, que permitem controlar de forma granular o acesso a sites que se enquadram nestas categorias perigosas, impedir downloads, automatizar uma mensagem de aviso para Usuários, ou restringir o acesso completamente.

Nosso banco de dados global de filtragem de URLs é sincronizado com a inteligência de ameaças do WildFire e proteções geradas automaticamente a cada 15 minutos, o que significa que as categorias de URL, incluindo malware e phishing, estão sempre atualizadas para que seus usuários e dados estejam sempre protegidos.

Palo Alto Networks PA-3260 – Next-Generation Firewall

PA-3260

- Alta disponibilidade (H.A.) com modos ativo/ativo ou ativo/standby;
- Instalação simplificada;
- Identificação de aplicações independente da porta, da encriptação SSL/SSH ou técnicas de evasões aplicadas;
- Políticas de segurança para todos os usuários em todos os locais;
- Proteções extendidas para todos os vetores de ataques com as subscrições de segurança: *Threat Prevention, WildFire® malware prevention, URL Filtering, DNS Security e IoT Security;*
- Possibilidade de ativar a funcionalidade de SD-Wan simplesmente ativando a subscrição no equipamento existente.

	PA-3260
Taxa de transferência de firewall (HTTP/appmix)*	8,3/9,2 Gbps
Taxa de transferência do Threat Prevention (HTTP/appmix)†	4,1/5,0 Gbps
Taxa de transferência da VPN IPsec‡	5,0 Gbps
Máximo de sessões	3 M
Novas sessões por segundo§	105.000
Sistemas virtuais (base/máx)‖	1/6

Observação: os resultados foram medidos no PAN-OS 10.0.

SOLUÇÃO PROPOSTA

Com o objetivo de atender as necessidades do Ministério Público do Estado do Amazonas - MPAM, propomos a seguinte solução.

Cenário #01: Solução de NGFW – HA – Suporte de 48 meses.

Part #	Description	QTY
PA-PAN-PA-3260	Palo Alto Networks PA-3260	2
PA-PAN-PA-3260-TP-4YR-HA2	Threat prevention subscription 3-year prepaid, PA-3260	2
PA-PAN-PA-3260-URL4-4YR-HA2	PANDB URL filtering subscription 3-year prepaid, PA-3260	2
PA-PAN-PA-3260-WF-4YR-HA2	WildFire subscription 3-year prepaid, PA-3260	2
PA-PAN-SVC-PREM-3260-4YR	Partner enabled premium support 3-year prepaid, PA-3260	2
PA-PAN-SFP-PLUS-CU-5M	SFP+ to SFP+ PASSIVE TWINAX	2

Serviços Servix		
Serviço Servix	• Planejamento e Pós instalação • Implementação Lógica • Implementação Física • Serviço de Migração	1
Serviço Servix	Serviço de Monitoramento da Solução	1
Treinamento	40h para 5 pessoas	1

INVESTIMENTO

Nosso compromisso é o de propor soluções com qualidade e eficiência, agregando valor ao seu negócio. Razão pela qual nos empenhamos para propor valores que acreditamos ser competitivos com o mercado. O valor da solução proposta é de:

CENÁRIO 48 meses + Serviços

PLANILHA MODELO PARA PROPOSTA					
CONTRATAÇÃO DE SERVIÇO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO EM ALTA DISPONIBILIDADE, COM MONITORAMENTO, PELO PERÍODO DE 48 (QUARENTA E OITO) MESES, INCLUINDO TREINAMENTO E SERVIÇO DE MIGRAÇÃO DA PLATAFORMA ATUAL.					
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTD**	**VALOR MENSAL**	**VALOR TOTAL**
1	SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE.	MÊS	48	R$ 45.418,00	R$ 2.180.064,00
2	SERVIÇO DE MONITORAMENTO DA SOLUÇÃO.	MÊS	48	R$ 70.349,00	R$ 3.376.752,00
3	SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL.	UNIDADE	1	R$ 23.660,00	R$ 23.660,00
4	SERVIÇO DE TREINAMENTO DA SOLUÇÃO.	PESSOA	5	R$ 12.133,00	R$ 60.665,00
TOTAIS				**R$ 151.560,00**	**R$ 5.641.141,00**

PACOTE DE SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DE SOLUÇÃO

PREMISSAS

- ✓ Todos os itens descritos nesta proposta estão sujeitos à execução pela Servix somente quando licenças e suporte ativos e vigentes junto ao Fabricante da solução;
- ✓ As tarefas de "Pré-instalação" serão executadas em horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Instalação" podem ser executadas em horário comercial ou de expediente da Contratante, contudo a Servix indica que tais tarefas sejam executadas fora do horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Configuração" podem ser executadas em horário comercial ou de expediente da Contratante, contudo a Servix indica que tais tarefas sejam executadas fora do horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Migração", quando contempladas em proposta, podem ser executadas em horário comercial ou de expediente da Contratante, contudo a Servix indica que tais tarefas sejam executadas fora do horário comercial ou de expediente da Contratante;
- ✓ As tarefas de "Pós-instalação" serão executadas em horário comercial ou de expediente da Contratante;

PRÉ-INSTALAÇÃO

- ✓ Reunião de Kickoff com a Contratante;
  - Apresentar o projeto aprovado e contratado;
  - Obter os contatos e definir os times e horário dos trabalhos;
  - Apresentar equipe de gerentes e analistas da Servix;
  - Apresentar o cronograma preliminar do projeto;
  - Definir datas e restrições para o início da instalação;
- ✓ Análise da topologia, arquitetura da rede e desenho do ambiente, considerando todos equipamentos já existentes instalados que serão envolvidos no projeto;
  - Enviar o Guia de Requisitos Físicos (espaço em rack, quantidade de pontos elétricos e etc.) e lógicos (VLANs, IPs, DNS, GATEWAY, NTP e etc.) da solução;
  - Coletar as informações e preencher o Guia de Configuração do Ambiente;
  - Verificar os equipamentos entregues de acordo com a solução desenhada;
  - Verificar itens extras que precisaremos prover para a instalação;
  - Revisar e discutir os desenhos e o plano de instalação do projeto com o cliente.
  - Cadastrar equipamentos no sistema de chamados Servix;

INSTALAÇÃO

- ✓ Instalação física do(s) equipamento(s) adquirido(s) e/ou contemplado(s) no escopo da proposta no local determinado pela equipe de tecnologia da Contratante;
- ✓ Posicionar rack(s) no(s) locai(s) designado(s) pela Contratante;
- ✓ Realizar e verificar a energização dos equipamentos no(s) rack(s);
- ✓ Identificar (etiquetar) todo o cabeamento apropriadamente (provisória ou definitivamente);
- ✓ Cabear a gerência do(s) equipamento(s) adquirido(s) ou contemplado(s) no escopo da proposta;
- ✓ Revisar todo o cabeamento após a conexão;

CONFIGURAÇÃO

- ✓ Configuração do sistema de administração e gerenciamento;
- ✓ Configuração de usuários de diferentes níveis de administração;
- ✓ Configuração seguindo as melhores práticas do Fabricante;
- ✓ Configuração seguindo as regras, diretivas e normas internas da Contratante;
- ✓ Configuração de parâmetros de rede;
- ✓ Configuração com Active Directory;
- ✓ Configuração das portas;
- ✓ Configurações de NAT (Network Address Translation);
- ✓ Configurações de PAT (Protocol Address Translation);
- ✓ Configuração configurações de DNS para MGMT;
- ✓ Configuração de Balanceamento/Failover de links nos equipamentos;
- ✓ Configurar e testar o autosupport ou ferramenta disponibilizada que automatize o envio de informações para facilitar o atendimento do suporte;
- ✓ **Itens com quantidade limitada de aplicação/configuração, de acordo com a proposta:**
    - Configuração Grupos e perfis de Acesso;
    - Configuração interfaces VLAN;
    - Configuração Zonas de segurança:
    - Configuração de políticas de segurança de saída de Internet;
    - Configuração nas configurações de VPN;

- Configuração de Assinaturas de tráfego;
- Configuração de rotas estáticas;

MIGRAÇÃO

- ✓ Backup das regras e políticas do ambiente atual (caso possível);
- ✓ Backup das configurações de rede do ambiente atual (caso possível);
- ✓ Migração de configuração de rede para o(s) novo(s) equipamento(s) contemplado(s) nesta proposta;
- ✓ Migração de regras para o(s) novo(s) equipamento(s) contemplado(s) nesta proposta;
- ✓ Migração de políticas para o(s) novo(s) equipamento(s) contemplado(s) nesta proposta;

PÓS-INSTALAÇÃO

- ✓ Esclarecimento de dúvidas e/ou instruções “Best Practices” para o ambiente;
- ✓ Entrega do documento de implementação final com o resumo do ambiente (AsBuilt);
- ✓ Obter termo de aceite e encerrar o projeto;
- ✓ Obter termo de capacidade técnica;
- ✓ Treinar a equipe da Contratante na abertura de chamados no Fabricante;
- ✓ Treinar a equipe da Contratante na abertura de chamados no Servix;

- Atestado de capacidade técnica:

A Servix, ao final da implementação da solução, poderá solicitar a emissão de um atestado de capacidade técnica, informando que a compras e/ou a prestação de serviços foi concluída satisfatoriamente de acordo com o proposto.

CONDIÇÕES COMERCIAIS

Pagamento

30 dias do faturamento.

Garantia e suporte

48 meses para todo o conjunto de software, hardware e licenças.

Impostos

Já estão inclusos nos valores apresentados comercialmente todos os impostos que incidem. Quaisquer tributos, encargos sociais e/ou obrigações legais que venham a ser criados, ou alterados, após a data da proposta, e que repercutam direta ou indiretamente nos preços, implicarão na revisão dos valores descritos nesta proposta.

Validade

O Conteúdo dessa proposta é válida por 60 dias.

Prazo de Entrega

Em até 45 dias úteis após o faturamento.

Frete

Incluso na proposta.

Moeda

Valores expressos em Reais do Brasil.

Dados Cadastrais

Empresa: Servix Informática LTDA - BA

CNPJ: 01.134.191/0003-09

Inscrição Estadual: 125.903.956

Endereço: Rua Santos Dumond, 57 – Sala 202, CEP: 45.653-380– Ilhéus – BA.

Telefone/FAX: (073) 3084-3970

Dados Bancários: Banco: Itaú / Agência: 0383 / Conta Corrente: 14835-0

TERMO DE ACEITE DA PROPOSTA

Proponente: Servix Informática Ltda., inscrita no CNPJ sob n. 01.134.191/0003-09, endereço na Rua Santos Dumond, 57 - Sala 202, CEP: 45.653-380– Ilhéus – BA**.**

Cliente: Neste ato, o **Ministério Público do Estado do Amazonas - MPAM** DECLARA, para todos os fins e efeitos legais e jurídicos, ter conhecimento de todos os termos, valores, condições e peculiaridades desta Proposta Comercial **SVX210597** ao qual já pactua e autoriza a Proponente a executar suas obrigações contidas no objeto da referida proposta e, consequentemente, emitir fatura (s) e nota (s) fiscal (is) contra o **Ministério Público do Estado do Amazonas - MPAM**. Na hipótese de as partes não formalizarem o futuro contrato de compra e venda, as partes declaram e acordam, que a presente proposta, possui força e natureza contratual, produzindo todos os efeitos legais e jurídicos.

São Paulo, _____de_____de_____.

Aceite:

_____

Nome:

Cargo:

CPF:

Carimbo da Empresa:

Testemunhas:

_____ _____

Nome: Nome:

Cargo: Cargo:

CPF: CPF:

[PGJ/AM] Serviço de Firewall em Alta Disponibilidade

Setor de Compras e Servicos <compras@mpam.mp.br>

Sex, 22/10/2021 10:37

Cco: mg@actar.com.br <mg@actar.com.br>; editais@algartelecom.com.br <editais@algartelecom.com.br>; compras@altasnet.com.br <compras@altasnet.com.br>; daniels@approachtec.com.br <daniels@approachtec.com.br>; comercial@arper.com.br <comercial@arper.com.br>; arpsist@arpsist.com.br <arpsist@arpsist.com.br>; andre.oliveira@arvvo.com.br <andre.oliveira@arvvo.com.br>; bffcompanybsb@gmail.com <bffcompanybsb@gmail.com>; comercial@blueeye.com.br <comercial@blueeye.com.br>; registro.viacontabil@gmail.com <registro.viacontabil@gmail.com>; sac@comdados-ba.com.br <sac@comdados-ba.com.br>; joao.wagnitz@compwire.com.br <joao.wagnitz@compwire.com.br>; vendas.core@coretecnologia.net.br <vendas.core@coretecnologia.net.br>; callebearaujo@gmail.com <callebearaujo@gmail.com>; fernando@cyberone.com.br <fernando@cyberone.com.br>; comercial@dask.com.br <comercial@dask.com.br>; contato@everco.com.br <contato@everco.com.br>; contato@fasthelp.com.br <contato@fasthelp.com.br>; contelb@contelb.com.br <contelb@contelb.com.br>; rafael.sampaio@future.com.br <rafael.sampaio@future.com.br>

Prezada Empresa Fornecedora,

Solicitamos proposta comercial para serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

É importante ressaltar que a proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como Razão Social; CNPJ; endereço completo; contatos telefônicos; e-mail; dados bancários; entre outros.

2 - A proposta deverá ter validade mínima de 60 dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência 13.2021.DTIC.0691989.2021.015252, de forma que a proposta atenda aos requisitos exigidos. Enviamos, também em anexo, uma planilha modelo para elaboração da proposta, indicando cada item que precisará ser cotado individualmente.

Solicitamos a gentileza de confirmar o recebimento desta mensagem.

Estamos à disposição para dirimir eventuais dúvidas, que deverão ser encaminhadas por escrito, através deste endereço eletrônico.

Desde já, agradecemos a colaboração.
Atenciosamente,

Felipe Beiragrande da Costa
Setor de Compras e Serviços
Procuradoria-Geral de Justiça
Ministério Público do Estado do Amazonas
CNPJ: 04.153.748/0001-85
Fones: (92) 3655-0748 / 0749 / 763

DESPACHO Nº 484.2021.01AJ-SUBADM.0711354.2021.015252

Tratam os autos de procedimento administrativo interno iniciado pelo Ofício 108 (0692180) da Diretoria de Tecnologia da Informação e Comunicação - DTIC, submetendo à aprovação da Subprocuradoria-Geral de Justiça para Assuntos Administrativos - SUBADM, o Termo de Referência n.º 013.2021.DTIC (0691989), que trata da contratação de serviço de solução de firewall pelo período de 48 (quarenta e oito) meses, incluindo treinamento e migração da plataforma atual, conforme especificações, quantitativos e prazos contidos no documento.

Os autos vieram à análise da assessoria jurídica, que opinou favoravelmente a aprovação do Termo de Referência, conforme teor do Parecer 118 (0711353).

Isto posto, **ACOLHO** a peça opinativa e **APROVO** o Termo em questão, **devendo o processo ser encaminhado ao Setor de Compras e Serviços - SCOMS**, para realização de pesquisa de preços e mercado e à **Diretoria de Orçamento e Finanças - DOF**, para as providências orçamentárias cabíveis.

Cumpra-se.

GABINETE DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), 18 de outubro de 2021.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 18/10/2021, às 12:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0711354** e o código CRC **7B0BA6B0**.

PARECER Nº 118.2021.01AJ-SUBADM.0711353.2021.015252

PROCESSO: 2021.015252

ASSUNTO: Termo de Referência para contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

PROCEDIMENTO DE CONTRATAÇÃO PÚBLICA. ANÁLISE DE MINUTA DE TERMO DE REFERÊNCIA. No caso em análise, das informações constantes no Termo de Referência 20, observa-se que todos os requisitos exigíveis estão presentes.Inteligência dos arts. 7º, 14 e 15, da Lei nº 8.666/93 c/c art. 9º do Decreto nº 5.450/05.

Tratam os autos de procedimento administrativo interno iniciado pelo Ofício 108 (0692180) da Diretoria de Tecnologia da Informação e Comunicação - DTIC, submetendo à aprovação da Subprocuradoria-Geral de Justiça para Assuntos Administrativos - SUBADM, o Termo de Referência n.º 013.2021.DTIC (0691989), que trata da contratação de serviço de solução de firewall pelo período de 48 (quarenta e oito) meses, incluindo treinamento e migração da plataforma atual, conforme especificações, quantitativos e prazos contidos no documento.

É o breve relatório. OPINO.

Como é cediço, a Administração Pública deverá sempre observar o cumprimento do **regime jurídico-administrativo**, que consiste em um conjunto harmônico de preceitos e regras que moldam a atuação dos entes estatais, impondo limitações e prerrogativas. No âmbito do procedimento de licitação, destacam-se, dentre os princípios que regem o Direito Administrativo, os princípios da impessoalidade e da indisponibilidade do interesse público.

Acerca do princípio da **impessoalidade**, de acordo com as lições de Celso Antônio Bandeira de Mello (2009), "*[...] a Administração Pública deve tratar a todos sem favoritismos, nem perseguições, simpatia ou animosidades políticas ou ideológicas [...]*". Já quanto ao princípio da **indisponibilidade do interesse público**, Matheus Carvalho (2018) assevera que se trata de preceito que impõe:

> […] limites da atuação administrativa e decorre o fato de que a impossibilidade de abrir mão do interesse público deve estabelecer ao administrador os seus critérios de conduta. De fato, o agente estatal não pode deixar de atuar quando as necessidades da coletividade assim exigirem, uma vez que suas atividades são necessárias à satisfação dos interesses do povo [...].

Nessa esteira, dispõe a Constituição da República Federativa do Brasil, em seu artigo 37, inciso XXI, *in verbis:*

> **Art. 37**. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: [...]
>
> **XXI** – ressalvados os casos especificados na legislação, as obras, serviços, compras e alienações serão contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes, com cláusulas que estabeleçam obrigações de pagamento, mantidas as condições efetivas da proposta, nos termos da lei, o qual somente permitirá as exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações.

Dessa forma, para garantir justamente a **impessoalidade** e a **supremacia do interesse público**, bem como para a manutenção do equilíbrio social e uma boa gestão da máquina pública, é necessária, por regra, a realização do processo de licitação que, como procedimento prévio ao contrato em que se escolhe a proposta mais vantajosa à persecução de seus fins, impede que seja desvirtuado, a critério do administrador, o regime jurídico-administrativo. Excepcionalmente, como sabido, poderão ser identificadas situações em que serão aplicados os regramentos legais para as hipóteses de dispensa e/ou inexigibilidade de licitação. **Em qualquer caso, o Termo de Referência é o balizador e o limitador da atuação da Administração Pública na procedimentalização da contratação**.

Feitas tais considerações, cumpre esclarecer que o presente Parecer cinge-se tão somente à análise do destacado Termo de Referência, à luz da legislação, doutrina e jurisprudência pertinentes; questões de oportunidade e conveniência, bem como juízo de valor acerca da contratação, fogem à alçada do parecerista.

Nesse sentido, cumpre assestar que o Termo de Referência, nomenclatura utilizada na legislação pertinente ao pregão (Lei Federal nº 10.520/02), que também consta na Lei de Licitação com o *nomen juris* de Projeto Básico, é peça técnica indispensável na fase interna da licitação, traduzindo a justificativa e a necessidade de realização de determinado objeto a ser contratado pela Administração Pública. Sobre o tema, a Lei n.º 8.666/93 assim dispõe:

> **Art. 7º.** As licitações para a execução de obras e para a prestação de serviços obedecerão ao disposto neste artigo e, em particular, à seguinte sequência:
>
> I - projeto básico;
>
> II - projeto executivo;
>
> (...)
>
> § 9º. O disposto neste artigo aplica-se também, no que couber, aos casos de dispensa e de inexigibilidade de licitação.
>
> (...)
>
> **Art. 14.** Nenhuma compra será feita sem a adequada caracterização de seu objeto e indicação dos recursos orçamentários para seu pagamento, sob pena de nulidade do ato e responsabilidade de quem lhe tiver dado causa.
>
> **Art. 15.** *Omissis*
>
> § 7º. Nas compras deverão ser observadas, ainda:
>
> I - a especificação completa do bem a ser adquirido sem indicação de marca;
>
> II - a definição das unidades e das quantidades a serem adquiridas em função do consumo e utilização prováveis, cuja estimativa será obtida, sempre que possível, mediante adequadas técnicas quantitativas de estimação;
>
> III - as condições de guarda e armazenamento que não permitam a deterioração do material.

No mesmo sentido, o Decreto nº 5.504/2005, que regulamenta o pregão, na sua forma eletrônica, exige o Termo de Referência na fase interna, conforme dicção do art. 9º:

> **Art. 9º** Na fase preparatória do pregão, na forma eletrônica, será observado o seguinte:
>
> **I – elaboração de termo de referência pelo órgão requisitante, com indicação do objeto de forma precisa, suficiente e clara, vedadas especificações que, por excessivas, irrelevantes ou desnecessárias, limitem ou frustrem a competição ou sua realização;**
>
> **II – aprovação do termo de referência pela autoridade competente;** […].
>
> §1º A autoridade competente motivará os atos especificados nos incisos II e III, indicando os elementos técnicos fundamentais que o apoiam, bem como quanto aos elementos contidos no orçamento estimativo e

no cronograma físico-financeiro de desembolso, se for o caso, elaborados pela administração.

§2º O termo de referência é o documento que deverá conter elementos capazes de propiciar avaliação do custo pela administração diante de orçamento detalhado, definição dos métodos, estratégia de suprimento, valor estimado em planilhas de acordo com o preço de mercado, cronograma físico-financeiro, se for o caso, critério de aceitação do objeto, deveres do contratado e do contratante, procedimentos de fiscalização e gerenciamento do contrato, prazo de execução e sanções, de forma clara, concisa e objetiva.

Em consonância com o acima aludido, o Tribunal de Contas da União já decidiu pela necessidade do referido estudo técnico preliminar:

> REPRESENTAÇÃO. PREGÃO ELETRÔNICO. CAUTELAR. OITIVA. AUDIÊNCIA. DIRECIONAMENTO A PRODUTOS DE DETERMINADO FABRICANTE. AUSÊNCIA DE ESTUDOS PRÉVIOS COMPROBATÓRIOS DA NECESSIDADE DAS ESPECIFICAÇÕES TÉCNICAS. CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS APÓS A ATUAÇÃO DESTA CORTE. REVOGAÇÃO DA CAUTELAR. MULTA. DETERMINAÇÕES.
>
> **- As especificações técnicas dos objetos a serem adquiridos devem decorrer de necessidades identificadas em estudos prévios ao certame licitatório.**
>
> **- Do processo administrativo para aquisição de bens e serviços deve constar os estudos e levantamentos que fundamentaram a fixação das especificações técnicas.**
>
> - É defesa a exigência de seguros em licitações que se destinem a compras de equipamentos sem previsão de pagamentos antecipados, salvo motivo justificado exposto no instrumento convocatório.
>
> - É defesa a exigência de número de registro no Ministério da Saúde, de produtos não incluídos na relação estabelecida pela Lei 6.360/1976, salvo motivo justificado, exposto no instrumento convocatório.
>
> (TCU, Acórdão 310/203, Processo 037.832/2011-5).

Com efeito, a contratação pretendida envolve definição de critérios técnicos detalhados, por se tratar de soluções de TI, os quais compõem de forma decisiva a especificação do serviço que se pretende contratar: solução de firewall pelo período de 48 (quarenta e oito) meses, incluindo treinamento e migração da plataforma atual,

Destarte, imperioso verificar se os elementos constitutivos do Termo de Referência se encontram todos presentes, mormente no que tange à especificação do objeto a ser licitado, ainda que possa haver alguma complementação posterior, bem como a forma pela qual o objeto da licitação deve ser executado, com a definição de métodos, estratégias de suprimentos e prazo de execução. Ao se consultar o compêndio de Orientações e Jurisprudência do TCU (disponível em *www.portaltcu.gov.br*), tem-se que o Termo de Referência deve conter, dentre outros, os seguintes elementos:

- Descrição do objeto do certame, de forma precisa, suficiente e clara;

- Critérios de aceitação do objeto;

- Critérios de avaliação do custo do bem ou serviço pela Administração, considerando os preços praticados no mercado;

- Valor estimado em planilhas de quantitativos e preços unitários, se for o caso;

- Prazo de execução do serviço ou de entrega do objeto;

- Definição dos métodos e estratégia de suprimento;

- Cronograma físico-financeiro, se for o caso;

- Deveres do contratado e do contratante;

- Prazo de garantia, quando for o caso;

- Procedimentos de fiscalização e gerenciamento do contrato;

- Sanções por inadimplemento

Dos critérios mínimos estabelecidos pela egrégia Corte Superior de Contas, constata-se que o Termo de Referência engloba tanto os elementos fáticos motivadores da contratação, quanto as balizas

objetivas que irão nortear o certame licitatório, conforme o caso.

No caso em análise, das informações constantes no Termo de Referência 13 (0691989), observa-se que todos os requisitos exigíveis estão presentes, a exemplo do objeto a ser contratado, com especificação de itens, suporte técnico e garantia; vistoria; prazos e condições de prestação do serviço e recebimento; das obrigações da contratada e contratante; da previsão de sanções administrativas e do procedimento para liquidação e pagamento. Em tempo, a despeito de inexistir item específico tratando sobre o procedimento de fiscalização e gerenciamento do contrato e/ou instrumento equivalente, há na minuta apresentada diretrizes de fiscalização, não havendo necessidade de maior detalhamento, especialmente em razão da natureza do objeto a ser contratado.

Dessa forma, considerando os fundamentos até aqui expostos, **OPINO** pela **APROVAÇÃO** do Termo de Referência.

Em tempo, importante frisar que a Lei nº 14.133/2021, a nova Lei de Licitações, em que pese não ter revogado de imediato todos os dispositivos da Lei nº 8.666/93, ja previu em seu artigo 6º, XXIII, a definição e os elementos do Termo de Referência, sendo indispensável que as unidades deste Ministério Público iniciem a cautelosa transposição dos ensinamentos do novo mandamento legal aos documentos correlatos às licitações e aos contratos administrativos vindouros, preparando-se para a total revogação da Lei n. 8.666/93.

É o parecer que submeto à apreciação de V. Ex.ª.

ASSESSORIA DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, Manaus (AM), 18 de outubro de 2021.

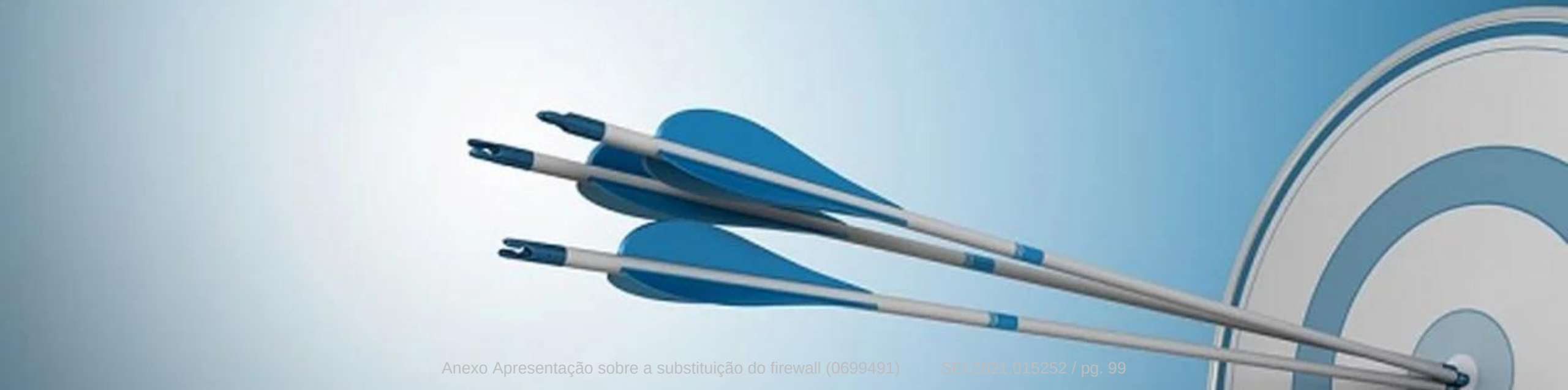
TEREZA CRISTINA MOTA DOS SANTOS PINTO
Assessora Jurídica
Ato PGJ 338/2020

Documento assinado eletronicamente por **Tereza Cristina Mota dos Santos Pinto**, **Assessor(a) Jurídico(a) de Subprocurador-Geral de Justiça**, em 18/10/2021, às 11:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0711353** e o código CRC **7B2DCC6E**.

Infraestrutura de TI: Melhorias para 2021

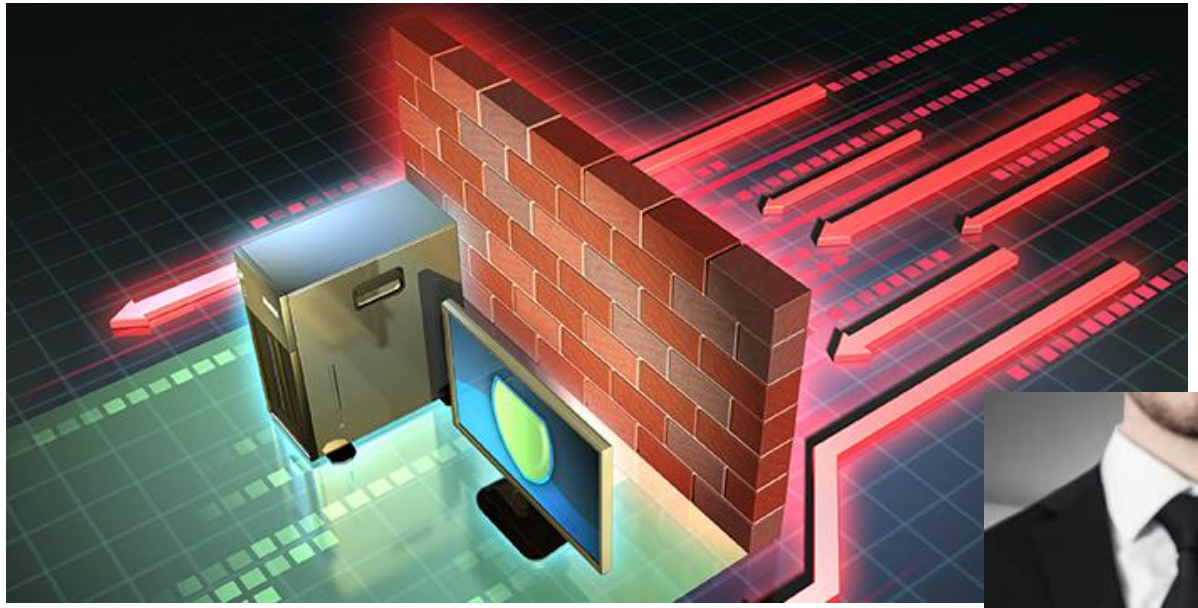
Substituição do Firewall principal



Infraestrutura de TI: Melhorias para 2021

O que é o Firewall? Qual o papel do Firewall principal?

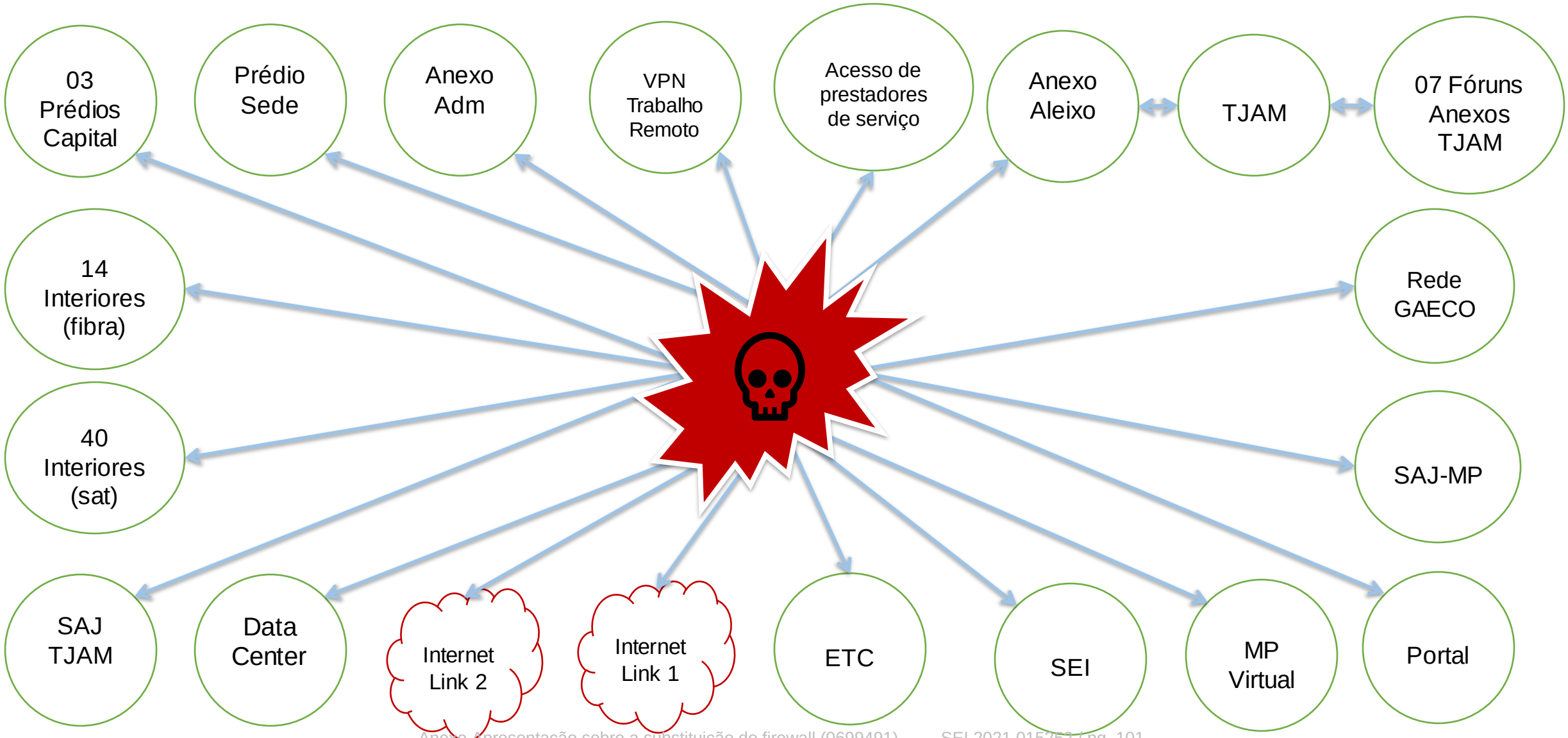
Segurança, SIM!



Mas ele é responsável por muito mais que isso...

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Infraestrutura de TI: Melhorias para 2021



Infraestrutura de TI: Melhorias para 2021

Firewall atual (Palo Alto) – Como estamos?

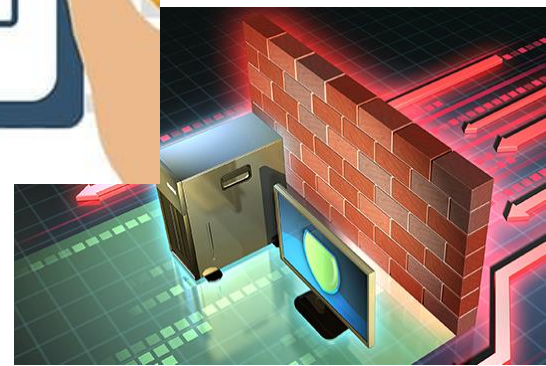
- Equipamento único (sem redundância)
- Em caso de falha, MPAM fica offline por semanas
- Equipamento obsoleto
- Software obsoleto
- Sem recursos avançados de segurança
- Performance insuficiente
- Licenças de atualização e manutenção vencendo

Infraestrutura de TI: Melhorias para 2021

Substituir Firewall – Garantir disponibilidade e segurança lógica

Requisitos necessários

- Redundância
- Performance à altura do crescimento do MPAM
- Recursos de segurança com tecnologia de ponta
- Hardware e Software sempre atualizados, nunca obsoletos
- Serviços de instalação e migração do atual
- Serviços de manutenção preventiva e corretiva
- Serviços de monitoramento e alertas automáticos



Infraestrutura de TI: Melhorias para 2021

Substituir Firewall – Opções avaliadas – Comparativo

	Renovar licenças	Compra Comum	Contrato de Serviço
Atende a todos os requisitos	✗	! Parcial	✓ Total
↳ Redundância	✗	✓	✓
↳ Performance	✗	! Temporário	✓ Sempre
↳ Recursos avançados de segurança	✗	! Temporário	✓ Sempre
↳ Obsolescência (Hw e Sw atualizado)	✗	! Temporário	✓ Sempre
Serviços de Instalação e Migração	⊘	✓	✓
Serviços de Gerência e Manutenção	! Limitado	! Limitado	✓ Completo
Serviços de Monitoramento e Alertas	✗	✗	✓
Pagamento	! De uma vez	! De uma vez	✓ Mensal

! DESCARTADA !

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Infraestrutura de TI: Melhorias para 2021

Substituir Firewall – Opções avaliadas – Estimativas de Custo

	Compra (Valor mensal)[1]	Serviço (Valor mensal)	Compra (Valor total)	Serviço (Valor total)[2]
Contrato para 3 anos	R$67.580,67	R$73.258,13	R$2.432.904,00	R$2.637.292,68
Contrato para 5 anos	R$57.761,80	R$55.831,83	R$3.465.708,00	R$3.349.909,80

[1] Apenas para comparação. Não é possível pagamento mensal na modalidade de compra.

[2] Apenas para comparação. O pagamento do contrato de serviço é feito de forma mensal.

Infraestrutura de TI: Melhorias para 2021

Substituir Firewall – Opções avaliadas – Comparativo

	Renovar licenças	Compra Comum	Contrato de Serviço
Atende a todos os requisitos	✗	! Parcial	✓ Total
↳ Redundância	✗	✓	✓
↳ Performance	✗	! Temporário	✓ Sempre
↳ Recursos avançados de segurança	✗	! Temporário	✓ Sempre
↳ Obsolescência (Hw e Sw atualizado)	✗	! Temporário	✓ Sempre
Serviços de Instalação e Migração	⊘	✓	✓
Serviços de Gerência e Manutenção	! Limitado	! Limitado	✓ Completo
Serviços de Monitoramento e Alertas	✗	✗	✓
Pagamento	! De uma vez	! De uma vez	✓ Mensal
Custo-benefício	⊘	! Baixo	✓ Alto

! DESCARTADA !

TERMO DE REFERÊNCIA Nº 13.2021.DTIC.0691989.2021.015252

1. OBJETO

1.1 Contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual.

2. JUSTIFICATIVA

2.1 A presença digital pervasiva é essencial a todos os ramos de atuação na sociedade, especialmente aos órgãos públicos que prestam serviço direto à população, como é o caso do Ministério Público do Estado do Amazonas (MPAM). Isto exige que os sistemas institucionais estejam ininterruptamente conectados à Internet e disponíveis para acesso.

2.2 Intrinsecamente, todo sistema, equipamento e rede conectados à Internet estão sujeitos aos mais diversos tipos de ameaças virtuais. O fluxo constante de complexas e evoluídas ameaças como worms, spywares, cavalos de tróia, hackers, ladrões de identidade e diversos outros tipos de ataques, advindos tanto do ambiente externo quanto do ambiente interno, ameaçam os dispositivos conectados. Os danos causados pelas pragas virtuais podem comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações, serviços e operações de rede, atingindo recursos essenciais para o funcionamento do MPAM, o que inclui seus bens tangíveis e intangíveis, como a reputação da instituição perante a sociedade.

2.3 A Segurança da Informação é o processo que define os artefatos e políticas necessários para a proteção e manutenção da disponibilidade, integridade, confidencialidade e autenticidade de estações, servidores, usuários e informações corporativas. Atualmente, este processo, em nenhuma circunstância, pode ser composto apenas de um software antivírus instalado nas estações de trabalho e um firewall simples de bloqueio de portas. As ameaças, que podem ser internas ou externas, seguem aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas, com múltiplas camadas de proteção, de forma a reduzir os riscos, minimizando a probabilidade e os impactos de um eventual ataque cibernético.

2.4 Dessa forma, o MPAM necessita manter permanentemente, sob pena de interrupção de suas atividades e prejuízos irreparáveis, uma solução corporativa de Segurança da Informação avançada e à altura dos desafios impostos pelas ameaças. A solução precisa permitir a identificação das tentativas de invasão aos sistemas informatizados do MPAM, impedir e mitigar as vulnerabilidades existentes, além de intervir tempestivamente quando necessário, protegendo a Instituição da maior gama de ataques internos e externos existentes. Um item crucial e imprescindível em qualquer solução de Segurança da Informação é conhecido como firewall de próxima geração (NGFW).

2.5 O MPAM dispõe atualmente de equipamento do tipo NGFW em operação, da marca Palo Alto. Entretanto, trata-se de um único equipamento, sem qualquer tipo de redundância para caso de falhas, que já está obsoleto quanto ao hardware e ao software, ou seja, já foi descontinuado pelo fabricante, não dispondo das tecnologias de segurança mais atuais e avançadas. Além disto, com o crescimento do MPAM e da necessidade de conexões cada vez mais rápidas, a performance do equipamento está muito aquém do necessário, impondo diminuição da eficiência das atividades da instituição. Por fim, as licenças de atualização das definições de detecção de ameaças e de suporte técnico expiram no mês de agosto do corrente ano. A expiração das licenças não impede totalmente o funcionamento do equipamento, mas diminui sua eficácia conforme o tempo passa e novas ameaças surgem, sem que seja possível atualizar o equipamento com as respectivas definições de detecção e bloqueio. Fica inequivocadamente estabelecido que a substituição deste equipamento por sistema superior é urgente.

2.6 O sistema em questão, além das funcionalidades direta e especificamente relacionadas a segurança da informação, provê diversas outras funcionalidades necessárias ao funcionamento do MPAM, como o uso de VPN, por exemplo, sendo indispensável ao funcionamento do órgão como um todo. É ele que permite a conexão segura, fidedigna e unificada de todas as localidades de funcionamento do MPAM, em todo o estado do Amazonas, que inclui mais de 10 unidades descentralizadas na capital e de 54 comarcas do interior, perrmitindo o uso de todos os recursos informatizados utilizados pelos membros e servidors para consecução de suas atividades com a eficiência exigida para atingir os objetivos de atendimento à sociedade com a qualidade esperada.

2.7 A solução proposta visa elevar o patamar da proteção do ambiente computacional do MPAM e permitir a contínua mensuração do nível de segurança em que as redes do MPAM se encontram, bem como identificar as ações que devem ser tomadas para mantê-las em nível de segurança aceitável.

2.8 A contratação desta solução também se justifica pelos resultados que podem ser obtidos, quais sejam:

2.8.1 Operações digitais mais seguras, incluindo o bloqueio de acessos indevidos, roubos e sequestros de informações sensíveis do MPAM.

2.8.2 Ambiente tecnológico mais confiável.

2.8.3 Fornecimento de serviços de tecnologia mais estáveis.

2.8.4 Menor tempo de indisponibilidade do ambiente e dos serviços informatizados.

2.8.5 Parque tecnológico mais seguro contra ataques ou invasões.

2.8.6 Capacidade de planejamento, priorização e alocação de recursos melhorados.

2.8.7 Desempenho institucional e profissional incrementado.

2.8.8 Maior qualificação da mão de obra técnica na execução dos serviços de Segurança da Informação.

2.8.9 Adoção das melhores práticas de mercado, com inovação e assertividade.

2.9 A presente demanda está alinhada com o plano estratégico 2017-2027 do MPAM, objetivo 3.02 - Aprimorar a infraestrutura, gestão e governança de tecnologia da informação, por meio da iniciativa estratégica 3.02.2.03 - "Elaborar e implementar projeto de modernização do datacenter", além de dar suporte ao objetivo 2.11 - "Ampliar e integrar soluções em tecnologias da informação e comunicacão".

3. DESCRIÇÃO DO OBJETO

3.1 O objeto deste Termo compreende a contratação de serviço de firewall de próxima geração em alta disponibilidade, pelo **período de 48 (quarenta e oito) meses**, para instalação na sede do Ministério Público do Estado do Amazonas (MPAM), doravante denominado como CONTRATANTE, compreendendo os serviços de instalação, configuração, migração e ativação de equipamentos de segurança; de sistema de monitoramento dos serviços providos e de treinamento para a equipe do CONTRATANTE, por empresa especializada nestes tipos de serviço, doravante denominada CONTRATADA, conforme condições e especificações detalhadas neste Termo de Referência.

3.2 A contratação terá um único lote, organizado conforme tabela a seguir:

LOTE	ITEM	DESCRIÇÃO	UND	QTDE
A	01	Serviço de Firewall em Alta Disponibilidade	Meses	48
	02	Serviço de Monitoramento da Solução	Meses	48
	03	Serviço de Migração do Ambiente Atual	Unidades	01
	04	Serviço de Treinamento da Solução	Pessoas	05

3.3 O Lote deverá possuir vencedor único, ou seja, ser arrematado por um mesmo fornecedor, uma vez que os bens e serviços pretendidos estão intrinsecamente relacionados. A adjudicação dos itens, dentro do mesmo lote, para empresas diferentes pode resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo ao CONTRATANTE.

4. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO

4.1 A licitante deve apresentar, juntamente com os demais documentos de habilitação, atestado(s) de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem já ter prestado serviços de firewall (Next Generation Firewall), de forma satisfatória, com capacidade de tráfego (*troughput*) de, no mínimo, 10 (dez) Gbps, incluindo fornecimento de equipamento(s), serviço de instalação, treinamento, monitoramento e garantia de, no mínimo, 12 (doze) meses, similares ao objeto deste Termo.

4.2 Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.

5. DETALHAMENTO DO OBJETO

5.1 ESPECIFICAÇÕES GERAIS - PARA TODOS OS ITENS

5.1.1 São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

5.1.2 Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de end-of-sale, end-of-

support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

5.1.3 Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a CONTRATANTE seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA);

5.1.4 O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 5.4.10, ou na exposição de ativos a riscos de segurança.

5.1.5 Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional MPAM.

5.1.6 A CONTRATADA deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

5.1.7 Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. Qualquer dano eventual de manuseio/transporte a CONTRATADA será obrigada a reparo imediato.

5.1.8 Quaisquer recursos materiais que tenham sido instalados nas dependências do CONTRATANTE pela CONTRATADA durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a CONTRATADA arcar com todos os custos referentes ao envio e transporte desses materiais.

5.1.9 Após o encerramento do contrato, caso haja a necessidade expressa pelo CONTRATANTE, a CONTRATADA deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada a prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do CONTRATANTE durante uma eventual transição para os serviços de outra contradada.

5.1.10 Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço será de propriedade do CONTRATANTE, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do CONTRATANTE.

5.1.11 A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

5.1.12 A CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE

5.2.1 O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de “Firewall” provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do CONTRATANTE e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

5.2.2 Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

5.2.3 Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

5.2.4 O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web.

5.2.5 Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela CONTRATADA.

5.2.6 Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

5.2.7 Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

5.2.8 Os serviços de instalação e implantação da solução serão de responsabilidade da CONTRATADA, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos serviços especificados.

5.2.9 Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

5.2.10 Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

5.2.11 O CONTRATANTE entregará à CONTRATADA, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do CONTRATANTE e configurados pela CONTRATADA quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o CONTRATANTE.

5.2.12 O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos *appliances* que compõem a solução, operando em alta disponibilidade.

5.2.13 Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo *appliance*, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 deste Termo, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

5.2.14 Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

5.2.15 A solução deve ser capaz de atender às seguintes especificações mínimas dos serviços, a serem ofertados em uma única plataforma:

5.2.15.1 VPN

5.2.15.1.1 Suportar VPN Site-to-Site e Client-To-Site.

5.2.15.1.2 Suportar IPSec VPN.

5.2.15.1.3 Suportar SSL VPN.

5.2.15.1.4 A VPN IPSEc deve suportar 3DES.

5.2.15.1.5 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

5.2.15.1.6 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.2.15.1.7 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

5.2.15.1.8 A VPN IPSEc deve suportar AES 128 e 256 (Advanced Encryption Standard).

5.2.15.1.9 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

5.2.15.1.10 Deverá ser suportado o uso de CA interna e CA externa de terceiros.

5.2.15.1.11 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

5.2.15.1.12 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

5.2.15.1.13 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

5.2.15.1.14 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

5.2.15.1.15 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

5.2.15.1.16 Atribuição de DNS nos clientes remotos de VPN.

5.2.15.1.17 Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

5.2.15.1.18 Suportar autenticação via AD/LDAP, certificado e base de usuários local.

5.2.15.1.19 Suportar leitura e verificação de CRL (certificate revocation list).

5.2.15.1.20 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

5.2.15.1.21 Deverá manter uma conexão segura com o portal durante a sessão.

5.2.15.1.22 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 ou superior (64 bits) e Mac OS X (v10.14 ou superior).

5.2.15.2 GEOLOCALIZAÇÃO

5.2.15.2.1 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.2.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.2.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas que as utilizem.

5.2.15.3 QOS E TRAFFIC SHAPPING

5.2.15.3.1 Suportar a criação de políticas de QoS por endereço de origem, por endereço de destino e por porta.

5.2.15.3.2 QoS deve possibilitar a definição de classes por banda garantida, banda máxima e fila de prioridade.

5.2.15.3.3 Disponibilizar estatísticas RealTime para classes de QoS.

5.2.15.3.4 Deve fazer controle de banda por aplicação, por usuário e por IP.

5.2.15.4 IDENTIFICAÇÃO DE USUÁRIOS

5.2.15.4.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.

5.2.15.4.2 A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários.

5.2.15.4.3 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites de usuários ou qualquer tipo de restrição de uso, como a utilização de sistemas virtuais ou segmentos de rede, mas não se limitando a estes.

5.2.15.4.4 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.2.15.4.5 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.7 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular.

5.2.15.4.8 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

5.2.15.5 CONTROLE DE APLICAÇÃO E FILTRO URL

5.2.15.5.1 Deve permitir especificar política por tempo, ou seja, a definição de regras

para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

5.2.15.5.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.5.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.

5.2.15.5.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

5.2.15.5.5 Possuir pelo menos 60 categorias de URLs.

5.2.15.5.6 Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

5.2.15.5.7 Permitir a customização de página de bloqueio.

5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).

5.2.15.5.9 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

5.2.15.5.10 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

5.2.15.5.11 Reconhecer pelo menos 2700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, e-mail e compartilhamento de arquivos.

5.2.15.5.12 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.

5.2.15.5.13 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

5.2.15.5.14 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a, Bittorrent e aplicações VOIP que utilizam criptografia proprietária.

5.2.15.5.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

5.2.15.5.16 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.

5.2.15.5.17 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.2.15.5.18 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação.

5.2.15.5.19 Identificar o uso de táticas evasivas via comunicações criptografadas.

5.2.15.5.20 Atualizar a base de assinaturas de aplicações automaticamente.

5.2.15.5.21 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

5.2.15.5.22 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

5.2.15.5.23 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo.

5.2.15.5.24 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

5.2.15.5.25 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

5.2.15.5.26 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

5.2.15.5.27 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, Emule, etc), possuindo granularidade de controle/políticas para cada um deles.

5.2.15.5.28 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (WhatsApp, AIM, Hangouts, Facebook Chat, etc), possuindo granularidade de controle/políticas para cada um deles.

5.2.15.5.29 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.

5.2.15.5.30 Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para cada uma delas.

5.2.15.5.31 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como a tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc).

5.2.15.5.32 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como o nível de risco da aplicação.

5.2.15.5.33 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como a categoria da aplicação.

5.2.15.5.34 Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto.

5.2.15.5.35 Deve possuir categoria específica para classificar domínios recém registrados, com menos de 32 (trinta e dois) dias.

5.2.15.6.36 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução.

5.2.15.6 PREVENÇÃO DE AMEAÇAS COM IPS, ANTIVÍRUS E ANTI-BOT

5.2.15.6.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

5.2.15.6.2 Deve incluir assinaturas de prevenção de intrusão (IPS).

5.2.15.6.3 Deve incluir assinaturas de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

5.2.15.6.4 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por toda a vigência do contrato.

5.2.15.6.5 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

5.2.15.6.6 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU ou memória do dispositivo.

5.2.15.6.7 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear.

5.2.15.6.8 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

5.2.15.6.9 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.6.10 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

5.2.15.6.11 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

5.2.15.6.12 Deve permitir o bloqueio de vulnerabilidades.

5.2.15.6.13 Deve permitir o bloqueio de exploits conhecidos.

5.2.15.6.14 Deve incluir proteção contra-ataques de negação de serviços.

5.2.15.6.15 Deverá possuir os seguintes mecanismos de inspeção de IPS: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

5.2.15.6.16 Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

5.2.15.6.17 Detectar e bloquear a origem de port scans.

5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos.

5.2.15.6.19 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

5.2.15.6.20 Possuir assinaturas para bloqueio de ataques de buffer overflow.

5.2.15.6.21 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.

5.2.15.6.23 Suportar bloqueio de arquivos por tipo.

5.2.15.6.24 Identificar e bloquear comunicação com botnets.

5.2.15.6.25 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.

5.2.15.6.27 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação através da console de gerência centralizada.

5.2.15.6.28 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

5.2.15.6.29 Os eventos devem identificar o país de onde partiu a ameaça.

5.2.15.6.30 A solução deve ter um mecanismo centralizado de correlação e relatório de evento para IPS, Antivírus e Anti-bot.

5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

5.2.15.6.33 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança.

5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox.

5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY

5.2.15.7.1 O relatório das emulações deve apresentar a listagem dos arquivos emulados.

5.2.15.7.2 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks.

5.2.15.7.3 Caso a Prevenção de Ameaças 0-Day seja ofertada no modelo de appliance, o hardware e software fornecido não podem constar, em momento algum durante a vigência do contrato, em listas de end-of-sale, end-of-support, end-of engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2.15.7.4 Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS.

5.2.15.7.5 A solução deve ser capaz de inspecionar o tráfego criptografado SSL.

5.2.15.7.6 A solução de Emulação, deve possuir engine onde remove os conteúdos ativos e exploits a partir do documento inspecionado.

5.2.15.7.7 A solução deve possuir engine onde faça Mitigação DNS, sendo ela possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso.

5.2.15.7.8 Implementar e identificar existência de malware em anexos de e-mail e URLs conhecidas.

5.2.15.7.9 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

5.2.15.7.10 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF.

5.2.15.7.11 A solução deve fornecer a capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, incluindo, no mínimo, as versões de Windows suportadas pela Microsoft.

5.2.15.7.12 A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

5.2.15.7.13 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.

5.2.15.7.14 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

5.2.15.7.15 Implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle).

5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

5.2.15.7.17 A solução de emulação, deverá suportar a inspeção/bloqueio de malwares em tempo real para determinar o veredito e bloqueio de um malware.

5.2.15.7.18 Implementar atualização a base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização.

5.2.15.7.19 Deve realizar bloqueio de ameaças avançadas de dia zero independente do sistema operacional.

5.2.15.7.20 O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regra individualmente visando otimizar a performance do equipamento.

5.2.15.7.21 A solução deve apresentar informações comportamental incluindo listagem de módulos e processos utilizados pelo malware e/ou código malicioso de forma sequencial.

5.2.15.7.22 Toda análise poderá ser realizada em nuvem, desde que do mesmo fabricante da solução.

5.2.15.7.23 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador para solicitar a análise.

5.2.15.7.24 Todas as máquinas virtuais utilizadas na nuvem do fabricante devem estar integralmente instaladas e licenciadas pelo período do contrato, sem a necessidade de intervenções por parte do administrador do sistema, e, as atualizações deverão ser providas pelo fabricante.

5.2.15.7.25 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.

5.2.15.7.26 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

5.2.15.7.27 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede, endereço IP.

5.2.15.7.28 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado. A solução deve suportar a inspeção de, no mínimo, os seguintes tipos de arquivos: CAB, DOC, DOCX, DOCM, DOT, DOTM, DOTX, EXE, HWP, JAR, PDF, PIF, PPAM, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, RAR, RTF, Seven-Z, SLDM, SLDX, SWF, TAR, TGZ, XLA, XLAM, XLL, XLW, XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, ZIP.

5.2.15.7.29 Implementar sincronização de hora através de protocolo NTP.

5.2.15.7.30 A solução, deve emular e eliminar malwares contidos em anexos de e-mail e documentos baixados da web.

5.2.15.7.31 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções e gráfico da taxa de transferência de tráfego monitorado.

5.2.15.7.32 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro.

5.2.15.7.33 A solução deve permitir visualizar a quantidade de arquivos emulados pela solução.

5.2.15.7.34 A solução deve permitir a visualização da fila de arquivos que serão emulados.

5.2.15.7.35 O relatório das emulações deve conter todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos.

5.2.15.7.36 A solução de sandboxing deve possuir mecanismo independente onde sua ação não depende de engines externas como antivírus, anti-malware.

5.2.15.7.37 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados.

5.2.15.7.38 O sistema de emulação deve exibir percentual de arquivos escaneados.

5.2.15.7.39 A solução deve permitir a criação de White list baseado em hash de arquivo.

5.2.15.7.40 A solução deve possuir serviço web online para categorização atualizada de sites e para definições de Widget atualizadas. As respostas recebidas pelo gateway de segurança são armazenadas localmente para otimizar o desempenho. Quando um acesso não puder ser categorizado com os dados armazenados localmente, a solução deve possuir funcionalidade que bloqueia ou permite o tráfego até que a mesma seja classificada.

5.2.15.8 NEXT GENERATION FIREWALL

5.2.15.8.1 Deverá possuir certificação ICSA para Firewall.

5.2.15.8.2 Deve permitir controle de acesso à internet por períodos do dia, mês e ano, permitindo a aplicação de políticas por horários e por dia da semana.

5.2.15.8.3 Deve permitir realizar checagem de regras para conformidade e sombreamento de regras prioritárias top-down.

5.2.15.8.4 Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado.

5.2.15.8.5 O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance.

5.2.15.8.6 Deve suportar atuação como cliente NTP (Network Time Protocol) versões 1, 2, 3 e 4.

5.2.15.8.7 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.

5.2.15.8.8 Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-interfaces lógicas associadas a VLANs.

5.2.15.8.9 A comunicação entre a solução de gerência e os appliances de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada;

5.2.15.8.10 Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos.

5.2.15.8.11 A solução deve permitir que em caso de falha de comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do appliance de segurança.

5.2.15.8.12 Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas e degradação.

5.2.15.8.13 Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário.

5.2.15.8.14 Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP.

5.2.15.8.15 A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: TACACS, RADIUS e certificados digitais.

5.2.15.8.16 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora.

5.2.15.8.17 Em caso de falhas nas rotas primárias deve desviar dinamicamente o

tráfego para um link secundário, roteamento com base em prioridades.

5.2.15.8.18 Deve implementar roteamento multicast (PIM-SM e PIM-DM).

5.2.15.8.19 Possuir funcionalidade de DHCP Relay e DHCP Server.

5.2.15.8.20 Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras.

5.2.15.8.21 Possuir base de regras singular sem separação de regras orientadas à versão de endereço IP utilizada.

5.2.15.8.22 Implementar sub-interfaces ethernet lógicas.

5.2.15.8.23 Deve suportar os seguintes tipos de NAT:

5.2.15.8.23.1 Dinâmico Many-to-1.

5.2.15.8.23.2 Dinâmico Many-to-Many.

5.2.15.8.23.3 Estático 1-to-1.

5.2.15.8.23.4 Estático Many-to-Many.

5.2.15.8.23.5 Estático bidirecional 1-to-1.

5.2.15.8.23.6 NAT de Origem.

5.2.15.8.23.7 NAT de Destino.

5.2.15.8.24 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

5.2.15.8.25 Deve implementar roteamento estático IPv4 e IPV6.

5.2.15.8.26 Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4.

5.2.15.8.27 Deve implementar roteamento dinâmico (OSPFv3) para IPv6.

5.2.15.8.28 Deve suportar aplicações multimídia como H.323 e SIP.

5.2.15.8.29 Deve permitir o funcionamento em modo transparente tipo “bridge”.

5.2.15.8.30 Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing).

5.2.15.8.31 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

5.2.15.8.32 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.

5.2.15.8.33 Deve ter a capacidade de inspecionar e bloquear tráfego operando nos modos de camada 2 (L2) e de camada 3 (L3).

5.2.15.8.34 Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações.

5.2.15.8.35 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações.

5.2.15.8.36 Promover a integração com LDAP e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações.

5.2.15.8.37 Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS.

5.2.15.8.38 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.

5.2.15.8.39 A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports".

5.2.15.8.40 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria.

5.2.15.8.41 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora.

5.2.15.8.42 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando alterações simultaneamente.

5.2.15.8.43 Habilidade de realizar upgrade via SCP ou https via interface WEB.

5.2.15.8.44 A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços.

5.2.15.8.45 A solução deverá possuir uma ferramenta onde o fabricante disponibilize

HotFixes de segurança e upgrades de versão para instalação simples e com downtime apenas no curto espaço de tempo de reinicialização.

5.2.15.8.46 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.8.47 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.8.48 Deverá suportar controle de política de firewall:

5.2.15.8.48.1 Por zona de segurança.

5.2.15.8.48.2 Por porta e protocolo.

5.2.15.8.48.3 Por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

5.2.15.8.48.4 Por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.2.15.8.49 Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo, em modo transparente, tanto em Layer 2, como em Layer 3.

5.2.15.8.50 O serviço de alta disponibilidade (HA) deve sincronizar todas as sessões, certificados de-criptografados, todas as Associações de Segurança das VPNs e todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS.

5.2.15.8.51 Deve possuir monitoração de falha de link.

5.2.15.8.52 A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces.

5.2.15.8.53 Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante.

5.2.15.8.54 Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). O fluxo mínimo de análise de regras legadas devem trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

5.2.15.8.55 Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.

5.2.15.8.56 Deve permitir a importação , criação e edição de regras SNORT.

5.2.15.9 GERÊNCIA

5.2.15.9.1 Deve possuir solução de gerenciamento e administração centralizado possibilitando o gerenciamento de diversos equipamentos de proteção de rede.

5.2.15.9.2 Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado para suportar, no mínimo, 25 Gbps de log por dia.

5.2.15.9.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

5.2.15.9.4 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

5.2.15.9.5 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

5.2.15.9.6 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS).

5.2.15.9.7 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

5.2.15.9.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

5.2.15.9.9 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração.

5.2.15.9.10 Suportar backup das configurações e rollback de configuração para a última configuração salva.

5.2.15.9.11 Suportar validação de regras antes de serem aplicadas.

5.2.15.9.12 Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing).

5.2.15.9.13 Deve permitir a visualização dos logs de uma regra específica em tempo real.

5.2.15.9.14 Deve possibilitar a integração com outras soluções de Gerencamento e Correlação de Eventos de Segurança (SIEM) de mercado desde que não sejam software livre.

5.2.15.9.15 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

5.2.15.9.16 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti- Malware) e similares.

5.2.15.9.17 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.

5.2.15.9.18 Deve ser possível exportar os logs em CSV.

5.2.15.9.19 Deve possibilitar a geração de relatórios de eventos no formato PDF.

5.2.15.9.20 Deve possibilitar rotação do log.

5.2.15.9.21 Deve suportar geração de relatórios com resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego.

5.2.15.9.22 Deve permitir a criação de relatórios personalizados.

5.2.15.9.23 Suportar enviar os relatórios de forma automática via arquivo em formato PDF.

5.2.15.9.24 A solução de gerência centralizada poderá ser entregue como *appliance* virtual, devendo ser compatível/homologado para o Acropolis Hypervisor Virtualization and Software - Nutanix. Caso não haja compatibilidade/homologação a CONTRATADA deverá entregar uma infraestrutura de virtualização adequada ou entregar este item da solução na forma de *appliance* físico.

5.2.15.9.25 Deve consolidar logs e relatórios de todos os dispositivos administrados.

5.2.15.9.26 Deve possuir capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

5.2.15.9.27 Deverá possuir mecanismo de detalhamento (Drill-Down) para navegação e análise dos logs em tempo real.

5.2.15.9.28 Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso.

5.2.15.9.29 Permitir a customização do padrão regulatório da própria instituição.

5.2.15.9.30 Permitir notificação instantânea ou emissão de relatório sobre mudanças de política de segurança que impactam negativamente a segurança.

5.2.15.9.31 Monitorar constantemente ou realizar emissão de relatório sobre o status de conformidade da solução aos padrões regulatórios informados.

5.2.15.9.32 Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade estabelecidas pelo CONTRATANTE ou de acordo com o padrão estabelecido pelo fabricante.

5.2.15.9.33 Gerar alertas ou emitir relatório de conformidade sobre o impacto de suas decisões na política de segurança trazendo as considerações regulatórias na gestão de segurança estabelecidas pelo CONTRATANTE ou de acordo com o padrão pré-determinado pelo fabricante.

5.2.15.9.34 Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.

5.2.15.9.35 Possuir alertas ou emitir relatório de políticas e as potenciais violações de conformidade.

5.2.15.9.36 Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.

5.2.15.9.37 Gerar relatórios diários com base nas configurações de segurança em tempo real.

5.2.15.9.38 Permitir que os relatórios possam ser salvos, enviados e impressos.

5.2.15.9.39 Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados.

5.2.15.9.40 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

5.2.15.9.41 Deverá possuir, no mínimo, disco de armazenamento de 500GB HDD e/ou 240GB SSD, ambos em RAID 1.

5.2.15.9.42 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

5.2.15.9.42.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação com principais eventos de segurança de acordo com a funcionalidade selecionada.

5.2.15.9.42.2 A solução deve possuir mecanismo para detectar login de administradores em horários irregulares.

5.2.15.9.42.3 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais.

5.2.15.9.42.4 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.

5.2.15.9.42.5 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius.

5.2.15.9.42.6 Permitir criações de políticas de acesso de usuários autenticada no Active Directory, que reconheçam os usuários de forma transparente.

5.2.15.9.42.7 Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados à solução.

5.2.15.9.42.8 Permitir a visualização de gráficos e mapa de ameaças.

5.2.15.9.42.9 Possuir mecanismo para que logs antigos sejam removidos automaticamente.

5.2.15.9.42.10 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.

5.2.15.9.42.11 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.

5.2.15.9.42.12 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real.

5.2.15.9.42.13 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria.

5.2.15.9.42.14 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

5.2.15.9.42.15 Caso necessite de licenciamento, a solução deverá vir totalmente licenciada para o nível mais alto de uso.

5.2.15.10 CAPACIDADES

5.2.15.10.1 Os valores mínimos e máximos a seguir servirão como margem para a CONTRATADA ofertar equipamentos que tenham capacidade compatível com os requisitos do CONTRATANTE durante o período de vigência do contrato.

5.2.15.10.2 A solução deve ser fornecida com kit para instalação em rack de 19”.

5.2.15.10.3 Os equipamentos ofertados na solução deverão ser capazes de operar com todos os recursos habilitados, mantendo os níveis de operação descritos na seção 5.9 - ACORDO DE NÍVEL DE SERVIÇO (SLA), deste Termo de Referência.

5.2.15.10.4 A CONTRATADA deverá fornecer todos os transceivers de 10G SFP+ tanto para a solução de firewall, como para os switchs do CONTRATANTE, bem como os cordões de fibra óptica. Ou seja, todas as portas de comunicação, interfaces e afins, deverão estar habilitadas e operacionais, sem custos adicionais.

5.2.15.10.5 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2.15.10.6 Cada conjunto da solução poderá ser entregue contemplando as capacidades mínimas da “Tabela de Capacidades” a seguir, podendo ser expandida

durante toda a vigência do contrato até os limites máximos especificados.

Tabela de Capacidades

	DESCRIÇÃO DO REQUISITO	MÍNIMO	MÁXIMO
5.2.15.10.7	Interface 10/100/1000 Mbit Ethernet	08	16
5.2.15.10.8	Interface 10Gbase-F SFP+	02	04
5.2.15.10.9	Interface de gerenciamento dedicada	01	01
5.2.15.10.10	Interface 10/100/1000 Mbit Ethernet BaseT dedicada para alta disponibilidade	01	01
5.2.15.10.11	Interface Console Serial	01	01
5.2.15.10.12	Fonte de alimentação redundante bivolt 100-240 VAC Hot-Swappable	02	02
5.2.15.10.13	Disco de armazenamento de 500GB HDD e/ou 240GB SSD RAID 1	01	02
5.2.15.10.14	Firewalls virtuais	10	20
5.2.15.10.15	Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps)	05	10
5.2.15.10.16	Throughput de AES-128 VPN (em Gbps)	04	08
5.2.15.10.17	Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps)	2,5	05
5.2.15.10.18	Conexões simultâneas (em milhões)	02	04
5.2.15.10.19	Novas conexões por segundo	100	180
5.2.15.10.20	Usuários conectados através de VPN SSL simultaneamente	200	400

* Baseado em amostras reais, ou seja, não serão aceitos testes usando UDP, HTTP 1M ou testes em laboratório.

5.3 ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO

5.3.1 Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

5.3.2 Deverá ser baseado em Dashboard, para fácil visualização.

5.3.3 Deve ser entregue com regras genéricas criadas pela CONTRATADA, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

5.3.4 O serviço da CONTRATADA deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo CONTRATANTE.

5.3.5 Deve possuir acesso WEB (HTTPS).

5.3.6 Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

5.3.7 Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

5.4 ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

5.4.1 O CONTRATANTE possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.2 O CONTRATANTE possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links “full-route” BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.3 A CONTRATADA deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

5.4.4 O CONTRATANTE possui infraestrutura hiper convergente, e para tanto usa o Acropolis

Hypervisor Virtualization and Software - Nutanix. Assim, caso a CONTRATADA necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do CONTRATANTE.

5.4.5 A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

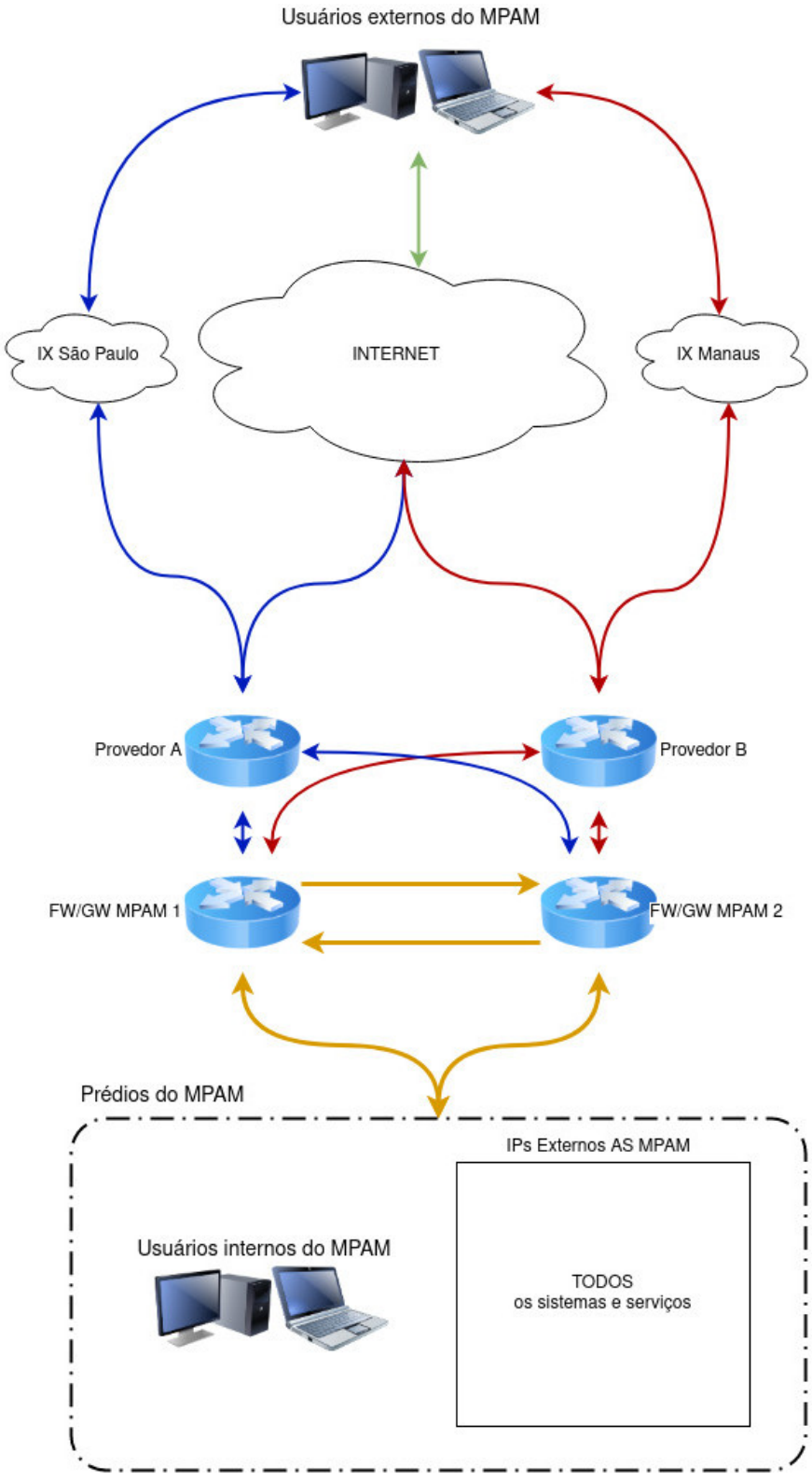
5.4.6 A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

5.4.7 A CONTRATADA deverá evitar, durante o processo de migração, interromper os serviços de rede do CONTRATANTE, nos horários das 8hs às 18hs, em dias de expediente do CONTRATANTE.

5.4.8 É de responsabilidade da CONTRATADA a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do CONTRATANTE fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

5.4.9 A CONTRATADA deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CONTRATANTE, sendo vedada sua cessão, locação ou venda a terceiros.

5.4.10 A topologia da solução deve seguir conforme imagem a seguir:



5.5 ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO

5.5.1 A CONTRATADA deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.5.2 A carga horária total para o treinamento deve ser de, no mínimo, 40 horas.

5.5.3 A CONTRATADA deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela FISCALIZAÇÂO.

5.5.4 O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como

atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fonecido em português do Brasil ou inglês.

5.5.5 O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do CONTRATANTE.

5.5.6 O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a CONTRATADA deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o CONTRATANTE. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.5.7 A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.5.8 A CONTRATADA deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.5.9 Caso o treinamento seja ofertado de forma presencial, o CONTRATANTE irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do CONTRATANTE.

5.5.10 O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a CONTRATADA deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do CONTRATANTE.

5.5.11 Será de responsabilidade da CONTRATADA prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.5.12 A CONTRATADA deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.5.13 Os instrutores designados pela CONTRATADA deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.5.14 A CONTRATADA deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.5.15 A CONTRATADA deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do CONTRATANTE e com finalidade de uso exclusivamente interno do CONTRATANTE, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela CONTRATADA.

5.6 SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS

5.6.1 A CONTRATADA deverá disponibilizar ao CONTRATANTE um número telefônico único,

um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entende-se por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS.

5.6.2 No atendimento por meio de telefone a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

5.6.3 O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

5.6.4 Cada chamado deverá conter, no mínimo, as seguintes informações:

5.6.4.1 Número único do registro/ocorrência - a ser fornecido pela CONTRATADA.

5.6.4.2 Identificação do atendente.

5.6.4.3 Identificação do solicitante.

5.6.4.4 Data e hora de abertura do chamado/início da interrupção.

5.6.4.5 Descrição da ocorrência.

5.6.4.6 Designação do equipamento, quando for o caso.

5.6.4.7 Ações corretivas tomadas.

5.6.4.8 Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

5.6.5 O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

5.6.6 O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA.

5.6.7 Não deverá haver qualquer limitação para o número de solicitações de reparo.

5.6.8 O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a CONTRATADA deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

5.7 GARANTIA TÉCNICA

5.7.1 A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

5.7.2 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.

5.7.3 Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.

5.7.4 A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao CONTRATANTE.

5.7.5 Caso sejam detectadas falhas ou bugs nos produtos, a CONTRATADA deverá realizar as atualizações necessárias à correção do problema.

5.7.6 A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

5.7.7 A CONTRATADA é a única responsável pelos produtos fornecidos ao CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

5.7.8 A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo CONTRATANTE, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

5.7.9 Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à CONTRATADA apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.

5.7.10 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser

utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

5.7.11 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o CONTRATANTE.

5.7.12 No que se refere a software, durante a vigência do Contrato, a CONTRATADA deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o CONTRATANTE. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

5.7.12.1 Patches, fixes, correções, updates e service packs.

5.7.12.2 Novas releases, builds e funcionalidades.

5.7.12.3 O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.

5.7.12.4 O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.

5.7.12.5 Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.

5.7.12.6 A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

5.7.12.7 A CONTRATADA deverá fornecer tais atualizações independentemente de solicitação expressa do CONTRATANTE.

5.7.12.8 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

5.7.12.9 As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA

5.8.1 Os serviços de manutenção *on-site*, serão prestados nas dependências do CONTRATANTE na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

5.8.2 O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do CONTRATANTE, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

5.8.3 A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

5.8.4 A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

5.8.5 Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

5.8.6 A CONTRATADA deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo CONTRATANTE ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser realizada nas dependências do CONTRATANTE, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

5.8.7 O CONTRATANTE poderá determinar à CONTRATADA a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da CONTRATADA.

5.8.8 Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional ao CONTRATANTE.

5.8.9 A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do CONTRATANTE.

5.8.10 O serviço de suporte deverá ser efetuado *on-site* sempre que se fizer necessário ou quando for solicitado pelo CONTRATANTE, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o CONTRATANTE.

5.8.11 Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do CONTRATANTE, a CONTRATADA deverá desinstalar, embalar e transportar o item defeituoso, instalar item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

5.8.12 Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar o CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

5.8.13 A CONTRATADA encaminhará mensagem de e-mail para o CONTRATANTE, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

5.8.14 Todos os custos diretos e indiretos para realização do atendimento presencial (*on-site*) serão de responsabilidade exclusiva da CONTRATADA.

5.8.15 Dentro do mesmo endereço, a ser executada pela CONTRATADA, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o CONTRATANTE.

5.8.16 Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

5.8.17 O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do CONTRATANTE, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

5.8.18 Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

5.9 ACORDO DE NÍVEL DE SERVIÇO (SLA)

5.9.1 Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos nesse Termo de Referência.

5.9.2 A CONTRATADA deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

5.9.3 A CONTRATADA deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

5.9.4 A realização de assistência técnica preventiva, caso não seja solicitada pelo CONTRATANTE, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do CONTRATANTE.

5.9.5 Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.6 Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.7 Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do CONTRATANTE, a solução será considerada como operando em Modo de Contingência.

5.9.8 Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

5.9.9 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais

recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual, este checkup faz parte da manutenção preventiva.

5.9.10 Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.

5.9.11 O Modo de Contingência se caracterizará por:

5.9.11.1 Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.

5.9.11.2 Funcionamento acima dos limiares de desempenho, conforme estabelecido nas cláusulas 5.9.5 e 5.9.6 acima.

5.9.11.3 Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante ou fora de garantia.

5.9.11.4 Operação com funcionalidades ou performance abaixo dos mínimos exigidos neste Termo.

5.9.12 Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.

5.9.13 O estado de Inoperância Total se caracterizará por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do CONTRATANTE.

5.9.14 O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela CONTRATADA.

6. VISTORIA TÉCNICA

6.1 As empresas licitantes PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades do CONTRATANTE, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

6.2 Nos casos em que houver vistoria, os locais envolvidos pelos trabalhos deverão ser cuidadosamente inspecionados pelos licitantes, observando, entre outros aspectos, o grau de dificuldade para a consecução dos serviços e procederão à rigorosa conferência das medidas e de outros aspectos julgados de interesse.

6.3 A vistoria deverá ser realizada, preferencialmente, por profissional(is) qualificado(s) e detentor(es) de conhecimento técnico relacionado ao objeto, devidamente credenciados.

6.4 Para que as pretensas licitantes possam participar da vistoria, será necessária que a mesma credencie um representante, através da apresentação, no ato da visita, de documento devidamente assinado, indicando o nome de seu colaborador, número da cédula de identidade e CPF e delegação de poderes para representá-la na visita. A falta deste documento impossibilitará que o representante e a empresa participem da vistoria.

6.5 Para a realização da vistoria, as empresas interessadas deverão apresentar duas cópias da Declaração de Vistoria, já preenchida com os dados da empresa e assinada pelo representante, sendo que uma cópia será assinada por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO do CONTRATANTE, e devolvida para empresa, e a outra será juntada ao processo de contratação, onde a empresa declara ter realizado a vistoria técnica.

6.6 A referida Declaração deverá ser apresentada posteriormente, na fase licitatória, nos termos definidos no edital do certame.

6.7 Caso opte por não realizar a vistoria, a licitante apresentará na fase licitatória, declaração de opção pela dispensa de vistoria.

6.8 Não serão admitidas quaisquer alegações de desconhecimento ou erro orçamentário por parte da futura contratada, quando do cumprimento as obrigações.

6.9 A licitante poderá vistoriar o local onde serão executados os serviços até o último dia útil anterior à data fixada para a abertura da sessão pública.

6.10 As visitas deverão ser previamente agendadas, com pelo menos 5 (cinco) dias úteis de antecedência, pelo telefone (92) 3655-0660/3655-0666 — DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período de segunda a sexta-feira, das 8 às 14hs, excluídos feriados e pontos facultativos.

6.11 A vistoria será realizada no endereço do Edifício-Sede do MPAM, Avenida Coronel Teixeira, 7.995, bairro Nova Esperança, CEP 69037-473, Manaus/AM.

6.12 Todos os custos associados com a visita e a inspeção serão de inteira responsabilidade da licitante.

7. PRAZOS PARA A PRESTAÇÃO DO SERVIÇO

7.1 A CONTRATADA deverá em, no máximo, 65 (sessenta e cinco) dias corridos, contados a partir da assinatura do contrato, finalizar a implantação, ativação e entrega dos sistemas e equipamentos que compõem os itens 01, 02 e 03, especificados neste Termo de Referência.

7.2 A CONTRATADA deverá em comum acordo com o CONTRATANTE, no prazo máximo de 120 (cento e vinte) dias corridos, contados a partir da assinatura do contrato, finalizar o treinamento indicado no item 04 deste Termo de Referência.

7.3 Antes de findar os prazos fixados nos itens anteriores, a CONTRATADA poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pelo CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, 410 da lei n. 8.666/93.

7.4 O prazo da prestação dos serviços objeto deste Termo de Referência deverá contar da assinatura do contrato, prorrogáveis de comum acordo, até o limite estabelecido na Lei n. 8.666/93, e suas alterações.

8. RECEBIMENTO

8.1 O recebimento será feito nas seguintes etapas:

8.1.1 Será emitido Termo Individual de ACEITE para cada item do Lote.

8.1.2 Será emitido Termo de Recebimento Definitivo para todo o Lote.

8.2 O recebimento dos serviços será realizado pela FISCALIZAÇÃO do CONTRATANTE.

8.3 Para fins de aceite a CONTRATADA deverá comunicar formalmente a efetiva disponibilização dos serviços para cada item do Lote.

8.4 Para a emissão do Termo Individual de ACEITE para o Item 01:

8.4.1 Será emitido após Período de Funcionamento Experimental de até 15 (quinze) dias, que se iniciará após comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.4.2 Durante Período de Funcionamento Experimental a FISCALIZAÇÃO deverá concluir os testes necessários para constatar o funcionamento regular dos serviços disponibilizados.

8.4.3 A FISCALIZAÇÃO realizará avaliação qualitativa das especificações dos equipamentos e funcionalidades que compõem a solução conforme exigências deste Termo.

8.5 Para a emissão do Termo Individual de ACEITE para o Item 02:

8.5.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.5.2 A FISCALIZAÇÃO realizará testes com as credenciais fornecidas, teste de uso da ferramenta e teste de disponibilidade necessários para constatar o funcionamento regular dos serviços disponibilizados.

8.6 Para a emissão do Termo Individual de ACEITE para o Item 03:

8.6.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito, por parte da CONTRATADA, incluindo evidencias que demonstrem inequivocadamente que todas os critérios estabelecidos na seção 5.4 deste Termo foram atendidos, atestando a efetiva disponibilização dos serviços.

8.6.2 A FISCALIZAÇÃO realizará avaliação qualitativa das evidências apresentadas considerando a disponibilidade dos serviços do CONTRATANTE.

8.7 Para a emissão do Termo Individual de ACEITE para o Item 04:

8.7.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.7.2 A FISCALIZAÇÃO observará os critérios estabelecidos neção 5.5 deste Termo.

8.8 Somente depois de realizados e aprovados os testes definidos, o CONTRATANTE, por meio da FISCALIZAÇÃO, emitirá o Termo de Aceite, atestando a conformidade com as especificações neste Termo de Referência, liberando o início de faturamento.

8.9 A contagem do prazo para a efetiva entrega e prestação de cada item de serviço especificado no lote será suspenso quando a CONTRATADA comunicar a efetiva disponibilização do serviço, e, se for o caso, será retomado no dia seguinte a partir da emissão de comunicado por escrito do CONTRATANTE indicando NÃO ACEITE do serviço em virtude de não conformidade com algum dos requisitos presentes nesse termo de referência.

9. PAGAMENTO

9.1 Para os Itens 01 e 02:

9.1.1 Mensalmente, a CONTRATADA deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por

Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

9.1.2 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada dia de funcionamento da solução em Modo de Contingênica além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

9.1.3 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada hora de funcionamento da solução em estado de Inoperância Total além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

9.1.4 A data de início de cobrança dos serviços deverá observar a data de emissão do Termo de Aceite, sendo que a primeira fatura corresponderá à prestação de serviços desde a data de emissão do Termo de Aceite, para cada item do Lote, até o último dia do respectivo mês, de forma pro rata.

9.1.5 As demais faturas deverão abranger o período do primeiro ao último dia do mês.

9.1.6 Os valores a serem faturados concernentes aos serviços objeto desta contratação estarão sujeitos a descontos nas situações de descumprimento das metas estabelecidas para os indicadores elencados na especificação do serviço, item Acordo de Nível de Serviço (SLA).

9.1.7 Os descontos aplicados nas faturas mensais não isentam a CONTRATADA de quaisquer sanções legais ou das sanções dispostas na seção 12 - SANÇÕES ADMINISTRATIVAS.

9.1.8 Os descontos aplicados nas faturas mensais, conforme dispostos acima, oriundos do descumprimento dos níveis mínimos de serviço estipulados no item Acordo de Nível de Serviço (SLA), não se configuram como penalidades ou multas.

9.1.9 No primeiro dia útil do mês subsequente, antes da emissão na nota fiscal, a CONTRATADA deverá enviar à FISCALIZAÇÃO relatório referente aos períodos, destacando eventuais descontos e as causas da(s) indisponibilidade(s) ocorridas na prestação dos serviços para a devida aprovação.

9.1.10 As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da CONTRATADA no que diz respeito ao atendimento dos níveis de serviços especificados no acordo de nível de serviço, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

9.2 Para os Itens 03 e 04:

9.2.1 A CONTRATADA deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

9.2.2 Os pagamentos relativos aos Itens serão realizados de uma única vez, no mês seguinte a emissão do Termo de Aceite.

9.3 Ao CONTRATANTE fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas neste Termo de Referência.

10. OBRIGAÇÕES DA CONTRATADA

10.1 Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo, observando as prescrições e as recomendações do fabricante/fornecedor, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

10.2 Comunicar imediatamente ao CONTRATANTE, por escrito, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto desta contratação, e prestar os esclarecimentos julgados necessários.

10.3 Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que o CONTRATANTE julgar necessário.

10.4 Manter contato e realizar o planejamento dos serviços com o CONTRATANTE de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

10.5 Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, o objeto deste Termo de Referência que não atenda às especificações exigidas, em que se verifiquem imperfeições, vícios, defeitos ou incorreções ou rejeitados pela fiscalização.

10.6 Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pelo CONTRATANTE em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste Termo de Referência.

10.7 Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.

10.8 Acatar as observações feitas pelo Fiscal do CONTRATANTE quanto à execução dos serviços.

10.9 Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

10.10 A inobservância das especificações constantes deste Termo de Referência implicará a não aceitação parcial ou total dos serviços, devendo a CONTRATADA refazer as partes recusadas sem direito a indenização.

10.11 Seguir as orientações da Lei n. 9.472/97, do Termo de Concessão ou autorização emitido pela ANATEL, e demais disposições regulamentares pertinentes aos serviços a serem prestados.

10.12 Todos os equipamentos fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área, tais como: ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações).

10.13 Credenciar junto ao CONTRATANTE um representante, denominado preposto, aceito pelo CONTRATANTE, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, indicando as formas de contato no mínimo telefone, para comunicação rápida e email para comunicação formal;

10.14 Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação.

10.15 Implantar a supervisão permanente dos serviços, de modo adequado e de forma a obter uma operação correta e eficaz.

10.16 A CONTRATADA se responsabilizará por todos os serviços não explícitos nestas especificações, mas necessários à execução dos serviços programados e ao perfeito funcionamento das instalações.

10.17 Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.

10.18 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

10.19 Acatar que o CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

10.20 São expressamente vedadas à CONTRATADA:

10.20.1 A veiculação de publicidade acerca do CONTRATANTE, salvo prévia e expressa autorização deste;

10.20.2 A subcontratação total/parcial é permitida apenas para o Item 04 mantendo os critérios estabelecidos na seção 5.5 deste Termo.

11. OBRIGAÇÕES DO CONTRATANTE

11.1 Fornecer à CONTRATADA as informações necessárias à fiel execução do objeto deste Termo de Referência.

11.2 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA durante o prazo de vigência deste Contrato.

11.3 Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n. 8.666/93, o exato cumprimento das obrigações previstas neste Termo.

11.4 Designar, e informar à CONTRATADA, fiscal do contrato e seu substituto, mantendo tais dados atualizados.

11.5 Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos materiais, de forma a assegurar o perfeito cumprimento do contrato.

11.6 Anotar em registro próprio e notificar a CONTRATADA, por escrito, a ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.

11.7 Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este Termo de Referência.

11.8 Fazer uso adequado dos equipamentos fornecidos pela CONTRATADA, seguindo as instruções constantes de seus manuais de uso.

11.9 Efetuar o pagamento devido pelos serviços prestados, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas.

12. SANÇÕES ADMINISTRATIVAS

12.1 Se a CONTRATADA, sem justa causa e/ou sem justificativa apresentada e aceita pelo CONTRATANTE, não cumprir as obrigações descritas neste Termo ou infringir preceitos legais, serão aplicadas, segundo a gravidade da falta, as seguintes penalidades:

12.1.1 Advertência por escrito - Será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem corno, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do MPAM.

12.1.2 Multa de 2% (dois por cento) sobre o valor global contratado, a cada reincidência na penalidade de advertência. Na hipótese de reincidência por 5 (cinco) vezes na penalidade de advertência, será considerado descumprimento total da obrigação, punível com as sanções previstas em lei.

12.1.3 Multa de 2% (dois por cento) sobre o valor global contratado, por dia de atraso, no caso de descumprimento do tempo máximo, conforme seção 7 - PRAZOS PARA A PRESTAÇÃO DO SERVIÇOS, limitado a 10 (dez) dias. O atraso superior a 10 (dez) dias será considerado como descumprimento total da obrigação, punível com as sanções previstas em lei.

12.1.4 Multa de 10% (dez por cento) sobre o valor global contratado, no caso de, sem justificativa aceita pelo CONTRATANTE, o vencedor não retirar a Nota de Empenho, a Autorização de Fornecimento de Materiais/Serviço ou não assinar o contrato deixando, assim, de cumprir os prazos fixados, sem prejuízo das demais sanções previstas.

12.1.5 Multa de até 20% (vinte por cento) sobre o valor global contratado, nos casos de INEXECUÇÃO PARCIAL do objeto contratado.

12.1.6 Multa de até 30% (trinta por cento) sobre o valor global contratado, nos casos de INEXECUÇÃO TOTAL do objeto contratado.

12.1.7 Multa de até 30% (trinta por cento) sobre o valor global contratado, na hipótese de rescisão do contrato por culpa da CONTRATADA.

13. ELABORAÇÃO

13.1 O presente Termo de Referência foi elaborado pela DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO, em conformidade com as atribuições legais e regimentais, estando em consonância com as disposições legais e normativas aplicáveis, com a necessidade, interesse e conveniência da Administração, sendo parte integrante do procedimento interno respectivo.

14. DECLARAÇÃO DO SOLICITANTE

14.1 Declaro que este Termo de Referência está de acordo com a Lei n. 8.666/93 e Lei n. 10.520/2002 e alterações.

THEO FERREIRA PARÁ
Agente de apoio - Manutenção/Informática

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

15. APROVAÇÃO

TADEU AZEVEDO DE MEDEIROS
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Theo Ferreira Pará**, **Agente de Apoio - Manutenção - Suporte Informática**, em 23/09/2021, às 17:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 24/09/2021, às 09:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Tadeu Azevedo de Medeiros**, **Diretor(a) de**

Tecnologia de Informação e Comunicação - DTIC, em 24/09/2021, às 16:14, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0691989** e o código CRC **CCAAFDF4**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 108.2021.DTIC.0692180.2021.015252

A Sua Excelência o Senhor

Doutor **GEBER MAFRA ROCHA**

Subprocurador-Geral de Justiça para Assuntos Administrativos

NESTE PRÉDIO

Assunto: Apresentar termo de referência para 013.2021.DTIC, que trata da contratação de serviço de solução de firewall, treinamento e migração da plataforma atual.

Senhor Subprocurador,

Honrado em cumprimentar Vossa Excelência, oportunidade em que **submeto** à aprovação, o Termo de Referência n.º 013.2021.DTIC, que trata da contratação de serviço de solução de firewall pelo período de **48 (quarenta e oito) meses**, incluindo treinamento e migração da plataforma atual, conforme especificações, quantitativos e prazos contidos no documento.

A contratatação se fundamenta nos seguintes pressupostos:

1. A Segurança da Informação é o processo que define os artefatos e políticas necessários para a proteção e manutenção da disponibilidade, integridade, confidencialidade e autenticidade de estações, servidores, usuários e informações corporativas. Atualmente, este processo, em nenhuma cirscunstância, pode ser composto apenas de um software antivírus instalado nas estações de trabalho e um firewall simples de bloqueio de portas. As ameaças, que podem ser internas ou externas, seguem aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas, com múltiplas camadas de proteção, de forma a reduzir os riscos, minimizando a probabilidade e os impactos de um eventual ataque cibernético.

2. Dessa forma, o MPAM necessita manter permanentemente, sob pena de interrupção de suas atividades e prejuízos irreparáveis, uma solução corporativa de Segurança da Informação avançada e à altura dos desafios impostos pelas ameaças virtuais. A solução precisa permitir a identificação das tentativas de invasão aos sistemas informatizados do MPAM, impedir e mitigar as vulnerabilidades existentes, além de intervir tempestivamente quando necessário, protegendo a Instituição da maior gama de ataques virtuais internos e externos existentes. Um item crucial e imprescindível em qualquer solução de Segurança da Informação é conhecido como firewall de próxima geração (NGFW).

3. O MPAM dispõe atualmente de equipamento do tipo NGFW em operação, da marca Palo Alto. Entretanto, trata-se de um único equipamento, sem qualquer tipo de

redundância para caso de falhas, que já está obsoleto quanto ao hardware e ao software, ou seja, já foi descontinuado pelo fabricante, não dispondo das tecnologias de segurança mais atuais e avançadas. Além disto, com o crescimento do MPAM e da necessidade de conexões cada vez mais rápidas, a performance do equipamento está muito aquém do necessário, impondo diminuição da eficiência das atividades da instituição. Por fim, as licenças de atualização das definições de detecção de ameaças e de suporte técnico expiram no mês de agosto do corrente ano. A expiração das licenças não impede totalmente o funcionamento do equipamento, mas diminui sua eficácia conforme o tempo passa e novas ameaças surgem, sem que seja possível atualizar o equipamento com as respectivas definições de detecção e bloqueio. Fica inequivocadamente estabelecido que a substituição deste equipamento por sistema superior é urgente.

4. O sistema em questão, além das funcionalidades direta e especificamente relacionadas a segurança da informação, provê diversas outras funcionalidades necessárias ao funcionamento do MPAM, como o uso de VPN, por exemplo, sendo indispensável ao funcionamento do órgão como um todo. É ele que permite a conexão segura, fidedigna e unificada de todas as localidades de funcionamento do MPAM, em todo o estado do Amazonas, que inclui mais de 10 unidades descentralizadas na capital e de 54 comarcas do interior, perrmitindo o uso de todos os recursos informatizados utilizados pelos membros e servidors para consecução de suas atividades com a eficiência exigida para atingir os objetivos de atendimento à sociedade com a qualidade esperada.

5. Devido à criticidade do sistema para o funcionamento do MPAM, foram definidos requisitos necessários para nortear a analise e escolha da solução para substituir o equipamento atual de forma a eliminar os problemas existentes e garantir a continuidade do negócio, com o menor risco possível e o melhor custo-benefício disponível. Os requisitos determinados como imprescindíveis foram: redundância, performance à altura do crescimento do MPAM e disponibilidade recursos de segurança com tecnologia de última geração.

6. Após analise das opções existentes, foi descartada a simples renovação das licenças do equipamento atual, pois esta não atenderia aos requisitos necessários para manter o funcionamento contínuo do MPAM. Restaram como opções de mercado uma aquisição simples de novos equipamentos ou a contratação dos equipamentos necessários na forma de serviço.

7. Em pesquisa de mercado, incluindo informações cedidas por fornecedores quanto a contratações realizadas por outros órgãos públicos, conforme pode ser verificado no documento anexo 0699491, ficou demonstrado que a melhor maneira para solução da situação é o provimento dos equipamentos necessários, incluindo serviços relacionados de gerência, manutenção e monitoramento, através de um contrato de serviço. Em comparação a uma simples aquisição de equipamentos, a opção de contrato de serviço atende de forma superior ao princípio da economicidade, uma vez que atende a todos os requisitos definidos com maior eficiência, não havendo risco de obsolescência de hardware e software, por exemplo, e inclui mais serviços prestados, como gerência e manutenção, por preços similares ou inferiores, dependendo das condições do contrato, em especial do período de duração.

8. Tanto para tornar o certame licitatório mais atrativo, uma vez que possibilita às licitantes vislumbrarem um período mais extenso para amortização dos investimentos relacionados à prestação dos serviços, quanto para garantir valores economicamente vantajosos e maiores estabilidade e previsibilidade à gestão administrativa, além de eliminar custos administrativos e riscos de insucesso necessariamente associados a renovações contratuais, foi definida a vigência inicial do contrato em **48 (quarenta e oito) meses**, uma vez que o objeto do termo de referência encaminhado é constituído de serviços de prestação continuada de aluguel de equipamentos e utilização de programas de informática.

Ante o exposto, solicito vossa aprovação do sobredito termo de referência. Caso seja aprovado, os autos devem ser encaminhados ao **SETOR DE COMPRAS E SERVIÇOS**, para realização da pesquisa de mercado.

Respeitosamente,

TADEU AZEVEDO DE MEDEIROS

Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Tadeu Azevedo de Medeiros**, **Diretor(a) de Tecnologia de Informação e Comunicação - DTIC**, em 24/09/2021, às 16:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0692180** e o código CRC **E6B1D59E**.

2021.015252 v19

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

NOTA DE AUTORIZAÇÃO DE DESPESAS/ADJUDICAÇÃO - NAD Nº 375.2021.DOF - ORÇAMENTO.0744829.2021.015252

1 - INFORMAÇÕES DA NOTA DE AUTORIZAÇÃO DE DESPESAS E ADJUDICAÇÃO

Procedimento Interno: 2021.015252 **Processo de Compra:** 345.2021.SCOMS.0731246.2021.015252 **Interessado:** Tadeu Azevedo de Medeiros - Diretor(a) de Tecnologia de Informação e Comunicação - DTIC	**Modalidade:** Ordinário **Origem:** A LICITAR **Credor:** A LICITAR

2 - DESCRIÇÃO ORÇAMENTÁRIA

Unidade Orçamentária: 03.101 - Procuradoria-Geral de Justiça do Amazonas **Fonte de Recurso:** 0100.000 - Recursos Ordinários **Programa de Trabalho:** 03.122.0001.2001.0001 - Administração da Unidade	**Elemento:** 3390.39 Serviços de Terceiros PJ **Subelemento:** 3390.40.11 - Locacao De Software

3 - CONTROLE ORÇAMENTÁRIO

SALDO ATUAL	DEDUÇÃO PREVISTA	SALDO APÓS DESPESA
R$ 12.842.778,60	R$ 5.828.425,84	R$ 7.014.352,76

4 - ESPECIFICAÇÃO DO OBJETO

Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

ITEM	ESPECIFICAÇÃO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Serviço de Firewall em Alta Disponibilidade	Meses	48	R$ 68.580,67	R$ 3.291.872,16
2	Serviço de Monitoramento da Solução	Meses	48	R$ 50.919,00	R$ 2.444.112,00
3	Serviço de Migração do Ambiente Atual	Unidade	1	R$ 30.553,33	R$ 30.553,33
4	Serviço de Treinamento da Solução	Pessoas	5	R$ 12.377,67	R$ 61.888,35
TOTAL					**R$ 5.828.425,84**

Saldo atual composto pelo valor disponível para o respectivo elemento da despesa, conforme demonstrativo da execução orçamentária obtido no sistema AFI/SEFAZ no dia 07 de Janeiro de 2022 (R$ 12.843.000,00), deduzido o total de Notas de Autorização de Despesas e Adjudicação emitidas ainda não executadas (R$ 221,40). O valor será transferido do elemento 3390.39 por inexistencia de saldo para o elemento indicado.

5 - CRONOGRAMA DE DESEMBOLSO

JANEIRO	FEVEREIRO	MARÇO	ABRIL	MAIO	JUNHO
R$ 5.828.425,84	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
JULHO	**AGOSTO**	**SETEMBRO**	**OUTUBRO**	**NOVEMBRO**	**DEZEMBRO**
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00

6 - DESPACHO DO ORDENADOR DE DESPESAS

( ) Encaminhe-se à Divisão de Contratos e Convênios.
(**X**) Encaminhe-se à Comissão Permanente de Licitação.
( ) Autorizo a despesa. Encaminhe-se à Assessoria Jurídica para manifestação acerca da forma da contratação.
( ) Autorizo a despesa. Adjudico em favor da empresa. Empenhe-se.

Documento assinado eletronicamente por **Francisco Edinaldo Lira de Carvalho**, **Diretor(a) de Orçamento e Finanças - DOF**, em 07/01/2022, às 12:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 10/01/2022, às 11:55, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0744829** e o código CRC **922279AD**.

2021.015252 v4

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 13.2022.CPL.0749455.2021.015252

Ilma. Sra.
CAROLINE ELLEN BEZERRA
Chefe da Divisão de Contratos e Convênios

Senhora Chefe,

Cumprimentando-a com o presente, informamos que tramitou nesta Comissão Permanente de Licitação o **Processo SEI n.º 2021.015252**, cujo objeto é a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.*

Considerando a análise realizada nos autos, especialmente, o **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, parece-nos patente a necessidade de estipulações contratuais aptas a salvaguardar os direitos das partes e consignar suas respectivas obrigações, consoante previsão do artigo 62, §4º, da Lei 8.666/93 abaixo transcrito:

> §4º É dispensável o "termo de contrato" e facultada a substituição prevista neste artigo, a critério da Administração e independentemente de seu valor, nos casos adquiridos, dos quais não resultem obrigações futuras, inclusive assistência técnica.

Nesse sentido, também, é o entendimento do Tribunal de Contas da União:

> A contratação deve ser formalizada obrigatoriamente por meio de termo de contrato sempre que houver obrigações futuras decorrentes do fornecimento de bens e serviços, independentemente da modalidade de licitação sua dispensa ou inexibilidade, conforme preconizado no art. 62, §4º, da Lei n.º 8.666/1993.

Considerando que esta Comissão depende da feitura do instrumento contratual correspondente para a execução das demais providências, **encaminhamos os autos** do Procedimento Interno em epígrafe à **Divisão de Contratos e Convênios – DCCON** para, caso compartilhado o entendimento desta Comissão, por obséquio, seja elaborada a respectiva Minuta do Termo Contratual.

Por derradeiro, **retornem** os autos a esta Comissão para que seja dado prosseguimento regular ao feito.

Atenciosamente,

Manaus, 11 de janeiro de 2022.

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ nº 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 11/01/2022, às 09:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0749455** e o código CRC **A9EB8299**.

MINUTA DE CONTRATO ADMINISTRATIVO Nº 2.2022.DCCON.0750392.2021.015252

* MINUTA DE DOCUMENTO

Termo de Contrato Administrativo que entre si celebram o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e a empresa _____, visando à prestação de serviço de solução de firewall de próxima geração.

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, por intermédio de sua **PROCURADORIA-GERAL DE JUSTIÇA**, órgão de sua Administração Superior, com sede na Avenida Coronel Teixeira, 7.995, Nova Esperança, 69.037-473, Manaus/AM, inscrita no CNPJ (MF) sob o n.º 04.153.748/0001-85, doravante denominada **CONTRATANTE**, neste ato representada por _____, portador do documento de identidade n.º _____ e inscrito no CPF (MF) sob o n.º _____ e a empresa _____, com sede na _____, inscrita no CNPJ (MF) sob o n.º _____, daqui por diante denominada **CONTRATADA**, neste ato representada pelo _____, portador do documento de identidade n.º _____ e inscrito no CPF (MF) sob o n.º _____, tendo em vista o que consta no Processo n.º **2021.015252**, doravante referido por **PROCESSO** e, em consequência do _____, resolvem firmar o presente **TERMO DE CONTRATO ADMINISTRATIVO PARA PRESTAÇÃO DE SERVIÇO DE INFORMÁTICA,** nos termos da Lei n.º 8.666/1993 e mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

O objeto do presente ajuste é a prestação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme as especificações constantes no Termo de Referência nº 20.2021.DTIC.0720733.2021.015252.

CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO:

O objeto deste ajuste compreende a contratação de serviço de firewall de próxima geração em alta disponibilidade, pelo **período de 48 (quarenta e oito) meses**, para instalação na sede do **CONTRATANTE**, compreendendo os serviços de instalação, configuração, migração e ativação de

equipamentos de segurança; de sistema de monitoramento dos serviços providos e de treinamento para a equipe do **CONTRATANTE**, pela **CONTRATADA**, conforme condições e especificações detalhadas neste Contrato.

Parágrafo primeiro. Os serviços serão prestados conforme o seguinte quantitativo:

ITEM	DESCRIÇÃO	UND	QTD
01	Serviço de Firewall em Alta Disponibilidade	Meses	48
02	Serviço de Monitoramento da Solução	Meses	48
03	Serviço de Migração do Ambiente Atual	Unidades	01
04	Serviço de Treinamento da Solução	Pessoas	05

Tabela 1 - Descrição e Quantitativo dos Serviços

CLÁUSULA TERCEIRA – DAS CARACTERÍSTICAS TÉCNICAS:

1. ESPECIFICAÇÕES GERAIS PARA TODOS OS ITENS:

1.1. São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

1.2. Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de *end-of-sale, end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

1.3. Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a **CONTRATANTE,** seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA).

1.4. O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 4.10, ou na exposição de ativos a riscos de segurança.

1.5. Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do **CONTRATANTE**.

1.6. A **CONTRATADA** deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

1.7. Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. A **CONTRATADA** será

obrigada ao reparo imediato de qualquer dano eventual de manuseio/transporte .

1.8. Quaisquer recursos materiais que tenham sido instalados nas dependências do **CONTRATANTE** pela **CONTRATADA** durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a **CONTRATADA** arcar com todos os custos referentes ao envio e transporte desses materiais.

1.9. Após o encerramento do contrato, caso haja a necessidade expressa pelo **CONTRATANTE**, a **CONTRATADA** deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada à prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do **CONTRATANTE** durante uma eventual transição para os serviços de outra contradada.

1.10. Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço, será de propriedade do **CONTRATANTE**, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do **CONTRATANTE**.

1.11. A **CONTRATADA** deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

1.12. A **CONTRATADA** deverá manter o **CONTRATANTE** atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

2. ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE:

2.1. O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de "Firewall" provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do **CONTRATANTE** e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

2.2. Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

2.3. Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

2.4. O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web.

2.5. Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela **CONTRATADA**.

2.6. Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

2.7. Deverá ser provida, por meio de um *appliance* físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

2.8. Os serviços de instalação e implantação da solução serão de responsabilidade da **CONTRATADA**, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se

fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos serviços especificados.

2.9. Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

2.10. Após a reunião de alinhamento, a **CONTRATADA** deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do **CONTRATANTE**.

2.11. O **CONTRATANTE** entregará à **CONTRATADA**, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do **CONTRATANTE** e configurados pela **CONTRATADA** quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o **CONTRATANTE**.

2.12. O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos *appliances* que compõem a solução, operando em alta disponibilidade.

2.13. Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo *appliance*, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 do Termo de Referência, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

2.14. Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

2.15. A solução deve ser capaz de atender às especificações mínimas dos serviços constante no **item 5.2.15 do Termo de Referência Nº 20.2021.DTIC.0720733.2021.015252**, integrante do Edital de Licitação nº _____, a serem ofertados em uma única plataforma.

3. ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO:

3.1. Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

3.2. Deverá ser baseado em Dashboard, para fácil visualização.

3.3. Deve ser entregue com regras genéricas criadas pela **CONTRATADA**, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

3.4. O serviço da **CONTRATADA** deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo **CONTRATANTE**.

3.5. Deve possuir acesso WEB (HTTPS).

3.6. Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

3.7. Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

4. ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

4.1. O **CONTRATANTE** possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser totalmente migradas

para a solução ofertada.

4.2. O **CONTRATANTE** possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links "full-route" BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

4.3. A **CONTRATADA** deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

4.4. O **CONTRATANTE** possui infraestrutura hiper convergente, e para tanto usa o Acropolis Hypervisor Virtualization and Software - Nutanix. Assim, caso a **CONTRATADA** necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do **CONTRATANTE**.

4.5. A **CONTRATADA** deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

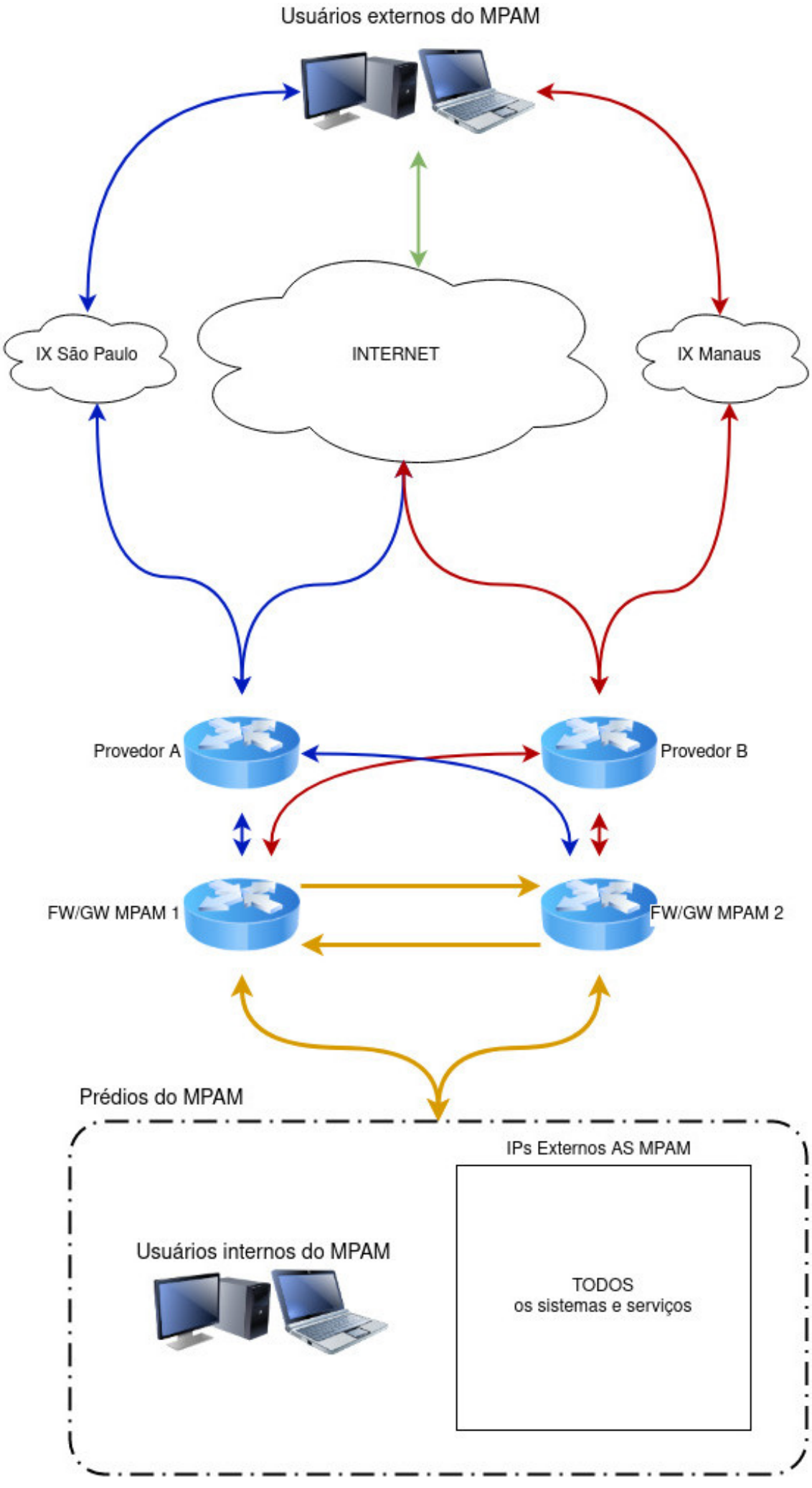
4.6. A **CONTRATADA** deverá finalizar o processo de migração após testes e aprovação pelo **CONTRATANTE** em até 60 (sessenta) dias após o seu início.

4.7. A **CONTRATADA** deverá evitar, durante o processo de migração, interromper os serviços de rede do **CONTRATANTE**, nos horários das 8hs às 18hs, em dias de expediente do **CONTRATANTE**.

4.8. É de responsabilidade da **CONTRATADA** a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do **CONTRATANTE** fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

4.9. A **CONTRATADA** deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do **CONTRATANTE**, sendo vedada sua cessão, locação ou venda a terceiros.

4.10. A topologia da solução deve seguir conforme imagem a seguir:


Usuários externos do MPAM
IX São Paulo
INTERNET
IX Manaus
Provedor A
Provedor B
FW/GW MPAM 1
FW/GW MPAM 2
Prédios do MPAM
IPs Externos AS MPAM
Usuários internos do MPAM
TODOS
os sistemas e serviços

5. ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO:

5.1. A **CONTRATADA** deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.2. A carga horária total para o treinamento deve ser de, no mínimo, **40 horas**.

5.3. A **CONTRATADA** deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela **FISCALIZAÇÂO**.

5.4. O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fonecido em português do Brasil ou inglês.

5.5. O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do **CONTRATANTE**.

5.6. O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a **CONTRATADA** deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o **CONTRATANTE**. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.7. A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.8. A **CONTRATADA** deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.9. Caso o treinamento seja ofertado de forma presencial, o **CONTRATANTE** irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do **CONTRATANTE**.

5.10. O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a **CONTRATADA** deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do **CONTRATANTE**.

5.11. Será de responsabilidade da **CONTRATADA** prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.12. A **CONTRATADA** deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.13. Os instrutores designados pela **CONTRATADA** deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.14. A **CONTRATADA** deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.15. A **CONTRATADA** deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do **CONTRATANTE** e com finalidade de uso exclusivamente interno do **CONTRATANTE**, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela **CONTRATADA**.

6. SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS:

6.1. A **CONTRATADA** deverá disponibilizar ao **CONTRATANTE** um número telefônico único, um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entende-se por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS.

6.2. No atendimento por meio de telefone a **CONTRATADA** fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

6.3. O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

6.4. Cada chamado deverá conter, no mínimo, as seguintes informações:

6.4.1. Número único do registro/ocorrência - a ser fornecido pela **CONTRATADA**.

6.4.2. Identificação do atendente.

6.4.3. Identificação do solicitante.

6.4.4. Data e hora de abertura do chamado/início da interrupção.

6.4.5. Descrição da ocorrência.

6.4.6. Designação do equipamento, quando for o caso.

6.4.7. Ações corretivas tomadas.

6.4.8. Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

6.5. O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

6.6. O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da **CONTRATADA**.

6.7. Não deverá haver qualquer limitação para o número de solicitações de reparo.

6.8. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos

relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a **CONTRATADA** deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

7. GARANTIA TÉCNICA:

7.1. A **CONTRATADA** deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

7.2. A **CONTRATADA** deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.

7.3. Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.

7.4. A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao **CONTRATANTE**.

7.5. Caso sejam detectadas falhas ou bugs nos produtos, a **CONTRATADA** deverá realizar as atualizações necessárias à correção do problema.

7.6. A **CONTRATADA** deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

7.7. A **CONTRATADA** é a única responsável pelos produtos fornecidos ao **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.

7.8. A **CONTRATADA** responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo **CONTRATANTE**, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

7.9. Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à **CONTRATADA** apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.

7.10. Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

7.11. A **CONTRATADA** deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o **CONTRATANTE**.

7.12. No que se refere a software, durante a vigência do Contrato, a **CONTRATADA** deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o **CONTRATANTE**. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

7.12.1. Patches, fixes, correções, updates e service packs.

7.12.2. Novas releases, builds e funcionalidades.

7.12.3. O provimento de upgrades para novas versões de mercado ou lançamentos, independente

da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.

7.12.4. O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.

7.12.5. Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.

7.12.6. A cada nova liberação de versão e release, a **CONTRATADA** deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

7.12.7. A **CONTRATADA** deverá fornecer tais atualizações independentemente de solicitação expressa do **CONTRATANTE**.

7.12.8. A **CONTRATADA** deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

7.12.9. As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

8. MANUTENÇÃO PREVENTIVA E CORRETIVA:

8.1. Os serviços de manutenção *on-site*, serão prestados nas dependências do **CONTRATANTE** na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

8.2. O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do **CONTRATANTE**, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

8.3. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

8.4. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

8.5. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

8.6. A **CONTRATADA** deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo **CONTRATANTE** ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser realizada nas dependências do **CONTRATANTE**, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

8.7. O **CONTRATANTE** poderá determinar à **CONTRATADA** a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da **CONTRATADA**.

8.8. Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da **CONTRATADA**, não devendo gerar qualquer ônus adicional ao **CONTRATANTE**.

8.9. A **CONTRATADA** deve emitir relatórios de todas as intervenções realizadas, preventivas e

corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do **CONTRATANTE**.

8.10. O serviço de suporte deverá ser efetuado *on-site* sempre que se fizer necessário ou quando for solicitado pelo **CONTRATANTE**, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o **CONTRATANTE**.

8.11. Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do **CONTRATANTE**, a **CONTRATADA** deverá desinstalar, embalar e transportar o item defeituoso, instalar item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

8.12. Quando da detecção de problemas ou inconformidades, a **CONTRATADA** deverá imediatamente abrir um chamado técnico, informar o **CONTRATANTE** e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

8.13. A **CONTRATADA** encaminhará mensagem de e-mail para o **CONTRATANTE**, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da **CONTRATADA** e/ou por meio de abertura de chamado a critério da equipe técnica do **CONTRATANTE**, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

8.14. Todos os custos diretos e indiretos para realização do atendimento presencial (*on-site*) serão de responsabilidade exclusiva da **CONTRATADA**.

8.15. Dentro do mesmo endereço, a ser executada pela **CONTRATADA**, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o **CONTRATANTE**.

8.16. Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

8.17. O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do **CONTRATANTE**, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

8.18. Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

8.19. A **CONTRATADA** deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da **CONTRATADA**, deve haver comunicação formal ao **CONTRATANTE**, incluindo as comprovações exigidas.

9. ACORDO DE NÍVEL DE SERVIÇO (SLA):

9.1. Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos neste termo.

9.2. A **CONTRATADA** deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

9.3. A **CONTRATADA** deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

9.4. A realização de assistência técnica preventiva, caso não seja solicitada pelo **CONTRATANTE**, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do **CONTRATANTE**.

9.5. Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

9.6. Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

9.7. Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do **CONTRATANTE**, a solução será considerada como operando em Modo de Contingência.

9.8. Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

9.9. A **CONTRATADA** deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual. Este checkup faz parte da manutenção preventiva.

9.10. Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.

9.11. O Modo de Contingência se caracteriza por:

9.11.1. Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.

9.11.2. Funcionamento acima dos limiares de desempenho, conforme estabelecido nos itens 9.5 e 9.6 acima.

9.11.3. Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante ou fora de garantia.

9.11.4. Operação com funcionalidade ou performance abaixo dos mínimos exigidos neste Termo.

9.12. Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.

9.13. O estado de Inoperância Total se caracteriza por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do **CONTRATANTE**.

9.14. O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela **CONTRATADA**.

CLÁUSULA QUARTA – DOS PRAZOS PARA A PRESTAÇÃO DOS SERVIÇOS:

A **CONTRATADA** deverá concluir a implantação, ativação e entrega dos sistemas e equipamentos que compõem os itens 01, 02 e 03, especificados cláusula anterior deste ajuste, **em até 65 (sessenta e cinco) dias corridos**, contados a partir da assinatura do contrato.

Parágrafo primeiro. A **CONTRATADA** deverá, em comum acordo com o **CONTRATANTE**, no prazo máximo de **120 (cento e vinte) dias corridos**, contados a partir da assinatura do contrato, finalizar o treinamento indicado no item 04 da cláusula anterior.

Parágrafo segundo. A **CONTRATADA** poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pela **CONTRATANTE**, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, da lei n. 8.666/93.

Parágrafo terceiro. Antes de findar os prazos fixados nos itens anteriores, a **CONTRATADA** poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pelo **CONTRATANTE,** que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, 410 da lei n. 8.666/93.

Parágrafo quarto. O prazo da prestação dos serviços deverá contar da assinatura do contrato, prorrogáveis de comum acordo, até o limite estabelecido na Lei n. 8.666/93, e suas alterações.

CLÁUSULA QUINTA – DO RECEBIMENTO:

O recebimento dos serviços será realizado pela **FISCALIZAÇÃO** do **CONTRATANTE**.

Parágrafo primeiro. O recebimento será feito nas seguintes etapas:

1. Será emitido Termo Individual de ACEITE para cada item do Contrato.
2. Será emitido Termo de Recebimento Definitivo para todo o Lote.

Parágrafo segundo. Para fins de aceite, a **CONTRATADA** deverá comunicar formalmente a efetiva disponibilização dos serviços para cada item do Lote:

1. Para a emissão do Termo Individual de ACEITE para o Item 01:

1.1. Será emitido após Período de Funcionamento Experimental de até 15 (quinze) dias, que se iniciará após comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

1.2. Durante Período de Funcionamento Experimental a **FISCALIZAÇÃO** deverá concluir os testes necessários para constatar o funcionamento regular dos serviços disponibilizados.

1.3. A **FISCALIZAÇÃO** realizará avaliação qualitativa das especificações dos equipamentos e funcionalidades que compõem a solução conforme exigências deste Termo.

2. Para a emissão do Termo Individual de ACEITE para o Item 02:

2.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

2.2. A **FISCALIZAÇÃO** realizará testes com as credenciais fornecidas, teste de uso da ferramenta e teste de disponibilidade necessários para constatar o funcionamento regular dos serviços disponibilizados.

3. Para a emissão do Termo Individual de ACEITE para o Item 03:

3.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito, por parte da **CONTRATADA**, incluindo evidencias que demonstrem inequivocadamente que todas os critérios estabelecidos na seção 5.4 deste Termo foram atendidos, atestando a efetiva disponibilização dos serviços.

3.2. A **FISCALIZAÇÃO** realizará avaliação qualitativa das evidências apresentadas considerando a disponibilidade dos serviços do **CONTRATANTE**.

4. Para a emissão do Termo Individual de ACEITE para o Item 04:

4.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

4.2. A **FISCALIZAÇÃO** observará os critérios estabelecidos na seção 5.5 deste Termo.

Parágrafo terceiro. Somente depois de realizados e aprovados os testes definidos, o **CONTRATANTE**, por meio da **FISCALIZAÇÃO**, emitirá o Termo de Aceite, atestando a conformidade com as especificações neste Contrato, liberando o início de faturamento.

Parágrafo quarto. A contagem do prazo para a efetiva entrega e prestação de cada item de serviço especificado no lote será suspenso quando a **CONTRATADA** comunicar a efetiva disponibilização do serviço, e, se for o caso, será retomado no dia seguinte a partir da emissão de comunicado por escrito do **CONTRATANTE** indicando NÃO ACEITE do serviço em virtude de não conformidade com algum dos requisitos presentes nesse termo de referência.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO:

A execução do objeto deste contrato dar-se-á indiretamente pela **CONTRATADA**, sob o regime de empreitada por preço global.

CLÁUSULA SÉTIMA – DAS GARANTIAS:

Os serviços ora pactuados são garantidos em conformidade com o Código de Proteção e Defesa do Consumidor, Lei n.º 8.078, de 11 de setembro de 1990, artigos 26 e 27, e nos termos do Item 7 da Cláusula Terceira deste Contrato.

CLÁUSULA OITAVA – GESTÃO E DA FISCALIZAÇÃO:

A **CONTRATANTE** nomeará um servidor ou comissão, por meio de ato específico, doravante denominado(a) **FISCALIZAÇÃO**, para gerir e fiscalizar a execução deste contrato, com autoridade para exercer, como representante da **CONTRATANTE**, toda e qualquer ação destinada ao acompanhamento da execução contratual, observando as determinações do artigo 67 da Lei n.º 8.666/93, em especial:

1. Abrir processo de gestão do presente contrato, fazendo constar todos os documentos referentes à fiscalização dos serviços.
2. Gerir, acompanhar e fiscalizar a execução dos serviços, realizando diretamente toda e qualquer comunicação com a **CONTRATADA**, mediante ofício ou outros documentos.
3. Atestar a respectiva nota fiscal/fatura emitida corretamente pela **CONTRATADA**, para a efetivação do pagamento correspondente.
4. Verificar quando da liquidação dos serviços a documentação de regularidade fiscal da **CONTRATADA**.
5. Indicar as ocorrências verificadas, determinando o que for necessário à regularização das faltas observadas.
6. Fixar prazo limite para realização das providências necessárias à regularização de eventuais vícios, defeitos ou incorreções resultantes da execução do presente contrato.
7. Solicitar à **CONTRATADA** e a seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento da avença e anexar aos autos cópia dos documentos que comprovem essas solicitações.
8. **Informar, com a antecedência necessária, o término do ajuste.**
9. Encaminhar à Administração Superior toda e qualquer modificação que se faça necessária e envolva acréscimo ou supressão de despesa e dilatação de prazos, para fins das providências administrativas indispensáveis.
10. Verificar a manutenção das condições de habilitação da **CONTRATADA**, exigindo sua regularização, durante a vigência do contrato.
11. Prestar as informações e os esclarecimentos necessários ao desenvolvimento das tarefas.
12. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições no curso de execução do objeto do contrato, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.
13. Rejeitar, no todo ou em parte, o fornecimento executado em desacordo com o contrato.
14. Comunicar à Administração, de forma imediata, as ocorrências que impliquem possíveis sanções à **CONTRATADA**, bem como as decisões e providências que ultrapassarem sua competência, para a adoção das medidas convenientes.
15. Praticar todos os demais atos e exigências que se fizerem necessários ao fiel cumprimento do presente contrato.

Parágrafo primeiro. A **FISCALIZAÇÃO** será exercida no interesse da **CONTRATANTE** e não exclui nem reduz as responsabilidades contratuais da **CONTRATADA**, inclusive perante terceiros, por quaisquer

irregularidades, e, na sua ocorrência, não implica corresponsabilidade do poder público ou de seus agentes e prepostos.

Parágrafo segundo. Quaisquer exigências da **FISCALIZAÇÃO** inerentes ao objeto deste contrato deverão ser prontamente atendidas pela **CONTRATADA**, sem qualquer ônus para a **CONTRATANTE**.

Parágrafo terceiro. A **CONTRATADA** deverá manter preposto, aceito pela **CONTRATANTE**, para representá-la administrativamente na execução do contrato, devendo, **no prazo máximo de 10 (dez) dias da assinatura do instrumento**, informar nome, telefone, endereços e outros meios de comunicação entre a **CONTRATANTE** e o preposto responsável pela execução do contrato operacional e financeira.

Parágrafo quarto. As comunicações e notificações feitas pela **CONTRATANTE** à **CONTRATADA**, a serem realizadas sob o âmbito do presente contrato, serão feitas por meio de ofícios, e-mails ou por telefone.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA:

Constituem obrigações da **CONTRATADA**:

1. Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo, observando as prescrições e as recomendações do fabricante/fornecedor, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.
2. Comunicar imediatamente, à **CONTRATANTE**, toda e qualquer irregularidade ou dificuldade que impossibilite a execução dos serviços objeto deste contrato.
3. Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que o **CONTRATANTE** julgar necessário.
4. Manter contato e realizar o planejamento dos serviços com o **CONTRATANTE** de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.
5. Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, o objeto deste ajuste que não atenda às especificações exigidas, em que se verifiquem imperfeições, vícios, defeitos ou incorreções ou rejeitados pela fiscalização.
6. Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pelo **CONTRATANTE** em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste contrato.
7. Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.
8. Acatar as observações feitas pela **FISCALIZAÇÃO** quanto à execução dos serviços.
9. Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.
10. Reparar, corrigir, remover ou substituir, às suas expensas, no todo ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.
11. Seguir as orientações da Lei n. 9.472/97, do Termo de Concessão ou autorização emitido pela ANATEL, e demais disposições regulamentares pertinentes aos serviços a serem prestados.
12. Credenciar junto ao **CONTRATANTE** um representante, denominado preposto, aceito pelo **CONTRATANTE**, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, indicando as formas de contato no mínimo telefone, para comunicação rápida e email para comunicação formal.
13. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação.

14. Implantar a supervisão permanente dos serviços, de modo adequado e de forma a obter uma operação correta e eficaz.
15. Responsabilizar-se por todos os serviços não explícitos nestas especificações, mas necessários à execução dos serviços programados e ao perfeito funcionamento das instalações.
16. Respeitar o sistema de segurança do **CONTRATANTE** e fornecer todas as informações solicitadas por ele.
17. Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.
18. Acatar que o **CONTRATANTE** não aceitará, sob nenhum pretexto, a transferência de responsabilidade da **CONTRATADA** para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

Parágrafo primeiro. A inadimplência da **CONTRATADA**, com referência aos encargos decorrentes dos serviços constantes deste contrato, não transfere à **CONTRATANTE** a responsabilidade por seu pagamento, nem pode onerar o objeto do contrato ou restringir a manutenção contratada.

Parágrafo segundo. A **CONTRATADA** declara, antecipadamente, aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos, explicações que a **CONTRATANTE** julgar necessário.

Parágrafo terceiro. A inobservância das especificações constantes deste Contrato implicará a não aceitação parcial ou total dos serviços, devendo a **CONTRATADA** refazer as partes recusadas sem direito a indenização.

Parágrafo quarto. Todos os equipamentos fornecidos pela **CONTRATADA**, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área, tais como: ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações).

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE:

Constituem obrigações do **CONTRATANTE**:

1. Fornecer à **CONTRATADA** as informações necessárias à fiel execução do objeto deste Termo.
2. Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA** durante o prazo de vigência deste Contrato.
3. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 8.666/93, o exato cumprimento das cláusulas e condições contratuais.
4. Designar, e informar à **CONTRATADA**, fiscal do contrato e seu substituto, mantendo tais dados atualizados.
5. Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos materiais, de forma a assegurar o perfeito cumprimento do contrato.
6. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.
7. Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este Termo.
8. Fazer uso adequado dos equipamentos fornecidos pela **CONTRATADA**, seguindo as instruções constantes de seus manuais de uso.
9. Efetuar regularmente o pagamento à **CONTRATADA**, conforme nota de empenho e dentro dos critérios estabelecidos neste contrato, quanto aos serviços efetivamente realizados, por meio de Ordem

Bancária, após o atesto das notas fiscais/faturas pela **CONTRATANTE**, bem como dos demais documentos exigidos neste termo.

CLÁUSULA DÉCIMA PRIMEIRA – DA VIGÊNCIA DO CONTRATO:

O presente contrato terá vigência de **48 (quarenta e oito) meses**, contados da sua assinatura, conforme art. 57, inciso IV, da Lei n.º 8.666/1993.

Parágrafo primeiro. O prazo acima referido terá início e vencimento em dia de expediente e terá eficácia legal após a publicação de seu extrato na impressa oficial.

CLÁUSULA DÉCIMA SEGUNDA – DO VALOR DO CONTRATO:

O valor global do presente contrato é de **R$ _____**, conforme a seguinte tabela:

ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO (B)	VALOR TOTAL
01	Serviço de Firewall em Alta Disponibilidade	Meses	48		
02	Serviço de Monitoramento da Solução	Meses	48		
03	Serviço de Migração do Ambiente Atual	Unidades	01		
04	Serviço de Treinamento da Solução	Pessoas	05		
TOTAL (R$)					

Parágrafo primeiro. A proposta apresentada pela **CONTRATADA**, datada de _____, faz parte deste instrumento contratual como anexo.

Parágrafo segundo. No preço total do contrato já estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, lucro e outros necessários ao cumprimento integral do objeto deste instrumento.

CLÁUSULA DÉCIMA TERCEIRA – DA LIQUIDAÇÃO E DO PAGAMENTO:

O pagamento será efetuado após a efetiva disponibilização dos serviços pela **CONTRATADA** e emissão pelo **CONTRATANTE** do Termo Individual de Aceite para cada item do Lote, mediante depósito na conta corrente da **CONTRATADA**, por meio de ordem bancária, seguindo as seguintes etapas:

1. Para os Itens 01 e 02:

1.1 Mensalmente, a **CONTRATADA** deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

1.2 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada dia de funcionamento da solução em Modo de Contingênica além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

1.3 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada hora de funcionamento da solução em estado de Inoperância Total além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

1.4 A data de início de cobrança dos serviços deverá observar a data de emissão do Termo de Aceite, sendo que a primeira fatura corresponderá à prestação de serviços desde a data de emissão do Termo de Aceite, para cada item do Lote, até o último dia do respectivo mês, de forma pro rata.

1.5 As demais faturas deverão abranger o período do primeiro ao último dia do mês.

1.6 Os valores a serem faturados concernentes aos serviços objeto desta contratação estarão sujeitos a descontos nas situações de descumprimento das metas estabelecidas para os indicadores elencados na especificação do serviço, item Acordo de Nível de Serviço (SLA).

1.7 Os descontos aplicados nas faturas mensais não isentam a **CONTRATADA** de quaisquer sanções legais ou das sanções dispostas na seção 12 - SANÇÕES ADMINISTRATIVAS.

1.8 Os descontos aplicados nas faturas mensais, conforme dispostos acima, oriundos do descumprimento dos níveis mínimos de serviço estipulados no item Acordo de Nível de Serviço (SLA), não se configuram como penalidades ou multas.

1.9 No primeiro dia útil do mês subsequente, antes da emissão na nota fiscal, a **CONTRATADA** deverá enviar à **FISCALIZAÇÃO** relatório referente aos períodos, destacando eventuais descontos e as causas da(s) indisponibilidade(s) ocorridas na prestação dos serviços para a devida aprovação.

1.10 As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da **CONTRATADA** no que diz respeito ao atendimento dos níveis de serviços especificados no acordo de nível de serviço, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

2. Para os Itens 03 e 04:

2.1 A **CONTRATADA** deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

2.2 Os pagamentos relativos aos Itens serão realizados de uma única vez, no mês seguinte a emissão do Termo de Aceite.

Parágrafo primeiro. A nota fiscal e os demais documentos exigidos no edital e neste contrato, para fins de liquidação e pagamento das despesas, deverão ser apresentados no Setor de Protocolo da **CONTRATANTE**, situado na Avenida Coronel Teixeira, n.º 7.995, Nova Esperança, Manaus/AM ou enviados ao e-mail **protocolo@mpam.mp.br.**

Parágrafo segundo. Ao **CONTRATANTE** fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas neste Termo.

Parágrafo terceiro. Nenhum pagamento será efetuado à **CONTRATADA** quando forem constatadas as irregularidades abaixo especificadas, sendo que tais situações não caracterizam inadimplência da **CONTRANTATE** e, por conseguinte, não geram direito à compensação financeira: a) os serviços/produtos não abrangidos pelo objeto contratual; b) ausência de comprovação da regularidade fiscal e trabalhista da **CONTRATADA**, e c) pendência de liquidação de qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

Parágrafo quarto. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação

regular, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

Parágrafo quinto. O atraso no pagamento decorrente das circunstâncias descritas na obrigação anterior, não exime a **CONTRATADA** de promover o pagamento de impostos e contribuições nas datas regulamentares.

Parágrafo sexto. O documento fiscal será devolvido à **CONTRATADA** caso contenha erros ou em caso de circunstância que impeça a sua liquidação, ficando o pagamento pendente até que seja sanado o problema. Nessa hipótese, o prazo para pagamento se iniciará após a regularização ou reapresentação do documento fiscal, não acarretando qualquer ônus para a **CONTRATANTE**.

Parágrafo sétimo. Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela **CONTRATANTE**, entre a data de vencimento e a do dia do efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, serão calculados por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = i ÷ 365 = (6÷100) ÷ 365 = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

Parágrafo oitavo. Aplica-se a mesma regra disposta no parágrafo anterior, na hipótese de eventual pagamento antecipado, observado o disposto no art. 40, XIV, "d", da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA:

As despesas oriundas deste contrato correrão à conta da seguinte dotação orçamentária: **Unidade Orçamentária**: _____; **Programa de Trabalho**: _____; **Fonte**: _____; **Natureza da Despesa**: _____, tendo sido emitida, pela **CONTRATANTE**, em _____, a Nota de Empenho n.º _____, no valor de **R$ _____ (_____)**.

Parágrafo único. No exercício seguinte, o valor de **R$ _____ (_____)**, relativo ao complemento do contrato, será empenhado à conta de dotações consignadas para o orçamento vindouro.

CLÁUSULA DÉCIMA QUINTA – DA GARANTIA CONTRATUAL:

Nos termos do art. 56 da Lei n º 8.666, de 21/6/1993, para segurança do integral cumprimento do Contrato, a **CONTRATADA** apresentará garantia, no prazo máximo de 10 (dez) dias da assinatura deste contrato, de **5% (cinco por cento)** do valor total do contrato, que corresponde à importância de **_____.**

1. Será ainda exigida prestação de garantia adicional de valor igual à diferença entre o valor limite de exequibilidade obtido durante o certame e o valor da proposta vencedora, desde que este seja inferior a 80% (oitenta por cento) da média aritmética calculada, nos termos do § 2º, do artigo 48, da Lei Federal nº 8.666/93.

2. No caso de acréscimo no valor contratual, a licitante vencedora obriga-se a depositar junto ao Ministério Público, na mesma modalidade, o valor referente à diferença da garantia. Mesma providência deverá ser tomada no caso de prorrogação no prazo contratual para adequar o vencimento da garantia ao disposto no subitem abaixo.

3. As garantias prestadas serão liberadas após a assinatura do Termo de Encerramento do contrato, e quando em dinheiro atualizadas monetariamente, conforme dispões o § 4º, do artigo 56 da Lei n. 8.666/93.

Parágrafo primeiro. A garantia prestada deverá formalmente cobrir pagamentos não efetuados pela **CONTRATADA** referentes à:

1. prejuízos advindos do não cumprimento do objeto do contrato;

2. prejuízos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

3. multas punitivas aplicadas pela Administração à **CONTRATADA**; e

4. obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**.

Parágrafo segundo. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no parágrafo primeiro.

Parágrafo terceiro. A garantia em dinheiro deverá ser efetuada em conta caução, devidamente designada para este fim, aberta em instituição financeira oficial e mediante autorização específica da **CONTRATANTE**.

Parágrafo quarto. A garantia deverá ter validade durante a execução do contrato e estender-se-á por mais **3 (três) meses após o término da vigência contratual**. Na hipótese de prorrogação do prazo de vigência contratual, a **CONTRATADA** deverá apresentar prorrogação equivalente de prazo de validade da referida garantia.

Parágrafo quinto. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato, por dia de atraso, observado o máximo de 2% (dois por cento).

Parágrafo sexto. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a retenção dos pagamentos devidos à **CONTRATADA** e/ou a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n.º 8.666, de 1993.

1. O bloqueio efetuado com base neste parágrafo não gera direito a nenhum tipo de compensação financeira à **CONTRATADA**.
2. A **CONTRATADA**, a qualquer tempo, poderá substituir o bloqueio efetuado por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

Parágrafo sétimo. A **CONTRATADA** se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, para o pagamento da multa contratual ou encargos trabalhistas e previdenciários, e ainda, na alteração do valor contratado, para manter o percentual inicial, **no prazo de até 10 (dez) dias**, contados da assinatura do termo aditivo ou a partir da data em que for notificada pela **CONTRATANTE**, a partir do qual se observará o disposto nesta cláusula.

Parágrafo oitavo. A garantia somente será liberada ante a comprovação de que a empresa pagou todos os encargos trabalhistas e previdenciárias decorrentes da contratação, bem como apresentação de toda a documentação solicitada no edital pela **CONTRATANTE**.

Parágrafo nono. Será considerada extinta a garantia:

1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da **CONTRATANTE**, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do contrato;
2. no prazo de três meses após o término da vigência, caso a **CONTRATANTE** não comunique a ocorrência de sinistros.

Parágrafo décimo. A garantia não será extinta, em caso de ocorrência de sinistro ou irregularidade, devidamente comunica à seguradora pela **FISCALIZAÇÃO.**

CLÁUSULA DÉCIMA SEXTA – DO REAJUSTAMENTO:

Os preços propostos não serão reajustados durante todo o período de vigência do contrato.

CLÁUSULA DÉCIMA SÉTIMA – DAS ALTERAÇÕES:

Competem a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei n.º 8.666/1993 e em outras disposições legais pertinentes, realizar, por escrito, por meio de Termo Aditivo, as alterações contratuais que julgarem convenientes.

Parágrafo único. A **CONTRATADA** fica obrigada a aceitar as alterações unilaterais, conforme disposto no art. 65, I, da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA OITAVA – DAS PENALIDADES:

Em caso de inexecução total ou parcial, execução imperfeita, ou qualquer inadimplemento ou infração contratual, a **CONTRATADA**, sem prejuízo das responsabilidades civil e criminal, ficará sujeita às seguintes penalidades:

1. advertência;
2. multas percentuais, nos termos do parágrafo segundo desta cláusula;
3. rescisão administrativa do contrato;
4. suspensão temporária do direito de participar de licitação e impedimento de contratar;
5. declaração de inidoneidade para licitar e contratar.

Parágrafo primeiro. As penas acima referidas serão propostas pela **FISCALIZAÇÃO** e impostas pela autoridade competente, assegurada à **CONTRATADA** a prévia e ampla defesa na via administrativa.

Parágrafo segundo. A Advertência por escrito será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem corno, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do **CONTRATANTE**.

Parágrafo terceiro. Serão aplicadas à **CONTRATADA** as seguintes multas:

I - **2% (dois por cento)** sobre o valor global contratado, a cada reincidência na penalidade de advertência. Na hipótese de reincidência por 5 (cinco) vezes na penalidade de advertência, será considerado descumprimento total da obrigação, punível com as sanções previstas em lei.

II - **2% (dois por cento)** sobre o valor global contratado, por dia de atraso, no caso de descumprimento do tempo máximo, conforme Clásula Quarta - DOS PRAZOS PARA A PRESTAÇÃO DOS SERVIÇOS, limitado a 10 (dez) dias. O atraso superior a 10 (dez) dias será considerado como descumprimento total da obrigação, punível com as sanções previstas em lei.

III - **10% (dez por cento)** sobre o valor global contratado, no caso de, sem justificativa aceita pelo **CONTRATANTE**, o vencedor não retirar a Nota de Empenho, a Autorização de Fornecimento de Materiais/Serviço ou não assinar o contrato deixando, assim, de cumprir os prazos fixados, sem prejuízo das demais sanções previstas.

IV - **até 20% (vinte por cento)** sobre o valor global contratado, nos casos de INEXECUÇÃO PARCIAL do objeto contratado.

V - **até 30% (trinta por cento)** sobre o valor global contratado, nos casos de INEXECUÇÃO TOTAL do objeto contratado.

VI - **até 30% (trinta por cento)** sobre o valor global contratado, na hipótese de rescisão do contrato por culpa da **CONTRATADA**.

Parágrafo quarto. As multas contratuais serão descontadas dos pagamentos a que fizer jus a **CONTRATADA**, podendo ser cobrado judicialmente, quando necessário.

CLÁUSULA DÉCIMA NONA – DA RESCISÃO DO CONTRATO:

A inadimplência das cláusulas e condições estabelecidas neste contrato, por parte da **CONTRATADA**, assegurará à **CONTRATANTE** o direito de rescindir o contrato, mediante notificação através de ofício, entregue diretamente ou por via postal, com prova de recebimento, sem ônus de qualquer espécie para Administração e prejuízo das sanções previstas neste ajuste.

Parágrafo primeiro. Rescisão Unilateral. Ficará o presente contrato rescindido unilateralmente pela **CONTRATANTE**, mediante formalização, assegurado o contraditório e a ampla defesa, nos termos do art. 78, incisos I a XII e XVII, da Lei n.º 8.666/93.

Parágrafo segundo. Rescisão Bilateral. Ficará o presente contrato rescindido por acordo entre as partes, desde que haja conveniência para a Administração, nos casos do art. 78, XIII a XVI, da Lei n.º 8.666/93.

Parágrafo terceiro. Rescisão Judicial. O presente contrato poderá ser rescindido, judicialmente, nos termos da lei.

Parágrafo quarto. A falta dos registros ou documentações, incluindo a ART ou RRT, ou, ainda, constatada a irregularidade, ensejará o rompimento do vínculo contratual, sem prejuízo das multas contratuais, bem como das demais cominações legais.

Parágrafo quinto. Fica vedado, à **CONTRATADA**, sob pena de rescisão contratual, CAUCIONAR ou utilizar o contrato para qualquer operação financeira, sem prévia e expressa anuência da **CONTRATANTE**.

CLÁUSULA VIGÉSIMA – DO VÍNCULO EMPREGATÍCIO:

Os empregados e prepostos da **CONTRATADA** não terão qualquer vínculo empregatício com a **CONTRATANTE**, correndo por conta exclusiva da primeira todas as obrigações decorrentes da legislação trabalhista, previdenciária, fiscal e comercial, as quais se obriga a saldar na época devida.

CLÁUSULA VIGÉSIMA PRIMEIRA – DAS NORMAS APLICÁVEIS:

O presente contrato deverá respeitar as seguintes leis e/ou decretos e resoluções:

1. Lei n.º 8.666/1993 – Licitações e Contratos;
2. Lei n.º 8.078/1990 – Código de Defesa do Consumidor;
3. Lei n.º 10.406/2002 – Código Civil Brasileiro.

Parágrafo único. A **CONTRATADA** declara conhecer todas essas normas e concorda em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

CLÁUSULA VIGÉSIMA SEGUNDA – DO TRATAMENTO DOS DADOS PESSOAIS:

As partes obrigam-se a realizar o tratamento de dados pessoais em obediências as disposições legais vigentes, nos moldes da Lei 13.709/2018 (LGPD), visando dar efetiva proteção aos dados coletados de pessoas naturais que possam identificá-las ou torná-las identificáveis.

1. O consentimento para o tratamento de dados pessoais, citado nesta Cláusula, se dará por meio da assinatura deste contrato.
2. O tratamento de dados pessoais se dará, exclusivamente, para os fins necessários ao cumprimento do objeto deste Contrato sem a possibilidade de tratamento futuro incompatível com a finalidade.
3. O usuário autoriza expressamente que suas informações e dados pessoais sejam compartilhados pela **CONTRATADA** com Autoridades públicas, administrativas e judiciais, que, no exercício de sua competência, exijam informações, mesmo que não haja ordem ou citação executiva ou judicial para esse

efeito, para os seguintes fins:

3.1. colaborar na investigação e denunciar fraudes, pirataria, violação de direitos de propriedade intelectual ou qualquer outro ato ilícito, bem como qualquer atividade ou circunstância que possa gerar responsabilidade legal para a **CONTRATADA** e/ou aos seus usuários;

3.2. resguardar um interesse público, a aplicação ou administração da justiça, o reconhecimento, exercício ou defesa de um direito em um processo judicial ou administrativo e/ou a resolução de disputas; e

3.3. cumprir com qualquer lei, regulamento ou disposição legal aplicável, ou algum mandato de autoridade competente devidamente fundamentado e motivado.

CLÁUSULA VIGÉSIMA TERCEIRA – DA PUBLICAÇÃO:

O presente contrato será publicado, sob a forma de extrato, no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, após a sua assinatura, correndo as despesas por conta da **CONTRATANTE**, nos termos do art. 61, parágrafo único, da Lei n.º 8.666/1993 e ATO PGJ N.º 082/2012.

CLÁUSULA VIGÉSIMA QUARTA – DAS DISPOSIÇÕES GERAIS:

A **CONTRATADA**, em cumprimento à Resolução n.º 37/2009 do Conselho Nacional do Ministério Público, declara que não possui sócios, gerentes ou diretores que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas.

Parágrafo único. Os casos omissos neste contrato serão resolvidos pela Administração Superior da **CONTRATANTE**, baseada na legislação vigente.

CLÁUSULA VIGÉSIMA QUINTA – DO FORO CONTRATUAL:

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na justiça estadual, no Foro de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

E por estarem de acordo, foi o presente termo de contrato, depois de lido e anuído, assinado digitalmente pelas partes e por duas testemunhas.

XXXXXXXXXXXXXXXXXXXX
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

XXXXXXXXXXXXXXXXXXXX
Representante Legal da Empresa

Documento assinado eletronicamente por **Ivanete de Oliveira Nascimento**, **Diretor(a) de Planejamento - DPLAN**, em 14/01/2022, às 14:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0750392** e o código CRC **FD9266B2**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 24.2022.DCCON.0751813.2021.015252

Manaus (Am.), 14 de janeiro de 2022.

Ao Sr. Presidente da Comissão Permanente de Licitação da PGJ/AM

Assunto: Encaminha minuta de contrato – Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade

Senhor Presidente,

Trata-se de Procedimento Interno que visa à contratação de empresa para prestação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme as especificações constantes no Termo de Referência nº 20.2021.DTIC.0720733.2021.015252 (0720733).

Assim, encaminho a minuta de contrato administrativo (0750392) elaborada por esta Divisão de Contratos e Convênios - DCCON, para conhecimento e adoção das medidas cabíveis a essa Comissão Permanente de Licitação.

Em tempo, informo que a referida minuta deve ser analisada e aprovada pela assessoria jurídica deste *Parquet*, nos termos do artigo 38, parágrafo único da Lei Federal de Licitação e Contratos, com atenção especial à CLÁUSULA VIGÉSIMA SEGUNDA – DO TRATAMENTO DOS DADOS PESSOAIS.

Atenciosamente,

Documento assinado eletronicamente por **Ivanete de Oliveira Nascimento**, **Diretor(a) de Planejamento - DPLAN**, em 14/01/2022, às 15:05, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0751813** e o código CRC **A7BC038E**.

MINUTA DE EDITAL DO PREGÃO ELETRÔNICO N.º 4.0__/2022-CPL/MP/PGJ

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** pelo presente edital e por intermédio da **PROCURADORIA GERAL DE JUSTIÇA**, cadastrada no CNPJ sob o n.º 04.153.748/0001-85, através da **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, designada pelo Ato PGJ n.º 185/2021 e alterações, torna público que, tendo em vista o que consta do **Processo SEI n.º 2021.015252,** fará realizar licitação, na modalidade **PREGÃO**, na forma **ELETRÔNICA, com critério de julgamento MENOR PREÇO POR LOTE (ÚNICO)**, em conformidade com o Ato PGJ n.º 389/2007; com a Lei nº 10.520, de 17/07/2002, com o **Decreto Federal n.º 10.024, de 20 de setembro de 2019**; Decreto nº 7892, de 23 de janeiro e 2013; com o Decreto Estadual n.º 24.818/2005, de 27/01/2005, e subsidiariamente com a Lei n.º 8.666, de 21 de junho de 1993 e suas alterações, e nos termos do art. 37, inciso XXI da Constituição Federal, mediante as condições estabelecidas neste Edital e anexos.

O contrato correspondente, ou o instrumento que vier a substituí-lo, será regido pela Lei n.º 8.666/93 e suas alterações.

PROCEDIMENTO SEI N.º 2021.015252
Recebimento das propostas: a partir da data de publicação do aviso no DOMPE.
Abertura das propostas: às 10 horas do dia **XX/XX/2022** (horário de Brasília).
Licitação Exclusiva para ME/EPP: (X) SIM ( ) NÃO
Endereço eletrônico: http://www.comprasgovernamentais.gov.br.
Código UASG: 925849

1. DAS DISPOSIÇÕES GERAIS

1.1. O pregão será realizado em sessão pública, por meio da utilização de recursos da tecnologia da informação – *internet*, utilizando-se, para tanto, de métodos de autenticação de acesso e recursos de criptografia, garantindo segurança em todas as fases do certame.
1.2. Os trabalhos serão conduzidos por servidor público integrante da **COMISSÃO PERMANENTE DE LICITAÇÃO** deste Órgão, por ato interno, denominado(a) PREGOEIRO(A), e membros da equipe de apoio, previamente credenciado no aplicativo http://www.comprasgovernamentais.gov.br.
1.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública, observarão rigorosamente o horário de **Brasília – DF**, e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

2. DO OBJETO

2.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para ***contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos.***

2.2. A licitação será em LOTE ÚNICO, composto de 4 (quatro) itens, conforme

especificações constantes no TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252:

LOTE	ITEM	DESCRIÇÃO	UND	QTDE
1	01	Serviço de Firewall em Alta Disponibilidade	Meses	48
	02	Serviço de Monitoramento da Solução	Meses	48
	03	Serviço de Migração do Ambiente Atual	Unidades	01
	04	Serviço de Treinamento da Solução	Pessoas	05

2.3. **Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão funcionar perfeitamente**, sem vícios, não constar em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os **softwares** comerciais deverão, ainda, ser instalados em sua **versão mais atualizada**, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o **hardware** a ser utilizado na prestação dos serviços deverá estar coberto por **garantia do fabricante, conforme descrição e demais especificações técnicas listadas no TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252, Anexo I deste Edital**, sob pena de ser recusado seu recebimento.

2.4. Os equipamentos deverão ser entregues na totalidade do(s) item(ns) constante(s) na nota de empenho, salvo nos casos de superveniência de fato excepcional ou imprevisível, alheio à vontade da contratada, solidamente justificada e demonstrada a causalidade entre o fato alegado e a impossibilidade de cumprimento do estabelecido neste, por meio de documentos comprobatórios hábeis, e expressamente autorizado pelo Fiscal do Contrato ou instrumento equivalente.

2.5. O critério de julgamento adotado será o **menor preço POR LOTE (ÚNICO)**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2.6. O objeto da futura contratação compreenderá, sobretudo, as especificações constantes do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252,** Anexo I deste Edital, sem prejuízo das demais prescrições figuradas no mencionado documento, bem assim na Minuta de Contrato Administrativo, Anexo II do Edital.

2.7. Os valores apresentados nos orçamentos e/ou propostas de preço deverão considerar inclusas todas as despesas relativas a frete, taxas, análises, amostras, impostos, licenças, encargos sociais, ou outras que possam influir direta ou indiretamente nos custos.

2.8. **Integra a presente licitação, como parte indissolúvel:**

a. Anexo I – TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;
b. Anexo II – Minuta de Contrato Administrativo;
c. Anexo III – Modelo de Declarações Complementares;
d. Anexo IV – Modelo de Proposta de Preços; e
e. Anexo V – Modelo de Solicitação de Cadastramento – SEFAZ/AM.

2.9. **VISTORIA TÉCNICA:** As empresas licitantes PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades do CONTRATANTE, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

2.9.1. As regras e demais disposições acerca da visita técnica encontra-se disciplinada no item 6 do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252.**

3. DOS RECURSOS ORÇAMENTÁRIOS

3.1. A despesa decorrente da contratação do objeto deste pregão, quando efetivada, deverá recair por conta dos recursos específicos consignados no orçamento da **PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS – PGJ/AM**. Programa 03.122.0001.2001.0001. Fonte 100, Elemento 339039.

4. DO CREDENCIAMENTO

4.1. As empresas interessadas em participar do certame deverão providenciar, previamente, o credenciamento perante a **SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO (SLTI), do MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO (MPOG)**, provedor do sistema eletrônico utilizado nesta licitação, no site http://www.comprasgovernamentais.gov.br, **por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.**

4.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave **de identificação e senha pessoal**, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento, regulamento e receber instruções detalhadas para sua correta utilização.

4.1.2. O credenciamento da licitante, bem como a sua manutenção, dependerá de registro cadastral atualizado no **SISTEMA DE CADASTRAMENTO UNIFICADO DE FORNECEDORES – SICAF**, em seu nível básico, que também será requisito obrigatório para fins de habilitação.

4.1.3. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS (entidade promotora da licitação) por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. É de responsabilidade do Cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.3.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

5. DAS CONDIÇÕES PARA PARTICIPAÇÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, legalmente constituídos, desde que atendam às condições exigidas deste Edital e seus Anexos, inclusive quanto à documentação exigida, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

5.1.1. **A licitante deverá declarar em campo próprio do sistema eletrônico a condição de microempresa ou empresa de pequeno porte**, para os fins previstos na Lei Complementar nº. 123/06.

5.1.1.1. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

5.2. O licitante deverá estar devidamente credenciado na **SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO – SLTI, do MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO**, através do site http://www.comprasgovernamentais.gov.br, **por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.**

5.3. O licitante deverá manifestar, **em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação**, e que sua proposta está em conformidade com as exigências do instrumento convocatório, nos termos do art. 21, parágrafo 2.º, do Decreto n.º 5.450/2005.

5.4. Será exigida do licitante **Declaração de Elaboração Independente de Proposta**, a qual será feita no campo do sistema ***Comprasnet*** destinado para tanto.

5.5. Todos os custos decorrentes da elaboração e apresentação de propostas serão de responsabilidade exclusiva da licitante, não sendo o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, em nenhum caso, responsável pelos mesmos, inclusive, pelas transações que forem efetuadas em nome do participante no Sistema Eletrônico ou por eventual desconexão.

5.6. **Não poderá participar,** direta ou indiretamente, desta licitação ou da execução dos serviços e do fornecimento de bens a eles necessários:

5.6.1. Os interessados que não atendam às condições deste Edital e seu(s) anexo(s);

5.6.2. As pessoas físicas e jurídicas que se enquadrem, em uma ou mais, das hipóteses elencadas no art. 9.º e seus incisos da Lei n.º 8.666/93;

5.6.3. As pessoas físicas e jurídicas que possuam sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e de sua **CPL**;

5.6.4. Empresa estrangeira não autorizada a funcionar no País e que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente

5.6.5. Interessado que se encontre em processo de Falência, Recuperação Judicial e Extrajudicial (conforme Lei nº. 11.101/05), salvo decisão judicial em contrário, concurso de credores, insolvência, dissolução, liquidação, fusão, cisão, incorporação, ou em regime de consórcio, qualquer que seja sua forma de constituição, salvo devidamente justificado;

5.6.6. Licitante que, por quaisquer motivos, tenha sido declarado inidôneo ou punido com suspensão e/ou impedimento de licitar e contratar por órgão da Administração Pública, Direta ou Indireta, Federal, Estadual, Municipal ou do Distrito Federal, desde que o ato tenha sido publicado na imprensa oficial ou registrado nos bancos de dados oficiais (SICAF e/ou outros), conforme o caso, pelo órgão que o praticou, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida sua reabilitação, consoante o art. 87, IV, da Lei 8.666/93;

5.6.7. Empresa que possua, em sua diretoria ou quadro técnico, funcionário público vinculado ao **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS ou à CPL;**

5.6.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

5.7. Como condição para participação no Pregão, a licitante assinalará "sim" ou "não" em campo próprio do Sistema eletrônico Comprasnet, relativo às seguintes declarações:

a) que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

a.1.) nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame;

a.2.) nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

b) que está ciente e concorda com as condições contidas no edital e seus anexos,
c) que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;
d) que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;
e) que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;
f) que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.
g) que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
h) que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

5.8. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste edital.

6. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, **exclusivamente por meio do sistema**, **concomitantemente com os documentos de habilitação** exigidos no edital, **proposta** com a descrição do objeto ofertado e o preço, **até a data e o horário estabelecidos para abertura da sessão pública (horário de Brasília), quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.**

6.1.1.

6.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

6.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

6.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

6.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6.8.1. Na proposta registrada no sistema, não deverá conter qualquer elemento que possa identificar a licitante, sob pena de desclassificação, sem prejuízo das sanções previstas nesse edital.

7. DO PREENCHIMENTO DA PROPOSTA

7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

7.1.1. Valor unitário e total do item;

7.1.2. Marca;

7.1.3. Fabricante;

7.1.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso, **sem identificação da licitante;**

7.1.4.1. Não serão aceitas propostas escritas contendo especificações que não contenham as informações necessárias à perfeita caracterização do objeto e suas especificidades, bem como especificações vagas, incompletas, ressalvado o subitem 7.6 deste Edital.

7.2. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

7.3. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

7.4. O **prazo de validade da proposta não será inferior** a **90 (noventa) dias**, a contar da data de sua apresentação.

7.5. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais ou estaduais, quando participarem de licitações públicas;

7.5.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a fiscalização do Tribunal de Contas do Estado do Amazonas e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7.6. O CNPJ da proponente, empresa cadastrada no SICAF e habilitada na licitação, deverá ser o mesmo para efeito de emissão das notas fiscais e posterior pagamento.

7.6. Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas, ou Anexos não solicitados, considerando-se que pelo preço proposto, a empresa obrigar-se-á a executar os serviços/entregar os produtos descritos neste edital.

7.8. Para efeito de elaboração das propostas, caso haja divergência entre a especificação contida neste edital e a no sistema SIASG, prevalecerá a descrita neste edital.

8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

8.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

8.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

8.2.1. Também será desclassificada a licitante que no momento do preenchimento do campo de ***"Descrição detalhada do objeto ofertado"*** no Sistema Comprasnet identifique sua empresa, o que não se confunde com a proposta inicial juntada ao Sistema e a proposta final/reajustada após convocação pelo Pregoeiro.

8.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

8.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

8.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.5.1. O lance deverá ser ofertado pelo valor total/unitário do item ou percentual de desconto.

8.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

8.7. O licitante somente poderá oferecer lance de **valor inferior** ao último por ele ofertado e registrado pelo sistema.

8.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,05 (cinco centavos).

8.9. O intervalo de tempo entre os lances enviados pelo mesmo licitante não poderá ser inferior a 20 (vinte) segundos e o intervalo entre lances não poderá ser inferior a 3 (três) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances (quando implementado).

8.10. Será adotado para o envio de lances no pregão eletrônico o modo de disputa **"ABERTO"**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.11. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

8.12. A prorrogação automática da etapa de lances, de que trata o item anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.13. **Não havendo novos lances** na forma estabelecida nos itens anteriores, a sessão pública **encerrar-se-á automaticamente.**

8.14. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

8.15. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia;

8.15.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

8.16. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

8.17. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada à identificação do licitante.
8.18. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
8.19. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.
8.20. O **Critério de Julgamento** adotado será o **menor preço POR LOTE (ÚNICO)**, conforme definido neste Edital e seus anexos.

8.20.1. Foi implementada regra e ferramenta no próprio Sistema Comprasnet que impede a aceitação pelo pregoeiro, na fase de negociação posterior à disputa de lances, de majoração (aumento) de preço unitário de item já definido na etapa de lances, pelo fornecedor, quer para os itens adjudicados individualmente, quer para os adjudicados em grupos. A alteração atende ao disposto no inciso XVII do art. 4° da Lei 10.520/2002 e ao Acórdão TCU 1872/2018.

8.21. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
8.22. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.
8.23. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.
8.24. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
8.25. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
8.26. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores,

será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.27. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances).

8.28. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

8.28.1. no País;

8.28.2. por empresas brasileiras;

8.28.3. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

8.28.4. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

8.29. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

8.30. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

8.30.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.30.2. O pregoeiro solicitará ao licitante melhor classificado que, no **prazo de 02 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

8.31. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

9. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

9.1. O pregoeiro solicitará ao licitante melhor classificado que, **no prazo máximo de 02 (duas) horas,** envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

9.2. Na proposta vencedora a ser enviada posteriormente deverá constar, conforme modelo do **Anexo IV**:

a) Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

a.1.) Não será admitido nos preços o fracionamento de centavo que ultrapassar duas casas decimais, desprezando-se sumariamente a fração remanescente;

a.2.) No preço deverão estar incluídas todas as despesas que influam no custo, tais como: impostos, transportes, seguros, taxas e outras despesas necessárias ao fornecimento dos materiais e à execução dos serviços correspondentes;

a.3.) Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

b) Prazo de validade da proposta de, no mínimo, **90 (noventa) dias corridos**, a contar da data de sua apresentação. As propostas que omitirem o prazo de validade serão entendidas como válidas pelo período supracitado;

c) Especificações claras, completas e minuciosas, com detalhes do objeto ofertado, inclusive marca, modelo, tipo e referência, no que couber, observadas as especificações mínimas e quantitativos contidos neste Edital e anexos;

d) A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

e) **Prazo entrega do plano de implementação:** Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

f) **Prazo início processo de migração/reunião alinhamento**: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;

g) **Prazo processo de migração**: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

h) Os seguintes dados da licitante: Razão Social, endereço, telefone/fax, número do CNPJ/MF, e-mail, se houver, Banco, agência, número da conta-corrente e praça de pagamento;

i) Nome, CNPJ ou CPF dos 3 (três) principais integrantes do quadro societário da licitante, assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade;

j) Contato para fins de faturamento: (indicar o nome, cargo, endereço, telefone, fax, e-mail de contato do responsável pelo recebimento das futuras notas de empenho);

k) Quando solicitada pelo Pregoeiro, **documentação técnica (manuais, catálogos ou prospectos)**, com as características detalhadas (marca, modelo, cor, tipo de material e

medidas) e imagens ilustrativas dos produtos propostos, que possibilitem a completa averiguação de conformidade com as especificações, visando facilitar a avaliação a ser realizada por técnicos deste Órgão.

9.3. As **Declarações Complementares**, referentes ao Anexo III do Edital, deverão ser efetuadas no momento da elaboração e envio da proposta pelos fornecedores, em seu próprio conteúdo ou documento apartado, sendo elas:

a) Declaração de cumprimento pleno dos requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.,** para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

b) Declaração expressa do licitante de que recebeu o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação (Anexo III);

c) Declaração, sob as penas da Lei, de que os documentos e declarações apresentados são fiéis e verdadeiros (Anexo III);

d) Declaração de que, caso seja vencedor do certame e não cadastrado no **SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhará a CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;

e) Declaração de que o preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

9.4. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato ou instrumento equivalente e aplicação de eventual sanção à Contratada, se for o caso.

9.4.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

9.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

9.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

10. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

10.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

10.1.1. A Proposta de Preços deverá ser apresentada conforme **Anexo IV**, constando dela todas as informações descritas no referido modelo, essenciais à avaliação pelo Pregoeiro.

10.1.2. A proposta e documentação, se necessário, será analisada pela equipe da **DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO – DTIC**, para fins de verificação do atendimento às características e exigências reclamadas no edital e anexos.

10.1.3. A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

10.2. **Serão desclassificadas as propostas que, ressalvado o disposto no subitem 5.7. deste Edital:**

10.2.1. Não atendam às exigências do edital e Anexos, sejam omissas ou apresentem irregularidades ou defeitos capazes de dificultar o julgamento;

10.2.2. Apresentar preço (global ou unitário) final superior ao preço máximo fixado pela Administração (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível, aplicando-se, subsidiariamente, as disposições previstas no parágrafo 1.º do artigo 48 da Lei n.º 8.666/93.

10.2.2.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

10.2.3. Também será desclassificada a licitante que no momento do preenchimento do campo de ***"Descrição detalhada do objeto ofertado"*** no Sistema Comprasnet identifique sua empresa, o que não se confunde com a proposta inicial juntada ao Sistema e a proposta final/reajustada após convocação pelo Pregoeiro.

10.3. A existência de **erros materiais ou omissões** nas propostas de preços das participantes não ensejará sua desclassificação antecipada.

10.3.1. Verificada a presença de erros sanáveis na proposta de preços, o Pregoeiro ou

Administração poderá realizar diligência junto à Licitante para a devida correção apenas das falhas apontadas, mediante apresentação de nova oferta, com desconto nunca inferior a **0,5% (cinco décimos percentuais) do valor total de sua última proposta, à exceção da primeira retificação que não necessitará de desconto, limitado a 3 (três) oportunidades, vedada a juntada de documentos novos.**

10.4. No que couber, se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta, **no prazo de 1 (um) dia útil, a contar da convocação pelo Pregoeiro**.

10.4.1. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

10.4.2. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas** de antecedência, e a ocorrência será registrada em ata;

10.5. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

10.6. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, **no prazo máximo de 02 (duas) horas, sob pena de não aceitação da proposta.**

10.6.1. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

10.6.2. Nas situações da compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos nos subitens acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de **05 (cinco) dias úteis contados da solicitação.**

10.6.2.1. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

10.6.2.2. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

10.6.2.3. No caso de não haver entrega da amostra ou havendo entrega de amostra fora das especificações previstas neste Edital, **a proposta do licitante será recusada.**

10.6.2.4. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

10.6.2.5. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

10.6.2.6. Após a divulgação do resultado final da licitação, as amostras entregues deverão ser recolhidas pelos licitantes no prazo de **10 (dez) dias corridos**, após o qual poderão ser descartadas ou incorporadas pela Administração, sem direito a ressarcimento.

10.6.2.7. Os licitantes deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.

10.7. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

10.8. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a sua continuidade.

10.9. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

10.9.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

10.9.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

10.10. No que couber, nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

10.11. **A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas neste edital e seus anexos, bem como, todas as especificações do objeto contidas na proposta vinculam a Contratada.**

10.12. Quando da proposta de preços não constar quaisquer dos prazos previstos, quer sejam os de garantia, validade dos produtos, validade da proposta ou de entrega, entender-se-á que estão aceitos os constantes do Edital.
10.13. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam as licitantes liberadas dos compromissos assumidos, podendo ser consultado acerca da manutenção dos preços ofertados.
10.14. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.
10.15. Sendo aceitável a proposta, o pregoeiro efetuará consulta "on-line" ao **sistema de Cadastramento Unificado de Fornecedores – SICAF**, para comprovar a regularidade do licitante.

10.15.1. Nos casos em que a habilitação exigir documentos que não estejam contemplados no SICAF, o pregoeiro solicitará do respectivo licitante o encaminhamento dos documentos de habilitação.

10.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

11. DA HABILITAÇÃO

11.1. Os documentos necessários à habilitação deverão estar com prazo vigente, à exceção daqueles que por sua natureza, não contenham validade, e poderão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de notas ou por servidor da CPL, ou por publicação em órgãos da imprensa oficial, **não sendo aceitos "protocolos" ou solicitação de documento** em substituição aos documentos requeridos neste edital.

11.1.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

11.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

11.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve

fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

11.1.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

11.1.2.3. No caso de impedimento indireto, o licitante será convocado para manifestação previamente à sua desclassificação.

11.1.3. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

11.1.4. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.2. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF **até o terceiro dia útil anterior à data prevista para recebimento das propostas;**

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

11.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **02 (duas) horas, sob pena de inabilitação.**

11.4. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

11.5. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.5.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a

centralização do recolhimento dessas contribuições.

11.6. Ressalvado o disposto no **subitem 6.3.**, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

11.7. Relativos à Habilitação Jurídica:

11.7.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.7.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio **www.portaldoempreendedor.gov.br;**

11.7.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada – EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

11.7.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

11.7.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

11.7.6. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

11.7.7. Os documentos relativos à Habilitação Jurídica indicados, deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.8. Relativo à Regularidade Fiscal e Trabalhista:

11.8.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

11.8.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.8.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.8.4. Prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

11.8.5. Prova de inscrição no cadastro de contribuintes Estadual e/ou Municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual, **ficando dispensada esta exigência, no caso de comprovação de regularidade prevista no subitem a seguir;**

11.8.6. Prova de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre, **afastando-se a necessidade de envio da inscrição prevista no subitem anterior;**

11.8.6.1. Caso o licitante seja considerado isento dos tributos estaduais/municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

11.8.7. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

11.8.8. A aceitação de certidões emitidas via internet ficará sujeita à confirmação de sua validade mediante consulta *on line* ao cadastro emissor respectivo.

11.9. Relativos à Qualificação Econômico-Financeira:

11.9.1. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, podendo ser apresentado de acordo com o Sistema Público de Escrituração Digital (SPED – Decreto Federal n.º 6.022/2007), que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

11.9.1.1 O Balanço apresentado deverá cumprir as seguintes formalidades: a) Indicação do número das páginas e números do livro onde estão inscritos o balanço patrimonial e a DRE (Demonstração do Resultado do Exercício) no Livro Diário. Além do acompanhamento do respectivo Termo de Abertura e Termo de Encerramento do mesmo; b) Assinatura do contador e do titular ou representante legal da empresa no balanço patrimonial e DRE (pode ser feita digitalmente); c) Prova de registro na Junta Comercial ou Cartório (devidamente carimbado, com etiqueta, chancela da Junta Comercial ou código de registro);

11.9.1.2. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

11.9.1.3. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

11.9.1.4. Quando solicitado ou autorizado pelo Pregoeiro, será permitido apresentação de balanço intermediário, desde que se decorra de lei ou contrato social/estatuto social da Licitante.

11.9.1.5. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

11.9.2. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar, considerados os riscos para a Administração, e, a critério da autoridade competente, o capital mínimo ou o patrimônio líquido mínimo 10% do valor estimado da contratação ou do item pertinente.

11.9.3. Certidões Negativas de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), expedida pela Central de Certidões do Tribunal de Justiça ou órgão equivalente do domicílio ou da sede do licitante, **expedida até 90 (noventa) dias antes da abertura desta licitação,** quando do documento não constar data expressa de validade;

11.9.3.1 Onde não houver **CENTRAL DE CERTIDÕES DO TRIBUNAL DE JUSTIÇA**, deverá ser apresentada Certidão emitida pela **SECRETARIA DO TRIBUNAL DE JUSTIÇA** ou órgão equivalente do domicílio ou da sede do licitante constando a quantidade de Cartórios Oficiais de Distribuição de Pedidos de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), devendo ser apresentadas Certidões expedidas na quantidade de cartórios indicadas no respectivo documento, no prazo referido no item 11.9.3;

11.9.3.2. Caso os prazos de validade não constem expressamente das certidões, serão considerados para esse fim, o prazo descrito no subitem 11.9.3. deste instrumento convocatório.

11.10. Relativos à Qualificação Técnica:

11.10.1. **Atestado(s) de Capacidade Técnica** fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a empresa licitante tenha prestado, a

contento, serviço de natureza e vulto compatíveis com o objeto deste instrumento, que permita(m) estabelecer, por comparação, proximidade de características funcionais técnicas, dimensionais, quantitativas e qualitativas, conforme Termo de Referência.

11.10.1.1. Entende-se como compatível o(s) atestado(s) de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem já ter prestado serviços de firewall (Next Generation Firewall), de forma satisfatória, com capacidade de tráfego (troughput) de, no mínimo, 10 (dez) Gbps, incluindo fornecimento de equipamento(s), serviço de instalação, treinamento, monitoramento e garantia de, no mínimo, 12 (doze) meses, similares ao objeto deste Termo.

11.10.1.2. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão(ões) deverá(ão) ser assinado(s) pelo responsável do setor competente do órgão;

11.10.1.3. No caso de pessoa jurídica de direito privado, o(s) atestado(s) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa.

11.10.1.4. A ausência de apresentação de atestado claro, legível e idôneo, em não conformidade com este Edital, tendo em vista o vulto da aquisição, será motivo de inabilitação, a critério do Pregoeiro.

11.11. Disposições Gerais da Habilitação:

11.11.1. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

11.11.2. Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos, o pregoeiro considerará o proponente **inabilitado**, sendo convocado outro licitante, observada a ordem de classificação, e assim **sucessivamente**, sem prejuízo das sanções legais cabíveis.

11.11.3. Sob pena de inabilitação os documentos apresentados deverão estar em nome da licitante, com o nº do CNPJ e o endereço respectivo, conforme segue:

11.11.3.1. se a licitante for a matriz, todos os documentos deverão estar em nome da matriz, e

11.11.3.2. se a licitante for a filial, todos os documentos deverão estar em nome da filial.

11.11.3.3. no caso dos subitens anteriores, serão dispensados da filial aqueles documentos que COMPROVADAMENTE, forem emitidos SOMENTE em nome da matriz, e vice-versa.

11.11.4. Caso os prazos de validade não constem expressamente das certidões apresentadas, será considerado para esse fim, o prazo descrito no subitem 11.9.3 deste instrumento convocatório.

11.11.5. Os originais das documentações habilitatórias, ou cópias autenticadas por meio de cartório competente, deverão ser encaminhados ao(à) pregoeiro(a), nos termos do subitem 11.13. do Edital.

11.11.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

11.12. **Havendo alguma restrição na comprovação da regularidade fiscal** para **microempresas e empresas de pequeno porte**, lhes será assegurado o prazo de **05 (cinco) dias úteis**, a contar do momento em que o licitante for declarado vencedor, prorrogáveis por igual período, **a requerimento da interessada e a critério da Administração Pública**, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa**.**

11.12.1. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

11.13. **Todos os documentos enviados eletronicamente deverão ser enviados em original, ou por cópia autenticada, devidamente assinado(s) pelo(s) representante(s) legal(is) no dia subsequente ao do resultado da habilitação**, impreterivelmente, **sob pena de desclassificação, observado o disposto no item 24.7 e subitens,** à Comissão Permanente de Licitação da Procuradoria-Geral de Justiça do Estado do Amazonas, Av. Coronel Teixeira, 7.995, Nova Esperança II, CEP: 69037-473.

11.13.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

11.14. Para fins de julgamento da habilitação no certame, considerar-se-á vigente o documento com prazo de validade, pelo menos, até a data de abertura da licitação.

11.15. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

11.16. Será inabilitado o licitante que não comprovar sua habilitação, deixar de apresentar quaisquer dos documentos exigidos para a habilitação, ou apresentá-los em desacordo

com o estabelecido neste Edital.

11.17. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.18. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

11.18.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

11.19. Atendidas as exigências habilitatórias fixadas neste Edital, o licitante será declarado **vencedor**, sendo-lhe adjudicado o objeto do certame, caso não haja interposição de recursos, encaminhando-se, em seguida os autos à autoridade competente para homologação.

11.20. Da sessão pública será lavrada ata circunstanciada, que mencionará todos os licitantes, a classificação dos lances, bem como as ocorrências que interessarem ao julgamento desta licitação.

12. DOS RECURSOS ADMINISTRATIVOS

12.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o **prazo de no mínimo 30 (trinta) minutos**, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

12.1.1. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

12.1.1.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

12.1.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito, cabendo o pregoeiro adjudicar o objeto da licitação à empresa licitante declarada vencedora.

12.2. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de **3 (três) dias corridos** para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros **3 (três) dias corridos**, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à

defesa de seus interesses.

12.2.1. Quando o prazo de interposição de Recursos Administrativos ou de Contrarrazões terminar em dia não útil, o prazo final será prorrogado para o primeiro dia útil subsequente.

12.3. A falta de manifestação imediata e motivada da licitante importará a decadência do direito de recurso e adjudicação do objeto pelo Pregoeiro à vencedora. Os recursos imotivados ou insubsistentes não serão recebidos.

12.3.1. Intenção motivada de recorrer é aquela que identifica, objetivamente, os fatos e o direito que a licitante pretende que sejam revistos pela autoridade superior àquela que proferiu a decisão

12.3.2. O não oferecimento de razões no prazo deste Edital fará deserto o recurso.

12.4. Os autos do processo permanecerão com vista franqueada aos interessados na **COMISSÃO PERMANENTE DE LICITAÇÃO**, Av. Coronel Teixeira n.º 7.995, Nova Esperança, Cep.: 69037-473, nos dias úteis, no horário das 8h. Às 14h. (horário local).

12.5. O recurso contra decisão do Pregoeiro terá **efeito suspensivo**.

12.6. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

12.7. Não serão providos recursos de **caráter protelatório**, fundada em mera insatisfação da licitante, podendo ainda ser aplicado, supletiva e subsidiariamente, no que couberem, as regras previstas na Lei n.º 13.105/2015 (Código de Processo Civil).

12.8. A alegação de preço inexequível por parte de uma das licitantes com relação à proposta de preços de outra licitante deverá ser devidamente comprovada.

12.9. A sessão pública do pregão somente será concluída após declarado o vencedor do certame e encerrado o prazo para manifestação de intenção de interposição de recurso, cabendo aos licitantes permanecerem conectados ao sistema até o final desta etapa.

12.10. Decididos os recursos, a autoridade competente fará a adjudicação do objeto da licitação ao licitante vencedor.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico ("chat") ou ainda, e-mail, de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

14.1. Não havendo recurso, de pronto, o Pregoeiro adjudicará o objeto do certame ao vencedor. Existindo recurso, após decisão, a autoridade competente adjudicará o objeto ao licitante vencedor.

14.1.1. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14.2. Homologado o resultado, o adjudicatário será convocado a comparecer, no prazo máximo de 5 (cinco) dias úteis, para celebrar o contrato ou retirar o instrumento equivalente, devendo manter as condições de habilitação exibidas na licitação.

14.2.1. Se o vencedor do certame não apresentar situação regular no ato da assinatura do contrato (ou retirada do instrumento equivalente), ou recusar-se a assiná-lo, ou sobrevier fato impeditivo de sua celebração, a sessão será retomada e os demais licitantes chamados, procedendo-se na forma do item 11.6.2, sem prejuízo das sanções cabíveis.

14.2.2. O vencedor do certame deverá apresentar ao órgão interessado, antes da assinatura do contrato (ou retirada do instrumento equivalente), nova proposta de preços escrita, com a devida recomposição dos custos unitários decorrentes da diminuição dos valores na fase de lances verbais, observado o subitem 8.7 deste Edital.

14.3. A homologação do resultado desta licitação não implicará direito à contratação.

15. DOS PRAZOS PARA A ENTREGA E DO RECEBIMENTO

15.1. A entrega dos serviços obedecerá às disposições do item 5 do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, sendo que após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

15.1.1. A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

15.1.2. A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

15.2. O recebimento dos serviços será realizado por servidores da ADQUIRENTE e

ocorrerá nos termos do item 9 do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252** e Cláusula Quinta da Minuta de Contrato (Anexo II).

16. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Garantia e Assistência Técnica ou emitido instrumento equivalente.

16.1.1. O adjudicatário terá o **prazo de 05 (cinco) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.1.1.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência eletrônica no e-mail constante da proposta, para que seja assinado eletronicamente pelo Sistema SEI ou aceito no prazo de 05 (cinco) dias, a contar da data de seu recebimento.

16.1.1.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

18.1.1.3. Nos termos do art. 6º do Decreto n º 40.674/2019, o termo contratual ou instrumento equivalente poderá ser assinado por certificação digital ou mediante assinatura eletrônica via Sistema Eletrônico de Informação - SEI, conforme disposição do ATO Nº 141/2017/PGJ;

16.1.1.3.1. O uso da senha de acesso ao Sistema Eletrônico de Informação - SEI é de **inteira** e **exclusiva responsabilidade da licitante**, incluindo qualquer acesso efetuado diretamente ou por seu representante, não cabendo ao **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, promotora da licitação, **qualquer responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.**

16.1.1.4. Para fins do atendimento do disposto no item anterior, antes da assinatura da Ata de Registro de Preços – ARP, será solicitado do representante da fornecedora o preenchimento de cadastro disponível no endereço eletrônico: https://sei.mpam.mp.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0 e envio dos seguintes documentos:

I – Documento de identidade;

II – Cadastro de Pessoa Física – CPF;

III – Comprovante de residência atualizado.

IV – Ato constitutivo e suas alterações, devidamente registrados; e

V – Ato de nomeação ou eleição de dirigentes ou procuração, quando for o caso, devidamente registrados.

16.1.1.5. Será dispensado da apresentação dos documentos referidos o representante que já os tiver enviado durante a sessão pública do pregão.

16.1.1.6. Ao assinar o termo contratual ou instrumento equivalente, a empresa adjudicatária obriga-se a fornecer/executar os bens/serviços a ela adjudicados, conforme especificações e condições contidas neste edital, em seus anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital;

16.2. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.2.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

16.2.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

16.2.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

16.3. A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

16.4. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.5. Na assinatura do contrato (instrumento equivalente) ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

16.6. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato (ou outro instrumento equivalente) ou a ata de registro de preços, a

Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação,

para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato (ou outro instrumento equivalente) ou a ata de registro de preços.

17. DAS OBRIGAÇÕES DA CONTRATADA

17.1. Além das obrigações compreendidas **nos itens 3, 5, 7 e 10 do TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, *Anexo I* a este Edital, bem como na Minuta do Termo de Garantia, *Anexo II*, serão também deveres da CONTRATADA:

17.1.1. Manter as condições de habilitação, como condição para emissão da nota de empenho, cuja confirmação será feita através de consulta ao SICAF ou através da internet nos respectivos sites dos órgãos emissores das certidões de regularidade fiscal.

17.2. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou recusar-se injustificadamente a receber a nota de empenho no prazo estabelecido, os demais licitantes serão convocados observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

17.2.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração.

17.3. A empresa deverá encaminhar, quando solicitado, via fax ou e-mail, banco, agência e número da conta-corrente, endereço, telefone e representante legal da empresa, com o nº do CNPJ e Inscrição Estadual ou Inscrição Municipal.

18. DAS OBRIGAÇÕES DA CONTRATANTE

18.1. As obrigações desta contratante constituem o **Item 11 do TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, *Anexo I* a este Edital.

19. DO PAGAMENTO

19.1. O pagamento resultante da contratação do objeto, será efetuado de acordo com este Edital, em consonância, também, com a proposta de preços aceita pela Administração.

19.2. O pagamento devido à CONTRATADA será creditado em conta-corrente por meio de ordem bancária, efetuado mediante apresentação de nota fiscal/fatura atestada e visada pelos órgãos de fiscalização e acompanhamento do fornecimento do material, no prazo não superior a 30 (trinta) dias, contados a partir do atesto da Administração na fatura apresentada.

19.2.1. As respectivas notas fiscais/faturas, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverão estar devidamente discriminadas, em nome da PROCURADORIA-GERAL DE JUSTIÇA, CNPJ n.º 04.153.748/0001-85, e acompanhada das respectivas Certidões Negativas de Débito para com a Seguridade Social, para com o Fundo de Garantia por Tempo de Serviço, junto à Justiça Trabalhista e, ainda, das certidões de regularidade junto à Fazenda Federal, Estadual e Municipal, conforme

descrito no link http://www.mpam.mp.br/servicos-sp-261893274/licitacoes/34-licitacoes/paginas-internas-licitacoes/2148-orientacaopagamentofornecedor;

19.2.2. Deverão constar das Notas Fiscais as especificações dos produtos, o número da Nota de Empenho e da Ata de Registro de Preços, conforme o caso;

19.2.3. Enquanto pendente de liquidação, por obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, nenhum pagamento será efetuado à Contratada, sem que isso gere direito a acréscimos de qualquer natureza.

19.3. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da CONTRATADA, importará prorrogação automática do prazo de vencimento da obrigação do Contratante.

19.4. Nenhum pagamento isentará o fornecedor das responsabilidades atinentes ao objeto contratual, nem tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

19.5. A nota fiscal (atestada) e os documentos exigidos no edital e no contrato (ou outro instrumento equivalente), para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, no Setor de Protocolo da CONTRATANTE.

19.6. Como condição para emissão da nota de empenho, a licitante vencedora deverá manter as mesmas condições de habilitação, cuja confirmação será feita através de consulta ao SICAF ou através da internet nos respectivos sites dos órgãos emissores das certidões de regularidade fiscal.

19.7. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou se recusar injustificadamente a recebê-la no prazo estabelecido, os demais licitantes serão convocados, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

19.7.1. **Como condição inafastável a que seja emitida Nota de Empenho à Fornecedora**, esta deverá, também, estar cadastrada junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores – da Secretaria da Fazendo do Estado do Amazonas – SEFAZ.

19.7.1.1. Com relação ao Cadastramento de Credores, a empresa deverá providenciar o envio dos documentos abaixo elencados ao órgão promotor da licitação (MPAM), durante o certame no próprio Sistema Comprasnet na fase de envio da proposta, quando convocado pelo Pregoeiro ou posteriormente após a adjudicação para o endereço eletrônico **licitacao@mpam.mp.br**, no prazo indicado no subitem anterior, sendo que naqueles primeiros momentos não serão motivos para sua desclassificação, todavia, poderá a vir responder a procedimento apuratório por eventual retardamento da licitação com possível aplicação das sanções previstas neste Edital, bem como perda do direito de preferência à contratação em favor dos demais licitantes subsequentes quando convocado posteriormente e deixar de atender no prazo fixado:

a) Carta solicitando o cadastramento (conforme Anexo V);
b) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;
c) Cópia legível dos dados bancários (por ex: extrato, cópia reprográfica de cartão bancário etc.).

20. DAS SANÇÕES ADMINISTRATIVAS

20.1. Comete infração administrativa, nos termos da Lei nº 10.520/2012, cumulada com aplicação de multa de 30% do valor total da proposta, o licitante/adjudicatário que:

20.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
20.1.2. não assinar a ata de registro de preços, quando cabível;
20.1.3. apresentar documentação falsa;
20.1.4. deixar de entregar os documentos exigidos no certame;
20.1.5. ensejar o retardamento da execução do objeto;
20.1.6. não mantiver a proposta;
20.1.7. cometer fraude fiscal;
20.1.8. comportar-se de modo inidôneo;

20.2. As sanções do item acima **também se aplicam aos integrantes do cadastro de reserva**, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente ou com justificativa recusada pela administração pública.

20.3. Considera-se comportamento inidôneo, entre outros, **a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes**, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

20.4. As sanções serão aplicadas pela **AUTORIDADE COMPETENTE**, em processo regular que assegure ao acusado o direito prévio da citação, do contraditório e da ampla defesa, com os recursos a ela inerentes.

20.5. A falta de regularização da documentação no prazo previsto no subitem 10.12. sujeitará a licitante à aplicação das sanções previstas neste edital.

20.6. As penalidades serão obrigatoriamente publicadas no Diário Eletrônico do Ministério Público do Estado do Amazonas e registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

20.7. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções aplicadas pela **AUTORIDADE COMPETENTE** poderá aplicar ao fornecedor as seguintes sanções:

20.7.1. **Advertência** por faltas leves, assim entendidas como aquelas que não

acarretarem prejuízos significativos ao objeto da contratação;

20.7.2. **Multas percentuais**, nos termos estabelecidos neste Edital;

20.7.3. **Suspensão de licitar e impedimento de contratar** com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

20.7.4. **Declaração de Inidoneidade** para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o CONTRATADO ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplica com base no item anterior.

20.7.5. **Impedimento de licitar e de contratar com o ESTADO DO AMAZONAS** e descredenciamento no SICAF, pelo prazo de até cinco anos;

20.8. Se a CONTRATADA, *sem justa causa*, não cumprir as obrigações assumidas ou infringir preceitos legais, serão aplicadas, segundo a gravidade da falta, as multas previstas no **item 12** do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252.**

20.9. As sanções de advertência, suspensão temporária de participar em licitação, impedimento de contratar com a Administração e declaração de inidoneidade para licitar ou contratar com a Administração Pública poderão ser aplicadas à CONTRATADA juntamente às de multa, as quais, por sua vez, **poderão ser descontadas dos pagamentos a serem efetuados.**

20.10. A inexecução total ou parcial do contrato enseja a sua rescisão pelos motivos legais.

20.11. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente.

20.11.1. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, o Estado ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

20.12. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias dos processos administrativos necessários à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

20.13. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

20.14. O processamento do PAR não interfere no seguimento regular dos processos

administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Estadual resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

20.15. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei Estadual nº 2.794, de 2003.

20.16. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

20.17. O fluxo procedimental quanto aos processos administrativos sancionadores no âmbito do Ministério Público do Estado do Amazonas está disciplinado no Ato PGJ n.º 187/2021 (publicado no DOMPE, Ed. 2170, de 12.07.2021).

21. DA REPACTUAÇÃO, REAJUSTE E REVISÃO DE PREÇOS

21.1. A interessada deverá protocolar o seu pedido de repactuação, reajuste e revisão de preços antes da assinatura da Ata de Registro de Preços ou de instrumento equivalente, **em até 5 (cinco) dias do recebimento da Nota de Empenho**, sob pena de não apreciação do pedido por intempestividade.

21.1.1. Deverá constar do pedido a planilha de custos e documentos comprovantes da situação superveniente, decorrente de caso fortuito ou de força maior.

21.1.2. A **CONTRATADA** deverá demonstrar de maneira clara a composição do preço de cada item constante de sua proposta, através de Planilha de Custos contendo, por exemplo: as parcelas relativas à mão de obra direta, demais insumos, encargos em geral, lucro e participação percentual em relação ao preço final.

21.2. A não-apresentação da planilha de custos impossibilitará o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** de proceder o reequilíbrio, reajuste ou revisão de preços, caso venha a empresa contratada solicitar qualquer uma dessas alterações no contrato (ou outro instrumento equivalente).

21.3. A cada pedido de reequilíbrio, reajuste ou revisão de preço, deverá a contratada comprovar e justificar as alterações havidas na planilha apresentada à época da elaboração da proposta, demonstrando a nova composição do preço.

21.4. No caso do detentor do registro de preços/contratado ser revendedor ou representante comercial deverá demonstrar de maneira clara a composição do preço constante de sua proposta, com descrição das parcelas relativas ao valor de aquisição do produto com notas fiscais de fábrica/indústria, encargos em geral, lucro e participação percentual de cada item em relação ao preço final (*planilha de custos*).

21.5. **A critério do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, poderá ser exigido da contratada, listas de preços expedidas pelos fabricantes, que conterão,

obrigatoriamente, a data de início de sua vigência e numeração sequencial, para instrução de pedidos de revisão de preços.

21.6. Na análise do pedido de reequilíbrio, reajuste ou revisão, dentre outros critérios, o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** adotará, para verificação dos preços constantes dos demonstrativos que acompanhem o pedido, pesquisa de mercado dentre empresas de reconhecido porte mercantil, produtoras e /ou comercializadoras, a ser realizada pela própria unidade ou por instituto de pesquisa, utilizando-se, também, de índices setoriais ou outros adotados pelo Governo Estadual, devendo a deliberação de deferimento ou indeferimento da alteração solicitada ser instruída com justificativa da escolha do critério e memória dos respectivos cálculos, para decisão da Administração.

21.7. O percentual de diferença entre os preços de mercado vigentes à época do julgamento da licitação, devidamente apurado, e os propostos pela CONTRATADA/Detentora do registro de preços será mantido durante toda a vigência do registro. O percentual não poderá ser alterado de forma a configurar reajuste econômico durante a vigência deste registro.

21.8. A repactuação, reajuste ou revisão do preço, caso deferido, somente terá validade a partir da data da publicação da deliberação na Imprensa Oficial.

21.9. **É vedado à contratada interromper o fornecimento ou a prestação do serviço enquanto aguarda o trâmite do processo de reequilíbrio, reajuste ou revisão de preços, estando, neste caso, sujeita às sanções previstas neste Edital.**

21.10. A repactuação, reajuste ou revisão levará em consideração preponderantemente as normas legais federais e estaduais, que são soberanas à previsão do conteúdo exposto neste item.

22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

22.1. Até o dia **xx/xx/2021, 03 (três) dias úteis antes da data designada para a abertura da sessão pública**, qualquer pessoa poderá impugnar este Edital, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.2. A impugnação poderá ser realizada por forma eletrônica (preferencialmente), pelo e-mail **licitacao@mpam.mp.br**, no horário local de expediente da Instituição, até às 14 horas (horário local) da data limite fixada ou por petição dirigida ou protocolada no endereço constante do Rodapé, endereçado à Comissão Permanente de Licitação.

24.3. Caberá ao Pregoeiro decidir sobre a impugnação, **no prazo de até 02 (dois) dias úteis contados da data de recebimento da petição**, prorrogáveis desde que devidamente justificado, limitado ao dia anterior à data prevista de abertura, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos Anexos.

22.4. Acolhida a impugnação ou determinadas as providências requeridas, será designada nova data para realização da sessão pública, salvo quando estas não afetarem a formulação das propostas.

22.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, **até o dia xx/xx/2021, 03 (três) dias úteis anteriores à data designada para abertura da sessão pública**, no horário local de expediente da Instituição (até às 14 horas – horário local), preferencialmente por meio eletrônico via internet ou no endereço indicado no rodapé do Edital, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.6. O pregoeiro responderá aos pedidos de esclarecimentos **no prazo de até 02 (dois) dias úteis contados da data de recebimento do pedido**, prorrogáveis desde que devidamente justificado, limitado ao dia anterior à data prevista de abertura, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos Anexos.

22.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

22.7.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

22.8. Os pedidos de impugnações e esclarecimentos, bem como as respectivas respostas, serão divulgados no site http://www.comprasgovernamentais.gov.br, na área Gestor Público/consultas/pregões/agendados (http://comprasnet.gov.br/acesso.asp?url=/livre/Pregao/lista_pregao_filtro.asp?Opc=0) e no **site oficial do MPAM**. O fornecedor, além do acesso livre, poderá visualizar também no menu principal, no link: "visualizar impugnações /esclarecimentos/avisos".

22.9. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

23. DAS DISPOSIÇÕES FINAIS

23.1. A **COMISSÃO PERMANENTE DE LICITAÇÃO** prestará todos os esclarecimentos solicitados pelos interessados nesta licitação, estando disponível para atendimento de segunda a sexta-feira, das 8 às 14 horas, na Av. Coronel Teixeira, 7.995, Nova Esperança, Manaus – AM, pelos telefones (92) 3655-0701, (92) 3655-0743 ou, ainda, pelo e-mail: **licitacao@mpam.mp.br**.

23.2. A **Autoridade Competente** designará o pregoeiro que conduzirá esta licitação, necessariamente escolhido dentre os Pregoeiros Oficiais do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.3. É facultada ao pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

23.3.1. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

23.3.2. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o subitem anterior, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas de antecedência**, e a ocorrência será registrada em ata.

23.4. A **Autoridade Competente** para determinar a contratação poderá revogar a licitação por razões de interesse público derivado de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

23.4.1. No caso de revogação ou anulação do procedimento licitatório, ficará assegurada oportunidade de ampla e prévia manifestação dos interessados, na forma da Lei.

23.4.2. A anulação pode ser declarada a qualquer tempo.

23.4.3. As licitantes não terão direito a indenização em decorrência de anulação do procedimento licitatório, ressalvado o direito do FORNECEDOR de boa-fé de ser ressarcida pelos encargos que tiver suportado em eventual cumprimento da obrigação decorrente da execução do objeto deste certame.

23.5. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.6. Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro, sob pena de abertura de procedimento apuratório em face da conduta do licitante.

23.7. Em caso de licitante vencedor sediado fora da cidade de Manaus, cujo envio de documentos e demais solicitações ensejem utilização de serviços postais, **será obrigatória a apresentação de cópia do comprovante de envio dos itens solicitados, como forma de confirmação do atendimento aos prazos previstos em cada subitem**.

23.7.1. O comprovante poderá ser enviado para o e-mail: licitacao@mpam.mp.br**.**

23.7.2. **O descumprimento dos prazos para envio dos documentos ou demais solicitações, sem apresentação de justificativa, ensejará a desclassificação da empresa licitante, sem prejuízo das sanções cabíveis.**

23.7.3. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

23.7.3.1. Os documentos eletrônicos produzidos com a utilização de processo de

certificação disponibilizada pela ICP-Brasil, nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

23.8. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

23.9. Fazem parte deste Edital os seguintes Anexos:

1. Anexo I – TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;
2. Anexo II – Minuta de Contrato Administrativo;
3. Anexo III – Modelo de Declarações Complementares;
4. Anexo IV – Modelo de Proposta de Preços; e
5. Anexo V – Modelo de Solicitação de Cadastramento – SEFAZ/AM.

23.10. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente normal no **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.**

23.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

23.12. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

23.13. Quando todos os licitantes forem inabilitados ou todas as propostas forem desclassificadas, o Pregoeiro poderá fixar aos licitantes o prazo de **3 (três) dias úteis** para apresentar nova documentação, ou nova proposta, escoimadas das causas que ensejaram a inabilitação ou desclassificação das empresas.

23.14. Nenhuma pessoa física ou jurídica ainda que credenciada poderá representar mais de uma empresa concorrente, sob pena de não participação das empresas representadas.

23.15. A homologação do resultado desta licitação não implicará direito à contratação.

23.16. Em substituição aos respectivos originais, todos os documentos poderão ser apresentados em cópia autenticada por Cartório competente ou conferida com o original por servidor da CPL. **Neste último caso, a autenticação administrativa poderá ser feita, preferencialmente, até o dia anterior à data prevista para o recebimento dos envelopes da Proposta e da Documentação**;

23.16.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

23.17. Somente serão aceitos propostas e lances encaminhados pelo sistema eletrônico.
23.18. É de inteira responsabilidade do licitante o acompanhamento do processo referente a este pregão eletrônico, no endereço eletrônico **http://www.comprasgovernamentais.gov.br**.
23.19. Para as demais condições de contratação, observar-se-ão as disposições constantes dos Anexos deste Edital.
23.20. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital, assim como no caso de divergências entre os lançamentos no Sistema COMPRASNET, prevalecerá o Edital.
23.21. Este Edital e seus Anexos poderão ser examinados sem ônus para o interessado, antes da realização da licitação, no formato eletrônico, através de consulta aos sítios **http://www.comprasgovernamentais.gov.br** e www.mpam.mp.br, ou através do correio eletrônico da CPL, licitacao@mpam.mp.br.

23.21.1. Poderão ser, também, adquiridos impressos mediante depósito da quantia referente ao custo reprográfico, calculado no produto de R$ 0,20 (vinte centavos) por página, depositado na conta-corrente n.º 13200-4, Agência 6019-4, do Banco Bradesco S/A (237), em nome do **FUNDO DE APOIO DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.**

23.22. Os casos omissos serão resolvidos pelo Pregoeiro, com base no Ato PGJ n.º 389/2007, na Lei n.º 10.520, de 17/07/2002, no Decreto Estadual n.º 21.178, de 27/09/2000, e, subsidiariamente, na Lei n.º 8.666/93 e alterações.
23.23. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas no foro da cidade de Manaus, com exclusão expressa de qualquer outro.

Manaus AM, xx de janeiro de 2022.

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

ANEXO I
TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252

ANEXO II
MINUTA DO CONTRATO ADMINISTRATIVO

MINUTA DE EDITAL DO PREGÃO ELETRÔNICO N.º 4.0__/2022-CPL/MP/PGJ

ANEXO III

MODELO DE DECLARAÇÕES COMPLEMENTARES

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.**, para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;
2. Os documentos e declarações apresentados são fiéis e verdadeiros, bem como que a empresa recebeu o Edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;
3. Estou ciente da obrigação de, caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhar os documentos necessários à CONTRATANTE, a fim de efetuar o referido cadastramento no prazo de cinco dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;
4. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

(Cidade-UF),_____ de _____ de 2022.

RAZÃO SOCIAL/CNPJ DA EMPRESA
Representante Legal

MINUTA DE EDITAL DO PREGÃO ELETRÔNICO N.º 4.0__/2022-CPL/MP/PGJ

ANEXO IV
MODELO DE PROPOSTA DE PREÇOS

Proposta que faz a empresa _____, inscrita no CNPJ (MF) nº _____, localizada _____, na cidade de _____, CEP _____, fone _____, fax _____, e-mail _____, para a prestação do serviço abaixo relacionado, de acordo com todas as especificações e condições estabelecidas no **Pregão Eletrônico n.º 4.0XX/2022-CPL/MP/PGJ**, promovido pelo Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça:

PLANILHA DE FORMAÇÃO DE PREÇOS

LOTE ÚNICO					
ITEM	**ESPECIFICAÇÃO**	**UNIDADE**	**QTD**	**VALOR UNITÁRIO (R$) (B)**	**VALOR TOTAL (R$) (A * B)**
1	Serviço de Firewall em Alta Disponibilidade	Meses	48		
2	Serviço de Monitoramento da Solução	Meses	48		
3	Serviço de Migração do Ambiente Atual	Unidade	1		
4	Serviço de Treinamento da Solução	Pessoas	5		
VALOR TOTAL DA PROPOSTA = R$ (por extenso)					

A _____(*nome da empresa*)_____ declara que concorda com todas as especificações do Edital.

a) **Prazo de validade da proposta**: _____
b) **Prazo entrega do plano de implementação:** Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.
c) **Prazo início processo de migração/reunião alinhamento**: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;
d) **Prazo processo de migração**: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.
e) **Dados Bancários**: (*indicar o nome e número do banco, nome e número completo da agência e número da conta-corrente*);
f) **Contato para fins de faturamento**: *(indicar o nome, cargo, endereço, telefone, fax, e-mail de contato do responsável pelo recebimento das futuras notas de empenho).*
g) **Dados dos 3 (três) principais integrantes do quadro societário da licitante**, assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade.

Nome: _____
CNPJ ou CPF: _____

DECLARAÇÕES:

1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.**, para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do **Ministério Público do Estado do Amazonas** e de sua **CPL;**
2. Os documentos e declarações apresentados são fiéis e verdadeiros, bem como que a empresa recebeu o Edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;
3. Estou ciente da obrigação de, caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhar os documentos necessários à CONTRATANTE, a fim de efetuar o referido cadastramento no prazo de cinco dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes

subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;

4. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

Local e data:

(*assinatura*)
(*nome do representante legal pela empresa*)
(*CPF do representante legal*)

MINUTA DE EDITAL DO PREGÃO ELETRÔNICO N.º 4.0__/2022-CPL/MP/PGJ

ANEXO V
MODELO DE SOLICITAÇÃO DE CADASTRAMENTO – SEFAZ/AM

(*cidade*), ____ de _____ de _____

À
Diretoria de Orçamento e Finanças
Procuradoria-Geral de Justiça do Estado do Amazonas
Av. Coronel Teixeira, 7995 – Nova Esperança
69037-473 MANAUS/AM

A empresa (*informar a razão social, CNPJ e endereço*) solicita a esse Setor o seu cadastro no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE – CADASTRAMENTO DE CREDORES – dessa **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ.**

Assim sendo, acompanha esta carta de solicitação de cadastramento a documentação abaixo listada, exigida para a efetivação do registro:

a) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

b) Cópia legível do comprovante (por ex: extrato, cópia reprográfica de cartão bancário, etc.) dos seguintes dados bancários:

Banco: _____
Agência: _____
Conta: _____

Razão Social e CNPJ da empresa
Nome completo e CPF do Representante Legal

DESPACHO Nº 4.2022.CPL.0753490.2021.015252

Objeto: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

Trata-se dos autos do procedimento interno em epígrafe, versando sobre o objeto de referência, instruído por solicitação formalizada através do **OFÍCIO Nº 108.2021.DTIC.0692180.2021.015252**, exarado pelo Sr. **Tadeu Azevedo de Medeiros**, Diretor(a) de Tecnologia de Informação e Comunicação - DTIC, datado de 24/09/2021.

O detalhamento do objeto foi realizado, inicialmente, por intermédio do **TERMO DE REFERÊNCIA Nº 13.2021.DTIC.0691989.2021.015252**, o qual foi analisado pela Assessoria Jurídica, via **PARECER Nº 118.2021.01AJ-SUBADM.0711353.2021.015252**, e aprovado pelo Exmo. Sr. Subprocurador-Geral de Justiça para Assuntos Administrativos, Ordenador de Despesas, via **DESPACHO Nº 484.2021.01AJ-SUBADM.0711354.2021.015252**, após o que foram os autos remetidos ao **SETOR DE COMPRAS E SERVIÇOS – SCS**, em 18/10/2021, para providências.

Nesse ínterim, o Setor demandante (DTIC) emitiu novo **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, devidamente encaminhado via **MEMORANDO Nº 148.2021.DTIC.0720865.2021.015252**, datado de 08/11/2021.

Tendo aquele setor colhido pesquisa de mercado aos autos, emitiu-se, em 24/11/2021, o **MAPA DEMONSTRATIVO DE PREÇOS Nº 130.2021.SCOMS.0731238.2021.015252** e, posteriormente, o **QUADRO - RESUMO DO PROCESSO DE COMPRA Nº 345.2021.SCOMS.0731246.2021.015252**, subsidiando, por sua vez, a elaboração da **NOTA DE AUTORIZAÇÃO DE DESPESAS/ADJUDICAÇÃO - NAD Nº 375.2021.DOF - ORÇAMENTO.0744829.2021.015252,** chancelada pelo Ordenador de Despesas em 10/01/2022.

Na sequência, vieram os autos a esta CPL no dia 10/01/2022. Porém, em análise perfunctória, considerou-se, conforme a descrição do objeto no **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, a possível necessidade de confecção de minuta de contrato, encaminhando, portanto, os autos à **DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON**, mediante **MEMORANDO Nº 13.2022.CPL.0749455.2021.015252**, em 11/02/2022, para análise e providências.

Por sua vez, a **DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON** juntou ao autos a Minuta de **CONTRATO ADMINISTRATIVO** (doc. 0750392), retornando os autos a esta Comissão em 14/01/2022.

Retornando os autos nesta CPL, considerando as nuances do caso, bem como a necessidade de assegurar a boa contratação e prover-se dos instrumentos necessários para seleção da melhor proposta à Administração, esta CPL confeccionou **MINUTA DE EDITAL DE PREGÃO ELETRÔNICO** (doc. 0753486), **cujo critério de seleção é pelo menor preço POR LOTE (ÚNICO).**

Sendo assim, **encaminhem-se os autos** do Processo em epígrafe à **SUBPROCURADORIA GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, a fim de cumprir o disposto no parágrafo único do artigo 38 da Lei n.º 8.666/93 e art. 37, *caput* da Constituição Federal, quanto à emissão do parecer jurídico e posterior aprovação pela Ordenadora de Despesas da **MINUTA DE CONTRATO ADMINISTRATIVO** (doc. 0750392) e **MINUTA DE EDITAL** (doc. 0753486).

Manaus, 19 de JANEIRO de 2022.

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ nº 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 19/01/2022, às 10:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0753490** e o código CRC **A06F55A7**.

PARECER Nº 1.2022.01AJ-SUBADM.0754777.2021.015252

Autos nº 2021.015252

Assunto: Contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual.

PROCEDIMENTO LICITATÓRIO. ANÁLISE DA MINUTA DE EDITAL E DA MINUTA DE CONTRATO. PREGÃO ELETRÔNICO. DEFINIÇÃO DO CRITÉRIO DE JULGAMENTO, MENOR PREÇO GLOBAL. Reputa-se adequada a modalidade selecionada para a contratação pretendida pela Administração – Pregão Eletrônico, do tipo menor preço por lote único –, uma vez que atende aos ditames legais e se afigura compatível com o conceito de "serviço comum", dado que o objeto dos autos teve seus padrões objetivamente definidos por especificações usuais no mercado, em consonância com o disposto no já transcrito parágrafo único do art. 1.° da Lei n.° 10.520/02. Em tempo, os itens a serem adquiridos encontram-se devidamente esmiuçados no item 2 do edital - Do Objeto. Quanto à Minuta do Contrato, verifica-se que todos os elementos contratuais necessários a respaldar com segurança a avença encontram-se presentes. Inteligência das Leis nºs 8.666/93 e 10.520/02 e do Decreto nº 3.555/00. Aprovação das Minutas de Edital e do Contrato.

Retornam os autos do procedimento deflagrado para viabilizar a contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual, desta vez para análise jurídica das minutas de contrato e edital que subsidiarão a realização da competente licitação.

O Termo de Referência 20 (0720733) foi devidamente aprovado - vide Parecer 118 (0711353) e Despacho 484 (07113524), incluindo-se, ainda, ajustes indicados pela *Chefia do Setor de Infraestrutura e Telecomunicações,* via memorando 148 (0720865).

O Setor de Compras e Serviços - SCOMS providenciou a emissão do Mapa Demonstrativo de Preços **130** (0731238), após pesquisa de mercado. Por corolário, juntou-se aos autos o Quadro-Resumo do Processo de Compra 345 (0731246), bem como a Nota de Autorização de Despesas/Adjudicação - NAD 375 (0744829).

Minutas do Contrato (0750392) e Minuta de Edital (0753486) devidamente acostadas aos autos.

A Comissão Permanente de Licitação - CPL, por intermédio do Despacho 4 (0754777), encaminhou os autos à SUBADM para fins de cumprimento do disposto no parágrafo único do artigo 38 da Lei n.º 8.666/93 e art. 37, *caput* da Constituição Federal, quanto à emissão do parecer jurídico e posterior aprovação pelo Ordenador de Despesas.

É o breve relatório. OPINO.

Tendo em conta a prévia aprovação do Termo de Referência 20 (0720733), passo a analisar a Minuta de

Edital (0753486) e de seus anexos II (Minuta de Contrato), III (modelo de declarações complementares), IV (modelo de proposta de preços) e V (modelo de solicitação de cadastramento - SEFAZ/AM).

Conforme dispõe o art. 37, XXI, da Constituição Federal, a Administração Pública deverá sempre observar o cumprimento do regime jurídico-administrativo, razão pelo qual a deflagração do procedimento licitatório constitui-se **como regra**. Segundo a melhor doutrina, a licitação caracteriza-se por ser um procedimento prévio de seleção, por meio do qual a Administração, mediante critérios previamente estabelecidos, busca escolher a melhor alternativa para a celebração de um Contrato Administrativo ou instrumento equivalente.

De acordo com o art. 4º, da Lei n.º 8.666/1993, todos os participantes de um certame têm direito público subjetivo à fiel observância do pertinente procedimento estabelecido pela Lei, podendo qualquer cidadão acompanhar o seu desenvolvimento, desde que não interfira de modo a perturbar ou impedir a realização dos trabalhos.

Nesse diapasão, insta ressaltar que o ordenamento jurídico pátrio dispõe que a Administração Superior deverá iniciar o certame com uma fase interna, que segundo MATHEUS CARVALHO (*in* Manual de Direito Administrativo. 4ª ed. Salvador: JusPodivm, 2019, p. 467), acontece quando: a "*Administração Pública está, internamente, se organizando para licitar, com a abertura do processo administrativo respectivo e com a realização dos atos preparatórios que justifiquem a realização do certame. O texto legal define requisitos a serem observados para início do procedimento*".

A Lei Federal nº 10.520/02, instituiu o Pregão como modalidade de licitação tendente à aquisição de "bens ou serviços comuns", definidos como aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado. Nesse sentido, estabelece o parágrafo único do art. 1º da referida lei:

> Art. 1º Para aquisição de bens e serviços comuns, poderá ser adotada a licitação na modalidade de pregão, que será regida por esta Lei.
>
> Parágrafo único. Consideram-se bens e serviços comuns, para os fins e efeitos deste artigo, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

Na realidade, a norma, ao restringir o âmbito de aplicação do Pregão, objetiva viabilizar a realização de um procedimento mais simples para aquisição de bens e serviços razoavelmente padronizados, possibilitando à Administração negociar o melhor preço, sem comprometer a viabilidade da proposta.

Dessa maneira, em observância aos preceitos legais acima mencionados, reconheço como **adequada** a modalidade selecionada para a contratação pretendida pela Administração – **Pregão Eletrônico**, do tipo **menor preço por lote único** –, uma vez que atende aos ditames legais e se afigura compatível com o conceito de "serviço comum", dado que o objeto dos autos teve seus padrões objetivamente definidos por especificações usuais no mercado, em consonância com o disposto no já transcrito parágrafo único do art. 1.° da Lei n.° 10.520/02. Em tempo, os itens a serem adquiridos encontram-se devidamente esmiuçados no item 2 do edital - Do Objeto.

O art. 21 do Decreto n° 3.555/00, elenca todos os atos essenciais a realização do Pregão nos seguintes termos:

> Art. 21. Os atos essenciais do pregão, inclusive os decorrentes de meios eletrônicos, serão documentados ou juntados no respectivo processo, cada qual oportunamente, compreendendo, sem prejuízo de outros, o seguinte:
>
> I - justificativa da contratação;
>
> II - termo de referência, contendo descrição detalhada do objeto, orçamento estimativo de custos e cronograma físico-financeiro de desembolso, se for o caso;
>
> III - planilhas de custo;
>
> IV - garantia de reserva orçamentária, com a indicação das respectivas rubricas;
>
> V - autorização de abertura da licitação;

VI - designação do pregoeiro e equipe de apoio;

VII - parecer jurídico;

VIII - edital e respectivos anexos, quando for o caso;

IX - minuta do termo do contrato ou instrumento equivalente, conforme o caso;

X - originais das propostas escritas, da documentação de habilitação analisada e dos documentos que a instruírem;

XI - ata da sessão do pregão, contendo, sem prejuízo de outros, o registro dos licitantes credenciados, das propostas escritas e verbais apresentadas, na ordem de classificação, da análise da documentação exigida para habilitação e dos recursos interpostos; e

XII - comprovantes da publicação do aviso do edital, do resultado da licitação, do extrato do contrato e dos demais atos relativos a publicidade do certame, conforme o caso.

No mais, como sabido, o Edital é o instrumento convocatório do certame, além de ser indispensável para o regular andamento do processo de licitação e vincular os licitantes e a Administração Pública. Cabe ao Edital e seus anexos dispor acerca das condições e regras de habilitação, critérios de julgamento, bem como definir as penalidades a serem cominadas, a forma de pagamento, dentre outros aspectos. Assim, em suma, cumpre-lhe atribuir mecanismos que assegurem e promovam a máxima competitividade e a igualdade entre os licitantes, de maneira que o resultado do certame seja o mais efetivo e legítimo aos interesses da Administração Pública.

In casu, considero presentes todos os elementos obrigatórios desse instrumento, em conformidade com o disposto no inciso III do art. 4º da Lei n° 10.520/02; no art. 40 da Lei n° 8.666/93, naquilo que é cabível e; no âmbito interno, no art. 7º do Ato PGJ nº 389/07 (regulamenta o Pregão Presencial e Eletrônico).

Quanto à Minuta de Contrato Administrativo (0750392), elaborada pela Divisão de Contratos e Convênios - DCCON, tem-se que, de acordo com a dicção legal do art. 54, da Lei n.º 8.666/1993, os contratos administrativos serão regulados por suas cláusulas e pelos preceitos de direito público, aplicando-se-lhes, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado.

O art. 55 da Lei n. 8.666/03, elenca as seguintes cláusulas necessárias para celebração de uma avença sob o regime de direito público:

Art. 55. São cláusulas necessárias em todo contrato as que estabeleçam:

I - o objeto e seus elementos característicos;

II - o regime de execução ou a forma de fornecimento;

III - o preço e as condições de pagamento, os critérios, data-base e periodicidade do reajustamento de preços, os critérios de atualização monetária entre a data do adimplemento das obrigações e a do efetivo pagamento;

IV - os prazos de início de etapas de execução, de conclusão, de entrega, de observação e de recebimento definitivo, conforme o caso;

V - o crédito pelo qual correrá a despesa, com a indicação da classificação funcional programática e da categoria econômica;

VI - as garantias oferecidas para assegurar sua plena execução, quando exigidas;

VII - os direitos e as responsabilidades das partes, as penalidades cabíveis e os valores das multas;

VIII - os casos de rescisão;

IX - o reconhecimento dos direitos da Administração, em caso de rescisão administrativa prevista no art. 77 desta Lei;

X - as condições de importação, a data e a taxa de câmbio para conversão, quando for o caso;

XI - a vinculação ao edital de licitação ou ao termo que a dispensou ou a inexigiu, ao convite e à proposta do licitante vencedor;

XII - a legislação aplicável à execução do contrato e especialmente aos casos omissos;

XIII - a obrigação do contratado de manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

No mesmo sentido, manifesta-se a Corte Federal de Contas ao se referir ao dever da Administração de observar os requisitos do contrato:

Observe a necessidade de apresentação de cláusulas contratuais específicas e precisas, sobretudo quanto

à definição do objeto da avença, do preço acordado, do tempo de execução e da atualização monetária do negócio jurídico, vedada a possibilidade de sub-rogação do pacto, conforme exigem os arts. 40, incisos XI e XIV, alíneas 'c' e 'd', 54, 55, caput, inciso III, 56, 61, 72 e 78, inciso VI, todos da Lei nº 8.666/1993. (ACÓRDÃO 1837/2009, PLENÁRIO).

Defina o objeto de forma precisa, suficiente e clara, não se admitindo discrepância entre os termos do edital, do termo de referência e da minuta de contrato, sob pena de comprometer o caráter competitivo do certame, em atendimento aos arts. 3º, inciso II, e 4º, inciso III, da Lei nº 10.520/2002 c/c art. 8º, inciso I do Decreto nº 3.555/2000. (ACÓRDÃO 531/2007, PLENÁRIO).

Especificamente, encontram-se previstos, *inter alia*, os prazos e condições de entrega e prestação dos serviços de firewall de próxima geração em alta disponibilidade, bem como fornecimento de equipamento de informática descrito no Termo de Referência por parte do contratado; as providências de instalação, bem como as exigências de garantia e de serviço, manutenções programadas, resolução de eventuais problemas e falhas, além das demais cláusulas gerais (gestão e fiscalização, obrigações da contratada e da contratante, liquidação e pagamento, vigência, penalidades, etc), tudo em conformidade com o que determina a Lei Licitatória e com as necessidades deste Ministério Público. Assim, ao examinar a minuta acostada, verifica-se que todos os elementos contratuais necessários a respaldar com segurança a avença encontram-se presentes.

No mais, os demais anexos do edital - Anexos III (modelo de declarações complementares), IV (modelo de proposta de preços) e V (modelo de solicitação de cadastramento - SEFAZ/AM) - estão de acordo com a legisçação de regência e viabilizam o antendimento de aspectos formais e burocráticos do presente procedimento licitatório.

Isto posto, pelos fatos e fundamentos ora apresentados, esta assessoria jurídica **OPINA favoravelmente à aprovação da Minuta de Edital (0753486) e da Minuta de Contrato Administrativo (0750392), assim como dos demais anexos do edital,** de forma a alicerçarem o respectivo procedimento licitatório.

É o parecer que submeto à apreciação de V. Exa.

ASSESSORIA DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, Manaus (AM), 20 de janeiro de 2022.

CLÁUDIA DE MORAES MARTINS PEREIRA

Assessora Jurídica - ATO Nº 337/2020.

Documento assinado eletronicamente por **Cláudia de Moraes Martins Pereira**, **Assessor(a) Jurídico(a) de Subprocurador-Geral de Justiça**, em 21/01/2022, às 11:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0754777** e o código CRC **DE60562F**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DESPACHO Nº 6.2022.01AJ-SUBADM.0754825.2021.015252

Autos nº 2021.015252

Assunto: Contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual.

Retornam os autos do procedimento deflagrado para viabilizar a Contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual, desta vez para análise jurídica das minutas de contrato e edital que subsidiarão a realização da competente licitação.

O Termo de Referência 20 (0720733) foi devidamente aprovado - vide Parecer 118 (0711353) e Despacho 484 (07113524), incluindo-se, ainda, ajustes indicados pela *Chefia do Setor de Infraestrutura e Telecomunicações,* via memorando 148 (0720865).

O Setor de Compras e Serviços - SCOMS providenciou a emissão do Mapa Demonstrativo de Preços **130** (0731238), após pesquisa de mercado. Por corolário, juntou-se aos autos o Quadro-Resumo do Processo de Compra 345 (0731246), bem como a Nota de Autorização de Despesas/Adjudicação - NAD 375 (0744829).

Minutas do Contrato (0750392) e Minuta de Edital (0753486) devidamente acostadas aos autos.

A Comissão Permanente de Licitação - CPL, por intermédio do Despacho 4 (0754777), encaminhou os autos à SUBADM para fins de cumprimento do disposto no parágrafo único do artigo 38 da Lei n.º 8.666/93 e art. 37, *caput* da Constituição Federal, quanto à emissão do parecer jurídico e posterior aprovação pelo Ordenador de Despesas.

Por sua vez, após instada, a assessoria jurídica acostou ao presente caderno administrativo o Parecer 6 (0754825), opinando favoravelmente pela aprovação da Minutas do Contrato Administrativo (0750392) e Minuta de Edital de Pregão Eletrônico(0753486), assim como dos demais anexos do edital, de forma a alicerçarem o respectivo procedimento licitatório.

Diante de todo o exposto, **ACOLHO** a supracitada peça opinativa e **APROVO a Minuta do Contrato Administrativo (0750392) e Minuta de Edital de Pregão Eletrônico(0753486), assim como os demais anexos do edital.** Ato contínuo, **DETERMINO** o encaminhamento dos autos à **CPL** para as providências de estilo.

Cumpra-se.

GABINETE DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus(Am), 20 de janeiro de 2022.

GÉBER MAFRA ROCHA

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 21/01/2022, às 12:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0754825** e o código CRC **8B8C7282**.

ATO Nº 185/2021/PGJ

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do ATO PGJ N.º 345/2007, datado de 26.03.2007, que estabelece normas para constituição da Comissão Permanente de Licitação, no âmbito desta Procuradoria-Geral de Justiça;

CONSIDERANDO a previsão expressa no art. 7.º da Lei n.º 3.147, de 06.07.2007, publicada no DOE de 09.07.2007;

CONSIDERANDO o teor do art. 29, inciso VII e XLI, da Lei Complementar n.º 011, de 17 de dezembro de 1993,

RESOLVE:

Art. 1.º – DESIGNAR o servidor EDSON FREDERICO LIMA PAES BARRETO, como Presidente, e os servidores SARAH MADALENA BARBOSA SANTOS CORTES, MAURÍCIO ARAÚJO MEDEIROS e IURY FECHINE RAMOS, Agentes de Apoio – Administrativo, em decorrência da experiência e capacitação técnica para, na qualidade de membros, comporem a Comissão Permanente de Licitação da Procuradoria-Geral de Justiça do Estado do Amazonas, pelo mandato de 1 (um) ano.

Art. 2.º – DESIGNAR o servidor MAURÍCIO ARAÚJO MEDEIROS, Agente de Apoio – Administrativo, para secretariar os trabalhos da Comissão ora composta.

Art. 3.º – INDICAR como substitutos eventuais os servidores FABÍOLA DE SOUZA MENDANHA e THIAGO NORONHA DAMASCENO OLIVEIRA, Agentes de Apoio – Administrativo, desta Procuradoria-Geral de Justiça.

Art. 4.º – DETERMINAR que os Pregoeiros Oficiais e Agentes de Contratação do Ministério Público sejam designados por ato próprio, podendo ser indicado, mediante Portaria, quem funcionará especificamente a cada pregão, assim como os membros da equipe de apoio.

Art. 5.º – Este Ato entrará em vigor a contar da data de 12 de julho de 2021.

Dê-se ciência, registre-se e cumpra-se.

GABINETE DO PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, em Manaus (Am.), 09 de julho de 2021.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral de Justiça

ATO Nº 186/2021/PGJ

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno - SEI N.º 2021.010249, em que figura, como parte interessada, o Exmo. Sr. Dr. GUSTAVO VAN DER LAARS, Promotor de Justiça de Entrância Inicial, titular da Promotoria de Justiça da Comarca de Alvarães;

CONSIDERANDO as disposições do r. DESPACHO N.º 337.2021.06AJ-SUBADM.0659292.2021.010249, de 07 de julho de 2021, expedido pela douta Subprocuradoria-Geral de Justiça para Assuntos Administrativos;

CONSIDERANDO o disposto no art. 29, inciso V, da Lei Complementar n.º 011, de 17 de dezembro de 1993;

RESOLVE:

EXONERAR a bacharela MARCYA LINS CAMPOS do cargo em comissão de Assessor de Promotoria de Justiça de Entrância Inicial, símbolo MP.06.03, a contar de 07.07.2021.

Publique-se, registre-se e cumpra-se.

GABINETE DO PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, em Manaus (Am.), 09 de julho de 2021.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral de Justiça

PORTARIA Nº 0948/2021/PGJ

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o teor da Portaria n.º 0754/2021/PGJ, que designou os Promotores de Justiça de Entrância Inicial e Substitutos como plantonistas durante do mês de abril/2021;

CONSIDERANDO o disposto no artigo 29, inciso XLI, da Lei Complementar n.º 011, de 17 de dezembro de 1993,

RESOLVE:

ALTERAR os termos da Portaria n.º 0754/2021/PGJ, datada de 30.03.2021, que designou os Promotores de Justiça de Entrância Inicial e Substitutos como plantonistas, na parte referente ao POLO 5 – BAIXO AMAZONAS, item 1 (Maués, Boa Vista do Ramos e Urucará), conforme abaixo especificado:

POLO 5 – BAIXO AMAZONAS

1. Maués, Boa Vista do Ramos e Urucará

Período: 16 a 30.04.2021 - Dr. ROBERTO NOGUEIRA

Dê-se ciência, registre-se e cumpra-se.

GABINETE DO PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, em Manaus (Am.), 23 de abril de 2021.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral de Justiça

PORTARIA Nº 1548/2021/PGJ

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o teor da Resolução n.º 054/98-CSMP, de 23 de setembro de 1998, que disciplina e define a manifestação dos Órgãos do Ministério Público de 1.ª e 2.ª instâncias, no que tange à apresentação de contrarrazões sempre que o advogado, ao interpor o Recurso de Apelação, invocar a aplicação do art. 600, § 4.º, do Código de Processo Penal;

RESOLVE:

DESIGNAR o Exmo. Sr. Dr. DANIEL LEITE BRITO, Promotor de Justiça de Entrância Final, Titular da 8.ª Promotoria de Justiça de Manaus (10.ª Vara Criminal), para oferecer as contrarrazões nos autos da Apelação Criminal n.º 0632081-98.2019.8.04.0001, em tramitação na Segunda Câmara Criminal do egrégio Tribunal de Justiça do Estado do Amazonas.

a) acolher, motivadamente, as razões recursais, modificando e tornando pública a decisão final exarada;

b) rejeitar, motivadamente, as razões recursais, encaminhando os autos ao Procurador-Geral de Justiça para apreciação final, que:

1. poderá, fundamentadamente, acolher as razões para ao final, reformar a sanção imposta, ou rejeitá-las mantendo a decisão atacada;

2. determinará a publicização da decisão final.

II – impetrar pedido de reconsideração contra decisão de aplicação de inidoneidade exarada pelo Procurador-Geral de Justiça que poderá:

a) acolher, motivadamente, o pedido de reconsideração, modificando e tornando pública a decisão final exarada;

b) rejeitar, motivadamente, o pedido de reconsideração, tornando pública a decisão exarada.

Parágrafo único. A autoridade competente providenciará, por meio da secretaria respectiva, a publicação no Diário Oficial Eletrônico - DOMPE de extrato da decisão exarada em face do recurso hierárquico ou do pedido de reconsideração.

Art. 11 A Comissão Permanente de Licitação – CPL deverá promover todos os atos de citação, intimação e / ou notificação dos interessados e ainda:

I – não havendo manifestação recursal e não havendo aplicação da sanção de multa, informar à Subprocuradoria-Geral de Justiça para Assuntos Administrativos – SUBADM acerca da inércia ocorrida;

II - inexistindo manifestação recursal e havendo aplicação de multa, determinar seu recolhimento à contratada /licitante sancionada:

a) no adimplemento do recolhimento, encaminhar os autos à Diretoria de Orçamento de Finanças – DOF e após, promover seu arquivamento;

b) no inadimplemento do recolhimento da multa, encaminhar os autos para o Procurador-Geral de Justiça, para análise quanto a conveniência e oportunidade de encaminhamento à Procuradoria-Geral do Estado, para devida inscrição em dívida ativa.

III – existindo manifestação recursal ou pedido de reconsideração, encaminhar à autoridade competente;

IV – após trânsito julgado administrativo, providenciar o lançamento das sanções junto aos sistemas competentes, tais como o Sistema de Cadastramento Unificado de Fornecedores - SICAF.

Art. 12 Ficam revogadas todas as disposições em contrário, em especial as dispostas no ATO PGJ N° 345/2007.

Art. 13 Este ato entra em vigor na data de sua publicação.

Publique-se, registre-se, cumpra-se.

Gabinete do Procurador-Geral de Justiça, em Manaus, 09 de julho de 2021.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral de Justiça

ATO Nº 188/2021/PGJ

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do ATO PGJ N.º 277/2007, datado de 05.07.2007, que regulamentou a utilização da modalidade pregão, na forma presencial, no âmbito do Ministério Público do Estado do Amazonas;

CONSIDERANDO o disposto no art. 5.º, do ATO PGJ N.º 345/2007, datado de 29.08.2007, que dispõe sobre a organização e as atribuições da Comissão Permanente de Licitação, e dá outras providências;

CONSIDERANDO o teor do ATO PGJ N.º 185/2021/PGJ, de 09 de julho de 2021;

CONSIDERANDO o teor do art. 29, inciso VII e XLI, da Lei Complementar n.º 011, de 17 de dezembro de 1993;

RESOLVE:

NOMEAR, a contar de 12.07.2021, os servidores EDSON FREDERICO LIMA PAES BARRETO, Agente de Apoio – Administrativo e Presidente da Comissão Permanente de Licitação, e MAURÍCIO ARAÚJO MEDEIROS, Agente de Apoio – Administrativo e Membro-Secretário da Comissão Permanente de Licitação, como Agentes de Contratação e Pregoeiros Oficiais do Ministério Público do Estado do Amazonas, bem como FABÍOLA DE SOUZA MENDANHA e THIAGO NORONHA DAMASCENO OLIVEIRA, Agentes de Apoio – Administrativos desta Procuradoria-Geral de Justiça, suplentes da Comissão Permanente de Licitação, como substitutos eventuais.

Publique-se. Registre-se. Cumpra-se.

GABINETE DO PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, em Manaus (Am.), 09 de julho de 2021.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral e Justiça

PORTARIA Nº 1583/2021/PGJ

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o disposto no art. 29, inciso XLI, da Lei Complementar n.º 011, de 17 de dezembro de 1993,

RESOLVE:

DESIGNAR o Exmo. Sr. Dr. LEONARDO TUPINAMBÁ DO VALLE, Promotor de Justiça de Entrância Inicial, para participar das audiências da Comarca de Urucará/AM, no dia 12.07.2021.

Dê-se ciência, registre-se e cumpra-se.

GABINETE DO PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, em Manaus (Am.), 09 de julho de 2021.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral de Justiça

EDITAL DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** pelo presente edital e por intermédio da **PROCURADORIA GERAL DE JUSTIÇA**, cadastrada no CNPJ sob o n.º 04.153.748/0001-85, através da **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, designada pelo Ato PGJ n.º 185/2021 e alterações, torna público que, tendo em vista o que consta do **Processo SEI n.º 2021.015252,** fará realizar licitação, na modalidade **PREGÃO**, na forma **ELETRÔNICA, com critério de julgamento MENOR PREÇO POR LOTE (ÚNICO)**, em conformidade com o Ato PGJ n.º 389/2007; com a Lei nº 10.520, de 17/07/2002, com o **Decreto Federal n.º 10.024, de 20 de setembro de 2019**; Decreto nº 7892, de 23 de janeiro e 2013; com o Decreto Estadual n.º 24.818/2005, de 27/01/2005, e subsidiariamente com a Lei n.º 8.666, de 21 de junho de 1993 e suas alterações, e nos termos do art. 37, inciso XXI da Constituição Federal, mediante as condições estabelecidas neste Edital e anexos.

O contrato correspondente, ou o instrumento que vier a substituí-lo, será regido pela Lei n.º 8.666/93 e suas alterações.

PROCEDIMENTO SEI N.º 2021.015252
Recebimento das propostas: a partir da data de publicação do aviso no DOMPE.
Abertura das propostas: às 10 horas do dia **21/02/2022** (horário de Brasília).
Licitação Exclusiva para ME/EPP: ( ) SIM (X) NÃO
Endereço eletrônico: http://www.comprasgovernamentais.gov.br.
Código UASG: 925849

1. DAS DISPOSIÇÕES GERAIS

1.1. O pregão será realizado em sessão pública, por meio da utilização de recursos da tecnologia da informação – *internet*, utilizando-se, para tanto, de métodos de autenticação de acesso e recursos de criptografia, garantindo segurança em todas as fases do certame.
1.2. Os trabalhos serão conduzidos por servidor público integrante da **COMISSÃO PERMANENTE DE LICITAÇÃO** deste Órgão, por ato interno, denominado(a) PREGOEIRO(A), e membros da equipe de apoio, previamente credenciado no aplicativo http://www.comprasgovernamentais.gov.br.
1.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública, observarão rigorosamente o horário de **Brasília – DF**, e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

2. DO OBJETO

2.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para ***contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos.***

2.2. A licitação será em LOTE ÚNICO, composto de 4 (quatro) itens, conforme especificações constantes no TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252:

LOTE	ITEM	DESCRIÇÃO	UND	QTDE
1	01	Serviço de Firewall em Alta Disponibilidade	Meses	48
	02	Serviço de Monitoramento da Solução	Meses	48
	03	Serviço de Migração do Ambiente Atual	Unidades	01
	04	Serviço de Treinamento da Solução	Pessoas	05

2.3. **Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão funcionar perfeitamente**, sem vícios, não constar em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os **softwares** comerciais deverão, ainda, ser instalados em sua **versão mais atualizada**, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o **hardware** a ser utilizado na prestação dos serviços deverá estar coberto por **garantia do fabricante, conforme descrição e demais especificações técnicas listadas no TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252, Anexo I deste Edital**, sob pena de ser recusado seu recebimento.

2.4. Os equipamentos deverão ser entregues na totalidade do(s) item(ns) constante(s) na nota de empenho, salvo nos casos de superveniência de fato excepcional ou imprevisível, alheio à vontade da contratada, solidamente justificada e demonstrada a causalidade entre o fato alegado e a impossibilidade de cumprimento do estabelecido neste, por meio de documentos comprobatórios hábeis, e expressamente autorizado pelo Fiscal do Contrato ou instrumento equivalente.

2.5. O critério de julgamento adotado será o **menor preço POR LOTE (ÚNICO)**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2.6. O objeto da futura contratação compreenderá, sobretudo, as especificações constantes do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252,** Anexo I deste Edital, sem prejuízo das demais prescrições figuradas no mencionado documento, bem assim na Minuta de Contrato Administrativo, Anexo II do Edital.

2.7. Os valores apresentados nos orçamentos e/ou propostas de preço deverão considerar inclusas todas as despesas relativas a frete, taxas, análises, amostras, impostos, licenças, encargos sociais, ou outras que possam influir direta ou indiretamente nos custos.

2.8. **Integra a presente licitação, como parte indissolúvel:**

a. Anexo I – TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;
b. Anexo II – Minuta de Contrato Administrativo;
c. Anexo III – Modelo de Declarações Complementares;
d. Anexo IV – Modelo de Proposta de Preços; e
e. Anexo V – Modelo de Solicitação de Cadastramento – SEFAZ/AM.

2.9. **VISTORIA TÉCNICA:** As empresas licitantes PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades do CONTRATANTE, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

2.9.1. As regras e demais disposições acerca da visita técnica encontra-se disciplinada no item 6 do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252.**

3. DOS RECURSOS ORÇAMENTÁRIOS

3.1. A despesa decorrente da contratação do objeto deste pregão, quando efetivada, deverá recair por conta dos recursos específicos consignados no orçamento da **PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS – PGJ/AM**. Programa 03.122.0001.2001.0001. Fonte 100, Elemento 339039.

4. DO CREDENCIAMENTO

4.1. As empresas interessadas em participar do certame deverão providenciar, previamente, o credenciamento perante a **SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO (SLTI), do MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO (MPOG)**, provedor do sistema eletrônico utilizado nesta licitação, no site http://www.comprasgovernamentais.gov.br, **por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.**

4.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave **de identificação e senha pessoal**, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento, regulamento e receber instruções detalhadas para sua correta utilização.

4.1.2. O credenciamento da licitante, bem como a sua manutenção, dependerá de registro cadastral atualizado no **SISTEMA DE CADASTRAMENTO UNIFICADO DE FORNECEDORES – SICAF**, em seu nível básico, que também será requisito obrigatório para fins de habilitação.

4.1.3. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS (entidade promotora da licitação) por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. É de responsabilidade do Cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.3.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

5. DAS CONDIÇÕES PARA PARTICIPAÇÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, legalmente constituídos, desde que atendam às condições exigidas deste Edital e seus Anexos, inclusive quanto à documentação exigida, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

5.1.1. **A licitante deverá declarar em campo próprio do sistema eletrônico a condição de microempresa ou empresa de pequeno porte**, para os fins previstos na Lei Complementar nº. 123/06.

5.1.1.1. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

5.2. O licitante deverá estar devidamente credenciado na **SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO – SLTI, do MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO**, através do site http://www.comprasgovernamentais.gov.br, **por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.**

5.3. O licitante deverá manifestar, **em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação**, e que sua proposta está em conformidade com as exigências do instrumento convocatório, nos termos do art. 21, parágrafo 2.º, do Decreto n.º 5.450/2005.

5.4. Será exigida do licitante **Declaração de Elaboração Independente de Proposta**, a qual será feita no campo do sistema ***Comprasnet*** destinado para tanto.

5.5. Todos os custos decorrentes da elaboração e apresentação de propostas serão de responsabilidade exclusiva da licitante, não sendo o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, em nenhum caso, responsável pelos mesmos, inclusive, pelas transações que forem efetuadas em nome do participante no Sistema Eletrônico ou por eventual desconexão.

5.6. **Não poderá participar,** direta ou indiretamente, desta licitação ou da execução dos serviços e do fornecimento de bens a eles necessários:

5.6.1. Os interessados que não atendam às condições deste Edital e seu(s) anexo(s);

5.6.2. As pessoas físicas e jurídicas que se enquadrem, em uma ou mais, das hipóteses elencadas no art. 9.º e seus incisos da Lei n.º 8.666/93;

5.6.3. As pessoas físicas e jurídicas que possuam sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e de sua **CPL**;

5.6.4. Empresa estrangeira não autorizada a funcionar no País e que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente

5.6.5. Interessado que se encontre em processo de Falência, Recuperação Judicial e Extrajudicial (conforme Lei nº. 11.101/05), salvo decisão judicial em contrário, concurso de credores, insolvência, dissolução, liquidação, fusão, cisão, incorporação, ou em regime de consórcio, qualquer que seja sua forma de constituição, salvo devidamente justificado;

5.6.6. Licitante que, por quaisquer motivos, tenha sido declarado inidôneo ou punido com suspensão e/ou impedimento de licitar e contratar por órgão da Administração Pública, Direta ou Indireta, Federal, Estadual, Municipal ou do Distrito Federal, desde que o ato tenha sido publicado na imprensa oficial ou registrado nos bancos de dados oficiais (SICAF e/ou outros), conforme o caso, pelo órgão que o praticou, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida sua reabilitação, consoante o art. 87, IV, da Lei 8.666/93;

5.6.7. Empresa que possua, em sua diretoria ou quadro técnico, funcionário público vinculado ao **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS ou à CPL;**

5.6.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

5.7. Como condição para participação no Pregão, a licitante assinalará "sim" ou "não" em campo próprio do Sistema eletrônico Comprasnet, relativo às seguintes declarações:

a) que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

a.1.) nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame;

a.2.) nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

b) que está ciente e concorda com as condições contidas no edital e seus anexos,
c) que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;
d) que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;
e) que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;
f) que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.
g) que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
h) que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

5.8. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste edital.

6. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, **exclusivamente por meio do sistema**, **concomitantemente com os documentos de habilitação** exigidos no edital, **proposta** com a descrição do objeto ofertado e o preço, **até a data e o horário estabelecidos para abertura da sessão pública (horário de Brasília), quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.**

6.1.1.

6.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos

sistemas.

6.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

6.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

6.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6.8.1. Na proposta registrada no sistema, não deverá conter qualquer elemento que possa identificar a licitante, sob pena de desclassificação, sem prejuízo das sanções previstas nesse edital.

7. DO PREENCHIMENTO DA PROPOSTA

7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

7.1.1. Valor unitário e total do item;

7.1.2. Marca;

7.1.3. Fabricante;

7.1.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso, **sem identificação da licitante;**

7.1.4.1. Não serão aceitas propostas escritas contendo especificações que não contenham as informações necessárias à perfeita caracterização do objeto e suas especificidades, bem como especificações vagas, incompletas, ressalvado o subitem 7.6 deste Edital.

7.2. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

7.3. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer

alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

7.4. O **prazo de validade da proposta não será inferior** a **90 (noventa) dias**, a contar da data de sua apresentação.

7.5. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais ou estaduais, quando participarem de licitações públicas;

7.5.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a fiscalização do Tribunal de Contas do Estado do Amazonas e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7.6. O CNPJ da proponente, empresa cadastrada no SICAF e habilitada na licitação, deverá ser o mesmo para efeito de emissão das notas fiscais e posterior pagamento.

7.6. Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas, ou Anexos não solicitados, considerando-se que pelo preço proposto, a empresa obrigar-se-á a executar os serviços/entregar os produtos descritos neste edital.

7.8. Para efeito de elaboração das propostas, caso haja divergência entre a especificação contida neste edital e a no sistema SIASG, prevalecerá a descrita neste edital.

8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

8.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

8.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

8.2.1. Também será desclassificada a licitante que no momento do preenchimento do campo de ***"Descrição detalhada do objeto ofertado"*** no Sistema Comprasnet identifique sua empresa, o que não se confunde com a proposta inicial juntada ao Sistema e a proposta final/reajustada após convocação pelo Pregoeiro.

8.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

8.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente

estas participarão da fase de lances.

8.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.5.1. O lance deverá ser ofertado pelo valor total/unitário do item ou percentual de desconto.

8.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

8.7. O licitante somente poderá oferecer lance de **valor inferior** ao último por ele ofertado e registrado pelo sistema.

8.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,05 (cinco centavos).

8.9. O intervalo de tempo entre os lances enviados pelo mesmo licitante não poderá ser inferior a 20 (vinte) segundos e o intervalo entre lances não poderá ser inferior a 3 (três) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances (quando implementado).

8.10. Será adotado para o envio de lances no pregão eletrônico o modo de disputa **"ABERTO"**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.11. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

8.12. A prorrogação automática da etapa de lances, de que trata o item anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.13. **Não havendo novos lances** na forma estabelecida nos itens anteriores, a sessão pública **encerrar-se-á automaticamente.**

8.14. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

8.15. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia;

8.15.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

8.16. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que

for recebido e registrado em primeiro lugar.

8.17. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada à identificação do licitante.

8.18. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

8.19. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

8.20. O **Critério de Julgamento** adotado será o **menor preço POR LOTE (ÚNICO)**, conforme definido neste Edital e seus anexos.

8.20.1. Foi implementada regra e ferramenta no próprio Sistema Comprasnet que impede a aceitação pelo pregoeiro, na fase de negociação posterior à disputa de lances, de majoração (aumento) de preço unitário de item já definido na etapa de lances, pelo fornecedor, quer para os itens adjudicados individualmente, quer para os adjudicados em grupos. A alteração atende ao disposto no inciso XVII do art. 4° da Lei 10.520/2002 e ao Acórdão TCU 1872/2018.

8.21. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

8.22. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

8.23. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

8.24. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

8.25. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

8.26. No caso de equivalência dos valores apresentados pelas microempresas e empresas

de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.27. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances).

8.28. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

8.28.1. no País;

8.28.2. por empresas brasileiras;

8.28.3. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

8.28.4. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

8.29. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

8.30. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

8.30.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.30.2. O pregoeiro solicitará ao licitante melhor classificado que, no **prazo de 02 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

8.31. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

9. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

9.1. O pregoeiro solicitará ao licitante melhor classificado que, **no prazo máximo de 02 (duas) horas,** envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

9.2. Na proposta vencedora a ser enviada posteriormente deverá constar, conforme modelo do **Anexo IV**:

a) Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em

algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93). Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

a.1.) Não será admitido nos preços o fracionamento de centavo que ultrapassar duas casas decimais, desprezando-se sumariamente a fração remanescente;

a.2.) No preço deverão estar incluídas todas as despesas que influam no custo, tais como: impostos, transportes, seguros, taxas e outras despesas necessárias ao fornecimento dos materiais e à execução dos serviços correspondentes;

a.3.) Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

b) Prazo de validade da proposta de, no mínimo, **90 (noventa) dias corridos**, a contar da data de sua apresentação. As propostas que omitirem o prazo de validade serão entendidas como válidas pelo período supracitado;

c) Especificações claras, completas e minuciosas, com detalhes do objeto ofertado, inclusive marca, modelo, tipo e referência, no que couber, observadas as especificações mínimas e quantitativos contidos neste Edital e anexos;

d) A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

e) **Prazo entrega do plano de implementação:** Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

f) **Prazo início processo de migração/reunião alinhamento**: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;

g) **Prazo processo de migração**: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

h) Os seguintes dados da licitante: Razão Social, endereço, telefone/fax, número do CNPJ/MF, e-mail, se houver, Banco, agência, número da conta-corrente e praça de pagamento;

i) Nome, CNPJ ou CPF dos 3 (três) principais integrantes do quadro societário da licitante, assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade;

j) Contato para fins de faturamento: (indicar o nome, cargo, endereço, telefone, fax, e-mail de contato do responsável pelo recebimento das futuras notas de empenho);

k) Quando solicitada pelo Pregoeiro, **documentação técnica (manuais, catálogos ou**

prospectos), com as características detalhadas (marca, modelo, cor, tipo de material e medidas) e imagens ilustrativas dos produtos propostos, que possibilitem a completa averiguação de conformidade com as especificações, visando facilitar a avaliação a ser realizada por técnicos deste Órgão.

9.3. As **Declarações Complementares**, referentes ao Anexo III do Edital, deverão ser efetuadas no momento da elaboração e envio da proposta pelos fornecedores, em seu próprio conteúdo ou documento apartado, sendo elas:

a) Declaração de cumprimento pleno dos requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.,** para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

b) Declaração expressa do licitante de que recebeu o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação (Anexo III);

c) Declaração, sob as penas da Lei, de que os documentos e declarações apresentados são fiéis e verdadeiros (Anexo III);

d) Declaração de que, caso seja vencedor do certame e não cadastrado no **SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhará a CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;

e) Declaração de que o preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

9.4. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato ou instrumento equivalente e aplicação de eventual sanção à Contratada, se for o caso.

9.4.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

9.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

9.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

10. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

10.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

10.1.1. A Proposta de Preços deverá ser apresentada conforme **Anexo IV**, constando dela todas as informações descritas no referido modelo, essenciais à avaliação pelo Pregoeiro.

10.1.2. A proposta e documentação, se necessário, será analisada pela equipe da **DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO – DTIC**, para fins de verificação do atendimento às características e exigências reclamadas no edital e anexos.

10.1.3. A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

10.2. **Serão desclassificadas as propostas que, ressalvado o disposto no subitem 5.7. deste Edital:**

10.2.1. Não atendam às exigências do edital e Anexos, sejam omissas ou apresentem irregularidades ou defeitos capazes de dificultar o julgamento;

10.2.2. Apresentar preço (global ou unitário) final superior ao preço máximo fixado pela Administração (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível, aplicando-se, subsidiariamente, as disposições previstas no parágrafo 1.º do artigo 48 da Lei n.º 8.666/93.

10.2.2.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

10.2.3. Também será desclassificada a licitante que no momento do preenchimento do campo de ***"Descrição detalhada do objeto ofertado"*** no Sistema Comprasnet identifique sua empresa, o que não se confunde com a proposta inicial juntada ao Sistema e a proposta final/reajustada após convocação pelo Pregoeiro.

10.3. A existência de **erros materiais ou omissões** nas propostas de preços das participantes não ensejará sua desclassificação antecipada.

10.3.1. Verificada a presença de erros sanáveis na proposta de preços, o Pregoeiro ou

Administração poderá realizar diligência junto à Licitante para a devida correção apenas das falhas apontadas, mediante apresentação de nova oferta, com desconto nunca inferior a **0,5% (cinco décimos percentuais) do valor total de sua última proposta, à exceção da primeira retificação que não necessitará de desconto, limitado a 3 (três) oportunidades, vedada a juntada de documentos novos.**

10.4. No que couber, se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta, **no prazo de 1 (um) dia útil, a contar da convocação pelo Pregoeiro**.

10.4.1. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

10.4.2. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas** de antecedência, e a ocorrência será registrada em ata;

10.5. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

10.6. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, **no prazo máximo de 02 (duas) horas, sob pena de não aceitação da proposta.**

10.6.1. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

10.6.2. Nas situações da compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos nos subitens acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de **05 (cinco) dias úteis contados da solicitação.**

10.6.2.1. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

10.6.2.2. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

10.6.2.3. No caso de não haver entrega da amostra ou havendo entrega de amostra fora das especificações previstas neste Edital, **a proposta do licitante será recusada.**

10.6.2.4. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

10.6.2.5. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

10.6.2.6. Após a divulgação do resultado final da licitação, as amostras entregues deverão ser recolhidas pelos licitantes no prazo de **10 (dez) dias corridos**, após o qual poderão ser descartadas ou incorporadas pela Administração, sem direito a ressarcimento.

10.6.2.7. Os licitantes deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.

10.7. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

10.8. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a sua continuidade.

10.9. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

10.9.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

10.9.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

10.10. No que couber, nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

10.11. **A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas neste edital e seus anexos, bem como, todas as especificações do objeto contidas na proposta vinculam a Contratada.**

10.12. Quando da proposta de preços não constar quaisquer dos prazos previstos, quer sejam os de garantia, validade dos produtos, validade da proposta ou de entrega, entender-se-á que estão aceitos os constantes do Edital.
10.13. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam as licitantes liberadas dos compromissos assumidos, podendo ser consultado acerca da manutenção dos preços ofertados.
10.14. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.
10.15. Sendo aceitável a proposta, o pregoeiro efetuará consulta "on-line" ao **sistema de Cadastramento Unificado de Fornecedores – SICAF**, para comprovar a regularidade do licitante.

10.15.1. Nos casos em que a habilitação exigir documentos que não estejam contemplados no SICAF, o pregoeiro solicitará do respectivo licitante o encaminhamento dos documentos de habilitação.

10.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

11. DA HABILITAÇÃO

11.1. Os documentos necessários à habilitação deverão estar com prazo vigente, à exceção daqueles que por sua natureza, não contenham validade, e poderão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de notas ou por servidor da CPL, ou por publicação em órgãos da imprensa oficial, **não sendo aceitos "protocolos" ou solicitação de documento** em substituição aos documentos requeridos neste edital.

11.1.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

11.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

11.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve

fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

11.1.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

11.1.2.3. No caso de impedimento indireto, o licitante será convocado para manifestação previamente à sua desclassificação.

11.1.3. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

11.1.4. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.2. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF **até o terceiro dia útil anterior à data prevista para recebimento das propostas;**

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

11.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **02 (duas) horas, sob pena de inabilitação.**

11.4. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

11.5. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.5.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a

centralização do recolhimento dessas contribuições.

11.6. Ressalvado o disposto no **subitem 6.3.**, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

11.7. Relativos à Habilitação Jurídica:

11.7.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.7.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio **www.portaldoempreendedor.gov.br;**

11.7.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada – EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

11.7.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

11.7.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

11.7.6. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

11.7.7. Os documentos relativos à Habilitação Jurídica indicados, deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.8. Relativo à Regularidade Fiscal e Trabalhista:

11.8.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

11.8.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.8.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.8.4. Prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

11.8.5. Prova de inscrição no cadastro de contribuintes Estadual e/ou Municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual, **ficando dispensada esta exigência, no caso de comprovação de regularidade prevista no subitem a seguir;**

11.8.6. Prova de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre, **afastando-se a necessidade de envio da inscrição prevista no subitem anterior;**

11.8.6.1. Caso o licitante seja considerado isento dos tributos estaduais/municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

11.8.7. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

11.8.8. A aceitação de certidões emitidas via internet ficará sujeita à confirmação de sua validade mediante consulta *on line* ao cadastro emissor respectivo.

11.9. Relativos à Qualificação Econômico-Financeira:

11.9.1. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, podendo ser apresentado de acordo com o Sistema Público de Escrituração Digital (SPED – Decreto Federal n.º 6.022/2007), que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

11.9.1.1 O Balanço apresentado deverá cumprir as seguintes formalidades: a) Indicação do número das páginas e números do livro onde estão inscritos o balanço patrimonial e a DRE (Demonstração do Resultado do Exercício) no Livro Diário. Além do acompanhamento do respectivo Termo de Abertura e Termo de Encerramento do mesmo; b) Assinatura do contador e do titular ou representante legal da empresa no balanço patrimonial e DRE (pode ser feita digitalmente); c) Prova de registro na Junta Comercial ou Cartório (devidamente carimbado, com etiqueta, chancela da Junta Comercial ou código de registro);

11.9.1.2. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

11.9.1.3. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

11.9.1.4. Quando solicitado ou autorizado pelo Pregoeiro, será permitido apresentação de balanço intermediário, desde que se decorra de lei ou contrato social/estatuto social da Licitante.

11.9.1.5. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

11.9.2. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar, considerados os riscos para a Administração, e, a critério da autoridade competente, o capital mínimo ou o patrimônio líquido mínimo 10% do valor estimado da contratação ou do item pertinente.

11.9.3. Certidões Negativas de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), expedida pela Central de Certidões do Tribunal de Justiça ou órgão equivalente do domicílio ou da sede do licitante, **expedida até 90 (noventa) dias antes da abertura desta licitação,** quando do documento não constar data expressa de validade;

11.9.3.1 Onde não houver **CENTRAL DE CERTIDÕES DO TRIBUNAL DE JUSTIÇA**, deverá ser apresentada Certidão emitida pela **SECRETARIA DO TRIBUNAL DE JUSTIÇA** ou órgão equivalente do domicílio ou da sede do licitante constando a quantidade de Cartórios Oficiais de Distribuição de Pedidos de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), devendo ser apresentadas Certidões expedidas na quantidade de cartórios indicadas no respectivo documento, no prazo referido no item 11.9.3;

11.9.3.2. Caso os prazos de validade não constem expressamente das certidões, serão considerados para esse fim, o prazo descrito no subitem 11.9.3. deste instrumento convocatório.

11.10. Relativos à Qualificação Técnica:

11.10.1. **Atestado(s) de Capacidade Técnica** fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a empresa licitante tenha prestado, a

contento, serviço de natureza e vulto compatíveis com o objeto deste instrumento, que permita(m) estabelecer, por comparação, proximidade de características funcionais técnicas, dimensionais, quantitativas e qualitativas, conforme Termo de Referência.

11.10.1.1. Entende-se como compatível o(s) atestado(s) de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem já ter prestado serviços de firewall (Next Generation Firewall), de forma satisfatória, com capacidade de tráfego (troughput) de, no mínimo, 10 (dez) Gbps, incluindo fornecimento de equipamento(s), serviço de instalação, treinamento, monitoramento e garantia de, no mínimo, 12 (doze) meses, similares ao objeto deste Termo.

11.10.1.2. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão(ões) deverá(ão) ser assinado(s) pelo responsável do setor competente do órgão;

11.10.1.3. No caso de pessoa jurídica de direito privado, o(s) atestado(s) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa.

11.10.1.4. A ausência de apresentação de atestado claro, legível e idôneo, em não conformidade com este Edital, tendo em vista o vulto da aquisição, será motivo de inabilitação, a critério do Pregoeiro.

11.11. Disposições Gerais da Habilitação:

11.11.1. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

11.11.2. Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos, o pregoeiro considerará o proponente **inabilitado**, sendo convocado outro licitante, observada a ordem de classificação, e assim **sucessivamente**, sem prejuízo das sanções legais cabíveis.

11.11.3. Sob pena de inabilitação os documentos apresentados deverão estar em nome da licitante, com o nº do CNPJ e o endereço respectivo, conforme segue:

11.11.3.1. se a licitante for a matriz, todos os documentos deverão estar em nome da matriz, e

11.11.3.2. se a licitante for a filial, todos os documentos deverão estar em nome da filial.

11.11.3.3. no caso dos subitens anteriores, serão dispensados da filial aqueles documentos que COMPROVADAMENTE, forem emitidos SOMENTE em nome da matriz, e vice-versa.

11.11.4. Caso os prazos de validade não constem expressamente das certidões apresentadas, será considerado para esse fim, o prazo descrito no subitem 11.9.3 deste instrumento convocatório.

11.11.5. Os originais das documentações habilitatórias, ou cópias autenticadas por meio de cartório competente, deverão ser encaminhados ao(à) pregoeiro(a), nos termos do subitem 11.13. do Edital.

11.11.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

11.12. **Havendo alguma restrição na comprovação da regularidade fiscal** para **microempresas e empresas de pequeno porte**, lhes será assegurado o prazo de **05 (cinco) dias úteis**, a contar do momento em que o licitante for declarado vencedor, prorrogáveis por igual período, **a requerimento da interessada e a critério da Administração Pública**, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa**.**

11.12.1. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

11.13. **Todos os documentos enviados eletronicamente deverão ser enviados em original, ou por cópia autenticada, devidamente assinado(s) pelo(s) representante(s) legal(is) no dia subsequente ao do resultado da habilitação**, impreterivelmente, **sob pena de desclassificação, observado o disposto no item 24.7 e subitens,** à Comissão Permanente de Licitação da Procuradoria-Geral de Justiça do Estado do Amazonas, Av. Coronel Teixeira, 7.995, Nova Esperança II, CEP: 69037-473.

11.13.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

11.14. Para fins de julgamento da habilitação no certame, considerar-se-á vigente o documento com prazo de validade, pelo menos, até a data de abertura da licitação.

11.15. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

11.16. Será inabilitado o licitante que não comprovar sua habilitação, deixar de apresentar quaisquer dos documentos exigidos para a habilitação, ou apresentá-los em desacordo

com o estabelecido neste Edital.

11.17. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.18. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

11.18.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

11.19. Atendidas as exigências habilitatórias fixadas neste Edital, o licitante será declarado **vencedor**, sendo-lhe adjudicado o objeto do certame, caso não haja interposição de recursos, encaminhando-se, em seguida os autos à autoridade competente para homologação.

11.20. Da sessão pública será lavrada ata circunstanciada, que mencionará todos os licitantes, a classificação dos lances, bem como as ocorrências que interessarem ao julgamento desta licitação.

12. DOS RECURSOS ADMINISTRATIVOS

12.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o **prazo de no mínimo 30 (trinta) minutos**, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

12.1.1. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

12.1.1.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

12.1.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito, cabendo o pregoeiro adjudicar o objeto da licitação à empresa licitante declarada vencedora.

12.2. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de **3 (três) dias corridos** para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros **3 (três) dias corridos**, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à

defesa de seus interesses.

12.2.1. Quando o prazo de interposição de Recursos Administrativos ou de Contrarrazões terminar em dia não útil, o prazo final será prorrogado para o primeiro dia útil subsequente.

12.3. A falta de manifestação imediata e motivada da licitante importará a decadência do direito de recurso e adjudicação do objeto pelo Pregoeiro à vencedora. Os recursos imotivados ou insubsistentes não serão recebidos.

12.3.1. Intenção motivada de recorrer é aquela que identifica, objetivamente, os fatos e o direito que a licitante pretende que sejam revistos pela autoridade superior àquela que proferiu a decisão

12.3.2. O não oferecimento de razões no prazo deste Edital fará deserto o recurso.

12.4. Os autos do processo permanecerão com vista franqueada aos interessados na **COMISSÃO PERMANENTE DE LICITAÇÃO**, Av. Coronel Teixeira n.º 7.995, Nova Esperança, Cep.: 69037-473, nos dias úteis, no horário das 8h. Às 14h. (horário local).

12.5. O recurso contra decisão do Pregoeiro terá **efeito suspensivo**.

12.6. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

12.7. Não serão providos recursos de **caráter protelatório**, fundada em mera insatisfação da licitante, podendo ainda ser aplicado, supletiva e subsidiariamente, no que couberem, as regras previstas na Lei n.º 13.105/2015 (Código de Processo Civil).

12.8. A alegação de preço inexequível por parte de uma das licitantes com relação à proposta de preços de outra licitante deverá ser devidamente comprovada.

12.9. A sessão pública do pregão somente será concluída após declarado o vencedor do certame e encerrado o prazo para manifestação de intenção de interposição de recurso, cabendo aos licitantes permanecerem conectados ao sistema até o final desta etapa.

12.10. Decididos os recursos, a autoridade competente fará a adjudicação do objeto da licitação ao licitante vencedor.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico ("chat") ou ainda, e-mail, de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

14.1. Não havendo recurso, de pronto, o Pregoeiro adjudicará o objeto do certame ao vencedor. Existindo recurso, após decisão, a autoridade competente adjudicará o objeto ao licitante vencedor.

14.1.1. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14.2. Homologado o resultado, o adjudicatário será convocado a comparecer, no prazo máximo de 5 (cinco) dias úteis, para celebrar o contrato ou retirar o instrumento equivalente, devendo manter as condições de habilitação exibidas na licitação.

14.2.1. Se o vencedor do certame não apresentar situação regular no ato da assinatura do contrato (ou retirada do instrumento equivalente), ou recusar-se a assiná-lo, ou sobrevier fato impeditivo de sua celebração, a sessão será retomada e os demais licitantes chamados, procedendo-se na forma do item 11.6.2, sem prejuízo das sanções cabíveis.

14.2.2. O vencedor do certame deverá apresentar ao órgão interessado, antes da assinatura do contrato (ou retirada do instrumento equivalente), nova proposta de preços escrita, com a devida recomposição dos custos unitários decorrentes da diminuição dos valores na fase de lances verbais, observado o subitem 8.7 deste Edital.

14.3. A homologação do resultado desta licitação não implicará direito à contratação.

15. DOS PRAZOS PARA A ENTREGA E DO RECEBIMENTO

15.1. A entrega dos serviços obedecerá às disposições do item 5 do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, sendo que após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

15.1.1. A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

15.1.2. A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

15.2. O recebimento dos serviços será realizado por servidores da ADQUIRENTE e

ocorrerá nos termos do item 9 do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252** e Cláusula Quinta da Minuta de Contrato (Anexo II).

16. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Garantia e Assistência Técnica ou emitido instrumento equivalente.

16.1.1. O adjudicatário terá o **prazo de 05 (cinco) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.1.1.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência eletrônica no e-mail constante da proposta, para que seja assinado eletronicamente pelo Sistema SEI ou aceito no prazo de 05 (cinco) dias, a contar da data de seu recebimento.

16.1.1.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

18.1.1.3. Nos termos do art. 6º do Decreto n º 40.674/2019, o termo contratual ou instrumento equivalente poderá ser assinado por certificação digital ou mediante assinatura eletrônica via Sistema Eletrônico de Informação - SEI, conforme disposição do ATO Nº 141/2017/PGJ;

16.1.1.3.1. O uso da senha de acesso ao Sistema Eletrônico de Informação - SEI é de **inteira** e **exclusiva responsabilidade da licitante**, incluindo qualquer acesso efetuado diretamente ou por seu representante, não cabendo ao **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, promotora da licitação, **qualquer responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.**

16.1.1.4. Para fins do atendimento do disposto no item anterior, antes da assinatura da Ata de Registro de Preços – ARP, será solicitado do representante da fornecedora o preenchimento de cadastro disponível no endereço eletrônico: **https://sei.mpam.mp.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0** e envio dos seguintes documentos:

I – Documento de identidade;

II – Cadastro de Pessoa Física – CPF;

III – Comprovante de residência atualizado.

IV – Ato constitutivo e suas alterações, devidamente registrados; e

V – Ato de nomeação ou eleição de dirigentes ou procuração, quando for o caso, devidamente registrados.

16.1.1.5. Será dispensado da apresentação dos documentos referidos o representante que já os tiver enviado durante a sessão pública do pregão.

16.1.1.6. Ao assinar o termo contratual ou instrumento equivalente, a empresa adjudicatária obriga-se a fornecer/executar os bens/serviços a ela adjudicados, conforme especificações e condições contidas neste edital, em seus anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital;

16.2. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.2.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

16.2.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

16.2.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

16.3. A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

16.4. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.5. Na assinatura do contrato (instrumento equivalente) ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

16.6. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato (ou outro instrumento equivalente) ou a ata de registro de preços, a

Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a

proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato (ou outro instrumento equivalente) ou a ata de registro de preços.

17. DAS OBRIGAÇÕES DA CONTRATADA

17.1. Além das obrigações compreendidas **nos itens 3, 5, 7 e 10 do TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, *Anexo I* a este Edital, bem como na Minuta do Termo de Garantia, *Anexo II*, serão também deveres da CONTRATADA:

17.1.1. Manter as condições de habilitação, como condição para emissão da nota de empenho, cuja confirmação será feita através de consulta ao SICAF ou através da internet nos respectivos sites dos órgãos emissores das certidões de regularidade fiscal.

17.2. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou recusar-se injustificadamente a receber a nota de empenho no prazo estabelecido, os demais licitantes serão convocados observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

17.2.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração.

17.3. A empresa deverá encaminhar, quando solicitado, via fax ou e-mail, banco, agência e número da conta-corrente, endereço, telefone e representante legal da empresa, com o nº do CNPJ e Inscrição Estadual ou Inscrição Municipal.

18. DAS OBRIGAÇÕES DA CONTRATANTE

18.1. As obrigações desta contratante constituem o **Item 11 do TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252**, *Anexo I* a este Edital.

19. DO PAGAMENTO

19.1. O pagamento resultante da contratação do objeto, será efetuado de acordo com este Edital, em consonância, também, com a proposta de preços aceita pela Administração.

19.2. O pagamento devido à CONTRATADA será creditado em conta-corrente por meio de ordem bancária, efetuado mediante apresentação de nota fiscal/fatura atestada e visada pelos órgãos de fiscalização e acompanhamento do fornecimento do material, no prazo não superior a 30 (trinta) dias, contados a partir do atesto da Administração na fatura apresentada.

19.2.1. As respectivas notas fiscais/faturas, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverão estar devidamente discriminadas, em nome da PROCURADORIA-GERAL DE JUSTIÇA, CNPJ n.º 04.153.748/0001-85, e acompanhada das respectivas Certidões Negativas de Débito para com a Seguridade Social, para com o Fundo de Garantia por Tempo de Serviço, junto à Justiça Trabalhista e, ainda, das certidões de regularidade junto à Fazenda Federal, Estadual e Municipal, conforme descrito no link http://www.mpam.mp.br/servicos-sp-261893274/licitacoes/34-

licitacoes/paginas-internas-licitacoes/2148-orientacaopagamentofornecedor;

19.2.2. Deverão constar das Notas Fiscais as especificações dos produtos, o número da Nota de Empenho e da Ata de Registro de Preços, conforme o caso;

19.2.3. Enquanto pendente de liquidação, por obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, nenhum pagamento será efetuado à Contratada, sem que isso gere direito a acréscimos de qualquer natureza.

19.3. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da CONTRATADA, importará prorrogação automática do prazo de vencimento da obrigação do Contratante.

19.4. Nenhum pagamento isentará o fornecedor das responsabilidades atinentes ao objeto contratual, nem tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

19.5. A nota fiscal (atestada) e os documentos exigidos no edital e no contrato (ou outro instrumento equivalente), para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, no Setor de Protocolo da CONTRATANTE.

19.6. Como condição para emissão da nota de empenho, a licitante vencedora deverá manter as mesmas condições de habilitação, cuja confirmação será feita através de consulta ao SICAF ou através da internet nos respectivos sites dos órgãos emissores das certidões de regularidade fiscal.

19.7. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou se recusar injustificadamente a recebê-la no prazo estabelecido, os demais licitantes serão convocados, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

19.7.1. **Como condição inafastável a que seja emitida Nota de Empenho à Fornecedora**, esta deverá, também, estar cadastrada junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores – da Secretaria da Fazendo do Estado do Amazonas – SEFAZ.

19.7.1.1. Com relação ao Cadastramento de Credores, a empresa deverá providenciar o envio dos documentos abaixo elencados ao órgão promotor da licitação (MPAM), durante o certame no próprio Sistema Comprasnet na fase de envio da proposta, quando convocado pelo Pregoeiro ou posteriormente após a adjudicação para o endereço eletrônico **licitacao@mpam.mp.br**, no prazo indicado no subitem anterior, sendo que naqueles primeiros momentos não serão motivos para sua desclassificação, todavia, poderá a vir responder a procedimento apuratório por eventual retardamento da licitação com possível aplicação das sanções previstas neste Edital, bem como perda do direito de preferência à contratação em favor dos demais licitantes subsequentes quando convocado posteriormente e deixar de atender no prazo fixado:

a) Carta solicitando o cadastramento (conforme Anexo V);

b) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;
c) Cópia legível dos dados bancários (por ex: extrato, cópia reprográfica de cartão bancário etc.).

20. DAS SANÇÕES ADMINISTRATIVAS

20.1. Comete infração administrativa, nos termos da Lei nº 10.520/2012, cumulada com aplicação de multa de 30% do valor total da proposta, o licitante/adjudicatário que:

20.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
20.1.2. não assinar a ata de registro de preços, quando cabível;
20.1.3. apresentar documentação falsa;
20.1.4. deixar de entregar os documentos exigidos no certame;
20.1.5. ensejar o retardamento da execução do objeto;
20.1.6. não mantiver a proposta;
20.1.7. cometer fraude fiscal;
20.1.8. comportar-se de modo inidôneo;

20.2. As sanções do item acima **também se aplicam aos integrantes do cadastro de reserva**, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente ou com justificativa recusada pela administração pública.

20.3. Considera-se comportamento inidôneo, entre outros, **a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes**, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

20.4. As sanções serão aplicadas pela **AUTORIDADE COMPETENTE**, em processo regular que assegure ao acusado o direito prévio da citação, do contraditório e da ampla defesa, com os recursos a ela inerentes.

20.5. A falta de regularização da documentação no prazo previsto no subitem 10.12. sujeitará a licitante à aplicação das sanções previstas neste edital.

20.6. As penalidades serão obrigatoriamente publicadas no Diário Eletrônico do Ministério Público do Estado do Amazonas e registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

20.7. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções aplicadas pela **AUTORIDADE COMPETENTE** poderá aplicar ao fornecedor as seguintes sanções:

20.7.1. **Advertência** por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

20.7.2. **Multas percentuais**, nos termos estabelecidos neste Edital;

20.7.3. **Suspensão de licitar e impedimento de contratar** com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

20.7.4. **Declaração de Inidoneidade** para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o CONTRATADO ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplica com base no item anterior.

20.7.5. **Impedimento de licitar e de contratar com o ESTADO DO AMAZONAS** e descredenciamento no SICAF, pelo prazo de até cinco anos;

20.8. Se a CONTRATADA, *sem justa causa*, não cumprir as obrigações assumidas ou infringir preceitos legais, serão aplicadas, segundo a gravidade da falta, as multas previstas no **item 12** do **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252.**

20.9. As sanções de advertência, suspensão temporária de participar em licitação, impedimento de contratar com a Administração e declaração de inidoneidade para licitar ou contratar com a Administração Pública poderão ser aplicadas à CONTRATADA juntamente às de multa, as quais, por sua vez, **poderão ser descontadas dos pagamentos a serem efetuados.**

20.10. A inexecução total ou parcial do contrato enseja a sua rescisão pelos motivos legais.

20.11. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente.

20.11.1. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, o Estado ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

20.12. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias dos processos administrativos necessários à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

20.13. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

20.14. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à

Administração Pública Estadual resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

20.15. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei Estadual nº 2.794, de 2003.

20.16. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

20.17. O fluxo procedimental quanto aos processos administrativos sancionadores no âmbito do Ministério Público do Estado do Amazonas está disciplinado no Ato PGJ n.º 187/2021 (publicado no DOMPE, Ed. 2170, de 12.07.2021).

21. DA REPACTUAÇÃO, REAJUSTE E REVISÃO DE PREÇOS

21.1. A interessada deverá protocolar o seu pedido de repactuação, reajuste e revisão de preços antes da assinatura da Ata de Registro de Preços ou de instrumento equivalente, **em até 5 (cinco) dias do recebimento da Nota de Empenho**, sob pena de não apreciação do pedido por intempestividade.

21.1.1. Deverá constar do pedido a planilha de custos e documentos comprovantes da situação superveniente, decorrente de caso fortuito ou de força maior.

21.1.2. A **CONTRATADA** deverá demonstrar de maneira clara a composição do preço de cada item constante de sua proposta, através de Planilha de Custos contendo, por exemplo: as parcelas relativas à mão de obra direta, demais insumos, encargos em geral, lucro e participação percentual em relação ao preço final.

21.2. A não-apresentação da planilha de custos impossibilitará o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** de proceder o reequilíbrio, reajuste ou revisão de preços, caso venha a empresa contratada solicitar qualquer uma dessas alterações no contrato (ou outro instrumento equivalente).

21.3. A cada pedido de reequilíbrio, reajuste ou revisão de preço, deverá a contratada comprovar e justificar as alterações havidas na planilha apresentada à época da elaboração da proposta, demonstrando a nova composição do preço.

21.4. No caso do detentor do registro de preços/contratado ser revendedor ou representante comercial deverá demonstrar de maneira clara a composição do preço constante de sua proposta, com descrição das parcelas relativas ao valor de aquisição do produto com notas fiscais de fábrica/indústria, encargos em geral, lucro e participação percentual de cada item em relação ao preço final (*planilha de custos*).

21.5. **A critério do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, poderá ser exigido da contratada, listas de preços expedidas pelos fabricantes, que conterão, obrigatoriamente, a data de início de sua vigência e numeração sequencial, para instrução

de pedidos de revisão de preços.

21.6. Na análise do pedido de reequilíbrio, reajuste ou revisão, dentre outros critérios, o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** adotará, para verificação dos preços constantes dos demonstrativos que acompanhem o pedido, pesquisa de mercado dentre empresas de reconhecido porte mercantil, produtoras e /ou comercializadoras, a ser realizada pela própria unidade ou por instituto de pesquisa, utilizando-se, também, de índices setoriais ou outros adotados pelo Governo Estadual, devendo a deliberação de deferimento ou indeferimento da alteração solicitada ser instruída com justificativa da escolha do critério e memória dos respectivos cálculos, para decisão da Administração.

21.7. O percentual de diferença entre os preços de mercado vigentes à época do julgamento da licitação, devidamente apurado, e os propostos pela CONTRATADA/Detentora do registro de preços será mantido durante toda a vigência do registro. O percentual não poderá ser alterado de forma a configurar reajuste econômico durante a vigência deste registro.

21.8. A repactuação, reajuste ou revisão do preço, caso deferido, somente terá validade a partir da data da publicação da deliberação na Imprensa Oficial.

21.9. **É vedado à contratada interromper o fornecimento ou a prestação do serviço enquanto aguarda o trâmite do processo de reequilíbrio, reajuste ou revisão de preços, estando, neste caso, sujeita às sanções previstas neste Edital.**

21.10. A repactuação, reajuste ou revisão levará em consideração preponderantemente as normas legais federais e estaduais, que são soberanas à previsão do conteúdo exposto neste item.

22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

22.1. Até o dia **15/02/2021, 03 (três) dias úteis antes da data designada para a abertura da sessão pública**, qualquer pessoa poderá impugnar este Edital, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.2. A impugnação poderá ser realizada por forma eletrônica (preferencialmente), pelo e-mail **licitacao@mpam.mp.br**, no horário local de expediente da Instituição, até às 14 horas (horário local) da data limite fixada ou por petição dirigida ou protocolada no endereço constante do Rodapé, endereçado à Comissão Permanente de Licitação.

24.3. Caberá ao Pregoeiro decidir sobre a impugnação, **no prazo de até 02 (dois) dias úteis contados da data de recebimento da petição**, prorrogáveis desde que devidamente justificado, limitado ao dia anterior à data prevista de abertura, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos Anexos.

22.4. Acolhida a impugnação ou determinadas as providências requeridas, será designada nova data para realização da sessão pública, salvo quando estas não afetarem a formulação das propostas.

22.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, **até o dia 15/02/2021, 03 (três) dias úteis anteriores à data designada para abertura da sessão pública**, no horário local de expediente da Instituição (até às 14 horas – horário local), preferencialmente por meio eletrônico via internet ou no endereço indicado no rodapé do Edital, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).
22.6. O pregoeiro responderá aos pedidos de esclarecimentos **no prazo de até 02 (dois) dias úteis contados da data de recebimento do pedido**, prorrogáveis desde que devidamente justificado, limitado ao dia anterior à data prevista de abertura, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos Anexos.
22.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

22.7.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

22.8. Os pedidos de impugnações e esclarecimentos, bem como as respectivas respostas, serão divulgados no site http://www.comprasgovernamentais.gov.br, na área Gestor Público/consultas/pregões/agendados (http://comprasnet.gov.br/acesso.asp?url=/livre/Pregao/lista_pregao_filtro.asp?Opc=0) e no **site oficial do MPAM**. O fornecedor, além do acesso livre, poderá visualizar também no menu principal, no link: "visualizar impugnações /esclarecimentos/avisos".
22.9. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

23. DAS DISPOSIÇÕES FINAIS

23.1. A **COMISSÃO PERMANENTE DE LICITAÇÃO** prestará todos os esclarecimentos solicitados pelos interessados nesta licitação, estando disponível para atendimento de segunda a sexta-feira, das 8 às 14 horas, na Av. Coronel Teixeira, 7.995, Nova Esperança, Manaus – AM, pelos telefones (92) 3655-0701, (92) 3655-0743 ou, ainda, pelo e-mail: **licitacao@mpam.mp.br**.
23.2. A **Autoridade Competente** designará o pregoeiro que conduzirá esta licitação, necessariamente escolhido dentre os Pregoeiros Oficiais do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.
23.3. É facultada ao pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

23.3.1. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível

a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

23.3.2. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o subitem anterior, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas de antecedência**, e a ocorrência será registrada em ata.

23.4. A **Autoridade Competente** para determinar a contratação poderá revogar a licitação por razões de interesse público derivado de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

23.4.1. No caso de revogação ou anulação do procedimento licitatório, ficará assegurada oportunidade de ampla e prévia manifestação dos interessados, na forma da Lei.

23.4.2. A anulação pode ser declarada a qualquer tempo.

23.4.3. As licitantes não terão direito a indenização em decorrência de anulação do procedimento licitatório, ressalvado o direito do FORNECEDOR de boa-fé de ser ressarcida pelos encargos que tiver suportado em eventual cumprimento da obrigação decorrente da execução do objeto deste certame.

23.5. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.6. Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro, sob pena de abertura de procedimento apuratório em face da conduta do licitante.

23.7. Em caso de licitante vencedor sediado fora da cidade de Manaus, cujo envio de documentos e demais solicitações ensejem utilização de serviços postais, **será obrigatória a apresentação de cópia do comprovante de envio dos itens solicitados, como forma de confirmação do atendimento aos prazos previstos em cada subitem**.

23.7.1. O comprovante poderá ser enviado para o e-mail: licitacao@mpam.mp.br**.**

23.7.2. **O descumprimento dos prazos para envio dos documentos ou demais solicitações, sem apresentação de justificativa, ensejará a desclassificação da empresa licitante, sem prejuízo das sanções cabíveis.**

23.7.3. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

23.7.3.1. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias

autenticadas em papel.

23.8. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

23.9. Fazem parte deste Edital os seguintes Anexos:

1. Anexo I – TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;
2. Anexo II – Minuta de Contrato Administrativo;
3. Anexo III – Modelo de Declarações Complementares;
4. Anexo IV – Modelo de Proposta de Preços; e
5. Anexo V – Modelo de Solicitação de Cadastramento – SEFAZ/AM.

23.10. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente normal no **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.**

23.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

23.12. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

23.13. Quando todos os licitantes forem inabilitados ou todas as propostas forem desclassificadas, o Pregoeiro poderá fixar aos licitantes o prazo de **3 (três) dias úteis** para apresentar nova documentação, ou nova proposta, escoimadas das causas que ensejaram a inabilitação ou desclassificação das empresas.

23.14. Nenhuma pessoa física ou jurídica ainda que credenciada poderá representar mais de uma empresa concorrente, sob pena de não participação das empresas representadas.

23.15. A homologação do resultado desta licitação não implicará direito à contratação.

23.16. Em substituição aos respectivos originais, todos os documentos poderão ser apresentados em cópia autenticada por Cartório competente ou conferida com o original por servidor da CPL. **Neste último caso, a autenticação administrativa poderá ser feita, preferencialmente, até o dia anterior à data prevista para o recebimento dos envelopes da Proposta e da Documentação**;

23.16.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

23.17. Somente serão aceitos propostas e lances encaminhados pelo sistema eletrônico.

23.18. É de inteira responsabilidade do licitante o acompanhamento do processo referente a este pregão eletrônico, no endereço eletrônico

http://www.comprasgovernamentais.gov.br.

23.19. Para as demais condições de contratação, observar-se-ão as disposições constantes dos Anexos deste Edital.

23.20. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital, assim como no caso de divergências entre os lançamentos no Sistema COMPRASNET, prevalecerá o Edital.

23.21. Este Edital e seus Anexos poderão ser examinados sem ônus para o interessado, antes da realização da licitação, no formato eletrônico, através de consulta aos sítios **http://www.comprasgovernamentais.gov.br** e www.mpam.mp.br, ou através do correio eletrônico da CPL, licitacao@mpam.mp.br.

23.21.1. Poderão ser, também, adquiridos impressos mediante depósito da quantia referente ao custo reprográfico, calculado no produto de R$ 0,20 (vinte centavos) por página, depositado na conta-corrente n.º 13200-4, Agência 6019-4, do Banco Bradesco S/A (237), em nome do **FUNDO DE APOIO DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.**

23.22. Os casos omissos serão resolvidos pelo Pregoeiro, com base no Ato PGJ n.º 389/2007, na Lei n.º 10.520, de 17/07/2002, no Decreto Estadual n.º 21.178, de 27/09/2000, e, subsidiariamente, na Lei n.º 8.666/93 e alterações.

23.23. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas no foro da cidade de Manaus, com exclusão expressa de qualquer outro.

M

Manaus AM, 03 de janeiro de 2022.

EDSON FREDERICO LIMA PAES BARRETO:85614017291

Assinado de forma digital por EDSON FREDERICO LIMA PAES BARRETO:85614017291
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR ASCON, ou=Presencial, ou=10470704000181, cn=EDSON FREDERICO LIMA PAES BARRETO:85614017291
Dados: 2022.02.04 17:28:45 -02'00'

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

ANEXO I
TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252

1. OBJETO

1.1 Contratação de **serviço de solução de firewall de próxima geração em alta disponibilidade**, com monitoramento, pelo **período de 48 (quarenta e oito) meses**, incluindo treinamento e serviço de migração da plataforma atual.

2. JUSTIFICATIVA

2.1 A presença digital pervasiva é essencial a todos os ramos de atuação na sociedade, especialmente aos órgãos públicos que prestam serviço direto à população, como é o caso do Ministério Público do Estado do Amazonas (MPAM). Isto exige que os sistemas institucionais estejam ininterruptamente conectados à Internet e disponíveis para acesso.

2.2 Intrinsecamente, todo sistema, equipamento e rede conectados à Internet estão sujeitos aos mais diversos tipos de ameaças virtuais. O fluxo constante de complexas e evoluídas ameaças como worms, spywares, cavalos de tróia, hackers, ladrões de identidade e diversos outros tipos de ataques, advindos tanto do ambiente externo quanto do ambiente interno, ameaçam os dispositivos conectados. Os danos causados pelas pragas virtuais podem comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações, serviços e operações de rede, atingindo recursos essenciais para o funcionamento do MPAM, o que inclui seus bens tangíveis e intangíveis, como a reputação da instituição perante a sociedade.

2.3 A Segurança da Informação é o processo que define os artefatos e políticas necessários para a proteção e manutenção da disponibilidade, integridade, confidencialidade e autenticidade de estações, servidores, usuários e informações corporativas. Atualmente, este processo, em nenhuma circunstância, pode ser composto apenas de um software antivírus instalado nas estações de trabalho e um firewall simples de bloqueio de portas. As ameaças, que podem ser internas ou externas, seguem aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas, com múltiplas camadas de proteção, de forma a reduzir os riscos, minimizando a probabilidade e os impactos de um eventual ataque cibernético.

2.4 Dessa forma, o MPAM necessita manter permanentemente, sob pena de interrupção de suas atividades e prejuízos irreparáveis, uma solução corporativa de Segurança da Informação avançada e à altura dos desafios impostos pelas ameaças. A solução precisa permitir a identificação das tentativas de invasão aos sistemas informatizados do MPAM, impedir e mitigar as vulnerabilidades existentes, além de intervir tempestivamente quando necessário, protegendo a Instituição da maior gama de ataques internos e externos existentes. Um item crucial e imprescindível em qualquer solução de Segurança da Informação é conhecido como firewall de próxima geração (NGFW).

2.5 O MPAM dispõe atualmente de equipamento do tipo NGFW em operação, da marca Palo Alto. Entretanto, trata-se de um único equipamento, sem qualquer tipo de redundância para caso de falhas, que já está obsoleto quanto ao hardware e ao software, ou seja, já foi descontinuado pelo fabricante, não dispondo das tecnologias de segurança mais atuais e avançadas. Além disto, com o crescimento do MPAM e da necessidade de conexões cada vez mais rápidas, a performance do equipamento está muito aquém do necessário, impondo diminuição da eficiência das atividades da instituição. Por fim, as licenças de atualização das definições de detecção de ameaças e de suporte técnico expiram no mês de agosto do corrente ano. A expiração das licenças não impede totalmente o funcionamento do equipamento, mas diminui sua eficácia conforme o tempo passa e novas ameaças surgem, sem que seja possível atualizar o equipamento com as respectivas definições de detecção e bloqueio. Fica inequivocadamente estabelecido que a substituição deste equipamento por sistema superior é urgente.

2.6 O sistema em questão, além das funcionalidades direta e especificamente relacionadas a segurança da informação, provê diversas outras funcionalidades necessárias ao funcionamento do MPAM, como o uso de VPN, por exemplo, sendo indispensável ao funcionamento do órgão como um todo. É ele que permite a conexão segura, fidedigna e unificada de todas as localidades de funcionamento do MPAM, em todo o estado do Amazonas, que inclui mais de 10 unidades descentralizadas na capital e de 54 comarcas do interior, perrmitindo o uso de todos os recursos informatizados utilizados pelos membros e servidors para consecução de suas atividades com a eficiência exigida para atingir os objetivos de atendimento à sociedade com a qualidade esperada.

2.7 A solução proposta visa elevar o patamar da proteção do ambiente computacional do MPAM e permitir a contínua mensuração do nível de segurança em que as redes do MPAM se encontram, bem como identificar as ações que devem ser tomadas para mantê-las em nível de segurança aceitável.

2.8 A contratação desta solução também se justifica pelos resultados que podem ser obtidos, quais sejam:

2.8.1 Operações digitais mais seguras, incluindo o bloqueio de acessos indevidos, roubos e sequestros de informações sensíveis do MPAM.

2.8.2 Ambiente tecnológico mais confiável.

2.8.3 Fornecimento de serviços de tecnologia mais estáveis.

2.8.4 Menor tempo de indisponibilidade do ambiente e dos serviços informatizados.

2.8.5 Parque tecnológico mais seguro contra ataques ou invasões.

2.8.6 Capacidade de planejamento, priorização e alocação de recursos melhorados.

2.8.7 Desempenho institucional e profissional incrementado.

2.8.8 Maior qualificação da mão de obra técnica na execução dos serviços de Segurança da Informação.

2.8.9 Adoção das melhores práticas de mercado, com inovação e assertividade.

2.9 A presente demanda está alinhada com o plano estratégico 2017-2027 do MPAM, objetivo 3.02 - Aprimorar a infraestrutura, gestão e governança de tecnologia da informação, por meio da iniciativa estratégica 3.02.2.03 - "Elaborar e implementar projeto de modernização do datacenter", além de dar suporte ao objetivo 2.11 - "Ampliar e integrar soluções em tecnologias da informação e comunicacão".

3. DESCRIÇÃO DO OBJETO

3.1 O objeto deste Termo compreende a contratação de serviço de firewall de próxima geração em alta disponibilidade, pelo **período de 48 (quarenta e oito) meses**, para instalação na sede do Ministério Público do Estado do Amazonas (MPAM), doravante denominado como CONTRATANTE, compreendendo os serviços de instalação, configuração, migração e ativação de equipamentos de segurança; de sistema de monitoramento dos serviços providos e de treinamento para a equipe do CONTRATANTE, por empresa especializada nestes tipos de serviço, doravante denominada CONTRATADA, conforme condições e especificações detalhadas neste Termo de Referência.

3.2 A contratação terá um único lote, organizado conforme tabela a seguir:

LOTE	ITEM	DESCRIÇÃO	UND	QTDE
A	01	Serviço de Firewall em Alta Disponibilidade	Meses	48
	02	Serviço de Monitoramento da Solução	Meses	48
	03	Serviço de Migração do Ambiente Atual	Unidades	01
	04	Serviço de Treinamento da Solução	Pessoas	05

3.3 O Lote deverá possuir vencedor único, ou seja, ser arrematado por um mesmo fornecedor, uma vez que os bens e serviços pretendidos estão intrinsecamente relacionados. A adjudicação dos itens, dentro do mesmo lote, para empresas diferentes pode resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo ao CONTRATANTE.

4. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO

4.1 A licitante deve apresentar, juntamente com os demais documentos de habilitação, atestado(s) de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem já ter prestado serviços de firewall (Next Generation Firewall), de forma satisfatória, com capacidade de tráfego (*troughput*) de, no mínimo, 10 (dez) Gbps, incluindo fornecimento de equipamento(s), serviço de instalação, treinamento, monitoramento e garantia de, no mínimo, 12 (doze) meses, similares ao objeto deste Termo.

4.2 Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.

5. DETALHAMENTO DO OBJETO

5.1 ESPECIFICAÇÕES GERAIS - PARA TODOS OS ITENS

5.1.1 São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

5.1.2 Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os

softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

5.1.3 Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a CONTRATANTE seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA);

5.1.4 O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 5.4.10, ou na exposição de ativos a riscos de segurança.

5.1.5 Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional MPAM.

5.1.6 A CONTRATADA deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

5.1.7 Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. Qualquer dano eventual de manuseio/transporte a CONTRATADA será obrigada a reparo imediato.

5.1.8 Quaisquer recursos materiais que tenham sido instalados nas dependências do CONTRATANTE pela CONTRATADA durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a CONTRATADA arcar com todos os custos referentes ao envio e transporte desses materiais.

5.1.9 Após o encerramento do contrato, caso haja a necessidade expressa pelo CONTRATANTE, a CONTRATADA deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada a prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do CONTRATANTE durante uma eventual transição para os serviços de outra contradada.

5.1.10 Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço será de propriedade do CONTRATANTE, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do CONTRATANTE.

5.1.11 A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

5.1.12 A CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE

5.2.1 O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de “Firewall” provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do CONTRATANTE e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

5.2.2 Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

5.2.3 Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

5.2.4 O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web.

5.2.5 Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela CONTRATADA.

5.2.6 Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

5.2.7 Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

5.2.8 Os serviços de instalação e implantação da solução serão de responsabilidade da CONTRATADA, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos

serviços especificados.

5.2.9 Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

5.2.10 Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

5.2.11 O CONTRATANTE entregará à CONTRATADA, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do CONTRATANTE e configurados pela CONTRATADA quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o CONTRATANTE.

5.2.12 O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos *appliances* que compõem a solução, operando em alta disponibilidade.

5.2.13 Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo *appliance*, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 deste Termo, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

5.2.14 Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

5.2.15 A solução deve ser capaz de atender às seguintes especificações mínimas dos serviços, a serem ofertados em uma única plataforma:

5.2.15.1 VPN

5.2.15.1.1 Suportar VPN Site-to-Site e Client-To-Site.

5.2.15.1.2 Suportar IPSec VPN.

5.2.15.1.3 Suportar SSL VPN.

5.2.15.1.4 A VPN IPSEc deve suportar 3DES.

5.2.15.1.5 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

5.2.15.1.6 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.2.15.1.7 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

5.2.15.1.8 A VPN IPSEc deve suportar AES 128 e 256 (Advanced Encryption Standard).

5.2.15.1.9 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

5.2.15.1.10 Deverá ser suportado o uso de CA interna e CA externa de terceiros.

5.2.15.1.11 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

5.2.15.1.12 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

5.2.15.1.13 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

5.2.15.1.14 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

5.2.15.1.15 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

5.2.15.1.16 Atribuição de DNS nos clientes remotos de VPN.

5.2.15.1.17 Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

5.2.15.1.18 Suportar autenticação via AD/LDAP, certificado e base de usuários local.

5.2.15.1.19 Suportar leitura e verificação de CRL (certificate revocation list).

5.2.15.1.20 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

5.2.15.1.21 Deverá manter uma conexão segura com o portal durante a sessão.

5.2.15.1.22 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 ou

superior (64 bits) e Mac OS X (v10.14 ou superior).

5.2.15.2 GEOLOCALIZAÇÃO

5.2.15.2.1 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.2.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.2.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas que as utilizem.

5.2.15.3 QOS E TRAFFIC SHAPPING

5.2.15.3.1 Suportar a criação de políticas de QoS por endereço de origem, por endereço de destino e por porta.

5.2.15.3.2 QoS deve possibilitar a definição de classes por banda garantida, banda máxima e fila de prioridade.

5.2.15.3.3 Disponibilizar estatísticas RealTime para classes de QoS.

5.2.15.3.4 Deve fazer controle de banda por aplicação, por usuário e por IP.

5.2.15.4 IDENTIFICAÇÃO DE USUÁRIOS

5.2.15.4.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.

5.2.15.4.2 A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários.

5.2.15.4.3 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites de usuários ou qualquer tipo de restrição de uso, como a utilização de sistemas virtuais ou segmentos de rede, mas não se limitando a estes.

5.2.15.4.4 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.2.15.4.5 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.7 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular.

5.2.15.4.8 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.

5.2.15.5 CONTROLE DE APLICAÇÃO E FILTRO URL

5.2.15.5.1 Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

5.2.15.5.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.5.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.

5.2.15.5.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

5.2.15.5.5 Possuir pelo menos 60 categorias de URLs.

5.2.15.5.6 Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

5.2.15.5.7 Permitir a customização de página de bloqueio.

5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente

bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).

5.2.15.5.9 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

5.2.15.5.10 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

5.2.15.5.11 Reconhecer pelo menos 2700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, e-mail e compartilhamento de arquivos.

5.2.15.5.12 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.

5.2.15.5.13 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

5.2.15.5.14 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a, Bittorrent e aplicações VOIP que utilizam criptografia proprietária.

5.2.15.5.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

5.2.15.5.16 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.

5.2.15.5.17 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.2.15.5.18 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação.

5.2.15.5.19 Identificar o uso de táticas evasivas via comunicações criptografadas.

5.2.15.5.20 Atualizar a base de assinaturas de aplicações automaticamente.

5.2.15.5.21 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

5.2.15.5.22 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

5.2.15.5.23 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo.

5.2.15.5.24 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

5.2.15.5.25 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

5.2.15.5.26 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

5.2.15.5.27 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, Emule, etc), possuindo granularidade de controle/políticas para cada um deles.

5.2.15.5.28 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (WhatsApp, AIM, Hangouts, Facebook Chat, etc), possuindo granularidade de controle/políticas para cada um deles.

5.2.15.5.29 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.

5.2.15.5.30 Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para cada uma delas.

5.2.15.5.31 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como a tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc).

5.2.15.5.32 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como o nível de risco da aplicação.

5.2.15.5.33 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como a categoria da aplicação.

5.2.15.5.34 Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto.

5.2.15.5.35 Deve possuir categoria específica para classificar domínios recém registrados, com menos de 32 (trinta e dois) dias.

5.2.15.6.36 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução.

5.2.15.6 PREVENÇÃO DE AMEAÇAS COM IPS, ANTIVÍRUS E ANTI-BOT

5.2.15.6.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

5.2.15.6.2 Deve incluir assinaturas de prevenção de intrusão (IPS).

5.2.15.6.3 Deve incluir assinaturas de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

5.2.15.6.4 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por toda a vigência do contrato.

5.2.15.6.5 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

5.2.15.6.6 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU ou memória do dispositivo.

5.2.15.6.7 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear.

5.2.15.6.8 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

5.2.15.6.9 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.6.10 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

5.2.15.6.11 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

5.2.15.6.12 Deve permitir o bloqueio de vulnerabilidades.

5.2.15.6.13 Deve permitir o bloqueio de exploits conhecidos.

5.2.15.6.14 Deve incluir proteção contra-ataques de negação de serviços.

5.2.15.6.15 Deverá possuir os seguintes mecanismos de inspeção de IPS: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

5.2.15.6.16 Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

5.2.15.6.17 Detectar e bloquear a origem de port scans.

5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos.

5.2.15.6.19 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

5.2.15.6.20 Possuir assinaturas para bloqueio de ataques de buffer overflow.

5.2.15.6.21 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.

5.2.15.6.23 Suportar bloqueio de arquivos por tipo.

5.2.15.6.24 Identificar e bloquear comunicação com botnets.

5.2.15.6.25 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.

5.2.15.6.27 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação através da console de gerência centralizada.

5.2.15.6.28 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de

resolução de nome para domínios maliciosos de botnets conhecidas.

5.2.15.6.29 Os eventos devem identificar o país de onde partiu a ameaça.

5.2.15.6.30 A solução deve ter um mecanismo centralizado de correlação e relatório de evento para IPS, Antivírus e Anti-bot.

5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

5.2.15.6.33 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança.

5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox.

5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY

5.2.15.7.1 O relatório das emulações deve apresentar a listagem dos arquivos emulados.

5.2.15.7.2 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks.

5.2.15.7.3 Caso a Prevenção de Ameaças 0-Day seja ofertada no modelo de appliance, o hardware e software fornecido não podem constar, em momento algum durante a vigência do contrato, em listas de end-of-sale, end-of-support, end-of engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2.15.7.4 Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS.

5.2.15.7.5 A solução deve ser capaz de inspecionar o tráfego criptografado SSL.

5.2.15.7.6 A solução de Emulação, deve possuir engine onde remove os conteúdos ativos e exploits a partir do documento inspecionado.

5.2.15.7.7 A solução deve possuir engine onde faça Mitigação DNS, sendo ela possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso.

5.2.15.7.8 Implementar e identificar existência de malware em anexos de e-mail e URLs conhecidas.

5.2.15.7.9 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

5.2.15.7.10 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF.

5.2.15.7.11 A solução deve fornecer a capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, incluindo, no mínimo, as versões de Windows suportadas pela Microsoft.

5.2.15.7.12 A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

5.2.15.7.13 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.

5.2.15.7.14 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

5.2.15.7.15 Implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle).

5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

5.2.15.7.17 A solução de emulação, deverá suportar a inspeção/bloqueio de malwares em tempo real para determinar o veredito e bloqueio de um malware.

5.2.15.7.18 Implementar atualização a base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização.

5.2.15.7.19 Deve realizar bloqueio de ameaças avançadas de dia zero independente do sistema operacional.

5.2.15.7.20 O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos

pacotes por regra individualmente visando otimizar a performance do equipamento.

5.2.15.7.21 A solução deve apresentar informações comportamental incluindo listagem de módulos e processos utilizados pelo malware e/ou código malicioso de forma sequencial.

5.2.15.7.22 Toda análise poderá ser realizada em nuvem, desde que do mesmo fabricante da solução.

5.2.15.7.23 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador para solicitar a análise.

5.2.15.7.24 Todas as máquinas virtuais utilizadas na nuvem do fabricante devem estar integralmente instaladas e licenciadas pelo período do contrato, sem a necessidade de intervenções por parte do administrador do sistema, e, as atualizações deverão ser providas pelo fabricante.

5.2.15.7.25 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.

5.2.15.7.26 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

5.2.15.7.27 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede, endereço IP.

5.2.15.7.28 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado. A solução deve suportar a inspeção de, no mínimo, os seguintes tipos de arquivos: CAB, DOC, DOCX, DOCM, DOT, DOTM, DOTX, EXE, HWP, JAR, PDF, PIF, PPAM, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, RAR, RTF, Seven-Z, SLDM, SLDX, SWF, TAR, TGZ, XLA, XLAM, XLL, XLW, XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, ZIP.

5.2.15.7.29 Implementar sincronização de hora através de protocolo NTP.

5.2.15.7.30 A solução, deve emular e eliminar malwares contidos em anexos de e-mail e documentos baixados da web.

5.2.15.7.31 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções e gráfico da taxa de transferência de tráfego monitorado.

5.2.15.7.32 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro.

5.2.15.7.33 A solução deve permitir visualizar a quantidade de arquivos emulados pela solução.

5.2.15.7.34 A solução deve permitir a visualização da fila de arquivos que serão emulados.

5.2.15.7.35 O relatório das emulações deve conter todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos.

5.2.15.7.36 A solução de sandboxing deve possuir mecanismo independente onde sua ação não depende de engines externas como antivírus, anti-malware.

5.2.15.7.37 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados.

5.2.15.7.38 O sistema de emulação deve exibir percentual de arquivos escaneados.

5.2.15.7.39 A solução deve permitir a criação de White list baseado em hash de arquivo.

5.2.15.7.40 A solução deve possuir serviço web online para categorização atualizada de sites e para definições de Widget atualizadas. As respostas recebidas pelo gateway de segurança são armazenadas localmente para otimizar o desempenho. Quando um acesso não puder ser categorizado com os dados armazenados localmente, a solução deve possuir funcionalidade que bloqueia ou permite o tráfego até que a mesma seja classificada.

5.2.15.8 NEXT GENERATION FIREWALL

5.2.15.8.1 Deverá possuir certificação ICSA para Firewall.

5.2.15.8.2 Deve permitir controle de acesso à internet por períodos do dia, mês e ano, permitindo a aplicação de políticas por horários e por dia da semana.

5.2.15.8.3 Deve permitir realizar checagem de regras para conformidade e sombreamento de regras prioritárias top-down.

5.2.15.8.4 Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado.

5.2.15.8.5 O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance.

5.2.15.8.6 Deve suportar atuação como cliente NTP (Network Time Protocol) versões 1, 2, 3 e 4.

5.2.15.8.7 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.

5.2.15.8.8 Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-interfaces lógicas associadas a VLANs.

5.2.15.8.9 A comunicação entre a solução de gerência e os appliances de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada;

5.2.15.8.10 Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos.

5.2.15.8.11 A solução deve permitir que em caso de falha de comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do appliance de segurança.

5.2.15.8.12 Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas e degradação.

5.2.15.8.13 Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário.

5.2.15.8.14 Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP.

5.2.15.8.15 A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: TACACS, RADIUS e certificados digitais.

5.2.15.8.16 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora.

5.2.15.8.17 Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário, roteamento com base em prioridades.

5.2.15.8.18 Deve implementar roteamento multicast (PIM-SM e PIM-DM).

5.2.15.8.19 Possuir funcionalidade de DHCP Relay e DHCP Server.

5.2.15.8.20 Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras.

5.2.15.8.21 Possuir base de regras singular sem separação de regras orientadas à versão de endereço IP utilizada.

5.2.15.8.22 Implementar sub-interfaces ethernet lógicas.

5.2.15.8.23 Deve suportar os seguintes tipos de NAT:

5.2.15.8.23.1 Dinâmico Many-to-1.

5.2.15.8.23.2 Dinâmico Many-to-Many.

5.2.15.8.23.3 Estático 1-to-1.

5.2.15.8.23.4 Estático Many-to-Many.

5.2.15.8.23.5 Estático bidirecional 1-to-1.

5.2.15.8.23.6 NAT de Origem.

5.2.15.8.23.7 NAT de Destino.

5.2.15.8.24 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

5.2.15.8.25 Deve implementar roteamento estático IPv4 e IPV6.

5.2.15.8.26 Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4.

5.2.15.8.27 Deve permitir a importação , criação e edição de regras SNORT.

5.2.15.8.28 Deve suportar aplicações multimídia como H.323 e SIP.

5.2.15.8.29 Deve permitir o funcionamento em modo transparente tipo “bridge”.

5.2.15.8.30 Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing).

5.2.15.8.31 Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.

5.2.15.8.32 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.

5.2.15.8.33 Deve ter a capacidade de inspecionar e bloquear tráfego operando nos modos de camada 2 (L2) e de camada 3 (L3).

5.2.15.8.34 Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações.

5.2.15.8.35 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar

o tráfego em nível de aplicações.

5.2.15.8.36 Promover a integração com LDAP e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações.

5.2.15.8.37 Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS.

5.2.15.8.38 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.

5.2.15.8.39 A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports".

5.2.15.8.40 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria.

5.2.15.8.41 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora.

5.2.15.8.42 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando alterações simultaneamente.

5.2.15.8.43 Habilidade de realizar upgrade via SCP ou https via interface WEB.

5.2.15.8.44 A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços.

5.2.15.8.45 A solução deverá possuir uma ferramenta onde o fabricante disponibilize HotFixes de segurança e upgrades de versão para instalação simples e com downtime apenas no curto espaço de tempo de reinicialização.

5.2.15.8.46 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.8.47 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.8.48 Deverá suportar controle de política de firewall:

5.2.15.8.48.1 Por zona de segurança.

5.2.15.8.48.2 Por porta e protocolo.

5.2.15.8.48.3 Por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

5.2.15.8.48.4 Por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.2.15.8.49 Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo, em modo transparente, tanto em Layer 2, como em Layer 3.

5.2.15.8.50 O serviço de alta disponibilidade (HA) deve sincronizar todas as sessões, certificados de-criptografados, todas as Associações de Segurança das VPNs e todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS.

5.2.15.8.51 Deve possuir monitoração de falha de link.

5.2.15.8.52 A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces.

5.2.15.8.53 Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante.

5.2.15.8.54 Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). O fluxo mínimo de análise de regras legadas devem trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

5.2.15.8.55 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

5.2.15.8.56 Deve suportar NAT64 e NAT46.

5.2.15.9 GERÊNCIA

5.2.15.9.1 Deve possuir solução de gerenciamento e administração centralizado possibilitando o gerenciamento de diversos equipamentos de proteção de rede.

5.2.15.9.2 Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a licença de maior capacidade do portfólio ou de capacidade ilimitada.

5.2.15.9.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

5.2.15.9.4 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

5.2.15.9.5 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

5.2.15.9.6 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS).

5.2.15.9.7 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

5.2.15.9.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

5.2.15.9.9 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração.

5.2.15.9.10 Suportar backup das configurações e rollback de configuração para a última configuração salva.

5.2.15.9.11 Suportar validação de regras antes de serem aplicadas.

5.2.15.9.12 Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing).

5.2.15.9.13 Deve permitir a visualização dos logs de uma regra específica em tempo real.

5.2.15.9.14 Deve possibilitar a integração com outras soluções de Gerencamento e Correlação de Eventos de Segurança (SIEM) de mercado desde que não sejam software livre.

5.2.15.9.15 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

5.2.15.9.16 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti- Malware) e similares.

5.2.15.9.17 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.

5.2.15.9.18 Deve ser possível exportar os logs em CSV.

5.2.15.9.19 Deve possibilitar a geração de relatórios de eventos no formato PDF.

5.2.15.9.20 Deve possibilitar rotação do log.

5.2.15.9.21 Deve suportar geração de relatórios com resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego.

5.2.15.9.22 Deve permitir a criação de relatórios personalizados.

5.2.15.9.23 Suportar enviar os relatórios de forma automática via arquivo em formato PDF.

5.2.15.9.24 A solução de gerência centralizada poderá ser entregue como *appliance* virtual, devendo ser compatível/homologado para o Acropolis Hypervisor Virtualization and Software - Nutanix. Caso não haja compatibilidade/homologação a CONTRATADA deverá entregar uma infraestrutura de virtualização adequada ou entregar este item da solução na forma de *appliance* físico.

5.2.15.9.25 Deve consolidar logs e relatórios de todos os dispositivos administrados.

5.2.15.9.26 Deve possuir capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

5.2.15.9.27 Deverá possuir mecanismo de detalhamento (Drill-Down) para navegação e análise dos logs em tempo real.

5.2.15.9.28 Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso.

5.2.15.9.29 Permitir a customização do padrão regulatório da própria instituição.

5.2.15.9.30 Permitir notificação instantânea ou emissão de relatório sobre mudanças de política de segurança que impactam negativamente a segurança.

5.2.15.9.31 Monitorar constantemente ou realizar emissão de relatório sobre o status de conformidade da solução aos padrões regulatórios informados.

5.2.15.9.32 Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade estabelecidas pelo CONTRATANTE ou de acordo com o padrão

estabelecido pelo fabricante.

5.2.15.9.33 Gerar alertas ou emitir relatório de conformidade sobre o impacto de suas decisões na política de segurança trazendo as considerações regulatórias na gestão de segurança estabelecidas pelo CONTRATANTE ou de acordo com o padrão pré-determinado pelo fabricante.

5.2.15.9.34 Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.

5.2.15.9.35 Possuir alertas ou emitir relatório de políticas e as potenciais violações de conformidade.

5.2.15.9.36 Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.

5.2.15.9.37 Gerar relatórios diários com base nas configurações de segurança em tempo real.

5.2.15.9.38 Permitir que os relatórios possam ser salvos, enviados e impressos.

5.2.15.9.39 Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados.

5.2.15.9.40 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

5.2.15.9.41 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

5.2.15.9.41.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação com principais eventos de segurança de acordo com a funcionalidade selecionada.

5.2.15.9.41.2 A solução deve possuir mecanismo para detectar login de administradores em horários irregulares.

5.2.15.9.41.3 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais.

5.2.15.9.41.4 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.

5.2.15.9.41.5 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius.

5.2.15.9.41.6 Permitir criações de políticas de acesso de usuários autenticada no Active Directory, que reconheçam os usuários de forma transparente.

5.2.15.9.41.7 Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados à solução.

5.2.15.9.41.8 Permitir a visualização de gráficos e mapa de ameaças.

5.2.15.9.41.9 Possuir mecanismo para que logs antigos sejam removidos automaticamente.

5.2.15.9.41.10 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.

5.2.15.9.41.11 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.

5.2.15.9.41.12 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real.

5.2.15.9.41.13 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria.

5.2.15.9.41.14 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

5.2.15.9.41.15 Caso necessite de licenciamento, a solução deverá vir totalmente licenciada para o nível mais alto de uso.

5.2.15.10 CAPACIDADES

5.2.15.10.1 Os valores mínimos e máximos a seguir servirão como margem para a CONTRATADA ofertar equipamentos que tenham capacidade compatível com os requisitos do CONTRATANTE durante o período de vigência do contrato.

5.2.15.10.2 A solução deve ser fornecida com kit para instalação em rack de 19”.

5.2.15.10.3 Os equipamentos ofertados na solução deverão ser capazes de operar com todos os recursos habilitados, mantendo os níveis de operação descritos na seção 5.9 - ACORDO DE NÍVEL DE SERVIÇO (SLA), deste Termo de Referência.

5.2.15.10.4 A CONTRATADA deverá fornecer todos os transceivers de 10G SFP+ tanto para a solução de firewall, como para os switchs do CONTRATANTE, bem como os cordões de fibra óptica. Ou seja, todas as portas de comunicação, interfaces e afins, deverão estar habilitadas e operacionais, sem custos adicionais.

5.2.15.10.5 Os hardwares e softwares oferecidos não podem constar¸ durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2.15.10.6 Para dimensionamento adequado da solução, a CONTRATADA deve levar em consideração a “Tabela de Capacidades” a seguir, que demonstra a demanda de recursos atual do CONTRATANTE, na coluna entitulada como "MÍNIMO", e a projeção de crescimento da demanda do CONTRATANTE, na coluna entitulada como "MÁXIMO". Cada conjunto da solução poderá ser entregue contemplando as capacidades mínimas da “Tabela de Capacidades”, podendo ser expandida durante toda a vigência do contrato de forma que atenda às demandas dos limites máximos especificados.

Tabela de Capacidades

	DESCRIÇÃO DO REQUISITO	MÍNIMO	MÁXIMO
5.2.15.10.7	Interface 10/100/1000 Mbit Ethernet	08	16
5.2.15.10.8	Interface 10Gbase-F SFP+	02	04
5.2.15.10.9	Interface de gerenciamento dedicada	01	01
5.2.15.10.10	Interface 10/100/1000 Mbit Ethernet BaseT dedicada para alta disponibilidade	01	01
5.2.15.10.11	Interface Console Serial	01	01
5.2.15.10.12	Fonte de alimentação redundante bivolt 100-240 VAC Hot-Swappable	02	02
5.2.15.10.13	Disco de armazenamento de 500GB HDD e/ou 240GB SSD RAID 1	01	02
5.2.15.10.14	Firewalls virtuais	10	20
5.2.15.10.15	Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps)	05	10
5.2.15.10.16	Throughput de AES-128 VPN (em Gbps)	04	08
5.2.15.10.17	Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps)	2,5	05
5.2.15.10.18	Conexões simultâneas (em milhões)	02	04
5.2.15.10.19	Novas conexões por segundo (em milhares)	100	180
5.2.15.10.20	Suportar e estar licenciado para acesso remoto Client-to-site (VPN SSL)	200	400

***** Baseado em amostras reais, ou seja, não serão aceitos testes usando UDP, HTTP 1M ou testes em laboratório.

5.3 ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO

5.3.1 Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

5.3.2 Deverá ser baseado em Dashboard, para fácil visualização.

5.3.3 Deve ser entregue com regras genéricas criadas pela CONTRATADA, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

5.3.4 O serviço da CONTRATADA deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo CONTRATANTE.

5.3.5 Deve possuir acesso WEB (HTTPS).

5.3.6 Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

5.3.7 Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

5.4 ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

5.4.1 O CONTRATANTE possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.2 O CONTRATANTE possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links “full-route” BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.3 A CONTRATADA deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

5.4.4 O CONTRATANTE possui infraestrutura hiper convergente, e para tanto usa o Acropolis Hypervisor Virtualization and Software - Nutanix. Assim, caso a CONTRATADA necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do CONTRATANTE.

5.4.5 A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

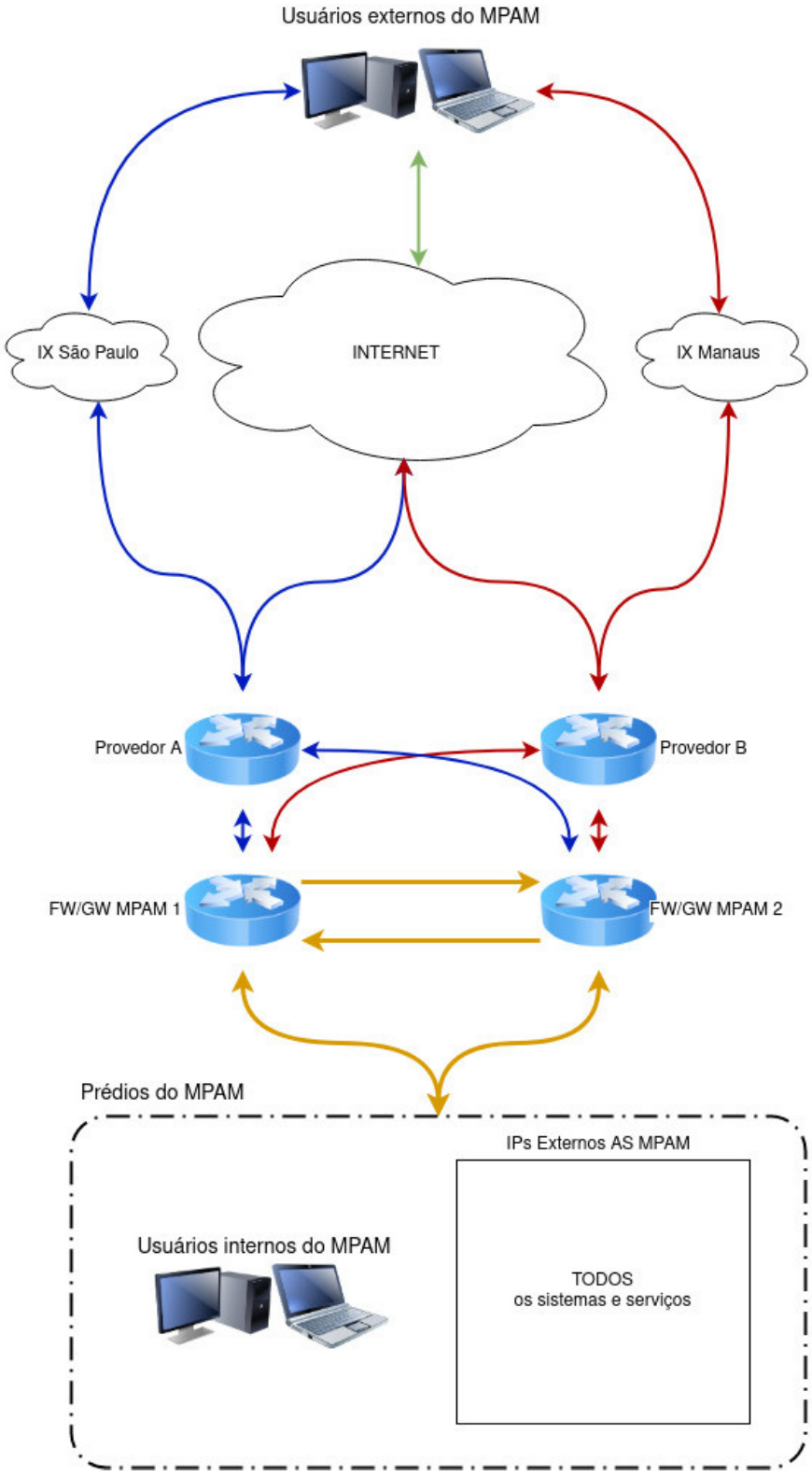
5.4.6 A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

5.4.7 A CONTRATADA deverá evitar, durante o processo de migração, interromper os serviços de rede do CONTRATANTE, nos horários das 8hs às 18hs, em dias de expediente do CONTRATANTE.

5.4.8 É de responsabilidade da CONTRATADA a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do CONTRATANTE fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

5.4.9 A CONTRATADA deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CONTRATANTE, sendo vedada sua cessão, locação ou venda a terceiros.

5.4.10 A topologia da solução deve seguir conforme imagem a seguir:



5.5 ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO

5.5.1 A CONTRATADA deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.5.2 A carga horária total para o treinamento deve ser de, no mínimo, 40 horas.

5.5.3 A CONTRATADA deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela FISCALIZAÇÂO.

5.5.4 O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fonecido em português do Brasil ou inglês.

5.5.5 O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do CONTRATANTE.

5.5.6 O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a CONTRATADA deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o CONTRATANTE. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.5.7 A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.5.8 A CONTRATADA deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.5.9 Caso o treinamento seja ofertado de forma presencial, o CONTRATANTE irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do CONTRATANTE.

5.5.10 O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a CONTRATADA deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do CONTRATANTE.

5.5.11 Será de responsabilidade da CONTRATADA prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.5.12 A CONTRATADA deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.5.13 Os instrutores designados pela CONTRATADA deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.5.14 A CONTRATADA deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.5.15 A CONTRATADA deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do CONTRATANTE e com finalidade de uso exclusivamente interno do CONTRATANTE, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela CONTRATADA.

5.6 SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS

5.6.1 A CONTRATADA deverá disponibilizar ao CONTRATANTE um número telefônico único, um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entende-se por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS.

5.6.2 No atendimento por meio de telefone a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

5.6.3 O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

5.6.4 Cada chamado deverá conter, no mínimo, as seguintes informações:

5.6.4.1 Número único do registro/ocorrência - a ser fornecido pela CONTRATADA.

5.6.4.2 Identificação do atendente.

5.6.4.3 Identificação do solicitante.

5.6.4.4 Data e hora de abertura do chamado/início da interrupção.

5.6.4.5 Descrição da ocorrência.

5.6.4.6 Designação do equipamento, quando for o caso.

5.6.4.7 Ações corretivas tomadas.

5.6.4.8 Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

5.6.5 O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

5.6.6 O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA.

5.6.7 Não deverá haver qualquer limitação para o número de solicitações de reparo.

5.6.8 O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a CONTRATADA deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

5.7 GARANTIA TÉCNICA

5.7.1 A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

5.7.2 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.

5.7.3 Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.

5.7.4 A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao CONTRATANTE.

5.7.5 Caso sejam detectadas falhas ou bugs nos produtos, a CONTRATADA deverá realizar as atualizações necessárias à correção do problema.

5.7.6 A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

5.7.7 A CONTRATADA é a única responsável pelos produtos fornecidos ao CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

5.7.8 A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo CONTRATANTE, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

5.7.9 Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à CONTRATADA apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.

5.7.10 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

5.7.11 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o CONTRATANTE.

5.7.12 No que se refere a software, durante a vigência do Contrato, a CONTRATADA deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o CONTRATANTE. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

5.7.12.1 Patches, fixes, correções, updates e service packs.

5.7.12.2 Novas releases, builds e funcionalidades.

5.7.12.3 O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.

5.7.12.4 O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.

5.7.12.5 Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.

5.7.12.6 A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

5.7.12.7 A CONTRATADA deverá fornecer tais atualizações independentemente de solicitação expressa do CONTRATANTE.

5.7.12.8 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

5.7.12.9 As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA

5.8.1 Os serviços de manutenção *on-site*, serão prestados nas dependências do CONTRATANTE na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

5.8.2 O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do CONTRATANTE, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

5.8.3 A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

5.8.4 A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

5.8.5 Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

5.8.6 A CONTRATADA deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo CONTRATANTE ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser realizada nas dependências do CONTRATANTE, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

5.8.7 O CONTRATANTE poderá determinar à CONTRATADA a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da CONTRATADA.

5.8.8 Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional ao CONTRATANTE.

5.8.9 A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do CONTRATANTE.

5.8.10 O serviço de suporte deverá ser efetuado *on-site* sempre que se fizer necessário ou quando for solicitado pelo CONTRATANTE, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o CONTRATANTE.

5.8.11 Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do CONTRATANTE, a CONTRATADA deverá desinstalar, embalar e transportar o item defeituoso, instalar

item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

5.8.12 Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar o CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

5.8.13 A CONTRATADA encaminhará mensagem de e-mail para o CONTRATANTE, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

5.8.14 Todos os custos diretos e indiretos para realização do atendimento presencial (*on-site*) serão de responsabilidade exclusiva da CONTRATADA.

5.8.15 Dentro do mesmo endereço, a ser executada pela CONTRATADA, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o CONTRATANTE.

5.8.16 Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

5.8.17 O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do CONTRATANTE, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

5.8.18 Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas.

5.9 ACORDO DE NÍVEL DE SERVIÇO (SLA)

5.9.1 Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos nesse Termo de Referência.

5.9.2 A CONTRATADA deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

5.9.3 A CONTRATADA deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

5.9.4 A realização de assistência técnica preventiva, caso não seja solicitada pelo CONTRATANTE, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do CONTRATANTE.

5.9.5 Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.6 Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.7 Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do CONTRATANTE, a solução será considerada como operando em Modo de Contingência.

5.9.8 Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

5.9.9 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual. Este checkup faz parte da manutenção preventiva.

5.9.10 Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.

5.9.11 O Modo de Contingência se caracteriza por:

5.9.11.1 Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.

5.9.11.2 Funcionamento acima dos limiares de desempenho, conforme estabelecido nas cláusulas 5.9.5 e 5.9.6 acima.

5.9.11.3 Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante ou fora de garantia.

5.9.11.4 Operação com funcionalidade ou performance abaixo dos mínimos exigidos neste Termo.

5.9.12 Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.

5.9.13 O estado de Inoperância Total se caracteriza por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do CONTRATANTE.

5.9.14 O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela CONTRATADA.

6. VISTORIA TÉCNICA

6.1 As empresas licitantes PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades do CONTRATANTE, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

6.2 Nos casos em que houver vistoria, os locais envolvidos pelos trabalhos deverão ser cuidadosamente inspecionados pelos licitantes, observando, entre outros aspectos, o grau de dificuldade para a consecução dos serviços e procederão à rigorosa conferência das medidas e de outros aspectos julgados de interesse.

6.3 A vistoria deverá ser realizada, preferencialmente, por profissional(is) qualificado(s) e detentor(es) de conhecimento técnico relacionado ao objeto, devidamente credenciados.

6.4 Para que as pretensas licitantes possam participar da vistoria, será necessária que a mesma credencie um representante, através da apresentação, no ato da visita, de documento devidamente assinado, indicando o nome de seu colaborador, número da cédula de identidade e CPF e delegação de poderes para representá-la na visita. A falta deste documento impossibilitará que o representante e a empresa participem da vistoria.

6.5 Para a realização da vistoria, as empresas interessadas deverão apresentar duas cópias da Declaração de Vistoria, já preenchida com os dados da empresa e assinada pelo representante, sendo que uma cópia será assinada por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO do CONTRATANTE, e devolvida para empresa, e a outra será juntada ao processo de contratação, onde a empresa declara ter realizado a vistoria técnica.

6.6 A referida Declaração deverá ser apresentada posteriormente, na fase licitatória, nos termos definidos no edital do certame.

6.7 Caso opte por não realizar a vistoria, a licitante apresentará na fase licitatória, declaração de opção pela dispensa de vistoria.

6.8 Não serão admitidas quaisquer alegações de desconhecimento ou erro orçamentário por parte da futura contratada, quando do cumprimento as obrigações.

6.9 A licitante poderá vistoriar o local onde serão executados os serviços até o último dia útil anterior à data fixada para a abertura da sessão pública.

6.10 As visitas deverão ser previamente agendadas, com pelo menos 5 (cinco) dias úteis de antecedência, pelo telefone (92) 3655-0660/3655-0666 — DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período de segunda a sexta-feira, das 8 às 14hs, excluídos feriados e pontos facultativos.

6.11 A vistoria será realizada no endereço do Edifício-Sede do MPAM, Avenida Coronel Teixeira, 7.995, bairro Nova Esperança, CEP 69037-473, Manaus/AM.

6.12 Todos os custos associados com a visita e a inspeção serão de inteira responsabilidade da licitante.

7. PRAZOS PARA A PRESTAÇÃO DO SERVIÇO

7.1 A CONTRATADA deverá em, no máximo, 65 (sessenta e cinco) dias corridos, contados a partir da assinatura do contrato, finalizar a implantação, ativação e entrega dos sistemas e equipamentos que compõem os itens 01, 02 e 03, especificados neste Termo de Referência.

7.2 A CONTRATADA deverá em comum acordo com o CONTRATANTE, no prazo máximo de 120 (cento e vinte) dias corridos, contados a partir da assinatura do contrato, finalizar o treinamento indicado no item 04 deste Termo de Referência.

7.3 Antes de findar os prazos fixados nos itens anteriores, a CONTRATADA poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pelo CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, 410 da lei n. 8.666/93.

7.4 O prazo da prestação dos serviços objeto deste Termo de Referência deverá contar da assinatura do contrato, prorrogáveis de comum acordo, até o limite estabelecido na Lei n. 8.666/93, e suas alterações.

8. RECEBIMENTO

8.1 O recebimento será feito nas seguintes etapas:

8.1.1 Será emitido Termo Individual de ACEITE para cada item do Lote.

8.1.2 Será emitido Termo de Recebimento Definitivo para todo o Lote.

8.2 O recebimento dos serviços será realizado pela FISCALIZAÇÃO do CONTRATANTE.

8.3 Para fins de aceite a CONTRATADA deverá comunicar formalmente a efetiva disponibilização dos serviços para cada item do Lote.

8.4 Para a emissão do Termo Individual de ACEITE para o Item 01:

8.4.1 Será emitido após Período de Funcionamento Experimental de até 15 (quinze) dias, que se iniciará após comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.4.2 Durante Período de Funcionamento Experimental a FISCALIZAÇÃO deverá concluir os testes necessários para constatar o funcionamento regular dos serviços disponibilizados.

8.4.3 A FISCALIZAÇÃO realizará avaliação qualitativa das especificações dos equipamentos e funcionalidades que compõem a solução conforme exigências deste Termo.

8.5 Para a emissão do Termo Individual de ACEITE para o Item 02:

8.5.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.5.2 A FISCALIZAÇÃO realizará testes com as credenciais fornecidas, teste de uso da ferramenta e teste de disponibilidade necessários para constatar o funcionamento regular dos serviços disponibilizados.

8.6 Para a emissão do Termo Individual de ACEITE para o Item 03:

8.6.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito, por parte da CONTRATADA, incluindo evidencias que demonstrem inequivocadamente que todas os critérios estabelecidos na seção 5.4 deste Termo foram atendidos, atestando a efetiva disponibilização dos serviços.

8.6.2 A FISCALIZAÇÃO realizará avaliação qualitativa das evidências apresentadas considerando a disponibilidade dos serviços do CONTRATANTE.

8.7 Para a emissão do Termo Individual de ACEITE para o Item 04:

8.7.1 Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da CONTRATADA atestando a efetiva disponibilização dos serviços.

8.7.2 A FISCALIZAÇÃO observará os critérios estabelecidos neção 5.5 deste Termo.

8.8 Somente depois de realizados e aprovados os testes definidos, o CONTRATANTE, por meio da FISCALIZAÇÃO, emitirá o Termo de Aceite, atestando a conformidade com as especificações neste Termo de Referência, liberando o início de faturamento.

8.9 A contagem do prazo para a efetiva entrega e prestação de cada item de serviço especificado no lote será suspenso quando a CONTRATADA comunicar a efetiva disponibilização do serviço, e, se for o caso, será retomado no dia seguinte a partir da emissão de comunicado por escrito do CONTRATANTE indicando NÃO ACEITE do serviço em virtude de não conformidade com algum dos requisitos presentes nesse termo de referência.

9. PAGAMENTO

9.1 Para os Itens 01 e 02:

9.1.1 Mensalmente, a CONTRATADA deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

9.1.2 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada dia de funcionamento da solução em Modo de Contingênica além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

9.1.3 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada hora de funcionamento da solução em estado de Inoperância Total além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

9.1.4 A data de início de cobrança dos serviços deverá observar a data de emissão do Termo de Aceite, sendo que a primeira fatura corresponderá à prestação de serviços desde a data de emissão do Termo de Aceite, para cada item do Lote, até o último dia do respectivo mês, de forma pro rata.

9.1.5 As demais faturas deverão abranger o período do primeiro ao último dia do mês.

9.1.6 Os valores a serem faturados concernentes aos serviços objeto desta contratação estarão sujeitos a descontos nas situações de descumprimento das metas estabelecidas para os indicadores elencados na especificação do serviço, item Acordo de Nível de Serviço (SLA).

9.1.7 Os descontos aplicados nas faturas mensais não isentam a CONTRATADA de quaisquer sanções legais ou das sanções dispostas na seção 12 - SANÇÕES ADMINISTRATIVAS.

9.1.8 Os descontos aplicados nas faturas mensais, conforme dispostos acima, oriundos do descumprimento dos níveis mínimos de serviço estipulados no item Acordo de Nível de Serviço (SLA), não se configuram como penalidades ou multas.

9.1.9 No primeiro dia útil do mês subsequente, antes da emissão na nota fiscal, a CONTRATADA deverá enviar à FISCALIZAÇÃO relatório referente aos períodos, destacando eventuais descontos e as causas da(s) indisponibilidade(s) ocorridas na prestação dos serviços para a devida aprovação.

9.1.10 As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da CONTRATADA no que diz respeito ao atendimento dos níveis de serviços especificados no acordo de nível de serviço, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

9.2 Para os Itens 03 e 04:

9.2.1 A CONTRATADA deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

9.2.2 Os pagamentos relativos aos Itens serão realizados de uma única vez, no mês seguinte a emissão do Termo de Aceite.

9.3 Ao CONTRATANTE fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas neste Termo de Referência.

10. OBRIGAÇÕES DA CONTRATADA

10.1 Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo, observando as prescrições e as recomendações do fabricante/fornecedor, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

10.2 Comunicar imediatamente ao CONTRATANTE, por escrito, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto desta contratação, e prestar os esclarecimentos julgados necessários.

10.3 Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que o CONTRATANTE julgar necessário.

10.4 Manter contato e realizar o planejamento dos serviços com o CONTRATANTE de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

10.5 Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, o objeto deste Termo de Referência que não atenda às especificações exigidas, em que se verifiquem imperfeições, vícios, defeitos ou incorreções ou rejeitados pela fiscalização.

10.6 Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pelo CONTRATANTE em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste Termo de Referência.

10.7 Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.

10.8 Acatar as observações feitas pelo Fiscal do CONTRATANTE quanto à execução dos serviços.

10.9 Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

10.10 A inobservância das especificações constantes deste Termo de Referência implicará a não aceitação parcial ou total dos serviços, devendo a CONTRATADA refazer as partes recusadas sem direito a indenização.

10.11 Seguir as orientações da Lei n. 9.472/97, do Termo de Concessão ou autorização emitido pela ANATEL, e demais disposições regulamentares pertinentes aos serviços a serem prestados.

10.12 Todos os equipamentos fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área, tais como: ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações).

10.13 Credenciar junto ao CONTRATANTE um representante, denominado preposto, aceito pelo CONTRATANTE, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, indicando as formas de contato no mínimo telefone, para comunicação rápida e email para comunicação formal;

10.14 Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica,

normas e legislação.

10.15 Implantar a supervisão permanente dos serviços, de modo adequado e de forma a obter uma operação correta e eficaz.

10.16 A CONTRATADA se responsabilizará por todos os serviços não explícitos nestas especificações, mas necessários à execução dos serviços programados e ao perfeito funcionamento das instalações.

10.17 Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.

10.18 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

10.19 Acatar que o CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

10.20 São expressamente vedadas à CONTRATADA:

10.20.1 A veiculação de publicidade acerca do CONTRATANTE, salvo prévia e expressa autorização deste;

10.20.2 A subcontratação total/parcial é permitida apenas para o Item 04 mantendo os critérios estabelecidos na seção 5.5 deste Termo.

11. OBRIGAÇÕES DO CONTRATANTE

11.1 Fornecer à CONTRATADA as informações necessárias à fiel execução do objeto deste Termo de Referência.

11.2 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA durante o prazo de vigência deste Contrato.

11.3 Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n. 8.666/93, o exato cumprimento das obrigações previstas neste Termo.

11.4 Designar, e informar à CONTRATADA, fiscal do contrato e seu substituto, mantendo tais dados atualizados.

11.5 Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos materiais, de forma a assegurar o perfeito cumprimento do contrato.

11.6 Anotar em registro próprio e notificar a CONTRATADA, por escrito, a ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.

11.7 Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este Termo de Referência.

11.8 Fazer uso adequado dos equipamentos fornecidos pela CONTRATADA, seguindo as instruções constantes de seus manuais de uso.

11.9 Efetuar o pagamento devido pelos serviços prestados, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas.

12. SANÇÕES ADMINISTRATIVAS

12.1 Se a CONTRATADA, sem justa causa e/ou sem justificativa apresentada e aceita pelo CONTRATANTE, não cumprir as obrigações descritas neste Termo ou infringir preceitos legais, serão aplicadas, segundo a gravidade da falta, as seguintes penalidades:

12.1.1 Advertência por escrito - Será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem corno, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do MPAM.

12.1.2 Multa de 2% (dois por cento) sobre o valor global contratado, a cada reincidência na penalidade de advertência. Na hipótese de reincidência por 5 (cinco) vezes na penalidade de advertência, será considerado descumprimento total da obrigação, punível com as sanções previstas em lei.

12.1.3 Multa de 2% (dois por cento) sobre o valor global contratado, por dia de atraso, no caso de descumprimento do tempo máximo, conforme seção 7 - PRAZOS PARA A PRESTAÇÃO DO SERVIÇOS, limitado a 10 (dez) dias. O atraso superior a 10 (dez) dias será considerado como descumprimento total da obrigação, punível com as sanções previstas em lei.

12.1.4 Multa de 10% (dez por cento) sobre o valor global contratado, no caso de, sem justificativa aceita pelo CONTRATANTE, o vencedor não retirar a Nota de Empenho, a Autorização de Fornecimento de Materiais/Serviço ou não assinar o contrato deixando, assim, de cumprir os prazos fixados, sem prejuízo das demais sanções previstas.

12.1.5 Multa de até 20% (vinte por cento) sobre o valor global contratado, nos casos de INEXECUÇÃO PARCIAL do objeto contratado.

12.1.6 Multa de até 30% (trinta por cento) sobre o valor global contratado, nos casos de INEXECUÇÃO TOTAL do objeto contratado.

12.1.7 Multa de até 30% (trinta por cento) sobre o valor global contratado, na hipótese de rescisão do contrato por culpa da

CONTRATADA.

13. ELABORAÇÃO

13.1 O presente Termo de Referência foi elaborado pela DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO, em conformidade com as atribuições legais e regimentais, estando em consonância com as disposições legais e normativas aplicáveis, com a necessidade, interesse e conveniência da Administração, sendo parte integrante do procedimento interno respectivo.

14. DECLARAÇÃO DO SOLICITANTE

14.1 Declaro que este Termo de Referência está de acordo com a Lei n. 8.666/93 e Lei n. 10.520/2002 e alterações.

THEO FERREIRA PARÁ
Agente de apoio - Manutenção/Informática

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

15. APROVAÇÃO

TADEU AZEVEDO DE MEDEIROS
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Theo Ferreira Pará**, **Agente de Apoio - Manutenção - Suporte Informática**, em 08/11/2021, às 10:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 08/11/2021, às 10:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Tadeu Azevedo de Medeiros**, **Diretor(a) de Tecnologia de Informação e Comunicação - DTIC**, em 08/11/2021, às 10:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0720733** e o código CRC **45D07F75**.

2021.015252 v7

ANEXO II
MINUTA DO CONTRATO ADMINISTRATIVO

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MINUTA DE CONTRATO ADMINISTRATIVO Nº 2.2022.DCCON.0750392.2021.015252

*** MINUTA DE DOCUMENTO**

Termo de Contrato Administrativo que entre si celebram o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e a empresa _____, visando à prestação de serviço de solução de firewall de próxima geração.

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, por intermédio de sua **PROCURADORIA-GERAL DE JUSTIÇA**, órgão de sua Administração Superior, com sede na Avenida Coronel Teixeira, 7.995, Nova Esperança, 69.037-473, Manaus/AM, inscrita no CNPJ (MF) sob o n.º 04.153.748/0001-85, doravante denominada **CONTRATANTE**, neste ato representada por _____, portador do documento de identidade n.º _____ e inscrito no CPF (MF) sob o n.º _____ e a empresa _____**,** com sede na _____, inscrita no CNPJ (MF) sob o n.º _____, daqui por diante denominada **CONTRATADA**, neste ato representada pelo _____, portador do documento de identidade n.º _____ e inscrito no CPF (MF) sob o n.º _____, tendo em vista o que consta no Processo n.º **2021.015252**, doravante referido por **PROCESSO** e, em consequência do _____, resolvem firmar o presente **TERMO DE CONTRATO ADMINISTRATIVO PARA PRESTAÇÃO DE SERVIÇO DE INFORMÁTICA,** nos termos da Lei n.º 8.666/1993 e mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

O objeto do presente ajuste é a prestação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme as especificações constantes no Termo de Referência nº 20.2021.DTIC.0720733.2021.015252.

CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO:

O objeto deste ajuste compreende a contratação de serviço de firewall de próxima geração em alta disponibilidade, pelo **período de 48 (quarenta e oito) meses**, para instalação na sede do **CONTRATANTE**, compreendendo os serviços de instalação, configuração, migração e ativação de equipamentos de segurança; de sistema de monitoramento dos serviços providos e de treinamento para a equipe do **CONTRATANTE**, pela **CONTRATADA**, conforme condições e especificações detalhadas neste Contrato.

Parágrafo primeiro. Os serviços serão prestados conforme o seguinte quantitativo:

ITEM	DESCRIÇÃO	UND	QTD
01	Serviço de Firewall em Alta Disponibilidade	Meses	48
02	Serviço de Monitoramento da Solução	Meses	48
03	Serviço de Migração do Ambiente Atual	Unidades	01
04	Serviço de Treinamento da Solução	Pessoas	05

Tabela 1 - Descrição e Quantitativo dos Serviços

CLÁUSULA TERCEIRA – DAS CARACTERÍSTICAS TÉCNICAS:

1. ESPECIFICAÇÕES GERAIS PARA TODOS OS ITENS:

1.1. São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

1.2. Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de *end-of-sale, end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

1.3. Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a **CONTRATANTE,** seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA).

1.4. O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 4.10, ou na exposição de ativos a riscos de segurança.

1.5. Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do **CONTRATANTE**.

1.6. A **CONTRATADA** deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

1.7. Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. A **CONTRATADA** será obrigada ao reparo imediato de qualquer dano eventual de manuseio/transporte .

1.8. Quaisquer recursos materiais que tenham sido instalados nas dependências do **CONTRATANTE** pela **CONTRATADA** durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a **CONTRATADA** arcar com todos os custos referentes ao envio e transporte desses materiais.

1.9. Após o encerramento do contrato, caso haja a necessidade expressa pelo **CONTRATANTE**, a **CONTRATADA** deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada à prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do **CONTRATANTE** durante uma eventual transição para os serviços de outra contradada.

1.10. Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço, será de propriedade do **CONTRATANTE**, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do **CONTRATANTE**.

1.11. A **CONTRATADA** deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

1.12. A **CONTRATADA** deverá manter o **CONTRATANTE** atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

2. ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE:

2.1. O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de “Firewall” provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do **CONTRATANTE** e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

2.2. Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

2.3. Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

2.4. O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o

atendimento via e-mail ou sítio Web.

2.5. Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela **CONTRATADA**.

2.6. Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

2.7. Deverá ser provida, por meio de um *appliance* físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

2.8. Os serviços de instalação e implantação da solução serão de responsabilidade da **CONTRATADA**, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos serviços especificados.

2.9. Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

2.10. Após a reunião de alinhamento, a **CONTRATADA** deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do **CONTRATANTE**.

2.11. O **CONTRATANTE** entregará à **CONTRATADA**, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do **CONTRATANTE** e configurados pela **CONTRATADA** quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o **CONTRATANTE**.

2.12. O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos *appliances* que compõem a solução, operando em alta disponibilidade.

2.13. Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo *appliance*, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 do Termo de Referência, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

2.14. Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

2.15. A solução deve ser capaz de atender às especificações mínimas dos serviços constante no **item 5.2.15 do Termo de Referência Nº 20.2021.DTIC.0720733.2021.015252**, integrante do Edital de Licitação nº _____, a serem ofertados em uma única plataforma.

3. ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO:

3.1. Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

3.2. Deverá ser baseado em Dashboard, para fácil visualização.

3.3. Deve ser entregue com regras genéricas criadas pela **CONTRATADA**, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

3.4. O serviço da **CONTRATADA** deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo **CONTRATANTE**.

3.5. Deve possuir acesso WEB (HTTPS).

3.6. Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

3.7. Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

4. ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

4.1. O **CONTRATANTE** possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

4.2. O **CONTRATANTE** possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links “full-route” BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

4.3. A **CONTRATADA** deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

4.4. O **CONTRATANTE** possui infraestrutura hiper convergente, e para tanto usa o Acropolis Hypervisor Virtualization and Software - Nutanix. Assim, caso a **CONTRATADA** necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do **CONTRATANTE**.

4.5. A **CONTRATADA** deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

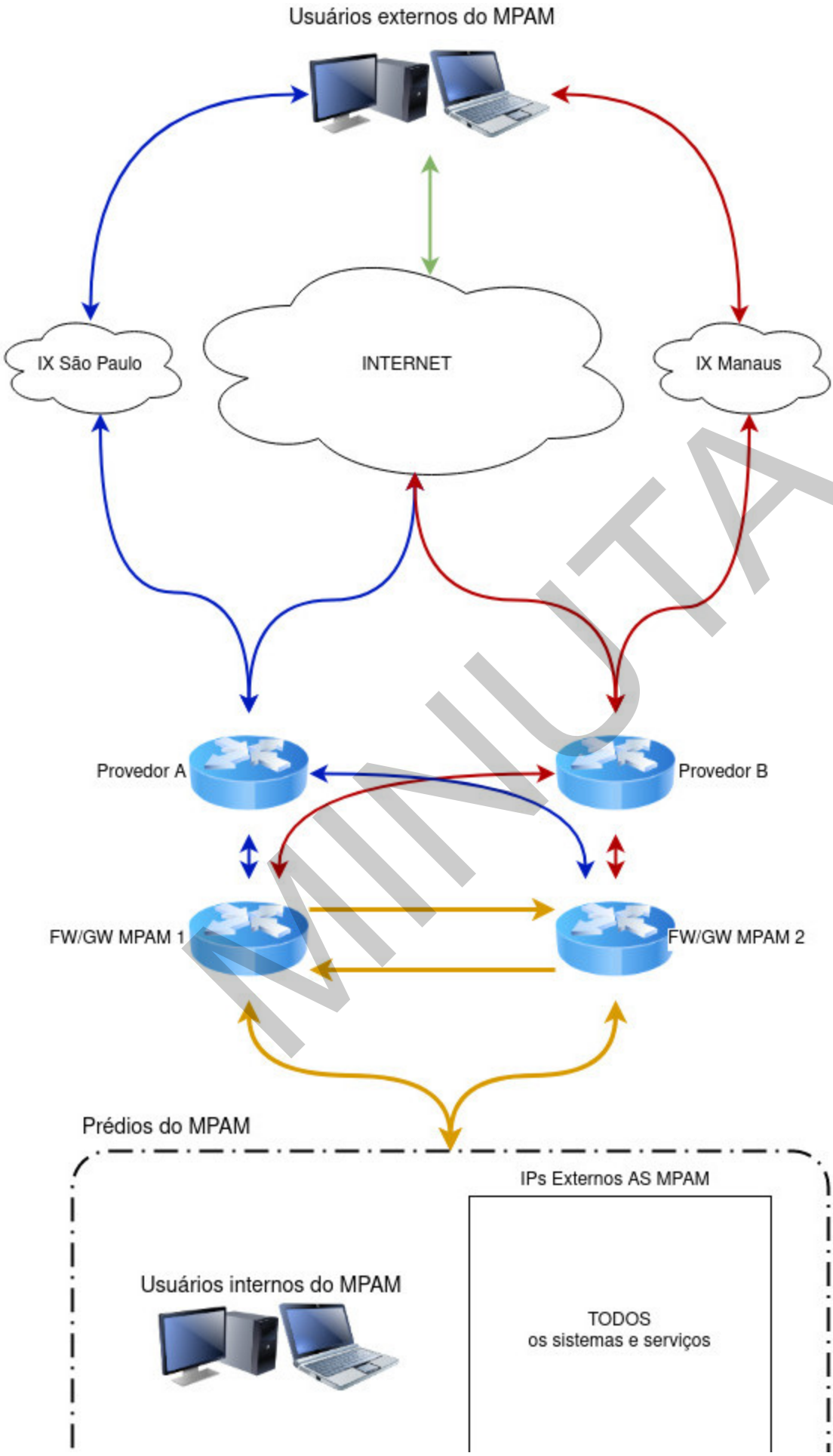
4.6. A **CONTRATADA** deverá finalizar o processo de migração após testes e aprovação pelo **CONTRATANTE** em até 60 (sessenta) dias após o seu início.

4.7. A **CONTRATADA** deverá evitar, durante o processo de migração, interromper os serviços de rede do **CONTRATANTE**, nos horários das 8hs às 18hs, em dias de expediente do **CONTRATANTE**.

4.8. É de responsabilidade da **CONTRATADA** a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do **CONTRATANTE** fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

4.9. A **CONTRATADA** deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do **CONTRATANTE**, sendo vedada sua cessão, locação ou venda a terceiros.

4.10. A topologia da solução deve seguir conforme imagem a seguir:


Usuários externos do MPAM
IX São Paulo
INTERNET
IX Manaus
Provedor A
Provedor B
FW/GW MPAM 1
FW/GW MPAM 2
Prédios do MPAM
IPs Externos AS MPAM
Usuários internos do MPAM
TODOS
os sistemas e serviços

5. ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO:

5.1. A **CONTRATADA** deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.2. A carga horária total para o treinamento deve ser de, no mínimo, **40 horas**.

5.3. A **CONTRATADA** deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela **FISCALIZAÇÃO**.

5.4. O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fonecido em português do Brasil ou inglês.

5.5. O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do **CONTRATANTE**.

5.6. O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a **CONTRATADA** deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o **CONTRATANTE**. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.7. A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.8. A **CONTRATADA** deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.9. Caso o treinamento seja ofertado de forma presencial, o **CONTRATANTE** irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do **CONTRATANTE**.

5.10. O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a **CONTRATADA** deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do **CONTRATANTE**.

5.11. Será de responsabilidade da **CONTRATADA** prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.12. A **CONTRATADA** deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.13. Os instrutores designados pela **CONTRATADA** deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.14. A **CONTRATADA** deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.15. A **CONTRATADA** deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do **CONTRATANTE** e com finalidade de uso exclusivamente interno do **CONTRATANTE**, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela **CONTRATADA**.

6. SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS:

6.1. A **CONTRATADA** deverá disponibilizar ao **CONTRATANTE** um número telefônico único, um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entende-se por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS.

6.2. No atendimento por meio de telefone a **CONTRATADA** fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

6.3. O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

6.4. Cada chamado deverá conter, no mínimo, as seguintes informações:

6.4.1. Número único do registro/ocorrência - a ser fornecido pela **CONTRATADA**.

6.4.2. Identificação do atendente.

6.4.3. Identificação do solicitante.

6.4.4. Data e hora de abertura do chamado/início da interrupção.

6.4.5. Descrição da ocorrência.

6.4.6. Designação do equipamento, quando for o caso.

6.4.7. Ações corretivas tomadas.

6.4.8. Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

6.5. O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

6.6. O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da **CONTRATADA**.

6.7. Não deverá haver qualquer limitação para o número de solicitações de reparo.

6.8. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a **CONTRATADA** deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

7. GARANTIA TÉCNICA:

7.1. A **CONTRATADA** deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

7.2. A **CONTRATADA** deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.

7.3. Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.

7.4. A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao **CONTRATANTE**.

7.5. Caso sejam detectadas falhas ou bugs nos produtos, a **CONTRATADA** deverá realizar as atualizações necessárias à correção do problema.

7.6. A **CONTRATADA** deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

7.7. A **CONTRATADA** é a única responsável pelos produtos fornecidos ao **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.

7.8. A **CONTRATADA** responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo **CONTRATANTE**, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

7.9. Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à **CONTRATADA** apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.

7.10. Os hardwares e softwares oferecidos não podem constar¸ durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

7.11. A **CONTRATADA** deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o **CONTRATANTE**.

7.12. No que se refere a software, durante a vigência do Contrato, a **CONTRATADA** deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o **CONTRATANTE**. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

7.12.1. Patches, fixes, correções, updates e service packs.

7.12.2. Novas releases, builds e funcionalidades.

7.12.3. O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.

7.12.4. O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.

7.12.5. Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.

7.12.6. A cada nova liberação de versão e release, a **CONTRATADA** deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

7.12.7. A **CONTRATADA** deverá fornecer tais atualizações independentemente de solicitação expressa do **CONTRATANTE**.

7.12.8. A **CONTRATADA** deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

7.12.9. As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

8. MANUTENÇÃO PREVENTIVA E CORRETIVA:

8.1. Os serviços de manutenção *on-site*, serão prestados nas dependências do **CONTRATANTE** na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

8.2. O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do **CONTRATANTE**, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

8.3. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

8.4. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

8.5. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

8.6. A **CONTRATADA** deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo **CONTRATANTE** ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser realizada nas dependências do **CONTRATANTE**, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

8.7. O **CONTRATANTE** poderá determinar à **CONTRATADA** a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da **CONTRATADA**.

8.8. Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da **CONTRATADA**, não devendo gerar qualquer ônus adicional ao **CONTRATANTE**.

8.9. A **CONTRATADA** deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do **CONTRATANTE**.

8.10. O serviço de suporte deverá ser efetuado *on-site* sempre que se fizer necessário ou quando for solicitado pelo **CONTRATANTE**, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o **CONTRATANTE**.

8.11. Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do **CONTRATANTE**, a **CONTRATADA** deverá desinstalar, embalar e transportar o item defeituoso, instalar item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

8.12. Quando da detecção de problemas ou inconformidades, a **CONTRATADA** deverá imediatamente abrir um chamado técnico, informar o **CONTRATANTE** e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

8.13. A **CONTRATADA** encaminhará mensagem de e-mail para o **CONTRATANTE**, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da **CONTRATADA** e/ou por meio de abertura de chamado a critério da equipe técnica do **CONTRATANTE**, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

8.14. Todos os custos diretos e indiretos para realização do atendimento presencial (*on-site*) serão de responsabilidade exclusiva da **CONTRATADA**.

8.15. Dentro do mesmo endereço, a ser executada pela **CONTRATADA**, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o **CONTRATANTE**.

8.16. Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

8.17. O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do **CONTRATANTE**, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

8.18. Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

8.19. A **CONTRATADA** deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da **CONTRATADA**, deve haver comunicação formal ao **CONTRATANTE**, incluindo as comprovações exigidas.

9. ACORDO DE NÍVEL DE SERVIÇO (SLA):

9.1. Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos neste termo.

9.2. A **CONTRATADA** deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

9.3. A **CONTRATADA** deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

9.4. A realização de assistência técnica preventiva, caso não seja solicitada pelo **CONTRATANTE**, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do **CONTRATANTE**.

9.5. Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

9.6. Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

9.7. Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do **CONTRATANTE**, a solução será considerada como operando em Modo de Contingência.

9.8. Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

9.9. A **CONTRATADA** deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual. Este checkup faz parte da manutenção preventiva.

9.10. Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.

9.11. O Modo de Contingência se caracteriza por:

9.11.1. Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.

9.11.2. Funcionamento acima dos limiares de desempenho, conforme estabelecido nos itens 9.5 e 9.6 acima.

9.11.3. Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante ou fora de garantia.

9.11.4. Operação com funcionalidade ou performance abaixo dos mínimos exigidos neste Termo.

9.12. Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.

9.13. O estado de Inoperância Total se caracteriza por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do **CONTRATANTE**.

9.14. O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela **CONTRATADA**.

CLÁUSULA QUARTA – DOS PRAZOS PARA A PRESTAÇÃO DOS SERVIÇOS:

A **CONTRATADA** deverá concluir a implantação, ativação e entrega dos sistemas e equipamentos que compõem os itens 01, 02 e 03, especificados cláusula anterior deste ajuste, **em até 65 (sessenta e cinco) dias corridos**, contados a partir da assinatura do contrato.

Parágrafo primeiro. A **CONTRATADA** deverá, em comum acordo com o **CONTRATANTE**, no prazo máximo de **120 (cento e vinte) dias corridos**, contados a partir da assinatura do contrato, finalizar o treinamento indicado no item 04 da cláusula anterior.

Parágrafo segundo. A **CONTRATADA** poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pela **CONTRATANTE**, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, da lei n. 8.666/93.

Parágrafo terceiro. Antes de findar os prazos fixados nos itens anteriores, a **CONTRATADA** poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pelo **CONTRATANTE,** que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, 410 da lei n. 8.666/93.

Parágrafo quarto. O prazo da prestação dos serviços deverá contar da assinatura do contrato, prorrogáveis de comum acordo, até o limite estabelecido na Lei n. 8.666/93, e suas alterações.

CLÁUSULA QUINTA – DO RECEBIMENTO:

O recebimento dos serviços será realizado pela **FISCALIZAÇÃO** do **CONTRATANTE**.

Parágrafo primeiro. O recebimento será feito nas seguintes etapas:

1. Será emitido Termo Individual de ACEITE para cada item do Contrato.
2. Será emitido Termo de Recebimento Definitivo para todo o Lote.

Parágrafo segundo. Para fins de aceite, a **CONTRATADA** deverá comunicar formalmente a efetiva disponibilização dos serviços para cada item do Lote:

1. Para a emissão do Termo Individual de ACEITE para o Item 01:

1.1. Será emitido após Período de Funcionamento Experimental de até 15 (quinze) dias, que se iniciará após comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

1.2. Durante Período de Funcionamento Experimental a **FISCALIZAÇÃO** deverá concluir os testes necessários para constatar o funcionamento regular dos serviços disponibilizados.

1.3. A **FISCALIZAÇÃO** realizará avaliação qualitativa das especificações dos equipamentos e funcionalidades que compõem a solução conforme exigências deste Termo.

2. Para a emissão do Termo Individual de ACEITE para o Item 02:

2.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

2.2. A **FISCALIZAÇÃO** realizará testes com as credenciais fornecidas, teste de uso da ferramenta e teste de disponibilidade necessários para constatar o funcionamento regular dos serviços disponibilizados.

3. Para a emissão do Termo Individual de ACEITE para o Item 03:

3.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito, por parte da **CONTRATADA**, incluindo evidencias que demonstrem inequivocadamente que todas os critérios estabelecidos na seção 5.4 deste Termo foram atendidos, atestando a efetiva disponibilização dos serviços.

3.2. A **FISCALIZAÇÃO** realizará avaliação qualitativa das evidências apresentadas considerando a disponibilidade dos serviços do **CONTRATANTE**.

4. Para a emissão do Termo Individual de ACEITE para o Item 04:

4.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

4.2. A **FISCALIZAÇÃO** observará os critérios estabelecidos na seção 5.5 deste Termo.

Parágrafo terceiro. Somente depois de realizados e aprovados os testes definidos, o **CONTRATANTE**, por meio da **FISCALIZAÇÃO**, emitirá o Termo de Aceite, atestando a conformidade com as especificações neste Contrato, liberando o início de faturamento.

Parágrafo quarto. A contagem do prazo para a efetiva entrega e prestação de cada item de serviço especificado no lote será suspenso quando a **CONTRATADA** comunicar a efetiva disponibilização do serviço, e, se for o caso, será retomado no dia seguinte a partir da emissão de comunicado por escrito do **CONTRATANTE** indicando NÃO ACEITE do serviço em virtude de não conformidade com algum dos requisitos presentes nesse termo de referência.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO:

A execução do objeto deste contrato dar-se-á indiretamente pela **CONTRATADA**, sob o regime de empreitada por preço global.

CLÁUSULA SÉTIMA – DAS GARANTIAS:

Os serviços ora pactuados são garantidos em conformidade com o Código de Proteção e Defesa do Consumidor, Lei n.º 8.078, de 11 de setembro de 1990, artigos 26 e 27, e nos termos do Item 7 da Cláusula Terceira deste Contrato.

CLÁUSULA OITAVA – GESTÃO E DA FISCALIZAÇÃO:

A **CONTRATANTE** nomeará um servidor ou comissão, por meio de ato específico, doravante denominado(a) **FISCALIZAÇÃO**, para gerir e fiscalizar a execução deste contrato, com autoridade para exercer, como representante da **CONTRATANTE**, toda e qualquer ação destinada ao acompanhamento da execução contratual, observando as determinações do artigo 67 da Lei n.º 8.666/93, em especial:

1. Abrir processo de gestão do presente contrato, fazendo constar todos os documentos referentes à fiscalização dos serviços.
2. Gerir, acompanhar e fiscalizar a execução dos serviços, realizando diretamente toda e qualquer comunicação com a **CONTRATADA**, mediante ofício ou outros documentos.
3. Atestar a respectiva nota fiscal/fatura emitida corretamente pela **CONTRATADA**, para a efetivação do pagamento correspondente.
4. Verificar quando da liquidação dos serviços a documentação de regularidade fiscal da **CONTRATADA**.
5. Indicar as ocorrências verificadas, determinando o que for necessário à regularização das faltas observadas.
6. Fixar prazo limite para realização das providências necessárias à regularização de eventuais vícios, defeitos ou incorreções resultantes da execução do presente contrato.
7. Solicitar à **CONTRATADA** e a seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento da avença e anexar aos autos cópia dos documentos que comprovem essas solicitações.
8. **Informar, com a antecedência necessária, o término do ajuste.**
9. Encaminhar à Administração Superior toda e qualquer modificação que se faça necessária e envolva acréscimo ou supressão de despesa e dilatação de prazos, para fins das providências administrativas indispensáveis.
10. Verificar a manutenção das condições de habilitação da **CONTRATADA**, exigindo sua regularização, durante a vigência do contrato.
11. Prestar as informações e os esclarecimentos necessários ao desenvolvimento das tarefas.
12. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições no curso de execução do objeto do contrato, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.
13. Rejeitar, no todo ou em parte, o fornecimento executado em desacordo com o contrato.
14. Comunicar à Administração, de forma imediata, as ocorrências que impliquem possíveis sanções à **CONTRATADA**, bem como as decisões e providências que ultrapassarem sua competência, para a adoção das medidas convenientes.
15. Praticar todos os demais atos e exigências que se fizerem necessários ao fiel cumprimento do presente contrato.

Parágrafo primeiro. A **FISCALIZAÇÃO** será exercida no interesse da **CONTRATANTE** e não exclui nem reduz as responsabilidades contratuais da **CONTRATADA**, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade do poder público ou de seus agentes e prepostos.

Parágrafo segundo. Quaisquer exigências da **FISCALIZAÇÃO** inerentes ao objeto deste contrato

deverão ser prontamente atendidas pela **CONTRATADA**, sem qualquer ônus para a **CONTRATANTE**.

Parágrafo terceiro. A **CONTRATADA** deverá manter preposto, aceito pela **CONTRATANTE**, para representá-la administrativamente na execução do contrato, devendo, **no prazo máximo de 10 (dez) dias da assinatura do instrumento**, informar nome, telefone, endereços e outros meios de comunicação entre a **CONTRATANTE** e o preposto responsável pela execução do contrato operacional e financeira.

Parágrafo quarto. As comunicações e notificações feitas pela **CONTRATANTE** à **CONTRATADA**, a serem realizadas sob o âmbito do presente contrato, serão feitas por meio de ofícios, e-mails ou por telefone.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA:

Constituem obrigações da **CONTRATADA**:

1. Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo, observando as prescrições e as recomendações do fabricante/fornecedor, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.
2. Comunicar imediatamente, à **CONTRATANTE**, toda e qualquer irregularidade ou dificuldade que impossibilite a execução dos serviços objeto deste contrato.
3. Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que o **CONTRATANTE** julgar necessário.
4. Manter contato e realizar o planejamento dos serviços com o **CONTRATANTE** de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.
5. Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, o objeto deste ajuste que não atenda às especificações exigidas, em que se verifiquem imperfeições, vícios, defeitos ou incorreções ou rejeitados pela fiscalização.
6. Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pelo **CONTRATANTE** em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste contrato.
7. Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.
8. Acatar as observações feitas pela **FISCALIZAÇÃO** quanto à execução dos serviços.
9. Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.
10. Reparar, corrigir, remover ou substituir, às suas expensas, no todo ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.
11. Seguir as orientações da Lei n. 9.472/97, do Termo de Concessão ou autorização emitido pela ANATEL, e demais disposições regulamentares pertinentes aos serviços a serem prestados.
12. Credenciar junto ao **CONTRATANTE** um representante, denominado preposto, aceito pelo **CONTRATANTE**, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, indicando as formas de contato no mínimo telefone, para comunicação rápida e email para comunicação formal.

13. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação.
14. Implantar a supervisão permanente dos serviços, de modo adequado e de forma a obter uma operação correta e eficaz.
15. Responsabilizar-se por todos os serviços não explícitos nestas especificações, mas necessários à execução dos serviços programados e ao perfeito funcionamento das instalações.
16. Respeitar o sistema de segurança do **CONTRATANTE** e fornecer todas as informações solicitadas por ele.
17. Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.
18. Acatar que o **CONTRATANTE** não aceitará, sob nenhum pretexto, a transferência de responsabilidade da **CONTRATADA** para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

Parágrafo primeiro. A inadimplência da **CONTRATADA**, com referência aos encargos decorrentes dos serviços constantes deste contrato, não transfere à **CONTRATANTE** a responsabilidade por seu pagamento, nem pode onerar o objeto do contrato ou restringir a manutenção contratada.

Parágrafo segundo. A **CONTRATADA** declara, antecipadamente, aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos, explicações que a **CONTRATANTE** julgar necessário.

Parágrafo terceiro. A inobservância das especificações constantes deste Contrato implicará a não aceitação parcial ou total dos serviços, devendo a **CONTRATADA** refazer as partes recusadas sem direito a indenização.

Parágrafo quarto. Todos os equipamentos fornecidos pela **CONTRATADA**, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área, tais como: ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações).

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE:

Constituem obrigações do **CONTRATANTE**:

1. Fornecer à **CONTRATADA** as informações necessárias à fiel execução do objeto deste Termo.
2. Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA** durante o prazo de vigência deste Contrato.
3. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 8.666/93, o exato cumprimento das cláusulas e condições contratuais.
4. Designar, e informar à **CONTRATADA**, fiscal do contrato e seu substituto, mantendo tais dados atualizados.
5. Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos materiais, de forma a assegurar o perfeito cumprimento do contrato.
6. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção e exigindo as

medidas reparadoras devidas.

7. Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este Termo.
8. Fazer uso adequado dos equipamentos fornecidos pela **CONTRATADA**, seguindo as instruções constantes de seus manuais de uso.
9. Efetuar regularmente o pagamento à **CONTRATADA**, conforme nota de empenho e dentro dos critérios estabelecidos neste contrato, quanto aos serviços efetivamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pela **CONTRATANTE**, bem como dos demais documentos exigidos neste termo.

CLÁUSULA DÉCIMA PRIMEIRA – DA VIGÊNCIA DO CONTRATO:

O presente contrato terá vigência de **48 (quarenta e oito) meses**, contados da sua assinatura, conforme art. 57, inciso IV, da Lei n.º 8.666/1993.

Parágrafo primeiro. O prazo acima referido terá início e vencimento em dia de expediente e terá eficácia legal após a publicação de seu extrato na impressa oficial.

CLÁUSULA DÉCIMA SEGUNDA – DO VALOR DO CONTRATO:

O valor global do presente contrato é de **R$ _____**, conforme a seguinte tabela:

ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO (B)	VALOR TOTAL
01	Serviço de Firewall em Alta Disponibilidade	Meses	48		
02	Serviço de Monitoramento da Solução	Meses	48		
03	Serviço de Migração do Ambiente Atual	Unidades	01		
04	Serviço de Treinamento da Solução	Pessoas	05		
TOTAL (R$)					

Parágrafo primeiro. A proposta apresentada pela **CONTRATADA**, datada de _____, faz parte deste instrumento contratual como anexo.

Parágrafo segundo. No preço total do contrato já estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, lucro e outros necessários ao cumprimento integral do objeto deste instrumento.

CLÁUSULA DÉCIMA TERCEIRA – DA LIQUIDAÇÃO E DO PAGAMENTO:

O pagamento será efetuado após a efetiva disponibilização dos serviços pela **CONTRATADA** e emissão pelo **CONTRATANTE** do Termo Individual de Aceite para cada item do Lote, mediante depósito na conta corrente da **CONTRATADA**, por meio de ordem bancária, seguindo as seguintes etapas:

1. Para os Itens 01 e 02:

1.1 Mensalmente, a **CONTRATADA** deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

1.2 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada dia de funcionamento da solução em Modo de Contingênica além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

1.3 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada hora de funcionamento da solução em estado de Inoperância Total além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

1.4 A data de início de cobrança dos serviços deverá observar a data de emissão do Termo de Aceite, sendo que a primeira fatura corresponderá à prestação de serviços desde a data de emissão do Termo de Aceite, para cada item do Lote, até o último dia do respectivo mês, de forma pro rata.

1.5 As demais faturas deverão abranger o período do primeiro ao último dia do mês.

1.6 Os valores a serem faturados concernentes aos serviços objeto desta contratação estarão sujeitos a descontos nas situações de descumprimento das metas estabelecidas para os indicadores elencados na especificação do serviço, item Acordo de Nível de Serviço (SLA).

1.7 Os descontos aplicados nas faturas mensais não isentam a **CONTRATADA** de quaisquer sanções legais ou das sanções dispostas na seção 12 - SANÇÕES ADMINISTRATIVAS.

1.8 Os descontos aplicados nas faturas mensais, conforme dispostos acima, oriundos do descumprimento dos níveis mínimos de serviço estipulados no item Acordo de Nível de Serviço (SLA), não se configuram como penalidades ou multas.

1.9 No primeiro dia útil do mês subsequente, antes da emissão na nota fiscal, a **CONTRATADA** deverá enviar à **FISCALIZAÇÃO** relatório referente aos períodos, destacando eventuais descontos e as causas da(s) indisponibilidade(s) ocorridas na prestação dos serviços para a devida aprovação.

1.10 As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da **CONTRATADA** no que diz respeito ao atendimento dos níveis de serviços especificados no acordo de nível de serviço, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

2. Para os Itens 03 e 04:

2.1 A **CONTRATADA** deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

2.2 Os pagamentos relativos aos Itens serão realizados de uma única vez, no mês seguinte a emissão do Termo de Aceite.

Parágrafo primeiro. A nota fiscal e os demais documentos exigidos no edital e neste contrato, para fins de liquidação e pagamento das despesas, deverão ser apresentados no Setor de Protocolo da **CONTRATANTE**, situado na Avenida Coronel Teixeira, n.º 7.995, Nova Esperança, Manaus/AM ou enviados ao e-mail **protocolo@mpam.mp.br.**

Parágrafo segundo. Ao **CONTRATANTE** fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas neste Termo.

Parágrafo terceiro. Nenhum pagamento será efetuado à **CONTRATADA** quando forem constatadas as irregularidades abaixo especificadas, sendo que tais situações não caracterizam inadimplência da **CONTRANTATE** e, por conseguinte, não geram direito à compensação financeira: a) os serviços/produtos não abrangidos pelo objeto contratual; b) ausência de comprovação da regularidade fiscal e trabalhista da **CONTRATADA**, e c) pendência de liquidação de qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

Parágrafo quarto. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

Parágrafo quinto. O atraso no pagamento decorrente das circunstâncias descritas na obrigação anterior, não exime a **CONTRATADA** de promover o pagamento de impostos e contribuições nas datas regulamentares.

Parágrafo sexto. O documento fiscal será devolvido à **CONTRATADA** caso contenha erros ou em caso de circunstância que impeça a sua liquidação, ficando o pagamento pendente até que seja sanado o problema. Nessa hipótese, o prazo para pagamento se iniciará após a regularização ou reapresentação do documento fiscal, não acarretando qualquer ônus para a **CONTRATANTE**.

Parágrafo sétimo. Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela **CONTRATANTE**, entre a data de vencimento e a do dia do efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, serão calculados por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = i ÷ 365 = (6÷100) ÷ 365 = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

Parágrafo oitavo. Aplica-se a mesma regra disposta no parágrafo anterior, na hipótese de eventual pagamento antecipado, observado o disposto no art. 40, XIV, "d", da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA:

As despesas oriundas deste contrato correrão à conta da seguinte dotação orçamentária: **Unidade Orçamentária**: _____; **Programa de Trabalho**: _____; **Fonte**: _____; **Natureza da Despesa**: _____, tendo sido emitida, pela **CONTRATANTE**, em _____, a Nota de Empenho n.º _____, no valor de **R$** _____ **(**_____**)**.

Parágrafo único. No exercício seguinte, o valor de **R$ _____ (_____)**, relativo ao complemento do contrato, será empenhado à conta de dotações consignadas para o orçamento vindouro.

CLÁUSULA DÉCIMA QUINTA – DA GARANTIA CONTRATUAL:

Nos termos do art. 56 da Lei n º 8.666, de 21/6/1993, para segurança do integral cumprimento do Contrato, a **CONTRATADA** apresentará garantia, no prazo máximo de 10 (dez) dias da assinatura deste contrato, de **5% (cinco por cento)** do valor total do contrato, que corresponde à importância de **_____.**

1. Será ainda exigida prestação de garantia adicional de valor igual à diferença entre o valor limite de exequibilidade obtido durante o certame e o valor da proposta vencedora, desde que este seja inferior a 80% (oitenta por cento) da média aritmética calculada, nos termos do § 2º, do artigo 48, da Lei Federal nº 8.666/93.

2. No caso de acréscimo no valor contratual, a licitante vencedora obriga-se a depositar junto ao Ministério Público, na mesma modalidade, o valor referente à diferença da garantia. Mesma providência deverá ser tomada no caso de prorrogação no prazo contratual para adequar o vencimento da garantia ao disposto no subitem abaixo.

3. As garantias prestadas serão liberadas após a assinatura do Termo de Encerramento do contrato, e quando em dinheiro atualizadas monetariamente, conforme dispões o § 4º, do artigo 56 da Lei n. 8.666/93.

Parágrafo primeiro. A garantia prestada deverá formalmente cobrir pagamentos não efetuados pela **CONTRATADA** referentes à:

1. prejuízos advindos do não cumprimento do objeto do contrato;

2. prejuízos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

3. multas punitivas aplicadas pela Administração à **CONTRATADA**; e

4. obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**.

Parágrafo segundo. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no parágrafo primeiro.

Parágrafo terceiro. A garantia em dinheiro deverá ser efetuada em conta caução, devidamente designada para este fim, aberta em instituição financeira oficial e mediante autorização específica da **CONTRATANTE**.

Parágrafo quarto. A garantia deverá ter validade durante a execução do contrato e estender-se-á por mais **3 (três) meses após o término da vigência contratual**. Na hipótese de prorrogação do prazo de vigência contratual, a **CONTRATADA** deverá apresentar prorrogação equivalente de prazo de validade da referida garantia.

Parágrafo quinto. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato, por dia de atraso, observado o máximo de 2% (dois por cento).

Parágrafo sexto. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a retenção dos pagamentos devidos à **CONTRATADA** e/ou a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n.º 8.666, de 1993.

1. O bloqueio efetuado com base neste parágrafo não gera direito a nenhum tipo de compensação financeira à **CONTRATADA**.

2. A **CONTRATADA**, a qualquer tempo, poderá substituir o bloqueio efetuado por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

Parágrafo sétimo. A **CONTRATADA** se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, para o pagamento da multa contratual ou encargos trabalhistas e previdenciários, e ainda, na alteração do valor contratado, para manter o percentual inicial, **no prazo de até 10 (dez) dias**, contados da assinatura do termo aditivo ou a partir da data em que for notificada pela **CONTRATANTE**, a partir do qual se observará o disposto nesta cláusula.

Parágrafo oitavo. A garantia somente será liberada ante a comprovação de que a empresa pagou todos os encargos trabalhistas e previdenciárias decorrentes da contratação, bem como apresentação de toda a documentação solicitada no edital pela **CONTRATANTE**.

Parágrafo nono. Será considerada extinta a garantia:

1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da **CONTRATANTE**, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do contrato;
2. no prazo de três meses após o término da vigência, caso a **CONTRATANTE** não comunique a ocorrência de sinistros.

Parágrafo décimo. A garantia não será extinta, em caso de ocorrência de sinistro ou irregularidade, devidamente comunica à seguradora pela **FISCALIZAÇÃO.**

CLÁUSULA DÉCIMA SEXTA – DO REAJUSTAMENTO:

Os preços propostos não serão reajustados durante todo o período de vigência do contrato.

CLÁUSULA DÉCIMA SÉTIMA – DAS ALTERAÇÕES:

Competem a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei n.º 8.666/1993 e em outras disposições legais pertinentes, realizar, por escrito, por meio de Termo Aditivo, as alterações contratuais que julgarem convenientes.

Parágrafo único. A **CONTRATADA** fica obrigada a aceitar as alterações unilaterais, conforme disposto no art. 65, I, da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA OITAVA – DAS PENALIDADES:

Em caso de inexecução total ou parcial, execução imperfeita, ou qualquer inadimplemento ou infração contratual, a **CONTRATADA**, sem prejuízo das responsabilidades civil e criminal, ficará sujeita às seguintes penalidades:

1. advertência;
2. multas percentuais, nos termos do parágrafo segundo desta cláusula;
3. rescisão administrativa do contrato;
4. suspensão temporária do direito de participar de licitação e impedimento de contratar;
5. declaração de inidoneidade para licitar e contratar.

Parágrafo primeiro. As penas acima referidas serão propostas pela **FISCALIZAÇÃO** e impostas pela autoridade competente, assegurada à **CONTRATADA** a prévia e ampla defesa na via administrativa.

Parágrafo segundo. A Advertência por escrito será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem corno, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do **CONTRATANTE**.

Parágrafo terceiro. Serão aplicadas à **CONTRATADA** as seguintes multas:

I - **2% (dois por cento)** sobre o valor global contratado, a cada reincidência na penalidade de advertência. Na hipótese de reincidência por 5 (cinco) vezes na penalidade de advertência, será considerado descumprimento total da obrigação, punível com as sanções previstas em lei.

II - **2% (dois por cento)** sobre o valor global contratado, por dia de atraso, no caso de descumprimento do tempo máximo, conforme Clásula Quarta - DOS PRAZOS PARA A PRESTAÇÃO DOS SERVIÇOS, limitado a 10 (dez) dias. O atraso superior a 10 (dez) dias será considerado como descumprimento total da obrigação, punível com as sanções previstas em lei.

III - **10% (dez por cento)** sobre o valor global contratado, no caso de, sem justificativa aceita pelo **CONTRATANTE**, o vencedor não retirar a Nota de Empenho, a Autorização de Fornecimento de Materiais/Serviço ou não assinar o contrato deixando, assim, de cumprir os prazos fixados, sem prejuízo das demais sanções previstas.

IV - **até 20% (vinte por cento)** sobre o valor global contratado, nos casos de INEXECUÇÃO PARCIAL do objeto contratado.

V - **até 30% (trinta por cento)** sobre o valor global contratado, nos casos de INEXECUÇÃO TOTAL do objeto contratado.

VI - **até 30% (trinta por cento)** sobre o valor global contratado, na hipótese de rescisão do contrato por culpa da **CONTRATADA**.

Parágrafo quarto. As multas contratuais serão descontadas dos pagamentos a que fizer jus a **CONTRATADA**, podendo ser cobrado judicialmente, quando necessário.

CLÁUSULA DÉCIMA NONA – DA RESCISÃO DO CONTRATO:

A inadimplência das cláusulas e condições estabelecidas neste contrato, por parte da **CONTRATADA**, assegurará à **CONTRATANTE** o direito de rescindir o contrato, mediante notificação através de ofício, entregue diretamente ou por via postal, com prova de recebimento, sem ônus de qualquer espécie para Administração e prejuízo das sanções previstas neste ajuste.

Parágrafo primeiro. Rescisão Unilateral. Ficará o presente contrato rescindido unilateralmente pela **CONTRATANTE**, mediante formalização, assegurado o contraditório e a ampla defesa, nos termos do art. 78, incisos I a XII e XVII, da Lei n.º 8.666/93.

Parágrafo segundo. Rescisão Bilateral. Ficará o presente contrato rescindido por acordo entre as partes, desde que haja conveniência para a Administração, nos casos do art. 78, XIII a XVI, da Lei n.º 8.666/93.

Parágrafo terceiro. Rescisão Judicial. O presente contrato poderá ser rescindido, judicialmente, nos termos da lei.

Parágrafo quarto. A falta dos registros ou documentações, incluindo a ART ou RRT, ou, ainda, constatada a irregularidade, ensejará o rompimento do vínculo contratual, sem prejuízo das multas

contratuais, bem como das demais cominações legais.

Parágrafo quinto. Fica vedado, à **CONTRATADA**, sob pena de rescisão contratual, CAUCIONAR ou utilizar o contrato para qualquer operação financeira, sem prévia e expressa anuência da **CONTRATANTE**.

CLÁUSULA VIGÉSIMA – DO VÍNCULO EMPREGATÍCIO:

Os empregados e prepostos da **CONTRATADA** não terão qualquer vínculo empregatício com a **CONTRATANTE**, correndo por conta exclusiva da primeira todas as obrigações decorrentes da legislação trabalhista, previdenciária, fiscal e comercial, as quais se obriga a saldar na época devida.

CLÁUSULA VIGÉSIMA PRIMEIRA – DAS NORMAS APLICÁVEIS:

O presente contrato deverá respeitar as seguintes leis e/ou decretos e resoluções:

1. Lei n.º 8.666/1993 – Licitações e Contratos;
2. Lei n.º 8.078/1990 – Código de Defesa do Consumidor;
3. Lei n.º 10.406/2002 – Código Civil Brasileiro.

Parágrafo único. A **CONTRATADA** declara conhecer todas essas normas e concorda em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

CLÁUSULA VIGÉSIMA SEGUNDA – DO TRATAMENTO DOS DADOS PESSOAIS:

As partes obrigam-se a realizar o tratamento de dados pessoais em obediências as disposições legais vigentes, nos moldes da Lei 13.709/2018 (LGPD), visando dar efetiva proteção aos dados coletados de pessoas naturais que possam identificá-las ou torná-las identificáveis.

1. O consentimento para o tratamento de dados pessoais, citado nesta Cláusula, se dará por meio da assinatura deste contrato.
2. O tratamento de dados pessoais se dará, exclusivamente, para os fins necessários ao cumprimento do objeto deste Contrato sem a possibilidade de tratamento futuro incompatível com a finalidade.
3. O usuário autoriza expressamente que suas informações e dados pessoais sejam compartilhados pela **CONTRATADA** com Autoridades públicas, administrativas e judiciais, que, no exercício de sua competência, exijam informações, mesmo que não haja ordem ou citação executiva ou judicial para esse efeito, para os seguintes fins:

   3.1. colaborar na investigação e denunciar fraudes, pirataria, violação de direitos de propriedade intelectual ou qualquer outro ato ilícito, bem como qualquer atividade ou circunstância que possa gerar responsabilidade legal para a **CONTRATADA** e/ou aos seus usuários;

   3.2. resguardar um interesse público, a aplicação ou administração da justiça, o reconhecimento, exercício ou defesa de um direito em um processo judicial ou administrativo e/ou a resolução de disputas; e

   3.3. cumprir com qualquer lei, regulamento ou disposição legal aplicável, ou algum mandato de autoridade competente devidamente fundamentado e motivado.

CLÁUSULA VIGÉSIMA TERCEIRA – DA PUBLICAÇÃO:

O presente contrato será publicado, sob a forma de extrato, no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, após a sua assinatura, correndo as despesas por conta da **CONTRATANTE**, nos termos do art. 61, parágrafo único, da Lei n.º 8.666/1993 e ATO PGJ N.º 082/2012.

CLÁUSULA VIGÉSIMA QUARTA – DAS DISPOSIÇÕES GERAIS:

A **CONTRATADA**, em cumprimento à Resolução n.º 37/2009 do Conselho Nacional do Ministério Público, declara que não possui sócios, gerentes ou diretores que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas.

Parágrafo único. Os casos omissos neste contrato serão resolvidos pela Administração Superior da **CONTRATANTE**, baseada na legislação vigente.

CLÁUSULA VIGÉSIMA QUINTA – DO FORO CONTRATUAL:

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na justiça estadual, no Foro de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

E por estarem de acordo, foi o presente termo de contrato, depois de lido e anuído, assinado digitalmente pelas partes e por duas testemunhas.

XXXXXXXXXXXXXXXXXXXX
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

XXXXXXXXXXXXXXXXXXXX
Representante Legal da Empresa

Documento assinado eletronicamente por **Ivanete de Oliveira Nascimento**, **Diretor(a) de Planejamento - DPLAN**, em 14/01/2022, às 14:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0750392** e o código CRC **FD9266B2**.

2021.015252 v88

EDITAL DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

ANEXO III

MODELO DE DECLARAÇÕES COMPLEMENTARES

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.**, para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;
2. Os documentos e declarações apresentados são fiéis e verdadeiros, bem como que a empresa recebeu o Edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;
3. Estou ciente da obrigação de, caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhar os documentos necessários à CONTRATANTE, a fim de efetuar o referido cadastramento no prazo de cinco dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;
4. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

(Cidade-UF),_____ de _____ de 2022.

RAZÃO SOCIAL/CNPJ DA EMPRESA
Representante Legal

EDITAL DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

ANEXO IV
MODELO DE PROPOSTA DE PREÇOS

Proposta que faz a empresa _____, inscrita no CNPJ (MF) nº _____, localizada _____, na cidade de _____, CEP _____, fone _____, fax _____, e-mail _____, para a prestação do serviço abaixo relacionado, de acordo com todas as especificações e condições estabelecidas no **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, promovido pelo Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça:

PLANILHA DE FORMAÇÃO DE PREÇOS

LOTE ÚNICO					
ITEM	**ESPECIFICAÇÃO**	**UNIDADE**	**QTD**	**VALOR UNITÁRIO (R$) (B)**	**VALOR TOTAL (R$) (A * B)**
1	Serviço de Firewall em Alta Disponibilidade	Meses	48		
2	Serviço de Monitoramento da Solução	Meses	48		
3	Serviço de Migração do Ambiente Atual	Unidade	1		
4	Serviço de Treinamento da Solução	Pessoas	5		
VALOR TOTAL DA PROPOSTA = R$ (por extenso)					

EDITAL DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

A _____(*nome da empresa)*_____ declara que concorda com todas as especificações do Edital.

a) Prazo de validade da proposta: _____

b) Prazo entrega do plano de implementação: Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

c) Prazo início processo de migração/reunião alinhamento: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;

d) Prazo processo de migração: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

e) Dados Bancários: (*indicar o nome e número do banco, nome e número completo da agência e número da conta-corrente*);

f) Contato para fins de faturamento: *(indicar o nome, cargo, endereço, telefone, fax, e-mail de contato do responsável pelo recebimento das futuras notas de empenho).*

g) Dados dos 3 (três) <u>principais integrantes</u> do quadro societário da licitante, assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade.

Nome: _____

CNPJ ou CPF: _____

<u>DECLARAÇÕES:</u>

1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.**, para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do **Ministério Público do Estado do Amazonas** e de sua **CPL;**
2. Os documentos e declarações apresentados são fiéis e verdadeiros, bem como que a empresa recebeu o Edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;
3. Estou ciente da obrigação de, caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhar os documentos necessários à CONTRATANTE, a fim de efetuar o referido

cadastramento no prazo de cinco dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;

4. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

Local e data:

(*assinatura*)
(*nome do representante legal pela empresa*)
(*CPF do representante legal*)

EDITAL DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

ANEXO V
MODELO DE SOLICITAÇÃO DE CADASTRAMENTO – SEFAZ/AM

(*cidade*), ____ de _____ de _____

À
Diretoria de Orçamento e Finanças
Procuradoria-Geral de Justiça do Estado do Amazonas
Av. Coronel Teixeira, 7995 – Nova Esperança
69037-473 MANAUS/AM

A empresa (*informar a razão social, CNPJ e endereço*) solicita a esse Setor o seu cadastro no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE – CADASTRAMENTO DE CREDORES – dessa **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ.**

Assim sendo, acompanha esta carta de solicitação de cadastramento a documentação abaixo listada, exigida para a efetivação do registro:

a) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

b) Cópia legível do comprovante (por ex: extrato, cópia reprográfica de cartão bancário, etc.) dos seguintes dados bancários:

Banco: _____
Agência: _____
Conta: _____

Razão Social e CNPJ da empresa
Nome completo e CPF do Representante Legal

Licitação

Ambiente: PRODUÇÃO

Disponibilizar Aviso de Licitação apenas para Divulgação

05/02/2022 12:46:09

Este Aviso de Licitação será Divulgado no Portal de Compras (www.gov.br/compras) na data de 08/02/2022.

Resumo do Aviso de Licitação

Órgão: 93320 - ESTADO DO AMAZONAS

UASG Responsável: 925849 - PROCURADORIA GERAL DE JUSTIÇA

Modalidade de Licitação: Pregão

Nº da Licitação: 04005/2022

Forma de Realização: Eletrônico

Característica: Tradicional

Modo de Disputa: Aberto

Nº do Processo: 2021.015252

Tipo de Licitação: Menor Preço

Quantidade de Itens: 4

☐ Equalização de ICMS ☐ Internacional

Objeto

Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.

Data da Divulgação: 08/02/2022

Data da Disponibilidade do Edital: A partir de 08/02/2022 às 08:00

Data/Hora da Abertura da Licitação: Em 21/02/2022 às 10:00

Disponibilizar apenas para Divulgação

Aviso de Licitação

Solução SERPRO

93320 - ESTADO DO AMAZONAS
925849 - PROCURADORIA GERAL DE JUSTIÇA

RELAÇÃO DE ITENS - PREGÃO ELETRÔNICO Nº 04005/2022-000

1 - Itens da Licitação

1 - Serviços de gerenciamento de sistemas computacionais

Descrição Detalhada: Serviço de Firewall em Alta Disponibilidade.
Tratamento Diferenciado: Não
Aplicabilidade Decreto 7174/2010: Não
Quantidade Total: 48
Critério de Julgamento: Menor Preço
Critério de Valor: Valor Estimado
Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 0,05
Local de Entrega (Quantidade): Manaus/AM (48)
Grupo: G1

2 - Serviços de gerenciamento de sistemas computacionais

Descrição Detalhada: Serviço de Monitoramento da Solução.
Tratamento Diferenciado: Não
Aplicabilidade Decreto 7174/2010: Não
Quantidade Total: 48
Critério de Julgamento: Menor Preço
Critério de Valor: Valor Estimado
Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 0,05
Local de Entrega (Quantidade): Manaus/AM (48)
Grupo: G1

3 - Serviços de gerenciamento de sistemas computacionais

Descrição Detalhada: Serviço de Migração do Ambiente Atual
Tratamento Diferenciado: Não
Aplicabilidade Decreto 7174/2010: Não
Quantidade Total: 1
Critério de Julgamento: Menor Preço
Critério de Valor: Valor Estimado
Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 0,05
Local de Entrega (Quantidade): Manaus/AM (1)
Grupo: G1

4 - Serviços de Gerenciamento de Sistemas Computacionais

Descrição Detalhada: Serviço de Treinamento da Solução.
Tratamento Diferenciado: Não
Aplicabilidade Decreto 7174/2010: Não
Quantidade Total: 5
Critério de Julgamento: Menor Preço
Critério de Valor: Valor Estimado
Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 0,05
Local de Entrega (Quantidade): Manaus/AM (5)
Grupo: G1

2 - Composição dos Grupos

Grupo 1			
Nº do Item	Descrição	Quantidade Total	Unidade de Fornecimento
1	Serviços de gerenciamento de sistemas computacionais	48	UND SERVIÇO TÉCNICO
2	Serviços de gerenciamento de sistemas computacionais	48	UND SERVIÇO TÉCNICO
3	Serviços de gerenciamento de sistemas computacionais	1	UND SERVIÇO TÉCNICO
4	Serviços de Gerenciamento de Sistemas Computacionais	5	UND SERVIÇO TÉCNICO

mora o(a) destinatário(a) quanto às providências recomendadas, podendo seu descumprimento implicar a adoção de medidas administrativas e ações judiciais cabíveis contra o(a) responsável; (b) tornar evidente o dolo do gestor de violar a ordem jurídica e de assunção dos riscos de dano, em caso de omissão ou descumprimento das providências recomendadas; (c) constituir-se o seu descumprimento em elemento probatório em sede processual.

Careiro Castanho/AM, 01 de fevereiro de 2022.

LEONARDO TUPINAMBÁ DO VALLE
PROMOTOR DE JUSTIÇA

DESPACHO Nº 2022/0000005765

NOTÍCIA DE FATO N. 162.2020.000047
Interessados: PREFEITURA MUNICIPAL DE HUMAITÁ/AM

Com a finalidade de apurar a prática da conduta vedada a agente público decorrente da sanção, promulgação e possível execução da Lei Municipal n. 853/2020, que concedeu isenção de taxa de utilização de espaço público para ocupantes do Mercado Municipal Hélio Lobo, nos meses de junho, julho e agosto do ano de 2020, houve a instauração de Procedimento
Preparatório Eleitoral perante a Promotoria Eleitoral da 17ª Zona Eleitoral do Estado do Amazonas.
Na Portaria do Procedimento Preparatório Eleitoral, determinou-se a instauração de procedimento não eleitoral e sua distribuição, por sorteio, a uma das Promotorias de Justiça de Humaitá/AM, tendo em vista que a prática de condutas vedadas a agentes públicos configura, em tese, ato de improbidade administrativa, nos termos do art. 73, parágrafo sétimo da Lei n. 9.504/97.
Para a instrução do presente procedimento extrajudicial, solicitou-se as seguintes informações:
i) qual o número de ocupantes/usuários de espaço público no Mercado Municipal Hélio Lobo, no Município de Humaitá/AM;
ii) qual o valor mensal pago pelos usuários/ocupantes de espaço público no Mercado Municipal Hélio Lobo, no Município de Humaitá/AM;
iii) qual o valor mensal arrecadado, pela Prefeitura Municipal de Humaitá, com o pagamento de taxa de ocupação de espaço público pelos usuários/ocupantes do Mercado Municipal de Humaitá/AM;
iv) a relação dos beneficiários de autorização de uso/ocupação de espaço público no Mercado Municipal de Humaitá/AM;
v) qual o impacto orçamentário decorrente da execução da Lei Municipal n. 853/2020 e qual a rubrica deixará de ser arrecadada/custeará o ônus decorrente da perda da arrecadação;
vi) se houve a prorrogação dos efeitos da Lei Municipal n. 853/2020, conforme autorização contida na Lei Municipal n. 853/2020.
Em resposta, a partir do Ofício n. 424/2021/Gab.Pref, a Prefeitura Municipal informou:
Excelentíssimo Promotor,
Apraz-nos cordialmente cumprimentá-lo, venho respeitosamente à presença de Vossa Excelência, comunicar que em resposta ao Ofício supracitado, após consulta ao Setor de Tributos, conforme Oficio n° 18/2021 — Setor de Tributos, de 16 de junho de 2021, seguem informações:
1. Atualmente o, Mercado Municipal Hélio Lobo conta com 99 (noventa e nove) ocupantes, cuja relação segue em anexo;
2. O valor mensal pago pelos ocupantes depende do Box utilizado, variando entre R$ 38,00 (trinta e pito reais), R$ 58,00 (cinquenta e oito reais) e R$ 118,00 (cento e dezoito reais), conforme planilha em anexo.
3. O valor arrecadado pela Prefeitura, com o pagamento de taxas do mercado, totaliza R$ 4.70200 (quatro mil setecentos e dois reais).
4. A relação dos ocupantes segue em anexo.
5. O impacto orçamentário (valor) que a promulgação da Lei 853/2020 deixou de arrecadar correspondeu a R$ R$ 14.106,00 (quatorze mil cento e seis reais).
6. Não houve prorrogação da Lei Municipal 853/2020. Sendo o que tínhamos para o momento.
A partir da avaliação das informações prestadas e dos documentos juntadas, pode-se verificar a concessão de uma isenção legal para o pagamento de uma taxa, em um período de exceção, decorrente da pandemia do Covid-19.
Apesar do fato de a isenção ter sido concedida em ano eleitoral, não se pode concluir, só por essa razão, a prática de um ato de improbidade administrativa.
Com efeito, a prática de ato de improbidade administrativa depende da demonstração da prática de uma conduta dolosa e caracterizadora de uma das condutas descritas nos arts. 9º e ss. da Lei n. 8.429/92. Especialmente a partir do sistema punitivo introduzido pela Lei n. 14.230/2021, gerador de impunidade e criador de barreiras à responsabilização de agentes públicos
ímprobos, há a exigência de que o ato de improbidade administrativa atentatório a princípios da Administração Pública acarrete uma lesão relevante ao bem jurídico para serem passíveis de sancionamento (art. 11, parágrafo terceiro da Lei n. 8.429/92).
Com isso, dada a ausência de provas da prática de ato configurador de improbidade administrativa, determino o arquivamento desta notícia de fato, nos termos do art. 23, IV da Resolução n. 6/2015/CSMP/MPAM.
Após, façam-me os autos conclusos.

Publique-se.

Cumpra-se.

Humaitá/AM, 31 de janeiro de 2022.

WESLEI MACHADO
Promotor de Justiça

ATOS DO CENTRO DE ESTUDOS E APERFEIÇOAMENTO FUNCIONAL

AVISO

Em anexo:
Resultado Final do XXI EXAME DE SELEÇÃO PARA CREDENCIAMENTO DE ESTAGIÁRIOS DE DIREITO DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

COMISSÃO PERMANENTE DE LICITAÇÃO

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 4.006/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2019.003706

OBJETO: Contratação de empresa especializada em serviços técnicos para a elaboração de Projeto Básico (memorial descritivo, orçamentos, planilhas, projetos e desenhos e dentre outros), levantamento preliminar (arquitetônico) das edificações e elaboração de projeto de incêndio dos prédios Edifício-Sede, Edifício Auditório Carlos Alberto Bandeira e Edifício Anexo Administrativo e descentralizado (Aleixo) da Procuradoria-Geral de Justiça, conforme as condições e especificações descritas neste Edital e seus anexos.

ABERTURA: 22/02/2022 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: no site www.comprasgovernamentais.gov.br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.
Informações adicionais, dúvidas e pedidos de esclarecimento deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones (92) 3655-0701 / (92) 3655-0743 ou pelo e-mail

licitacao@mpam.mp.br.

Manaus, 03 de fevereiro de 2022.

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 4.008/2021-CPL/MP/PGJ
PROCESSO SEI N.º 2021.018515

OBJETO: Formação de registro de preços, para eventual aquisição de equipamentos, materiais e ferramentas de informática para atividades de manutenção e suporte, objetivando atender às demandas desta Procuradoria-Geral de Justiça do Estado do Amazonas, pelo período de 12 (doze) meses, conforme as condições e especificações descritas no Edital e seus anexos.

ABERTURA: 24/02/2022, às 10h. (horário de Brasília).

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: Portal de Compras do Governo Federal no site https://www.comprasgovernamentais.gov.br/.

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimento / impugnações deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones (92) 3655-0701 / (92) 3655-0743 (Whatsapp Business) ou pelo e-mail institucional licitacao@mpam.mp.br.

Manaus, 03 de fevereiro de 2022.

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 4.007/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.016776

OBJETO: Formação de registro de preços para contratação de empresa especializada na prestação de serviços técnicos para operação dos sistemas de sonorização e comunicação audiovisual no Ministério Público do Estado do Amazonas, por 12 (doze) meses, descritos quantificados e qualificados conforme as especificações e as condições constantes de seu Edital e anexos.

ABERTURA: 23/02/2022 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: no site www.comprasgovernamentais.gov.br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.
Informações adicionais, dúvidas e pedidos de esclarecimento deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones (92) 3655-0701 / (92) 3655-0743 ou pelo e-mail licitacao@mpam.mp.br.

Manaus, 03 de fevereiro de 2022.

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.015252

OBJETO: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, para atendimento das necessidades da Procuradoria-Geral de Justiça - PGJ, conforme as condições e especificações descritas no Edital e seus anexos.

ABERTURA: 21/02/2022 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: no site www.comprasgovernamentais.gov.br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.
Informações adicionais, dúvidas e pedidos de esclarecimento deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones (92) 3655-0701 / (92) 3655-0743 ou pelo e-mail licitacao@mpam.mp.br.

Manaus, 03 de fevereiro de 2022.

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

PORTARIA Nº 03/2022/CPL

A COMISSÃO PERMANENTE DE LICITAÇÃO, no uso de suas atribuições legais previstas no art. 1º, inciso V, do Ato PGJ n.º 345/2007, com supedâneo no Ato PGJ nº 187/2021, de 12 de julho de 2021, e;

CONSIDERANDO a avença firmada entre esta Procuradoria-Geral de Justiça e a empresa HORIZONTE MÓVEIS DE ESCRITÓRIO – EIRELI, inscrita no CNPJ nº 06.536.588/0001-89, por meio da ATA DE REGISTRO DE PREÇO Nº 12.2021.CPL.0657928.2020.016910 (doc. cópia n.º 0761441), relativa à formação de Registro de Preços para futura aquisição de mobiliário em geral com garantia total do fabricante por no mínimo 60 (sessenta) meses, a contar da data da entrega, com representante e assistência técnica em Manaus, para atender às necessidades da Procuradoria-Geral de Justiça por um período de 12 (doze) meses;

CONSIDERANDO que a referida ATA DE REGISTRO DE PREÇO Nº 12.2021.CPL.0657928.2020.016910 (doc. cópia n.º 0761441) originou-se do Pregão Eletrônico nº 4.013/2021-CPL/MP/PGJ-SRP (doc. cópia n.º 0761438);

CONSIDERANDO que a empresa HORIZONTE MÓVEIS DE ESCRITÓRIO – EIRELI, inscrita no CNPJ sob o nº 06.536.588/0001-89, supostamente deixou de cumprir termos da referida Ata de RP, ao solicitar extenso prazo para entrega dos materias descritos na AUTORIZAÇÃO DE FORNECIMENTO DE MATERIAIS E SERVIÇO Nº 88.2021.SCOMS.0668499.2021.007734 (doc. cópia n.º 0761283), relacionada à NOTA DE EMPENHO Nº 2021NE0000959 (doc. cópia nº 0761286);

CONSIDERANDO a determinação exarada através do DESPACHO Nº 509.2021.03AJ-SUBADM.0731227.2021.007734 (doc. cópia 0761308), da lavra do Exmo. Sr. Subprocurador-Geral de Justiça para Assuntos Administrativos, Dr. GÉBER MAFRA ROCHA, no sentido da perquirição de provável conduta faltosa da empresa;

ESTADO DO AMAZONAS
PREFEITURA MUNICIPAL DE MAUÉS
COMISSÃO PERMANENTE DE LICITAÇÃO – CPL

AVISO DE LICITAÇÃO

A Comissão Permanente de Licitação da Prefeitura de Maués, torna pública a abertura da TOMADA DE PREÇO Nº 002/2022 – CPL, a ser realizado no dia 21 de fevereiro de 2022, às 10h00min, cujo o objeto é CONTRATAÇÃO DE PESSOA JURÍDICA PARA ADEQUAÇÃO DE ESTRADAS VICINAIS NO MUNICÍPIO DE MAUÉS/AM, ORUNDO DO CONVÊNIO FEDERAL Nº 907808/2020 – MDR/CAIXA.
O Edital e o Projeto Básico e seus anexos encontram-se à disposição dos interessados, nesta Comissão, localizada na Rua Quintino Bocaiúva, 244, Bairro Centro – Maués - Amazonas, CEP: 69.190-000. Mediante o pagamento do DAM, no valor de R$ 500,00 (quinhentos reais).
Maués/AM, 04 de fevereiro de 2022.
FABÍOLA ARAÚJO DA SILVA
Presidente da Comissão Permanente de Licitação - CPL

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.015252

OBJETO: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, para atendimento das necessidades da Procuradoria-Geral de Justiça - PGJ, conforme as condições e especificações descritas no Edital e seus anexos.

ABERTURA: 21/02/2022 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: no site www.comprasgovernamentais.gov.br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimento deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones **(92) 3655-0701** / **(92) 3655-0743** ou pelo e-mail **licitacao@mpam.mp.br**.

Manaus, 03 de fevereiro de 2022.

EDSON FREDERICO LIMA PAES BARRETO:85614017291
Assinado de forma digital por EDSON FREDERICO LIMA PAES BARRETO:85614017291
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR ASCON, ou=Presencial, ou=10470704000181, cn=EDSON FREDERICO LIMA PAES BARRETO:85614017291
Dados: 2022.02.03 16:36:02 -04'00'

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO N.º 4.006/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2019.003706

OBJETO: Contratação de empresa especializada em serviços técnicos para a elaboração de Projeto Básico (memorial descritivo, orçamentos, planilhas, projetos e desenhos e dentre outros), levantamento preliminar (arquitetônico) das edificações e elaboração de projeto de incêndio dos prédios Edifício-Sede, Edifício Auditório Carlos Alberto Bandeira e Edifício Anexo Administrativo e descentralizado (Aleixo) da Procuradoria-Geral de Justiça, conforme as condições e especificações descritas neste Edital e seus anexos.

ABERTURA: 22/02/2022 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: no site www.comprasgovernamentais.gov.br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimento deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones **(92) 3655-0701** / **(92) 3655-0743** ou pelo e-mail **licitacao@mpam.mp.br**.

Manaus, 03 de fevereiro de 2022.

EDSON FREDERICO LIMA PAES BARRETO:85614017291
Assinado de forma digital por EDSON FREDERICO LIMA PAES BARRETO:85614017291
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR ASCON, ou=Presencial, ou=10470704000181, cn=EDSON FREDERICO LIMA PAES BARRETO:85614017291
Dados: 2022.02.03 16:36:25 -04'00'

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO N.º 4.007/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.016776

OBJETO: Formação de registro de preços para contratação de empresa especializada na prestação de serviços técnicos para operação dos sistemas de sonorização e comunicação audiovisual no Ministério Público do Estado do Amazonas, por 12 (doze) meses, descritos quantificados e qualificados conforme as especificações e as condições constantes de seu Edital e anexos.

ABERTURA: 23/02/2022 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: no site www.comprasgovernamentais.gov.br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimento deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones **(92) 3655-0701** / **(92) 3655-0743** ou pelo e-mail **licitacao@mpam.mp.br**.

Manaus, 03 de fevereiro de 2022.

EDSON FREDERICO LIMA PAES BARRETO:85614017291
Assinado de forma digital por EDSON FREDERICO LIMA PAES BARRETO:85614017291
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR ASCON, ou=Presencial, ou=10470704000181, cn=EDSON FREDERICO LIMA PAES BARRETO:85614017291
Dados: 2022.02.03 16:54:31 -04'00'

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO N.º 4.008/2021-CPL/MP/PGJ
PROCESSO SEI N.º 2021.018515

OBJETO: Formação de registro de preços, para eventual aquisição de equipamentos, materiais e ferramentas de informática para atividades de manutenção e suporte, objetivando atender às demandas desta Procuradoria-Geral de Justiça do Estado do Amazonas, pelo período de 12 (doze) meses, conforme as condições e especificações descritas no Edital e seus anexos.

ABERTURA: 24/02/2022, às 10h. (horário de Brasília).

ENTREGA DAS PROPOSTAS: a partir de 07/02/2022.

LOCAL: Portal de Compras do Governo Federal no site **https://www.comprasgovernamentais.gov.br/.**

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimento / impugnações deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelos telefones **(92) 3655-0701 / (92) 3655-0743 (Whatsapp Business)** ou pelo e-mail institucional **licitacao@mpam.mp.br**.

Manaus, 03 de fevereiro de 2022.

EDSON FREDERICO LIMA PAES BARRETO:85614017291
Assinado de forma digital por EDSON FREDERICO LIMA PAES BARRETO:85614017291
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR ASCON, ou=Presencial, ou=10470704000181, cn=EDSON FREDERICO LIMA PAES BARRETO:85614017291
Dados: 2022.02.03 16:35:30 -04'00'

Edson Frederico Lima Paes Barreto
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021
Matrícula n.º 001.042-1A

IPAAM

COMUNICADO

Manauara V Empreendimentos Imobiliários SPE Ltda., torna público que recebeu do IPAAM, a Licença de Instalação n.º 008/2022, que autoriza a implantação de um Condomínio Residencial Multifamiliar denominado "Viver Veredas" em uma área útil de 2,47 ha, conforme Licença Ambiental Única de Supressão Vegetal – LAU-SV Nº 019/2022, localizada na Avenida do CETUR, S/nº, Bairro Tarumã, Manaus-AM, para Complexo Habitacional, com validade de **02 Anos**.

IPAAM

COMUNICADO

Manauara V Empreendimentos Imobiliários SPE Ltda, torna público que recebeu do IPAAM, a LAU de Supressão Vegetal n.º 019/2022, que autoriza a supressão da vegetação para a Implantação de um Residencial Multifamiliar em uma área de 2,99 ha, conforme Licença de Instalação – L.I Nº 008/2022, situada na Avenida do CETUR, S/nº, Bairro Tarumã, Manaus-AM para Supressão Vegetal, com validade de 01 Ano.

PODER LEGISLATIVO
ASSEMBLEIA LEGISLATIVA DO ESTADO DO AMAZONAS

AVISO DE REABERTURA DE LICITAÇÃO SUSPENSA
PREGÃO PRESENCIAL Nº 31/2021

A Comissão Permanente de Licitação da Assembleia Legislativa do Estado do Amazonas torna público para conhecimento de todos os interessados que realizara-rá licitação, na modalidade PREGÃO PRESENCIAL N° 31/2021-ALEAM, tipo menor preço global.
OBJETO: Contratação de serviço de engenharia para a realização de reparos e adequações nas instalações físicas do prédio destinados ao Centro de Mídias da Diretoria de Comunicação, conforme os quantitativos, especificações e condições, exigências estabelecidas neste Edital e Termo de Referência.
A reabertura está prevista para o dia 21 de fevereiro de 2022, às 09h00min (horário local), endereço: Assembléia Legislativa do Estado do Amazonas, Av. Mario Ypiranga Monteiro (Antiga Recife), nº 3950, Edifício Deputado José de Jesus Lins Albuquerque, Bairro: Parque 10 de Novembro, Manaus/AM (Sala da Comissão Permanente de Licitação – 6º Andar)
O Edital e seus anexos estarão disponíveis a partir desta publicação. Os interessados em participar do certame poderão solicitá-lo através do e-mail cpl@aleam.gov.br, no horário das 8 às 13 horas.
Manaus, 04 de fevereiro de 2022.
JULIO CESAR LANGBECK SOARES NETO
PRESIDENTE-CPL

PODER LEGISLATIVO
ASSEMBLEIA LEGISLATIVA DO ESTADO DO AMAZONAS

AVISO DE REABERTURA DE LICITAÇÃO SUSPENSA
PREGÃO PRESENCIAL Nº 32/2021

A Comissão Permanente de Licitação da Assembleia Legislativa do Estado do Amazonas torna público para conhecimento de todos os interessados que realizara-rá licitação, na modalidade PREGÃO PRESENCIAL N° 32/2021-ALEAM, tipo menor preço global.
OBJETO: Contratação de serviço de engenharia para a adaptações no estacionamento da Assembleia legislativa, conforme os quantitativos, especificações e condições, exigências estabelecidas neste Edital e Termo de Referência.
A reabertura está prevista para o dia 22 de fevereiro de 2022, às 09h00min (horário local), endereço: Assembléia Legislativa do Estado do Amazonas, Av. Mario Ypiranga Monteiro (Antiga Recife), nº 3950, Edifício Deputado José de Jesus Lins Albuquerque, Bairro: Parque 10 de Novembro, Manaus/AM (Sala da Comissão Permanente de Licitação – 6º Andar)
O Edital e seus anexos estarão disponíveis a partir desta publicação. Os interessados em participar do certame poderão solicitá-lo através do e-mail cpl@aleam.gov.br, no horário das 8 às 13 horas.
Manaus, 04 de fevereiro de 2022.
JULIO CESAR LANGBECK SOARES NETO
PRESIDENTE-CPL

Prefeitura de Manaus

AVISO DE REVOGAÇÃO

(Processo n. 2022/16330/20696/00002 – SEMAD/UGCM)

A COMISSÃO MUNICIPAL DE LICITAÇÃO da **PREFEITURA DE MANAUS** torna público que o **PREGÃO ELETRÔNICO N. 017/2022 – (UGCM/SEMAD) CML/PM,** cujo objeto consiste no "Eventual fornecimento de kit educativo para atender aos órgãos e entidades da Administração Pública Direta e Indireta da Prefeitura de Manaus, participantes do Registro de Preços" fica **REVOGADO** conforme Despacho desta Presidência.

Maiores informações na Comissão Municipal de Licitação, telefone 0xx-92-3215 6333/ 6378, das 09 às 15h (horário de Brasília).

Manaus, 04 de fevereiro de 2022.

JOSÉ FABIANO AFFONSO SOBRINHO
Presidente da Subcomissão de Educação da
Comissão Municipal de Licitação – CML

eneva

DE ACORDO COM A LEI ESTADUAL N°. 3.785/2012

Eneva S.A., torna público que recebeu do IPAAM, a LAU de Supressão Vegetai n.° 020/2022, que autoriza a supressão vegetal para perfuração do Poço de Gás *Natural* LEAD AM-T-85-E objetivando verificar a existência de acumulações de gás *natural na* área do Bloco AM-T-85, que está localizado no Bloco Exploratório AMT-85, no estado do Amazonas, no município de Silves, a aproximadamente 300 km da capital Manaus em uma área de 2,4820 ha, Localizada na MRG Direita da Estrada da Várzea, s/n°, km 12, Zona Rural, Silves-AM, para Supressão Vegetal, com validade de 01 Ano.

eneva

DE ACORDO COM A LEI ESTADUAL N° 3.785/2012

Eneva S.A., torna público que recebeu do **IPAAM.** a Licença de Instalação n.° 010/2022, que autoriza a Perfuração de Poço Profundo para fins de Pesquisa de Gás Natural denominado LEAD LEAD AM-T-85 **E, em** uma área de 2,57 ha, no Bloco AM-T-85, Grupo Javari, composto de depósitos flúviolacustre-deltáicos das formações Alter do Chão, conforme Licença Ambiental Única de Supressão/IPAAM/ N° 020/2022, localizada na Margem esquerda do Rio Itabani, Zona Rural no município de Silves-AM, para Exploração/Explotação de Gás Natural, com validade de 01 Ano.

IPAAM

COMUNICADO

E F Alves de Souza Eireli., torna público que recebeu do IPAAM, a Licença de Operação n.º 293/2020 1ª Alteração, que autoriza o transporte fluvial de combustível derivado de petróleo (gasolina e óleo diesel), localizada na Av. Francisco Queiroz, nº 327, Sala 10, Colônia de Santo Antônio, Manaus-AM, para Transporte Fluvial de Combustível, com validade de 1.418 dias.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

PORTARIA N° 229/2022/SUBADM

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno n.º 2022.002822 – SEI,

CONSIDERANDO o teor do ATO PGJ N.º 389/2007, datado de 26.11.2007, que regulamenta a utilização da modalidade Pregão no âmbito do Ministério Público do Estado do Amazonas,

RESOLVE:

I – DESIGNAR o servidor **EDSON FREDERICO LIMA PAES BARRETO**, Agente de Apoio – Administrativo, Presidente da Comissão Permanente de Licitação, como Pregoeiro do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ (Solução de firewall de próxima geração em alta disponibilidade)**, e, para auxiliá-lo, bem como substituí-lo em seus impedimentos ou afastamentos, o servidor **MAURÍCIO ARAÚJO MEDEIROS**, Agente de Apoio – Administrativo;

II – DESIGNAR os servidores **IURY FECHINE RAMOS** e **SARAH MADALENA BARBOSA SANTOS CORTES**, ambos Agentes de Apoio – Administrativo, membros da Comissão Permanente de Licitação desta Instituição, para compor a Equipe de Apoio do referido Pregão.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus, 11 de fevereiro de 2022.

ALBERTO RODRIGUES DO NASCIMENTO JÚNIOR
Procurador-Geral de Justiça

Documento assinado eletronicamente por **Alberto Rodrigues do Nascimento Júnior**, **Procurador(a) - Geral de Justiça**, em 11/02/2022, às 13:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0767097** e o código CRC **DFCE3629**.

2022.002822 0767097v3

Solicitação de esclarecimento - PE 4.005/2022 - CPL/MP/PGJ

Jefferson Matos Silva <jefferson.matos@servix.com>

Ter, 15/02/2022 08:36

Para: Comissao Permanente de Licitacao <licitacao@mpam.mp.br>

Cc: Bárbara Simões da Costa <barbara.costa@servix.com>; Luiz Datri <luiz.datri@servix.com>

Prezados Senhores, boa tarde.

Interessados na participação do certame em epígrafe, solicitamos os esclarecimentos que seguem.

Questionamento 01:

5.2.15.6.6. A solução fornece gerenciamento apartado do plano de dados do restante da solução. Logo, quando utilizado toda a capacidade do hardware de NGFW, seu plano de gerência continua funcional sem que haja indisponibilidade do appliance ou necessidade de desativação da funcionalidade de IPS. Compreendemos que esse método atende o item, está correto o entendimento?

Questionamento 02:

5.2.15.7.16. A solução permite analisar os arquivos dentro dos fluxos de SMTP e POP3 e identificar se o conteúdo do email é maligno ou benigno e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?

Questionamento 03:

5.2.15.7.30. A solução permite o emular os anexos contidos nos emails e documentos baixados da web, classificar esses anexos e documentos baixados como benigno e malignos e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?

Questionamento 04:

5.2.15.9.39. A solução permite o correlacionamento de eventos e logs, classificando em níveis de severidade, através de métricas de tempo, objetos, IP de origem e destino, usuários, nome do ataque, país de origem. A partir dessas métricas é possível visualizar graficamente as informações e correlacionar as evidências apresentadas. Compreendemos que esse método atende o item, está correto o entendimento?

Atenciosamente,

--

Servix Informática Ltda
Rua Pequetita, 215 | 7º andar
Vila Olímpia | São Paulo - SP

Jefferson Matos
Analista Jurídico
(11) 3525-3420
(11) 98265-0967

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 56.2022.CPL.0768833.2021.015252

Aos Senhores

TADEU AZEVEDO DE MEDEIROS

Diretor de Tecnologia da Informação e Comunicação

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

NESTE EDIFÍCIO

Assunto: Pedido de Esclarecimento interposto aos termos do Edital de **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**. Encaminha-se para análise e resposta.

Ilustríssimos Senhores,

Cumprimentando-os cordialmente e, considerando a realização do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, cujo objeto é a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.*, oportunamente, **encaminho pedido de esclarecimento** (doc. 0768830) apresentado pela empresa **SERVIX INFORMÁTICA LTDA**, para conhecimento e, no que couber, respostas.

Considerando a abertura da Sessão do Pregão em epígrafe em 21/02/2022, solicito que os autos retornem a esta CPL, no máximo, fim do expediente do dia **17/02/2022**, para elaboração e emissão da respectiva decisão, em face do que dispõe o subitem 22.5 do instrumento convocatório.

Desde já, coloco-me à disposição para auxiliar no que for necessário.

Atenciosamente,

EDSON FREDERICO LIMA PAES BARRETO

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 15/02/2022, às 11:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0768833** e o código CRC **40154AB2**.

PEDIDO DE ESCLARECIMENTO - PREGÃO ELETRÔNICO N.º 4.005/2022

Perola Pletsch <perola.pletsch@pisontec.com.br>

Ter, 15/02/2022 14:31

Para: Comissao Permanente de Licitacao <licitacao@mpam.mp.br>

Cc: Estela Carvalho <estela@pisontec.com.br>; Cristina Moreira <vendasgov4@pisontec.com.br>; Carla Carvalho <carla.carvalho@pisontec.com.br>; Deborah financeiro <financeiro@pisontec.com.br>; Michel Pisontec <michel@pisontec.com.br>

1 anexos (3 MB)

AB. 21.02 PE 4005.2022 UASG 925849 MPAM Firewall (E).pdf;

Ao
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Ref. PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

Objeto - O objeto da presente licitação é a escolha da proposta mais vantajosa para contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos.

Ilmo.(a) Sr.(a) Pregoeiro(a),

A empresa Pisontec Comércio e Serviços em Tecnologia da Informação EIRELI, inscrita no CNPJ Nº 12.007.998/0001-35, situada em Olinda/PE, vem respeitosamente, solicitar **ESCLARECIMENTO**, conforme termos elencados a seguir.

I – O serviço está sendo executado ou já foi em algum momento?
Se a reposta for positiva:
a) qual empresa é ou foi responsável?
b) Quantos profissionais atuam atualmente no serviço?

II - Será necessário fornecimentos de peças e/ou materiais ou softwares?

III - O serviço poderá ser executado remotamente?

IV – A apresentação de Profissionais Certificados integrantes no quadro de funcionários da Licitante, deve ser realizada apenas no ato da assinatura do contrato, sendo aceitos profissionais certificados cuja contratação se dê por prestação de serviço, sem vínculo trabalhista com a Licitante.

V – Qual o valor estimado?

VI – Se existir serviços de manutenção de equipamentos, necessário disponibilizar a lista contendo as marcas e os modelos dos respectivos equipamentos.

Agradecemos sua atenção ficando no aguardo de breve resposta.

Atenciosamente,

Perola Pletsch | Setor Jurídico

www.pisontec.com.br |
perola.pletsch@pisontec.com.br

office: +55 81 3257-5110

SOLICITAÇÃO DE ESCLARECIMENTOS REF. PREGÃO ELETRÔNICO Nº 4005/2022

Cristian Teles <cristian.teles@arvvo.com.br>

Ter, 15/02/2022 16:27

Para: Comissao Permanente de Licitacao <licitacao@mpam.mp.br>

Cc: Jessica Figueiredo <Jessica.figueiredo@arvvo.com.br>; André Bello <andre.bello@arvvo.com.br>; Andre Oliveira <andre.oliveira@arvvo.com.br>; Edson Gomes <edson.gomes@arvvo.com.br>

Prezados Srs, boa tarde!

Após análise do referido Edital e seus anexos, solicitamos os seguintes esclarecimentos, de acordo com os itens abaixo:

Esclarecimento 01

5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.

Para a identificação dos usuários poderá ser utilizado o serviço agregado ao servidor de gerenciamento para integração ao base de usuários LDAP, nem a necessidade de instalação de agentes ou software de clientes nos servidores Active Directory?

Esclarecimento 02

5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).

Após o bloqueio, serão aceitas soluções que a liberação e a continuação da navegação sejam permitidas após avaliação do responsável pela manutenção da solução ofertada ?

Esclarecimento 03

5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

Entendemos que a topologia e arquitetura de implementação do sistema de IPS deve ser capaz de interceptar todo trafego e tomar as ações de inspeção assim estipuladas quando em modo Inline e apenas registrar em modo Mirror/TAP. A topologia de implementação MTA se faz equivocada neste sentido, visto que em modo In-line ou TAP “todo” o trafego será analisado e o modo MTA se faz necessário em soluções de proteção de messageria. Neste caso o conceito de IPS não faz uso dessa topologia de comunicação para analise de apenas do trafego de mensagens de e-mail. Esta correto nosso entendimento?

Esclarecimento 04

15.8.1 Deverá possuir certificação ICSA para Firewall.

A certificação ICSA depende de contratação para ser emitida em ordem que, os testes realizados por outras empresas certificadoras, realizam os mesmos testes de performance com abrangência internacionais. Levando isto em consideração, entendemos que a solução ofertada pode ser certificada em outros

laboratórios desde que atenda aos requisitos de testes submetidos de forma equivalente aos executados pela ICSA.

Atenciosamente,

CRISTIAN TELES
Licitações e Contratos

61 98238-8379
cristian.teles@arvvo.com.br
Brasília - SHN Quadra 1 BL. A Sala 1114
ED. Le Quartier - CEP 70.701-010

scan me

WWW.ARVVO.COM.BR

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 59.2022.CPL.0769231.2021.015252

Aos Senhores

TADEU AZEVEDO DE MEDEIROS

Diretor de Tecnologia da Informação e Comunicação

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

NESTE EDIFÍCIO

Assunto: Pedidos de Esclarecimentos interpostos aos termos do Edital de **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**. Encaminha-se para análise e resposta.

Ilustríssimos Senhores,

Cumprimentando-os cordialmente e, considerando a realização do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, cujo objeto é a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.*, oportunamente, **encaminho pedidoS de esclarecimentos** apresentados, o primeiro, pela empresa **PISONTEC SOLUTIONS** (doc. 0769227) e o outro pela empresa **ARVOO TECNOLOGIA** (doc. 0769228), para conhecimento e, no que couber, respostas.

Considerando a abertura da Sessão do Pregão em epígrafe em 21/02/2022, solicito que os autos retornem a esta CPL, no máximo, fim do expediente do dia **17/02/2022**, para elaboração e emissão da respectiva decisão, em face do que dispõe o subitem 22.5 do instrumento convocatório.

Desde já, coloco-me à disposição para auxiliar no que for necessário.

Atenciosamente,

EDSON FREDERICO LIMA PAES BARRETO

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 15/02/2022, às 16:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0769231** e o código CRC **6987570D**.

2021.015252 v2

IMPUGNAÇÃO AOS TERMOS DO EDITAL DE PREGÃO ELETRÔNICA N. 4005/2022 - -CPL/MP/PGJ

Raul Luiz Martins Peregrino <raul.peregrino@oi.net.br>

Ter, 15/02/2022 20:31

Para: Comissao Permanente de Licitacao <licitacao@mpam.mp.br>

Cc: Raul Luiz Martins Peregrino <raul.peregrino@oi.net.br>

1 anexos (1 MB)

Impugnação - PE nº 4005_2022 - Ministério Público do Estado do Amazonas v1.pdf;

Ilmo. Sr. Pregoeiro do Ministério Público do Estado do Amazonas

REF.: IMPUGNAÇÃO AOS TERMOS DO EDITAL DE PREGÃO ELETRÔNICA N. 4005/2022 - -CPL/MP/PGJ

OI S.A., em Recuperação Judicial, sociedade anônima, com sede na Cidade do Rio de Janeiro, Estado do Rio de Janeiro, na Rua do Lavradio, 71, 2º andar, Bairro Centro, inscrita no CNPJ/MF sob o nº 76.535.764/0001-43, doravante denominadas OI, vem, por seu representante legal, com fulcro no art. 24, do Decreto 10.024/2019, apresentar Impugnação aos termos do Edital em referência, apresentar Impugnação aos termos do Edital em referência, pelas razões a seguir expostas:

Raul Luiz Martins Peregrino
Oi Soluções
Vendas Oi Soluções Governo NO
(031 92) 3131-6118
(031 92) 99603-0456
raul.peregrino@oi.net.br

Ilmo. Sr. Pregoeiro do Ministério Público do Estado do Amazonas

REF.: IMPUGNAÇÃO AOS TERMOS DO EDITAL DE PREGÃO ELETRÔNICA N. 4005/2022 - -CPL/MP/PGJ

OI S.A., em Recuperação Judicial, sociedade anônima, com sede na Cidade do Rio de Janeiro, Estado do Rio de Janeiro, na Rua do Lavradio, 71, 2º andar, Bairro Centro, inscrita no CNPJ/MF sob o nº 76.535.764/0001-43, doravante denominadas OI, vem, por seu representante legal, com fulcro no art. 24, do Decreto 10.024/2019, apresentar Impugnação aos termos do Edital em referência, apresentar Impugnação aos termos do Edital em referência, pelas razões a seguir expostas:

Razões de Impugnação

O Ministério Público do Estado do Amazonas instaurou procedimento licitatório na modalidade Pregão Eletrônico, registrado sob o n.º 4.005/2022-CPL/MP/PGJ, visando a "*contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos."*

Contudo, a Oi tem este seu intento frustrado perante as imperfeições do Edital, contra as quais se investe, justificando-se tal procedimento ante as dificuldades observadas para participar de forma competitiva do certame.

Saliente-se que o objetivo da Administração Pública ao iniciar um processo licitatório é exatamente obter proposta mais vantajosa para contratação de bem ou serviço que lhe seja necessário, observados os termos da legislação aplicável, inclusive quanto à promoção da máxima competitividade possível entre os interessados.

Entretanto, com a manutenção das referidas exigências, a competitividade pretendida e a melhor contratação almejada, poderão restar comprometidas o que não se espera, motivo pelo qual a Oi impugna os termos do Edital e seus anexos, o que o faz por meio da presente manifestação.

ALTERAÇÕES A SEREM FEITAS NO EDITAL E NOS ANEXOS

1. EXIGÊNCIA ABUSIVA

O item 5.6.3 do Edital prevê que não podem participar do certame empresas que tenham sócios, diretores, gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL.

Ocorre que, tais exigências mostram-se excessivas, na medida em que não possuem finalidade correlata à execução do objeto.

Além disso, as empresas de capital aberto que possuem um volume muito expressivo de acionistas, encontrarão grande dificuldade no processo de levantamento de informações tão específicas, como o grau de parentesco e vínculo empregatício de seu quadro acionário, as quais inclusive, não são informadas quando da aquisição das ações pelo público em geral.

Nesse contexto, é relevante destacar que o instrumento convocatório deve se abster de incluir cláusulas e exigências desnecessárias à finalidade da contratação, bem como aquelas que frustrem o caráter competitivo do certame.

A exigência imposta pelo Edital é medida extremamente restritiva à participação de interessados, cuja consequência direta será reduzir a participação das empresas que, nos termos da regulamentação dos serviços de telecomunicações, possuem outorga para prestação de todos os serviços licitados.

Cumpre destacar que quanto aos serviços de telecomunicações - objeto ora licitado -, estes são regulados pela Lei Geral de Telecomunicações (Lei 9.472, de 16 de julho de1997), a qual dispõe em seu artigo 6º o seguinte:

> "Art. 6º Os serviços de telecomunicações serão organizados com base no **princípio da livre ampla e justa competição entre todas as prestadoras,**

> **devendo, o Poder Público atuar para propiciá-la**, bem como para corrigir os efeitos da competição imperfeita e reprimir as infrações da ordem econômica.” (grifo nosso)

Ratificando o dever do poder público de ampliar a competição entre as Operadoras, com padrões de qualidade compatíveis com as exigências dos usuários, o art. 2º, inciso III, da LGT assim determina:

> “Art. 2° O Poder Público tem o dever de:
>
> (...)
>
> III - adotar medidas que **promovam a competição e a diversidade dos serviços**, incrementem sua oferta e propiciem padrões de qualidade compatíveis com a exigência dos usuários;” (grifo nosso)

Ademais, o inciso I do § 1º do art. 3º da Lei n.º 8.666/93 assim dispõe:

> “Art. 3º A licitação destina-se a garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.
>
> § 1º É vedado aos agentes públicos:
>
> I - **admitir, prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo**, inclusive nos casos de sociedades cooperativas, e estabeleçam preferências ou distinções em razão da naturalidade, da sede ou domicílio dos licitantes ou de qualquer outra circunstância impertinente ou irrelevante para o específico objeto do contrato, ressalvado o disposto nos §§ 5º a 12 deste artigo e no art. 3º da Lei nº 8.248, de 23 de outubro de 1991;” (grifo nosso)

Inexiste no mercado uma ampla gama de opções, o que impede a inclusão de qualquer tipo de condição que impeça ou dificulte a participação das operadoras em procedimentos licitatórios, sob pena de efetiva redução na competição.

Ante o exposto, requer a exclusão da exigência prevista no item 5.6.3 do Edital.

2. DA VEDAÇÃO DE PARTICIPAÇÃO DE LICITANTES EM REGIME DE CONSÓRCIO

O item 5.6.5 do Edital veda a participação de empresas que estejam constituídas em consórcio.

Primeiramente, cumpre elucidar algumas questões referentes ao mercado de telecomunicações. É cediço que no âmbito da oferta de serviços de telecomunicações, verifica-se a escassez de competitividade, predominando no mercado poucas empresas. Tal fenômeno caracteriza-se pela própria natureza do mercado em questão, ora a entrada de empresas que exploram tal serviço é restrita, haja vista a necessidade de grande aporte de capitais, instalação de infra-estruturais e dentre outros fatores que impedem a existência de um número razoável de empresas disponíveis para prestar o referido serviço.

Há ainda de se ressaltar que o desenvolvimento da economia amplamente globalizada implicou na formação de grupos econômicos em escala mundial, sendo o mercado de telecomunicações um dos grandes exemplos. A economia das grandes corporações reduziu ainda mais a oferta de serviços de telecomunicações, ocorrendo em escala global a aglomeração de companhias e formação de um mercado eminentemente oligopolista.

Traçadas as linhas gerais referentes ao mercado de telecomunicações, pode-se afirmar com convicção que as restrições de participação de empresas nas licitações devem ser, mais que em outros casos, muito bem justificadas e necessárias. Isto porque, em homenagem aos princípios da competitividade e isonomia, apenas pode se podem admitir as restrições objetivas e legítimas.

Nesse sentido, não pode prosperar a imposição editalícia de impedimento de participação de empresas em regime de consórcio. Tal determinação fulmina diretamente a competitividade do certame por não existir grande número de empresas qualificadas para prestação do serviço licitado e pela própria complexidade do objeto licitado. Ademais, verifica-se que o próprio artigo 33 da Lei n.º 8666/93 permite expressamente a participação de empresas em consórcio.

Corroborando tal entendimento, verifica-se a primorosa lição de Marçal Justen Filho sobre a permissão de consórcio na licitação. Se num primeiro momento a associação de empresas em consórcio pode gerar a diminuição da competitividade, em outras circunstâncias, como a do presente caso, pode ser um elemento que a garanta, senão vejamos:

> "Mas o consórcio também pode prestar-se a resultados positivos e compatíveis com a ordem jurídica. **Há hipóteses em que as circunstâncias do mercado e (ou) complexidade do objeto tornam problemática a**

> **competição.** Isso se passa quando grande quantidade de empresas, isoladamente, não dispuserem de condições para participar da licitação. **Nesse caso, o instituto do consórcio é via adequada para propiciar ampliação do universo de licitantes.** É usual que a Administração Pública apenas autorize a participação de empresas em consórcio quando as dimensões e complexidade do objeto ou as circunstâncias concretas exijam a associação entre os particulares. São as hipóteses em que ***apenas*** **poucas empresas estariam aptas a preencher as condições especiais exigidas para a licitação**."[1] (grifo nosso)

Com espantosa precisão, o entendimento de Marçal Justen Filho subsume-se perfeitamente ao caso em questão. O mercado é naturalmente restrito e o objeto da licitação complexo a ponto de reduzir a participação de empresas, sendo a competitividade reduzida por essas características. Nesse sentido, a imposição de mais uma restrição apenas põe em risco o princípio da competitividade.

A possibilidade de a Administração permitir a participação de consórcios em licitação está prevista no art. 33 da Lei n.º. 8.666/1993, art. 17 do Decreto n.º. 3.555/2000 e art. 16 do Decreto n.º. 5.450/2005. Tais normativos apresentam as regras que devem ser obedecidas pela Administração atinentes à participação de empresas em consórcio nos certames

Nesse sentido, cumpres observar o que determina a Lei nº 8.666/93:

> *"Art. 3º - A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.*
>
> ***§ 1º É vedado aos agentes públicos:***
>
> ***I - admitir, prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo e estabeleçam preferências*** *ou distinções em razão da naturalidade, da sede ou domicílio dos licitantes* ***ou de qualquer outra*** *circunstância impertinente ou irrelevante para o específico objeto do* ***contrato****;"*

Vale lembrar que dentre os Princípios da Administração, o da Legalidade é o mais importante e do qual decorrem os demais, por ser essência ao Estado de Direito e ao Estado Democrático de

[1] JUSTEN FILHO, Marçal. *Comentários à Lei de Licitações e Contratos Administrativos*. 14. Ed. São Paulo: Editora Dialética, 2010, p. 495.

Direito. **Note que na atividade administrativa permite-se a atuação do agente público, apenas se concedida ou deferida por norma legal**, ao passo que ao particular é permitido fazer tudo quanto não estiver proibido pela lei. Toda atividade administrativa vincula-se a tal princípio, que se encontra consagrado em nossa Constituição Federal (Art. 5º, II, XXXV e Art. 37).

Ora, mantida a restrição quanto ao formato da participação das empresas em consórcio, a Impugnante estará, juntamente com outras prestadoras de serviços de telecomunicações, prejudicada de participar desta competição! O licitante, nesta licitação, pode (e deve), com segurança, eficiência e vantajosidade, admitir a participação de empresas consorciadas, sem quaisquer limitações, como sempre o fez, **porque a associação de empresas pode representar a apresentação da melhor proposta para a Administração.**

Nesse sentido, cumpre trazer os seguintes entendimentos do TCU acerca da matéria:

> "No entender da Unidade Técnica, não obstante constituir faculdade da Administração permitir ou não a participação de empresas em consórcio nas aludidas convocações, no presente caso, **a vedação teria ocorrido sem a adequada motivação, o que teria inviabilizado a participação de mais licitantes, em prejuízo do princípio da ampla competição**." (Acórdão 59/2006 - Plenário)

> "Não prospera também o argumento de que a possibilidade de formação de consórcio no Edital afastaria eventual restrição à competitividade da licitação. **A constituição de consórcio visa, em última instância, a junção de 2 (duas) ou mais empresas para realização de determinado empreendimento, objetivando, sob a ótica da Administração Pública, proporcionar a participação de um maior número de empresas na competição, quando constatado que grande parte delas não teria condições de participar isoladamente do certame**. (...)" (Acórdão n.º 1.591/2005, Plenário, rel. Ministro Guilherme Palmeira) (grifo nosso)

Nota-se, tanto do entendimento doutrinário quanto jurisprudencial, que a permissão de consórcios nas licitações tem aspecto bifronte, podendo gerar ou restringir a competitividade. Não obstante, conforme se demonstrou acima, a formação de consórcios é medida válida e necessária, que irá beneficiar a Administração com o aumento da participação de empresas na licitação, aumentando a competição entre elas e reduzindo, inevitavelmente, o preço final da contratação.

Da mesma forma, não deve haver restrições quanto ao consórcio de empresas que sejam coligadas, controladoras e controladas. Isso porque, decorrente das particularidades do mercado

e da economia globalizada, é comum a existência no âmbito das telecomunicações conglomerados econômicos que necessitam dessa ferramenta jurídica para participarem das licitações. Frise-se que muitas das vezes a prestação do serviço por empresa isolada não é o suficiente, necessitando da atuação em conjunto para a consecução do objeto da licitação.

Ante o exposto, de forma a possibilitar a participação de um maior número de empresas no certame, garantindo a sua competitividade e a busca pela proposta mais vantajosa à Administração Pública requer seja excluído o item 5.6.5 do Edital **para que seja permitida a participação em consórcio de empresas,** nos termos do art. 33 da Lei n.º 8.666/93.

3. IMPEDIMENTO À PARTICIPAÇÃO DE EMPRESAS SUSPENSAS DE LICITAR COM A ADMINISTRAÇÃO PÚBLICA EM GERAL

O item 5.6.6 do Edital veda a participação de empresas que estejam cumprindo penalidade de suspensão do direito de licitar com a Administração Pública Direta ou Indireta Federal, Estadual, Municipal ou do Distrito Federal.

Com efeito, o art. 87, inciso III, da Lei n.º 8.666/1993 prevê, dentre as modalidades de penalidades em caso de inexecução total ou parcial do contrato, a **suspensão temporária de participação em licitação e impedimento de contratar com a Administração**.

Diante do acima exposto, faz-se necessário esclarecer que os conceitos de Administração e Administração Pública são distintos, nos termos dos incisos XI e XII do art. 6º da Lei de Licitações, *in verbis*:

> "Art. 6º - Para os fins desta Lei, considera-se:
>
> XI - Administração Pública - a administração direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, abrangendo inclusive as entidades com personalidade jurídica de direito privado sob controle do poder público e das fundações por ele instituídas ou mantidas;
>
> XII - Administração - órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente;"

Da análise dos dispositivos legais, verifica-se que as expressões "Administração Pública" e "Administração" são distintas.

Nesse sentido, importante citar a lição de Marçal Justen Filho a respeito do tema:

> "**Administração Pública**: A expressão é utilizada em acepção ampla e não deve ser identificada com 'Poder Executivo'. Indica as pessoas de direito público que participam de uma contratação, ainda quando esta contratação se efetive através de órgãos do Poder Judiciário e do Poder Legislativo. Além da chamada 'Administração Direta' (União, Estados e Distrito Federal, Municípios), a expressão também abrange a 'Administração Indireta' (autarquias, empresas públicas e sociedades de economia mista). Além disso, as 'fundações' instituídas ou mantidas com recursos públicos ou outras pessoas de direito privado sob controle estatal estão abarcadas no conceito."
>
> "**Administração**: A expressão isolada é utilizada para identificar a unidade específica que, no caso concreto, está atuando. A distinção entre Administração Pública e Administração é utilizada em algumas passagens na disciplina da Lei n.º 8.666. A hipótese de maior relevância encontra-se no art. 87, incs. III e IV, a propósito das sanções de suspensão temporária do direito de licitar ou de contratar e de declaração de inidoneidade."[2]

Da mesma forma entende Jessé Torres Pereira:

> "A distinção, para os fins de aplicação desta lei, entre Administração e Administração Pública encontra importantes aplicações. Ilustre-se com a intrincada questão de estabelecer-se a extensão das penalidades de suspensão e de declaração de inidoneidade, ambas acarretando a supressão temporária do direito de participar de licitações e de contratar. Tratando-se de suspensão, a supressão se dá em face da Administração; na hipótese de inidoneidade, o cumprimento da punição é em face da Administração Público."[3]

Este entendimento foi ratificado em recentes decisões do Plenário do **Tribunal de Contas da União**, segundo o qual **os efeitos jurídicos da referida sanção <u>está adstrita ao órgão que a aplicou.</u>** Nesse sentido, destaca-se:

> **"-** ACÓRDÃO Nº 266/2019 - TCU - Plenário
>
> "9.3. dar ciência à Defensoria Pública da União, com fundamento no art. 7º da Resolução-TCU 265/2014, para que sejam adotadas medidas internas

[2] JUSTEN FILHO, Marçal. *Comentários à lei de licitações e contratos administrativos*. 15ª ed. São Paulo: Editora Dialética, 2012, p. 142.

[3] PEREIRA JUNIOR, Jessé Torres. *Comentários à lei das licitações e contratações da administração pública.* 7 ed. Rio de Janeiro: Editora Renovar, 2007, p. 125.

com vistas à prevenção de ocorrências semelhantes acerca da inabilitação, no Pregão Eletrônico 83/2018, da licitante Portal Turismo e Serviços EIRELI, em desconformidade com a legislação em vigor e o entendimento deste Tribunal (Acórdãos 3.243/2012, 3.439/2012, 2.242/2013, 3.645/2013, 504/2015 e 1.764/2017), **no sentido de que a suspensão do direito de licitar prevista no inciso III do art. 87 da Lei 8.666/1993 produz efeitos apenas em relação ao órgão ou entidade contratante que aplicou a penalidad**e;"

"DATA: 13/02/2019
ASSUNTO: SANÇÕES ADMINISTRATIVAS
ACÓRDÃO 269/2019 - PLENÁRIO

Dar ciência à Financiadora de Estudos e Projetos – Finep, com fundamento no art. 7º da Resolução – TCU 265/2014, acerca das seguintes falhas (…), para que sejam adotadas medidas internas com vistas à prevenção de ocorrência de outras semelhantes:

1. a interpretação dada ao art. 7º da Lei 10.520/2002 afronta a jurisprudência do TCU, a qual é no sentido de que as sanções previstas nesse dispositivo se limitam ao **ente federado sancionador** (Acórdãos 2.242/2013, 2.081/2014 e 2.530/2015, todos do Plenário deste Tribunal, entre outros);

2. a interpretação dada ao art. 38, inciso II, da Lei 13.303/2016 está equivocada, uma vez que **o impedimento de participar de licitações em razão desse dispositivo se refere tão somente a sanções aplicadas pela própria entidade**, e não a sanções aplicadas por outra empresa pública ou sociedade de economia mista."

Vale mencionar que este já era o **entendimento "histórico" do Tribunal de Contas da União**, conforme se nota dos acórdãos nº 1.727/2006-1ª Câmara, nº 2.617/2010-2ª Câmara, nº 1.539/2010-Plenário e da Decisão nº 352/98-Plenário.

Assim, ao apresentar comparativo entre a sanção de suspensão do direito de licitar/impedimento de contratar e a declaração de inidoneidade, defende que a ***Administração*** é entendida, pela definição constante do inciso XI do art. 6º do diploma legal em comento, como sendo o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente – vale dizer, o *órgão público*. Já a **Administração Pública** é definida como sendo

o universo de órgãos e entidades da União, dos Estados, do Distrito Federal e dos Municípios, nos termos do inciso XII do art. 6º da Lei n.º 8.666.

Portanto, requer seja alterado o item 5.6.6 do Edital, para que seja vedada a participação apenas das empresas suspensas de licitar e impedidas de contratar com este órgão público licitante, e não com a Administração Pública em geral.

4. DA EXIGÊNCIA DE EMISSÃO DE NOTA FISCAL COM CNPJ DA EMPRESA CONTRATADA

O Edital deste certame licitatório, no item 7.6 do Edital exige que: *"O CNPJ da proponente, empresa cadastrada no SICAF e habilitada na licitação, deverá ser o mesmo para efeito de emissão das notas fiscais e posterior pagamento."*

A mencionada exigência, no entanto, não encontra previsão legal e, além disso, se mostra ofensora a prescrições licitatórias e tributárias. Vejamos.

Inicialmente, vale destacar que o princípio da legalidade é elemento basilar do regime jurídico-administrativo, considerado a "diretriz básica da conduta dos agentes da Administração" (CARVALHO FILHO, 2011, p. 18). Nesse sentido, é considerado aspecto indissociável de toda a atividade administrativa, vinculando as ações do administrador à lei, sendo decorrência direta do Estado Democrático de Direito.

Dessa forma, não pode o administrador furtar-se ao cumprimento da lei. Mais que isso, sua liberdade de ação deverá ser balizada inexoravelmente por texto legal. CELSO ANTÔNIO BANDEIRA DE MELLO (2011, p. 108) define com clareza que "o princípio da legalidade, no Brasil, significa que a Administração nada pode fazer senão o que a lei determina". Com isso, verifica-se que a liberdade administrativa diferencia-se da civil por ser positiva, ou seja, a lei define claramente os limites da atuação do administrador, enquanto a segunda é negativa, sendo legal todas as ações que não contrariem a lei.

Do ponto de vista licitatório, o artigo 29 da Lei n. 8.666/93 possibilita, ao participante da licitação, que comprove sua regularidade fiscal com documentação **do domicílio ou da sede**. Portanto, cabe à proponente a alternativa na apresentação de um ou outro, ou seja, tem a licitante a prerrogativa, autorizada em lei, de apresentar **documentação da sua filial ou da matriz**.

Sobre o tema, o Tribunal de Contas da União já se manifestou afirmando "[...] que, se a matriz participa da licitação, todos os documentos de regularidade fiscal devem ser apresentados em seu nome e de acordo com o seu CNPJ. Ao contrário, se a filial é que participa da licitação, todos os documentos de regularidade fiscal devem ser apresentados em seu nome e de acordo com o seu próprio CNPJ." (Acórdão n. 3.056/2008 - Plenário).

Vale salientar que **matriz e filial não são pessoas jurídicas distintas**. A matriz e a filial representam estabelecimentos diferentes pertencentes à mesma pessoa jurídica (TCU, Acórdão n. 3.056/2008 - Plenário). Por isso, não há óbice em o estabelecimento matriz ter sido habilitado e a filial entregar os produtos/serviços contratados.

Entretanto, *no que concerne à questão tributária*, a diferenciação matriz/filial assume relevância. Isto porque, sendo os serviços de telecomunicação tributados por ICMS (art. 155, II, da CF/88), imposto estadual, **cada filial é contribuinte no Estado em que domiciliada**.

Melhor explicando: não obstante o CNPJ da matriz conste da Fatura apresentada, mensalmente, à Administração Pública, as notas fiscais, em atendimento à legislação que regula o recolhimento dos tributos incidentes sobre os serviços prestados (telecomunicação), são emitidas em cada local da prestação do serviço.

Assim, uma vez que o ICMS é incidente sobre a prestação de serviços de telecomunicações e sendo esse um tributo de competência estadual, em cada Estado onde o serviço de telecomunicações é prestado pela Oi, se dá a emissão da nota fiscal correspondente, razão pela qual as notas fiscais são emitidas pelas filiais.

Diante do exposto, ao emitir a nota fiscal com o CNPJ da filial, não obstante o contrato seja firmado pela Oi - Matriz, a Oi nada mais faz do que cumprir os pressupostos legais que regem a matéria tributária, sem prejuízo da Lei n. 8.666/93 que, como se vê aqui, igualmente encontra-se observada em sua íntegra.

Assim, frise-se, não obstante a participação da proponente no certame licitatório se dê com apresentação de seus documentos da matriz **OU** da Filial, na forma do artigo 29 da Lei n. 8.666/93, as notas fiscais devem ser emitidas no CNPJ da filial do local onde é prestado o serviço, pois é este estabelecimento, nos termos do artigo 127, II, do Código Tributário Nacional, o contribuinte de ICMS para o Estado.

Diante do exposto, requer a alteração do item em comento para que, de forma a cumprir os pressupostos legais que regem a matéria tributária, sem prejuízo da Lei 8.666/93, seja emitida nota fiscal com o CNPJ da filial, não obstante o contrato possa ser firmado pela matriz na forma do art. 29 da Lei n. 8666/93.

5. PAGAMENTO VIA NOTA FISCAL COM CÓDIGO DE BARRAS

O item 19.2 do Edital estabelece que o pagamento deverá ser realizado por de crédito em conta corrente, mediante ordem bancária.

Ocorre que tal sistema de pagamento encontra-se em dissonância com o procedimento de pagamento adotado relativamente aos serviços de telecomunicações, uma vez que esses **são pagos mediante apresentação de fatura (nota fiscal com código de barras), ou mediante**

SIAFI nos casos de órgãos vinculados à Administração Pública Federal, como é o caso da ANATEL.

Como é cediço, o SIAFI é um sistema informatizado que controla a execução orçamentária, financeira, patrimonial e contábil dos órgãos da Administração Pública direta federal, das autarquias, fundações e empresas públicas federais e das sociedades de economia mista que estiverem contempladas no orçamento fiscal e (ou) no orçamento da seguridade social da União.

Assim, as unidades gestoras registram seus documentos (empenho, ordem bancária etc.) e o SIAFI efetua automaticamente todos os lançamentos contábeis necessários para se ter conhecimento atualizado das receitas, despesas e disponibilidades financeiras do Tesouro Nacional.

Com efeito, esse sistema de faturamento e cobrança, o qual permite o reconhecimento rápido e eficiente do pagamento, é baseado em código de barras.

Qualquer outra forma de pagamento, como o depósito em conta corrente previsto no Edital, causará transtornos ao sistema de contas a receber da empresa de telecomunicações contratada.

Ademais, a Oi utiliza o sistema de faturamento, por meio de Nota Fiscal/Fatura, emitida com código de barras para pagamento, em apenas uma via, modelo 22, em razão das várias vantagens que essa forma de pagamento proporciona.

Tal sistema proporciona vantagens à empresa prestadora dos serviços, haja vista que reduz a inadimplência e garante a satisfação do cliente.

Ante o exposto, para a melhor adequação do instrumento convocatório à realidade do setor de telecomunicações, requer a alteração do item 19.2 do Edital, a fim de permitir que o pagamento seja realizado mediante autenticação de código de barras, facilitando, assim, o reconhecimento eficiente do pagamento.

6. INDEVIDA APRESENTAÇÃO DE CERTIDÕES DE REGULARIDADE MENSALMENTE

O item 19.2.1 do Edital, os itens 9.1.1 e 9.2.1 do Termo de Referência e a Cláusula Décima Terceira, itens 1.1 e 2.1 da Minuta do Contrato estabelecem que a Contratante deverá apresentar os comprovantes de regularidade fiscal/social/trabalhista mensalmente, ou seja, no momento do pagamento junto com a nota fiscal/fatura.

Inicialmente é importante observar que tal obrigação não encontra guarida na Lei n.º 8.666/93, portanto, sem lastro legal.

Não obstante tal fato, é importante observar que a exigência de apresentação das certidões de regularidade juntamente com as notas fiscais não é razoável. Explica-se: as certidões de regularidade fiscal/social/trabalhista possuem um período de vigência que ultrapassa o período mensal (30 dias).

Assim, a apresentação mensal das referidas certidões foge dos padrões lógicos, visto que o prazo de validade das mesmas ultrapassa o período de trinta dias.

É de suma importância observar que não está se discutindo aqui a necessidade da manutenção dos requisitos de habilitação durante toda a execução do contrato. Tal fato é inquestionável! O que se discute nesta análise é a desproporcionalidade e ilegalidade em exigir a apresentação mensal desses requisitos, principalmente, pelos mesmos possuírem período de vigência superior à 30 (trinta) dias.

Vale corroborar, que a Administração Pública possui fé pública para certificar as informações apresentadas nas certidões. Se a certidão informa que seu prazo de validade é de 120 dias, porque a contratada deverá apresentar a certidão mensalmente?

Verifica-se a incongruência na aplicação da exegese do item 19.2.1 do Edital, dos itens 9.1.1 e 9.2.1 do Termo de Referência e da Cláusula Décima Terceira, itens 1.1 e 2.1 da Minuta do Contrato. Como se sabe, a atividade administrativa exige prestígio aos princípios da razoabilidade e proporcionalidade.

Carlos Ari Sundfeld, na obra “Fundamentos de Direito Público” afirma o seguinte acerca da proporcionalidade (fls. 165):

> *“A proporcionalidade é expressão quantitativa da razoabilidade. É inválido o ato desproporcional em relação à situação que o gerou ou à finalidade que pretende atingir.”*

Ora, o administrador está jungido ao Princípio da Legalidade, portanto, ao determinar obrigações que não possuem previsão legal, atua de forma desproporcional e irrazoável.

Para José dos Santos Carvalho Filho, "razoabilidade é a qualidade do que é razoável, ou seja, aquilo que se situa dentro dos limites aceitáveis, ainda que os juízos de valor que provocaram a conduta possam dispor-se de forma um pouco diversa"[4].

O princípio da regra da razão expressa-se em procurar a solução que está mais em harmonia com as regras de direito existentes e que, por isso, parece a mais satisfatória, em atenção à preocupação primária da segurança, temperada pela justiça, que é a base do Direito.

A Administração Pública está obrigada a adotar a alternativa que melhor prestigie a racionalidade do procedimento e de seus fins.

Nesse sentido, Marçal Justen Filho ensina que:

> "O princípio da proporcionalidade restringe o exercício das competências públicas, proibindo o excesso. A medida limite é a salvaguarda dos interesses públicos e privados em jogo. Incumbe ao Estado adotar a medida menos danosa possível, através da compatibilização entre os interesses sacrificados e aqueles que se pretende proteger."[5]

Diante disso, requer a alteração do item 19.2.1 do Edital, dos itens 9.1.1 e 9.2.1 do Termo de Referência e da Cláusula Décima Terceira, itens 1.1 e 2.1 da Minuta do Contrato para que não exija a apresentação mensal das certidões de regularidade fiscal/trabalhista/sociais, sob pena de ferir os Princípios da Razoabilidade, da Proporcionalidade, da Legalidade e ainda, o da fé pública inerente aos documentos públicos (certidões).

7. RETENÇÃO DO PAGAMENTO PELA CONTRATANTE

O item 19.2.3 do Edital e a Cláusula Décima Terceira, parágrafo terceiro da Minuta do Contrato dispõem sobre hipóteses de retenção do pagamento que não encontram previsão legal.

Entretanto, o art. 87 da Lei de Licitações define rol taxativo de sanções aplicáveis à Contratada, prevendo a hipótese de advertência, multa, suspensão temporária de participação em licitação, impedimento de contratar com a Administração e declaração de inidoneidade para licitar ou contratar com a Administração Pública. Não obstante, **não consta em nenhum momento a previsão de retenção dos pagamentos.**

[4] CARVALHO FILHO, José dos Santos. *Manual de Direito Administrativo*. 24. Ed. Rio de Janeiro: Editora Lumen Juris, 2011, p. 36.
[5] JUSTEN FILHO, Marçal. *Comentários à Lei de Licitações e Contratos Administrativos*. 14. Ed. São Paulo: Editora Dialética, 2010, p. 78.

Nesse sentido, deve-se impedir que o Edital imponha à Contratada medidas que não estejam relacionadas ao art. 87 da Lei 8.666/1993, em obediência ao princípio da legalidade. Dessa forma, pode-se afirmar que a exigência editalícia em comento não tem razão de ser, sendo impossível promover a retenção dos pagamentos como sanção ao não cumprimento da regularidade fiscal.

Esse é entendimento recentemente esposado pelo Tribunal de Contas da União – TCU, no sentido de que a perda da regularidade fiscal no curso de contratos de execução continuada ou parcelada justifica a imposição de sanções à Contratada, mas **não autoriza a retenção de pagamentos por serviços prestados:**

> "Consulta formulada pelo Ministério da Saúde suscitou possível divergência entre o Parecer da Procuradoria Geral da Fazenda Nacional (PGFN) 401/2000 e a Decisão nº 705/1994 – Plenário do TCU, **relativamente à legalidade de pagamento a fornecedores em débito com o sistema da seguridade social que constem do Sistema de Cadastramento Unificado de Fornecedores (Sicaf)**. A consulente registra a expedição, pelo Ministério do Planejamento, Orçamento e Gestão de orientação baseada no Parecer 401/2000 da PGFN, no sentido de que "os bens e serviços efetivamente entregues ou realizados devem ser pagos, ainda que constem irregularidades no Sicaf". Tal orientação, em seu entendimento, colidiria com a referida decisão, por meio do qual o Tribunal firmou o entendimento de que os órgãos e as entidades da Administração Pública Federal devem exigir, nos contratos de execução continuada ou parcelada, a comprovação, por parte da contratada, da regularidade fiscal, incluindo a da seguridade social. O relator, ao endossar o raciocínio e conclusões do diretor de unidade técnica, **ressaltou a necessidade de os órgãos e entidade da Administração Pública Federal incluírem, "nos editais e contratos de execução continuada ou parcelada, cláusula que estabeleça a obrigação do contratado de manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação", além das sanções resultantes de seu descumprimento. Acrescentou que a falta de comprovação da regularidade fiscal e o descumprimento de cláusulas contratuais "podem motivar a rescisão contratual, a execução da garantia para ressarcimento dos valores e indenizações devidos à Administração e a aplicação das penalidades previstas no art. 87 da Lei nº 8.666/93, mas não a retenção do pagamento". Caso contrário estaria a Administração incorrendo em enriquecimento sem causa. Observou, também, que a retenção de pagamento ofende o princípio da legalidade**

> **por não constar do rol do art. 87 da Lei nº 8.666/93. O Tribunal, então, decidiu responder à consulente que os órgãos e entidades da Administração Pública Federal devem: a) "… exigir, nos contratos de execução continuada ou parcelada, a comprovação, por parte da contratada, da regularidade fiscal, incluindo a seguridade social, sob pena de violação do disposto no § 3º do art. 195 da Constituição Federal"; b) "… incluir, nos editais e contratos de execução continuada ou parcelada, cláusula que estabeleça a obrigação do contratado de manter, durante a integral execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação, prevendo, como sanções para o inadimplemento a essa cláusula, a rescisão do contrato e a execução da garantia para ressarcimento dos valores e indenizações devidos à Administração, além das penalidades já previstas em lei (arts. 55, inciso XIII, 78, inciso I, 80, inciso III, e 87, da Lei nº 8.666/93)**". (Acórdão n.º 964/2012-Plenário, TC 017.371/2011-2, rel. Min. Walton Alencar Rodrigues, 25.4.2012) (grifo nosso)

Na mesma esteira encontra-se a jurisprudência do STJ:

> "ADMINISTRATIVO. CONTRATO. ECT. PRESTAÇÃO DE SERVIÇOS DE TRANSPORTE. DESCUMPRIMENTO DA OBRIGAÇÃO DE MANTER A REGULARIDADE FISCAL. RETENÇÃO DO PAGAMENTO DAS FATURAS. IMPOSSIBILIDADE.
>
> 1. A exigência de regularidade fiscal para a participação no procedimento licitatório funda-se na Constituição Federal, que dispõe no § 3º do art. 195 que "a pessoa jurídica em débito com o sistema da seguridade social, como estabelecido em lei, não poderá contratar com o Poder Público nem dele receber benefícios ou incentivos fiscais ou creditícios", e deve ser mantida durante toda a execução do contrato, consoante o art. 55 da Lei 8.666/93.
>
> 2. O ato administrativo, no Estado Democrático de Direito, está subordinado ao princípio da legalidade (CF/88, arts. 5º, II, 37, caput, 84, IV), o que equivale assentar que a Administração poderá atuar tão somente de acordo com o que a lei determina.
>
> **3. Deveras, não constando do rol do art. 87 da Lei 8.666/93 a retenção do pagamento pelos serviços prestados, não poderia a ECT aplicar a referida sanção à empresa contratada, sob pena de violação ao princípio constitucional da legalidade. Destarte, o descumprimento de cláusula**

contratual pode até ensejar, eventualmente, a rescisão do contrato (art. 78 da Lei de Licitações), mas não autoriza a recorrente a suspender o pagamento das faturas e, ao mesmo tempo, exigir da empresa contratada a prestação dos serviços.

4. Consoante a melhor doutrina, a supremacia constitucional 'não significa que a Administração esteja autorizada a reter pagamentos ou opor-se ao cumprimento de seus deveres contratuais sob alegação de que o particular encontra-se em dívida com a Fazenda Nacional ou outras instituições. A administração poderá comunicar ao órgão competente a existência de crédito em favor do particular para serem adotadas as providências adequadas. A retenção de pagamentos, pura e simplesmente, caracterizará ato abusivo, passível de ataque inclusive através de mandado de segurança.' (Marçal Justen Filho. Comentários à Lei de Licitações e Contratos Administrativos, São Paulo, Editora Dialética, 2002, p. 549).

5. Recurso especial a que se nega provimento." (REsp 633.432/MG, Rel. Ministro LUIZ FUX, PRIMEIRA TURMA, julgado em 22/02/2005, DJ 20/06/2005, p. 141)

Assim, existindo na data de pagamento pendências fiscais, poderá a Administração, atendendo ao princípio da legalidade, aplicar uma das sanções definidas no art. 87 da Lei de Licitações, não sendo admissível a imposição de sanção que fuja ao rol taxativo do dispositivo legal citado. Frise-se que o princípio da legalidade, sendo o elemento basilar do regime jurídico-administrativo, é considerado como aspecto indissociável de toda a atividade administrativa, vinculando as ações do administrador à lei, sendo decorrência direta do Estado Democrático de Direito. Dessa forma, impor sanção que extrapola a lei importa em desrespeito inexorável ao princípio da legalidade.

Diante disso, tendo em vista que a suspensão do pagamento pelos serviços prestados não consta no rol do art. 87 da Lei n.º 8.666/93, o qual elenca as sanções pela inexecução total ou parcial do contrato, requer a modificação do item 19.2.3 do Edital e da Cláusula Décima Terceira, parágrafo terceiro da Minuta do Contrato.

8. DAS PENALIDADES EXCESSIVAS

Os itens 20.1 do Edital, os itens 12.1.5, 12.1.6 e 12.1.7 do Termo de Referência e a Cláusula Décima Oitava, parágrafo terceiro, itens IV, V e VI da Minuta do Contrato determinam a aplicação de multas que extrapolam o limite de 10% (dez por cento) sobre o valor do contrato estabelecido

pelo Decreto n.º 22.626/33, em vigor conforme Decreto de 29 de novembro de 1991. A fixação de multa nesse patamar também ofende a Medida Provisória n.º 2.172/01 (e suas reedições), aplicável a todas as modalidades de contratação, inclusive aquelas firmadas entre particulares e Administração Pública.

O art. 87, inciso III, da Lei de Licitações determina que na hipótese de inexecução total ou parcial do contrato a Administração poderá aplicar a sanção de "multa, na forma prevista no instrumento convocatório ou no contrato". Ocorre que não há no dispositivo em questão qualquer limite à aplicação da multa, o que gera, automaticamente, sua interpretação indissociável com o princípio da proporcionalidade, conforme se observa do entendimento de Marçal Justen Filho sobre o tema:

> "Então, o instrumento jurídico fundamental para elaboração de uma teoria quanto às sanções atinentes à contratação administrativa reside na proporcionalidade. Isso significa que, tendo a Lei previsto um elenco de quatro sanções, dotadas de diverso grau de severidade, impõe-se adequar as sanções mais graves às condutas mais reprováveis. **A reprovabilidade da conduta traduzir-se-á na aplicação de sanção proporcionada correspondente**"[6] (grifo nosso)

Nesse sentido, deve-se guardar a proporcionalidade entre o fato gerador da sanção e o *quantum* a ser exigido, como bem alinhava o art. 2º, parágrafo único, inciso VI, da Lei n.º 9.784/1999, por exigir "adequação entre meios e fins, vedada a imposição de obrigações, restrições e sanções em medida superior àquelas estritamente necessárias para o atendimento do interesse público".

Não é o que se observa no caso em questão. A multa definida no percentual acima exposto gera para a Contratada gravame completamente desproporcional, ferindo os princípios da proporcionalidade e da própria legalidade.

A doutrina alemã do princípio da proporcionalidade, amplamente aceita e praticada no sistema jurídico brasileiro, traz como método de sua aplicação a análise de seus três sub-princípios: adequação (G*eeignetheit*), necessidade (*Notwendigkeit*) e proporcionalidade em sentido estrito (V*erhältnismäßig im engeren Sinn*). O pressuposto da adequação determina que a medida aplicada deve guardar relação entre meio e fim, de modo que seja a mais adequada para a resolução da questão. A necessidade diz respeito à escolha da medida menos gravosa para atingir sua efetividade. E, por fim, a proporcionalidade em sentido estrito é a ponderação entre o

[6] JUSTEN FILHO, Marçal. *Comentários à Lei de Licitações e Contratos Administrativos*. 14. Ed. São Paulo: Editora Dialética, 2010, p. 884.

meio-termo e a justa-medida da ação que se deseja perpetrar, verificando-se se a medida alcançará mais vantagens que desvantagens.

Tal princípio é reconhecido e definido por José dos Santos Carvalho Filho da seguinte forma:

> "Segundo a doutrina alemã, para que a conduta estatal observe o princípio da proporcionalidade, há de revestir-se de tríplice fundamento: 1) adequação, significando que o meio empregado na atuação deve ser compatível com o fim colimado; 2) **exigibilidade**, porque a conduta deve ser necessária, não havendo outro meio menos gravoso ou oneroso para alcançar o fim público, ou seja, **o meio escolhido é o que causa o menor prejuízo possível para os indivíduos**; 3) **proporcionalidade em sentido estrito, quando as vantagens a serem conquistadas superarem as desvantagens**."[7] (grifo nosso)

No presente caso, verifica-se que a sanção de multa fixada no referido percentual até se encaixam no primeiro pressuposto, sendo adequadas ao cumprimento de seu fim. No entanto, o mesmo não se pode dizer quanto à necessidade. A quantidade fixada à título de multa é medida completamente desnecessária para punir o descumprimento da regra do Edital, uma vez que poderia causar menor prejuízo para o particular e mesmo assim atingir o fim desejado. Entende-se que a aplicação de multa com fito pedagógico pode ser entendida como razoável, mas a sua definição em patamares elevados torna a sanção desnecessária. Isso porque existem meios menos gravosos, mas mesmo assim a Administração optou pela escolha do pior método.

Por fim, verifica-se que a sanção aplicada à Contratada não preenche também o pré-requisito da proporcionalidade em sentido estrito. É flagrante que o presente percentual de multa pune a Contratada sobremaneira, excedendo-se desarrazoadamente quando se observa o fato que a ensejou. É perfeita a aplicação da metáfora de Jellinek que "não se abatem pardais disparando canhões".

Observa-se, portanto, que a Administração, ao fixar a penalidade em comento, descumpriu completamente o princípio da proporcionalidade, sendo necessária a revisão de tal medida. Cumpre ainda ressaltar que não quer a Contratada se eximir do cumprimento das sanções estabelecidas se de fato viesse a descumprir o contrato e dar ensejo a rescisão deste. Pede-se apenas que estas sejam aplicadas de forma proporcional ao fato que as ensejou.

[7] CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo.** 24ª Ed. rev., ampl. e atual. Rio de Janeiro: Lumen Júris Editora, 2011, p. 38.

Noutro giro, verifica-se que o próprio STJ reconheceu que diante do caráter vago do art. 87 da Lei de Licitações, a Administração deve-se balizar pelo princípio da proporcionalidade:

> "Mandado de Segurança. Declaração de Inidoneidade. Descumprimento do Contrato Administrativo. Culpa da Empresa Contratada. Impossibilidade de Aplicação de Penalidade mais Grave a Comportamento que não é o mais Grave. Ressalvada a aplicação de Outra Sanção pelo Poder Público.
>
> **Não é lícito ao Poder Público**, diante da imprecisão da lei, **aplicar os incisos do artigo 87 sem qualquer critério**. Como se pode observar pela leitura do dispositivo, há uma gradação entre as sanções. Embora não esteja o administrador submetido ao princípio da pena específica, vigora no Direito Administrativo o princípio da proporcionalidade.
>
> Não se questiona, pois, a responsabilidade civil da empresa pelos danos, mas apenas **a necessidade de imposição da mais grave sanção a conduta que, embora tenha causado grande prejuízo, não é o mais grave comportamento**." (MS n.º 7.311/DF)

Vê-se que tal entendimento corrobora o que fora acima alinhavado, demonstrando que a fixação da sanção, bem como o *quantum* referente à multa deve ocorrer tendo como base o princípio da proporcionalidade.

Por todo o exposto, requer a adequação do item 20.1 do Edital, dos itens 12.1.5, 12.1.6 e 12.1.7 do Termo de Referência e da Cláusula Décima Oitava, parágrafo terceiro, itens IV, V e VI da Minuta do Contrato, para que as multas aplicadas observem o limite de 10% (dez por cento) sobre o valor do contrato

9. VALOR DA GARANTIA

A Cláusula Décima Quinta da Minuta do Contrato estipula que a garantia a ser apresentada deverá corresponder ao percentual de 5% (cinco por cento) sob o valor do contrato.

Todavia, o artigo 56, § 2º, da Lei 8.666/1993 estipula que a garantia exigida não excederá a 5% (cinco por cento) do valor total do contrato.

Como se sabe, a atividade administrativa exige prestígio aos princípios da razoabilidade e proporcionalidade.

Para José dos Santos Carvalho Filho, “razoabilidade é a qualidade do que é razoável, ou seja, aquilo que se situa dentro dos limites aceitáveis, ainda que os juízos de valor que provocaram a conduta possam dispor-se de forma um pouco diversa[8]”.

O princípio da regra da razão se expressa em procurar a solução que está mais em harmonia com as regras de direito existentes e que, por isso, parece a mais satisfatória, em atenção à preocupação primária da segurança, temperada pela justiça, que é a base do Direito.

A Administração Pública está obrigada a adotar a alternativa que melhor prestigie a racionalidade do procedimento e de seus fins.

Nesse sentido, Marçal Justen Filho ensina que:

> “O princípio da proporcionalidade restringe o exercício das competências públicas, proibindo o excesso. A medida limite é a salvaguarda dos interesses públicos e privados em jogo. Incumbe ao Estado adotar a medida menos danosa possível, através da compatibilização entre os interesses sacrificados e aqueles que se pretende proteger[9].”

O princípio da razoabilidade deve ser observado pela Administração Pública à medida que sua conduta se apresente dentro dos padrões normais de aceitabilidade. Se atuar fora desses padrões, algum vício estará, sem dúvida, contaminando o comportamento estatal. Não pode, portanto, existir violação ao referido princípio quando a conduta administrativa é inteiramente revestida de licitude.

Com efeito, o princípio da razoabilidade se fundamenta nos princípios da legalidade e da finalidade, como ensina Celso Antônio Bandeira de Mello:

> “A Administração Pública, ao atuar no exercício de discrição, terá que estabelecer critérios aceitáveis do ponto de vista racional, em sintonia com o senso normal de pessoas equilibradas e respeitosa das finalidades que presidiram a outorga da competência exercida.
>
> (...)
>
> Com efeito, o fato de a lei conferir ao administrador certa liberdade (margem de discrição) significa que lhe deu o encargo de adotar, ante a diversidade de

[8] CARVALHO FILHO, José dos Santos. *Manual de Direito Administrativo*. 24. Ed. Rio de Janeiro: Editora Lumen Juris, 2011, p. 36.
[9] JUSTEN FILHO, Marçal. *Comentários à Lei de Licitações e Contratos Administrativos*. 14. Ed. São Paulo: Editora Dialética, 2010, p. 78.

> situações a serem enfrentadas, a providência mais adequada a cada qual delas. Não significa como é evidente, que lhe haja outorgado o poder de agir ao sabor exclusivo de seu líbito, de seus humores, paixões pessoais, excentricidades ou critérios personalíssimos, e muito menos significa que liberou a Administração para manipular a regra de Direito de maneira a sacar dela efeitos não pretendidos nem assumidos pela lei aplicanda. Em outras palavras: ninguém poderia aceitar como *critério exegético de uma lei* que esta sufrague as providências *insensatas* que o administrador queira tomar; é dizer, que avalize previamente condutas desarrazoadas, pois isto corresponderia a irrogar dislates à própria regra de Direito[10].”

Logo, quando se pretender imputar à conduta administrativa a condição de ofensiva ao princípio da razoabilidade, terá que estar presente a ideia de que a ação é efetiva e indiscutivelmente ilegal. Inexiste, por conseguinte, conduta legal vulneradora do citado princípio.

Assim, o princípio da razoabilidade acarreta a impossibilidade de impor consequências de severidade incompatível com a irrelevância de defeitos. Sob esse ângulo, as exigências da Lei ou do Edital devem ser interpretadas como instrumentais.

Desta feita, a apresentação de garantia equivalente ao percentual máximo permitido em Lei não é razoável, razão pela qual se requer a modificação da Cláusula Décima Quinta da Minuta do Contrato, para que a garantia exigida não corresponda ao limite máximo de 5% (cinco por cento).

10. DOS ITENS TÉCNICOS

10.1. POSSIBILIDADE DE SUBCONTRATAÇÃO DOS SERVIÇOS

O item 10.20.2 “*A subcontratação total/parcial é permitida apenas para o Item 04 mantendo os critérios estabelecidos na seção 5.5 deste Termo;* ”

Nesse sentido, cumpre trazer à colação a redação do artigo 72 da Lei n.º 8.666/93:

> “Art. 72. O contratado, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar **partes** da obra, **serviço** ou fornecimento, até o limite admitido, em cada caso, pela Administração.” (grifo nosso)

[10] MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. 28 ed. São Paulo: Editora Malheiros. 2010, p. 108.

Ora, além da Lei prever que a Administração permita ao ente privado, que queira contratar consigo, subcontratar apenas partes dos serviços, tem-se que essas fases ou etapas devem se remeter à atividade meio do serviço licitado, **sendo vedada a subcontratação do serviço todo ou a atividade fim que a Administração está a licitar**, tendo em vista a análise dos critérios de habilitação para que a Administração contrate um ente privado realmente idôneo.

Nesse sentido é a lição de MARÇAL JUSTEN FILHO acerca da subcontratação:

> "A hipótese torna-se cabível, por exemplo, quando o objeto licitado comporta uma execução complexa, em que algumas fases, etapas ou aspectos **apresentam grande simplicidade e possam ser desempenhados por terceiros sem que isso acarrete prejuízo**. A evolução dos princípios organizacionais produziu o fenômeno denominado de 'terceirização', que deriva dos princípios da especialização e da concentração das atividades. **Em vez de desempenhar integralmente todos os ângulos de uma atividade, as empresas tornam-se especialistas em certos setores.**". [Comentários à Lei de Licitações e Contratos Administrativos, Dialética, 12ª edição, p.757] (grifamos)

Assim, está ratificada a impossibilidade da subcontratação, pela Contratada, de serviço ou atividade fim.

Neste diapasão, cumpre colacionar jurisprudência do TCU com o mesmo entendimento:

> "É ilegal e inconstitucional a sub-rogação da figura da contratada ou a divisão das responsabilidades por elas assumidas, ainda que de forma solidária, por contrariar os princípios constitucionais da moralidade e da eficiência." (Acórdão nº 3.475/2006, 1ª C., rel. Min. Marcos Bemquerer)

> "(...) firmar o entendimento de que, em contratos administrativos, é ilegal e inconstitucional a sub-rogação da figura da contratada ou a divisão das responsabilidades por elas assumidas, ainda que de forma solidária, por contrariar os princípios constitucionais da moralidade e da eficiência (art. 37, caput, da Constituição Federal), o princípio da supremacia do interesse público, o dever geral de licitar (art. 37, XXI, da Constituição) e os arts. 2º, 72 e 78, inciso VI, da Lei 8.666/96." (Acórdão nº 909/2003, Plenário, rel. Min. Augusto Sherman Cavalcanti)

Todavia, deve-se solicitar a alteração dos em comento, para que seja permitida a subcontratação parcial dos serviços, cujo a característica seja de aplicação

temporária, nos termos do art. 72 da Lei n.º 8.666/93, a fim de que seja garantida a ampliação da competitividade;

10.2. DOS PRAZOS DE ENTREGA

Os subitens “e”, “f” e “g” do item 9.2 referente aos apontamentos da proposta vencedora temos:

e) Prazo entrega do plano de implementação: Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

f) Prazo início processo de migração/reunião alinhamento: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;

g) Prazo processo de migração: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

Os prazos apresentados nos subitens supracitados são extremamente curtos e não favorecem a ampla concorrência.

Para o subitem “E” O desenho da solução e todas as nuances características do objeto proposto, são deliberados na reunião de alinhamento com a equipe da contratante. Desta forma, 5 dias úteis não são suficientes para este fim.

Com base no exposto, solicitamos a ampliação do prazo para 10 dias úteis;

Com relação ao item “F” que define o início do processo de migração da solução, o prazo de 5 dias úteis é totalmente inexequível. Para que seja possível qualquer ação de migração, se faz necessário que os equipamentos pertencentes a solução tenha sidos entregue.

Com base no exposto, solicitamos a ampliação do prazo para 60 dias, considerando o atual momento que vivemos e as dificuldades de deslocamento nos dias atuais;

Com relação ao item “G” que define o término do processo de migração da solução, o prazo de 60 dias necessita ser revisto.

Com base no exposto, solicitamos a ampliação do prazo para 90 dias, considerando o atual momento que vivemos e as dificuldades de deslocamento nos dias atuais;

10.3. DA SOLUÇÃO DE GERENCIAMENTO

A solução prevê uma gerência centralizada como descreve o item 5.2.7:

5.2.7 Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança;

Por questões de segurança e compliance com a ISO27001, não é fornecido senha de "ESCRITA" para nenhum item, appliance ou serviço.

Com base no exposto, entendemos que somente senha de LEITURA atende as necessidades da contratante para esta solução.

10.4. DA EXIGÊNCIA DE PROFISSIONAL

Para atendimento da solução contratada o item 5.8.19 exige:

5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da prestação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas;

Solicitamos que esta exigência possa ser substituída por uma declaração do fabricante que a empresa contratada é plenamente capaz de atender todos os itens do objeto desta contratação.

Pedido

Para garantir o atendimento aos princípios norteadores dos procedimentos licitatórios, a **Oi**, requer que V. Sª julgue motivadamente a presente Impugnação, no prazo de 24 horas, acolhendo-a e promovendo as alterações necessárias nos termos do Edital e seus anexos, sua consequente republicação e suspensão da data de realização do certame.

Manaus - AM, 15 de fevereiro de 2022.

RAUL LUIZ MARTINS PEREGRINO:69018669172

Assinado de forma digital por RAUL LUIZ MARTINS PEREGRINO:69018669172
Dados: 2022.02.15 20:27:41 -04'00'

Raul Luiz Martins Peregrino

CPF 690.186.691-72

Executivo de Negócios

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 60.2022.CPL.0769299.2021.015252

Aos Senhores

TADEU AZEVEDO DE MEDEIROS

Diretor de Tecnologia da Informação e Comunicação

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

NESTE EDIFÍCIO

Assunto: Impugnação interposta aos termos do Edital de **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**. Encaminha-se para análise e resposta.

Ilustríssimos Senhores,

Cumprimentando-os cordialmente e, considerando a realização do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, cujo objeto é a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.*, oportunamente, **encaminho impugnação** apresentada pela empresa **OI S.A., em Recuperação Judicial** (doc. 0769297 e 0769298), para conhecimento e, no que couber, respostas quanto aos quesitos eminentemente técnicos.

Considerando a abertura da Sessão do Pregão em epígrafe em 21/02/2022, solicito que os autos retornem a esta CPL, no máximo, fim do expediente do dia **18/02/2022**, para elaboração e emissão da respectiva decisão, em face do que dispõe o subitem 22.5 do instrumento convocatório.

Desde já, coloco-me à disposição para auxiliar no que for necessário.

Atenciosamente,

EDSON FREDERICO LIMA PAES BARRETO

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 16/02/2022, às 00:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0769299** e o código CRC **B695D53E**.

PARECER Nº 2.2022.SIET.0771082.2021.015252

OBJETO: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.
ORIGEM: Processo de Compra 2021.015252

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar pedido de esclarecimento interposto aos termos do Edital de **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, originados das empresas: **SERVIX INFORMÁTICA LTDA** (0768833), **PISONTEC SOLUTIONS** (0769231) e **ARVOO TECNOLOGIA** (0769231). Trata ainda, do pedido de imougação da empresa **OI S.A.** (0769299).

2. Análise

O presente parecer se baseia nas disposições do Termo de Referência n. 20.2021.DTIC.0720733.2021.015252, Anexo I ao Edital do certame, SEI 0763629, em seus diversos itens confome abaixo:

2.1 SERVIX INFORMÁTICA LTDA

Questionamento 01

Item - 5.2.15.6.6 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU ou memória do dispositivo.

Pergunta - A solução fornece gerenciamento apartado do plano de dados do restante da solução. Logo, quando utilizado toda a capacidade do hardware de NGFW, seu plano de gerência continua funcional sem que haja indisponibilidade do appliance ou necessidade de desativação da funcionalidade de IPS. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Sim, o entendimento está correto.

Questionamento 02

Item - 5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

Pergunta - A solução permite analisar os arquivos dentro dos fluxos de SMTP e POP3 e identificar se o conteúdo do email é maligno ou benigno e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Especificamente para o MTA (Message Transfer Agent), sim, o entendimento está correto. Não obstante, as demais topologias devem seguir sendo suportadas.

Questionamento 03

Item - 5.2.15.7.30 A solução, deve emular e eliminar malwares contidos em anexos de e-mail e documentos baixados da web.

Pergunta - A solução permite o emular os anexos contidos nos emails e documentos baixados da web, classificar esses anexos e documentos baixados como benigno e malignos e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Sim, o entendimento está correto.

Questionamento 04

Item - 5.2.15.9.39 Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados.

Pergunta - A solução permite o correlacionamento de eventos e logs, classificando em níveis de severidade, através de métricas de tempo, objetos, IP de origem e destino, usuários, nome do ataque, país de origem. A partir dessas métricas é possível visualizar graficamente as informações e correlacionar as evidências apresentadas. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Sim, o entendimento está correto.

2.2 PISONTEC SOLUTIONS

Questionamento I

Item - Geral/Ambiente

Pergunta - O serviço está sendo executado ou já foi em algum momento?

Se a reposta for positiva:

a) qual empresa é ou foi responsável?

b) Quantos profissionais atuam atualmente no serviço?

Resposta - O serviço objeto deste certame hoje é executado internamente no órgão, por profissionais técnicos especializados que são servidores concursados efetivos.

Questionamento II

Item - Geral

Pergunta - Será necessário fornecimentos de peças e/ou materiais ou softwares?

Resposta – Sim, todos os itens necessários para o cumprimento total das exigências dispostas no Edital n. 4005/2022-CPL/MP/PGJ, seus anexos, bem como no Termo de Referência n. 20.2021.|DTIC.0720733.2021.015252, são de responsabilidade da CONTRATANTE, exceto disposição em contrário explícita nestes documentos.

Questionamento III

Item - Geral

Pergunta - O serviço poderá ser executado remotamente?

Resposta – Sim, o serviço poderá ser executado remotamente, exceto em casos que impeçam esta modalidade, como em defeitos de hardware, por exemplo. Entretanto, como dita o Edital e o Tremo de Referência, os equipamentos devem ser instalados nas dependências da CONTRATANTE.

Indicamos a leitura minuciosa de todos os itens do Edital e do Termo de Referência, especialmente este último, que contém todas as especificações técnicas do serviço desejado, incluindo as previsões para as manutenções, SLA, formas de prestação do serviço, entre outros.

Questionamento IV

Item – 5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas.

Pergunta - A apresentação de Profissionais Certificados integrantes no quadro de funcionários da Licitante, deve ser realizada apenas no ato da assinatura do contrato, sendo aceitos profissionais certificados cuja contratação se dê por prestação de serviço, sem vínculo trabalhista com a Licitante.

Resposta - Deve-se atender plenamente o disposto no item 5.8.19 do Termo de Referência, não havendo vedação para comprovação do vínculo dos profissionais exigidos com a CONTRATANTE através de contrato de terceirização.

Questionamento V

Item - Não relacionado à DTIC

Pergunta - Qual o valor estimado?

Resposta - Não relacionado à DTIC

Questionamento VI

Item - Geral

Pergunta - Se existir serviços de manutenção de equipamentos, necessário disponibilizar a lista contendo as marcas e os modelos dos respectivos equipamentos.

Resposta - Todos os itens necessários para o cumprimento total das exigências dispostas no Edital n. 4005/2022-CPL/MP/PGJ, seus anexos, bem como no Termo de Referência n. 20.2021.|DTIC.0720733.2021.015252, são de responsabilidade da CONTRATANTE, exceto disposição em contrário explícita nestes documentos, ou seja, todas as manutenções nos equipamentos que fazem parte da solução integrante dos serviços objeto deste certame devem ser realizadas conforme exigências dos documentos supracitados. Indicamos a leitura minuciosa de todos os itens do Edital e do Termo de Referência, especialmente este último, que contém todas as especificações técnicas do serviço desejado, incluindo as previsões para as manutenções, SLA, formas de prestação do serviço, entre outros.

2.3 ARVOO TECNOLOGIA

Esclarecimento 01

Item - 5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.

Pergunta - Para a identificação dos usuários poderá ser utilizado o serviço agregado ao servidor de gerenciamento para integração ao base de usuários LDAP, nem a necessidade de instalação de agentes ou software de clientes nos servidores Active Directory?

Resposta - A função exigida pelos itens deve estar integrada à solução ofertada, não sendo aceitas instalações de servidores separados para suprir a funcionalidade desejada.

Esclarecimento 02

Item - 5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).

Pergunta - Após o bloqueio, serão aceitas soluções que a liberação e a continuação da navegação sejam permitidas após avaliação do responsável pela manutenção da solução ofertada?

Resposta - Não, a solução deve ser capaz de permitir que o usuário decida se continua o acesso a algo potencialmente perigoso, mesmo após um alerta/bloqueio, sem a intervenção da equipe técnica de gerenciamento da solução.

Esclarecimento 03

Item - 5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

Pergunta - Entendemos que a topologia e arquitetura de implementação do sistema de IPS deve ser capaz de interceptar todo trafego e tomar as ações de inspeção assim estipuladas quando em modo Inline e apenas registrar em modo Mirror/TAP. A topologia de implementação MTA se faz equivocada neste sentido, visto que em modo In-line ou TAP "todo" o trafego será analisado e o modo MTA se faz necessário em soluções de proteção de messageria. Neste caso o conceito de IPS não faz uso dessa topologia de comunicação para analise de apenas do trafego de mensagens de e-mail. Esta correto nosso entendimento?

Resposta - Apesar de tecnicamente o entendimento estar correto para os conceitos de IPS/IDS de soluções tradicionais de firewall, como o objeto deste certame visa a contratação de firewall de próxima geração (NGFW), é padrão de mercado que o tratamento do fluxo de emails seja feito em conjunto com todo o fluxo de dados.

Esclarecimento 04

Item - 5.2.15.8.1 Deverá possuir certificação ICSA para Firewall

Pergunta - A certificação ICSA depende de contratação para ser emitida em ordem que, os testes realizados por outras empresas certificadoras, realizam os mesmos testes de performance com abrangência internacionais. Levando isto em consideração, entendemos que a solução ofertada pode ser certificada em outros laboratórios desde que atenda aos requisitos de testes submetidos de forma equivalente aos executados pela ICSA.

Resposta - O objetivo deste certame é obter uma solução que eleve o patamar da proteção do ambiente computacional em todos os sentidos possíveis, incluindo equipamentos de qualidade excepcional, de forma a diminuir ao máximo o risco de prejuízos para o Ministério Público do Estado do Amazonas. A certificação solicitada é uma garantia do diferencial de qualidade desejado presente nos equipamentos dos melhores fabricantes do mercado, em diversas marcas, ou seja, não exigem contratação separada ou adicional para a CONTRATADA. Desta forma, sob pena de prejuízos advindos de soluções com qualidade inferior à necessária para o MPAM, todas exigências presentes no Termo de Referência devem ser atendidas, incluindo a certificação ICSA do item 5.2.15.8.1.

2.4 OI S.A.

Pedidos de impugnação dos capítulos:

"1. EXIGÊNCIA ABUSIVA"

"2. DA VEDAÇÃO DE PARTICIPAÇÃO DE LICITANTES EM REGIME DE CONSÓRCIO"

"3. IMPEDIMENTO À PARTICIPAÇÃO DE EMPRESAS SUSPENSAS DE LICITAR COM A ADMINISTRAÇÃO PÚBLICA EM GERAL"

“4. DA EXIGÊNCIA DE EMISSÃO DE NOTA FISCAL COM CNPJ DA EMPRESA CONTRATADA”

“5. PAGAMENTO VIA NOTA FISCAL COM CÓDIGO DE BARRAS”

“6. INDEVIDA APRESENTAÇÃO DE CERTIDÕES DE REGULARIDADE MENSALMENTE”

“7. RETENÇÃO DO PAGAMENTO PELA CONTRATANTE”

“8. DAS PENALIDADES EXCESSIVAS”

“9. VALOR DA GARANTIA”

Resposta: Não relacionado à DTIC

Pedido de impugnação do capítulo “10.1 POSSIBILIDADE DE SUBCONTRATAÇÃO DOS SERVIÇOS”

Resposta: Sob pena de degradação da qualidade final dos serviços prestados, bem como falta de conformidade entre os serviços prestados, além de desorganização, impossibilidades de padronização de todos os procedimentos e dificuldades de estabelecer escopos e responsabilidades com agilidade, os itens 01, 02, e 03 não devem ser prestados por empresas diferentes, o que inclui subcontratações. Soma-se ao exposto o fato dos itens 01, 02 e 03 serem serviços contínuos e, em conjunto, formarem o cerne da atividade que a CONTATANTE deseja contratar para execução. Como brevemente exposto no item 3.3, do Termo de Referência, os bens e serviços pretendidos estão intrinsecamente relacionados e a realização dos serviços por empresas diferentes pode resultar em soluções incompatíveis, o que acarretaria prejuízo ao CONTRATANTE. A descrição individualizada do objeto no caso dos itens 01, 02 e 03, dentro do Lote do certame, se deu única e exclusivamente para melhor entendimento e organização do Termo de Referência, bem como pela diferença das quantidades de cada um. Entretanto, estes itens são partes do único serviço desejado, que poderia ser descrito como o “serviço para prover o Ministério Público de uma solução, em todos os aspectos, de firewall de próxima geração em alta disponibilidade”

Pedido de impugnação do capítulo “10.2 DOS PRAZOS DE ENTREGA”

Item: 9.2, “e” - Prazo para entrega do plano de implementação

Resposta: O objetivo deste certame é a contratação de empresa especializada nos serviços descritos pelo objeto, pelo que se espera vasta experiência de seu corpo técnico, incluindo a execução de vários projetos como o que virá a ser executado pela CONTRATADA. Por óbvio, um corpo técnico com a experiência necessária para projetos deste porte e complexidade já possui plano de implementação básico, com itens indispensáveis e comuns a todo serviço do tipo, para os equipamentos que utiliza prontos e formatados, restando apenas os pequenos ajustes decorrentes de cada cenário de seus clientes. Sendo assim, considera-se o prazo indicado pela alínea “e", da entrega do plano de implementação, de 05 (cinco) dias úteis após a reunião de alinhamento é perfeitamente exequível.

Além disto, conforme descrito nas justificativas deste certame, este é um serviço crítico, essencial e contínuo, ou seja, qualquer atraso pode gerar risco desnecessário para o MPAM.

Item: 9.2, “f” - Prazo para início do processo de migração/reunião de alinhamento

Resposta: Conforme disposto no Edital e Termo de Referência, o início da migração se dá com a reunião de alinhamento e não com a efetiva instalação e configuração de equipamentos. Desta forma, não há que se falar em distensão de prazo para entrega de equipamentos. O prazo apenas exige um tempo máximo para o acontecimento da reunião de alinhamento incial, que inclusive pode ser realizada via videoconferência. Sendo assim, considera-se o prazo indicado de 05 (cinco) dias úteis após assinatura do contrato perfeitamente exequível.

Item: 9.2, “g” - Prazo para finalizar o processo de migração

Resposta: Durante a pesquisa de mercado, que precede a confecção do Termo de Referência, foram consideradas todas as dificuldades do momento atual e de deslocamento, caracteríticas de nossa região. Mesmo com as dificuldades impostas pela pandemia, em todas as consultas a diversos

fornecedores, dos mais diversos fabricantes, o prazo de 60 dias excede o indicado como necessário para este tipo de projeto por todos.

De toda forma, conforme Termo de Referência, o prazo de 60 dias só é contado enquanto há dependências por parte da CONTRATADA e fica suspenso em caso de dependências por parte da CONTRATANTE.

Além disto, conforme descrito nas justificativas deste certame, este é um serviço crítico, essencial e contínuo, ou seja, qualquer atraso pode gerar risco desnecessário para o MPAM. E, no caso da migração, pode significar uma parada completa do funcionamento do órgão.

Sendo assim, considera-se o prazo indicado pefeitamente exequível, não devendo ser alterado.

Pedido de impugnação do capítulo "10.3 DA SOLUÇÂO DE GERENCIAMENTO"

Item: 5.2.7

Resposta: A administração e gerenciamento da solução será realizada em conjunto pela equipe técnica da CONTRATANTE e da CONTRADA, sendo impraticável e ineficiente que os equipamentos da solução estejam indisponíveis para uma das equipes. A imposição por parte da CONTRATADA de não fornecer senhas que permitam escrita acabaria por gerar morosidade na resolução de problemas rotineiros e, por conseguinte, gerando prejuízos ao funcionamento eficiente do MPAM. Sendo assim, a exigência do item em questão deve permanecer inalterada.

Pedido de impugnação do capítulo "10.4 DA EXIGÊNCIA DE PROFISSIONAL"

Item: 5.8.19

Resposta: O objeto deste certame é um serviço crítico, essencial e contínuo para o funcionamento do MPAM e inclui manutenção preventiva e corretiva, com SLA bem definido. A exigência em questão visa garantir que o atendimento prestado pela CONTRATADA tenha a qualidade e a capacidade necessária, a qualquer momento, para manter o funcionamento ininterrupto dos serviços do MPAM. Sendo assim, não é suficiente uma simples declaração do fabricante como solicitado, devendo ser mantida a exigência do Termo de Referência, sob pena de prejuízos ao MPAM.

Manaus, 18 de fevereiro de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ

Coordenador da Área de Redes

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 18/02/2022, às 16:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Theo Ferreira Pará**, **Agente de Apoio - Manutenção - Suporte Informática**, em 18/02/2022, às 16:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0771082**

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DECISÃO Nº 8.2022.CPL.0771060.2021.015252

PEDIDOS DE ESCLARECIMENTOS INTERPOSTOS AOS TERMOS DO EDITAL DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ, PELO SENHOR **JEFFERSON MATOS**, REPRESENTANDO A EMPRESA **SERVIX INFORMÁTICA LTDA.**; PELA SENHORA **PEROLA PLETSCH,** REPRESENTANDO A EMPRESA **PISONTEC SOLUTIONS;** SENHOR **CRISTIAN TELES**, REPRESENTANDO A EMPRESA **ARVVO TECNOLOGIA** E **IMPUGNAÇÃO** ENCAMINHADA PELO SENHOR **RAUL LUIZ MARTINS PEREGRINO**, REPRESENTANDO A EMPRESA **OI S.A., EM RECUPERAÇÃO JUDICIAL,** TODOS EM 15 DE FEVEREIRO DE 2022. PRESSUPOSTOS LEGAIS: LEGITIMIDADE E INTERESSE DE AGIR, A EXISTÊNCIA DE UM ATO ADMINISTRATIVO E FUNDAMENTAÇÃO, ATENDIDOS. TEMPESTIVIDADE LIMITADA AO HORÁRIO DE EXPEDIENTE NO ÓRGÃO CONDUTOR DO CERTAME. NO MÉRITO, REPUTAR ESCLARECIDO. MANTER O EDITAL E DATA DO CERTAME.

1. DA DECISÃO

Analisados todos os pressupostos de admissibilidade e os aspectos objeto da peça dirigida, esta **COMISSÃO PERMANENTE DE LICITAÇÃO**, com fundamento no artigo 13, § 1.º do ATO PGJ N.º 389/2007 e art. 17, II c/c art. 23 e seus parágrafos do Decreto Federal n.º 10.024/2019, decide:

a) **Receber e conhecer** do **PEDIDO DE ESCLARECIMENTO** interposto pelo Senhor **JEFFERSON MATOS,** representando a empresa **SERVIX INFORMÁTICA LTDA**, aos termos do Edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ (doc. 0763629), pelo qual se busca a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual,* posto que **TEMPESTIVO;**

b) **Receber e NÃO conhecer** dos **PEDIDOS DE ESCLARECIMENTOS** interpostos pela Senhora **PEROLA PLETSCH,** representando a empresa **PISONTEC SOLUTIONS;** Senhor **CRISTIAN TELES**, representando a empresa **ARVVO TECNOLOGIA** e a **IMPUGNAÇÃO** apresentada pelo Senhor **RAUL LUIZ MARTINS PEREGRINO**, representando a **OI S.A., EM RECUPERAÇÃO JUDICIAL**, aos termos do Edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ (doc. 0763629), pelo qual se busca a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual,* **posto que intempestivos;**

c) Pelo ***princípio da precaução, motivação dos atos administrativos*** e em prol da ***ampliação da concorrência***, **no mérito, reputando-se, portanto, esclarecidas** as solicitações, conforme

discorrido na presente peça;

d) **Manter o edital e a data de realização do certame, uma vez que não houve nenhuma alteração do objeto**, em consonância com o art. 21, § 4º da Lei n.° 8.666/93.

2. DO RELATÓRIO

2.1. DAS RAZÕES DOS ESCLARECIMENTOS

2.1.1. JEFFERSON MATOS, representando a empresa **SERVIX INFORMÁTICA LTDA (doc. 0768830):**

Adentrou ao e-mail institucional desta Comissão Permanente de Licitação, no dia 25/03/2021, às 16h05min, o pedido de esclarecimento aos termos do Edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, apresentado pelo Senhor **JEFFERSON MATOS,** representando a empresa **SERVIX INFORMÁTICA LTDA (doc. 0768830)**, questionando, disposição técnica do objeto da contratação almejada. Eis a transcrição do teor da solicitação:

> Questionamento 01:
>
> 5.2.15.6.6. A solução fornece gerenciamento apartado do plano de dados do restante da solução. Logo, quando utilizado toda a capacidade do hardware de NGFW, seu plano de gerência continua funcional sem que haja indisponibilidade do appliance ou necessidade de desativação da funcionalidade de IPS. Compreendemos que esse método atende o item, está correto o entendimento?
>
> Questionamento 02:
>
> 5.2.15.7.16. A solução permite analisar os arquivos dentro dos fluxos de SMTP e POP3 e identificar se o conteúdo do email é maligno ou benigno e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?
>
> Questionamento 03:
>
> 5.2.15.7.30. A solução permite o emular os anexos contidos nos emails e documentos baixados da web, classificar esses anexos e documentos baixados como benigno e malignos e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?
>
> Questionamento 04:
>
> 5.2.15.9.39. A solução permite o correlacionamento de eventos e logs, classificando em níveis de severidade, através de métricas de tempo, objetos, IP de origem e destino, usuários, nome do ataque, país de origem. A partir dessas métricas é possível visualizar graficamente as informações e correlacionar as evidências apresentadas. Compreendemos que esse método atende o item, está correto o entendimento?

2.1.2. PEROLA PLETSCH, representando a empresa **PISONTEC SOLUTIONS (doc. 0769227):**

Adentrou ao e-mail institucional desta Comissão Permanente de Licitação, no dia 25/03/2021, às 15h51min e 16h58min, o pedido de esclarecimento aos termos do Edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, apresentado pela Senhora **PEROLA PLETSCH,** representando a empresa **PISONTEC SOLUTIONS (doc. 0769227)**, questionando, disposição técnica do objeto da contratação almejada. Eis a transcrição do teor da solicitação:

> Ao
> MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
> Ref. PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ
>
> Objeto - O objeto da presente licitação é a escolha da proposta mais vantajosa para contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos.
>
> Ilmo.(a) Sr.(a) Pregoeiro(a),
>
> A empresa Pisontec Comércio e Serviços em Tecnologia da Informação EIRELI, inscrita no CNPJ Nº 12.007.998/0001-35, situada em Olinda/PE, vem respeitosamente, solicitar ESCLARECIMENTO, conforme termos elencados a seguir.
>
> I – O serviço está sendo executado ou já foi em algum momento? Se a reposta for positiva: a) qual empresa é ou foi responsável? b) Quantos profissionais atuam atualmente no serviço?
>
> II - Será necessário fornecimentos de peças e/ou materiais ou softwares?
>
> III - O serviço poderá ser executado remotamente?
>
> IV – A apresentação de Profissionais Certificados integrantes no quadro de funcionários da Licitante, deve ser realizada apenas no ato da assinatura do contrato, sendo aceitos profissionais certificados cuja contratação se dê por prestação de serviço, sem vínculo trabalhista com a Licitante.
>
> V – Qual o valor estimado?
>
> VI – Se existir serviços de manutenção de equipamentos, necessário disponibilizar a lista contendo as marcas e os modelos dos respectivos equipamentos.
>
> Agradecemos sua atenção ficando no aguardo de breve resposta.
>
> Atenciosamente,

2.1.3. CRISTIAN TELES, representando a empresa **ARVVO TECNOLOGIA (doc. 0769228):**

Adentrou ao e-mail institucional desta Comissão Permanente de Licitação, no dia

25/03/2021, às 17h21min, o pedido de esclarecimento aos termos do Edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, apresentado pelo Senhor **CRISTIAN TELES**, representando a empresa **ARVVO TECNOLOGIA (doc. 0769228)**, questionando, disposição técnica do objeto da contratação almejada. Eis a transcrição do teor da solicitação:

> Prezados Srs, boa tarde!
>
> Após análise do referido Edital e seus anexos, solicitamos os seguintes esclarecimentos, de acordo com os itens abaixo:
>
> Esclarecimento 01
>
> 5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
>
> 5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.
>
> Para a identificação dos usuários poderá ser utilizado o serviço agregado ao servidor de gerenciamento para integração ao base de usuários LDAP, nem a necessidade de instalação de agentes ou software de clientes nos servidores Active Directory?
>
> Esclarecimento 02
>
> 5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).
>
> Após o bloqueio, serão aceitas soluções que a liberação e a continuação da navegação sejam permitidas após avaliação do responsável pela manutenção da solução ofertada ?
>
> Esclarecimento 03
>
> 5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.
>
> Entendemos que a topologia e arquitetura de implementação do sistema de IPS deve ser capaz de interceptar todo trafego e tomar as ações de inspeção assim estipuladas quando em modo Inline e apenas registrar em modo Mirror/TAP. A topologia de implementação MTA se faz equivocada neste sentido, visto que em modo Inline ou TAP “todo” o trafego será analisado e o modo MTA se faz necessário em soluções de proteção de messageria. Neste caso o conceito de IPS não faz uso dessa topologia de comunicação para analise de apenas do trafego de mensagens de e-mail. Esta correto nosso entendimento?
>
> Esclarecimento 04

15.8.1 Deverá possuir certificação ICSA para Firewall. A certificação ICSA depende de contratação para ser emitida em ordem que, os testes realizados por outras empresas certificadoras, realizam os mesmos testes de performance com abrangência internacionais. Levando isto em consideração, entendemos que a solução ofertada pode ser certificada em outros laboratórios desde que atenda aos requisitos de testes submetidos de forma equivalente aos executados pela ICSA.

2.2. DAS RAZÕES DA IMPUGNAÇÃO

2.2.1. RAUL LUIZ MARTINS PEREGRINO, representando a **OI S.A., EM RECUPERAÇÃO JUDICIAL (doc. 0769297 e 0769298):**

Adentrou ao e-mail institucional desta Comissão Permanente de Licitação, no dia 25/03/2021, às 17h21min, o pedido de esclarecimento aos termos do Edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, apresentado pelo Senhor **RAUL LUIZ MARTINS PEREGRINO**, representando a **OI S.A., EM RECUPERAÇÃO JUDICIAL (doc. 0769297 e 0769298)**, questionando, disposição técnica do objeto da contratação almejada. Eis a transcrição do teor da solicitação:

Ilmo. Sr. Pregoeiro do Ministério Público do Estado do Amazonas

REF.: IMPUGNAÇÃO AOS TERMOS DO EDITAL DE PREGÃO ELETRÔNICA N. 4005/2022 - -CPL/MP/PGJ

OI S.A., em Recuperação Judicial, sociedade anônima, com sede na Cidade do Rio de Janeiro, Estado do Rio de Janeiro, na Rua do Lavradio, 71, 2º andar, Bairro Centro, inscrita no CNPJ/MF sob o nº 76.535.764/0001-43, doravante denominadas OI, vem, por seu representante legal, com fulcro no art. 24, do Decreto 10.024/2019, apresentar Impugnação aos termos do Edital em referência, apresentar Impugnação aos termos do Edital em referência, pelas razões a seguir expostas:

Razões de Impugnação

O Ministério Público do Estado do Amazonas instaurou procedimento licitatório na modalidade Pregão Eletrônico, registrado sob o n.º 4.005/2022-CPL/MP/PGJ, visando a "contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos."

Contudo, a Oi tem este seu intento frustrado perante as imperfeições do Edital, contra as quais se investe, justificando-se tal procedimento ante as dificuldades observadas para participar de forma competitiva do certame.

Saliente-se que o objetivo da Administração Pública ao iniciar um processo licitatório é exatamente obter proposta mais vantajosa para contratação de bem ou serviço que lhe seja necessário, observados os termos da legislação aplicável, inclusive quanto à promoção da máxima competitividade possível entre os interessados.

Entretanto, com a manutenção das referidas exigências, a

competitividade pretendida e a melhor contratação almejada, poderão restar comprometidas o que não se espera, motivo pelo qual a Oi impugna os termos do Edital e seus anexos, o que o faz por meio da presente manifestação.

ALTERAÇÕES A SEREM FEITAS NO EDITAL E NOS ANEXOS

1. EXIGÊNCIA ABUSIVA

O item 5.6.3 do Edital prevê que não podem participar do certame empresas que tenham sócios, diretores, gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL.

Ocorre que, tais exigências mostram-se excessivas, na medida em que não possuem finalidade correlata à execução do objeto.

Além disso, as empresas de capital aberto que possuem um volume muito expressivo de acionistas, encontrarão grande dificuldade no processo de levantamento de informações tão específicas, como o grau de parentesco e vínculo empregatício de seu quadro acionário, as quais inclusive, não são informadas quando da aquisição das ações pelo público em geral.

Nesse contexto, é relevante destacar que o instrumento convocatório deve se abster de incluir cláusulas e exigências desnecessárias à finalidade da contratação, bem como aquelas que frustrem o caráter competitivo do certame.

A exigência imposta pelo Edital é medida extremamente restritiva à participação de interessados, cuja consequência direta será reduzir a participação das empresas que, nos termos da regulamentação dos serviços de telecomunicações, possuem outorga para prestação de todos os serviços licitados.

Cumpre destacar que quanto aos serviços de telecomunicações - objeto ora licitado -, estes são regulados pela Lei Geral de Telecomunicações (Lei 9.472, de 16 de julho de1997), a qual dispõe em seu artigo 6º o seguinte:

> *"Art. 6º Os serviços de telecomunicações serão organizados com base no* ***princípio da livre ampla e justa competição entre todas as prestadoras, devendo, o Poder Público atuar para propiciá-la****, bem como para corrigir os efeitos da competição imperfeita e reprimir as infrações da ordem econômica." (grifo nosso)*

Ratificando o dever do poder público de ampliar a competição entre as Operadoras, com padrões de qualidade compatíveis com as exigências dos usuários, o art. 2º, inciso III, da LGT assim determina:

> *"Art. 2° O Poder Público tem o dever de: (...)*

III - adotar medidas que promovam a competição e a diversidade dos serviços, incrementem sua oferta e propiciem padrões de qualidade compatíveis com a exigência dos usuários;" (grifo nosso)

Ademais, o inciso I do § 1º do art. 3º da Lei n.º 8.666/93 assim dispõe:

"Art. 3o A licitação destina-se a garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.

§ 1 o É vedado aos agentes públicos:

I - admitir, prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo, inclusive nos casos de sociedades cooperativas, e estabeleçam preferências ou distinções em razão da naturalidade, da sede ou domicílio dos licitantes ou de qualquer outra circunstância impertinente ou irrelevante para o específico objeto do contrato, ressalvado o disposto nos §§ 5o a 12 deste artigo e no art. 3o da Lei no 8.248, de 23 de outubro de 1991;" (grifo nosso)

Inexiste no mercado uma ampla gama de opções, o que impede a inclusão de qualquer tipo de condição que impeça ou dificulte a participação das operadoras em procedimentos licitatórios, sob pena de efetiva redução na competição.

Ante o exposto, requer a exclusão da exigência prevista no item 5.6.3 do Edital.

2. DA VEDAÇÃO DE PARTICIPAÇÃO DE LICITANTES EM REGIME DE CONSÓRCIO

O item 5.6.5 do Edital veda a participação de empresas que estejam constituídas em consórcio. Primeiramente, cumpre elucidar algumas questões referentes ao mercado de telecomunicações. É cediço que no âmbito da oferta de serviços de telecomunicações, verifica-se a escassez de competitividade, predominando no mercado poucas empresas. Tal fenômeno caracteriza-se pela própria natureza do mercado em questão, ora a entrada de empresas que exploram tal serviço é

restrita, haja vista a necessidade de grande aporte de capitais, instalação de infra-estruturais e dentre outros fatores que impedem a existência de um número razoável de empresas disponíveis para prestar o referido serviço.

Há ainda de se ressaltar que o desenvolvimento da economia amplamente globalizada implicou na formação de grupos econômicos em escala mundial, sendo o mercado de telecomunicações um dos grandes exemplos. A economia das grandes corporações reduziu ainda mais a oferta de serviços de telecomunicações, ocorrendo em escala global a aglomeração de companhias e formação de um mercado eminentemente oligopolista.

Traçadas as linhas gerais referentes ao mercado de telecomunicações, pode-se afirmar com convicção que as restrições de participação de empresas nas licitações devem ser, mais que em outros casos, muito bem justificadas e necessárias. Isto porque, em homenagem aos princípios da competitividade e isonomia, apenas pode se podem admitir as restrições objetivas e legítimas.

Nesse sentido, não pode prosperar a imposição editalícia de impedimento de participação de empresas em regime de consórcio. Tal determinação fulmina diretamente a competitividade do certame por não existir grande número de empresas qualificadas para prestação do serviço licitado e pela própria complexidade do objeto licitado. Ademais, verifica-se que o próprio artigo 33 da Lei n.º 8666/93 permite expressamente a participação de empresas em consórcio.

Corroborando tal entendimento, verifica-se a primorosa lição de Marçal Justen Filho sobre a permissão de consórcio na licitação. Se num primeiro momento a associação de empresas em consórcio pode gerar a diminuição da competitividade, em outras circunstâncias, como a do presente caso, pode ser um elemento que a garanta, senão vejamos:

> *"Mas o consórcio também pode prestar-se a resultados positivos e compatíveis com a ordem jurídica. Há hipóteses em que as circunstâncias do mercado e (ou) complexidade do objeto tornam problemática a competição. Isso se passa quando grande quantidade de empresas, isoladamente, não dispuserem de condições para participar da licitação. Nesse caso, o instituto do consórcio é via adequada para propiciar ampliação do universo de licitantes. É usual que a Administração Pública apenas autorize a participação de empresas em consórcio quando as dimensões e complexidade do objeto ou as circunstâncias concretas exijam a associação entre os particulares. São as hipóteses em que apenas poucas empresas estariam aptas a preencher as condições especiais exigidas para a licitação."1 (grifo nosso)*

Com espantosa precisão, o entendimento de Marçal Justen Filho subsume-se perfeitamente ao caso em questão. O mercado é naturalmente restrito e o objeto da licitação complexo a ponto de reduzir a participação de empresas, sendo a competitividade reduzida por essas características. Nesse sentido, a imposição de mais uma restrição

apenas põe em risco o princípio da competitividade. A possibilidade de a Administração permitir a participação de consórcios em licitação está prevista no art. 33 da Lei n.º. 8.666/1993, art. 17 do Decreto n.º. 3.555/2000 e art. 16 do Decreto n.º. 5.450/2005. Tais normativos apresentam as regras que devem ser obedecidas pela Administração atinentes à participação de empresas em consórcio nos certames

Nesse sentido, cumpres observar o que determina a Lei nº 8.666/93:

> *"Art. 3º - A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.*
>
> *§ 1 o É vedado aos agentes públicos:*
>
> *I - admitir, prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo e estabeleçam preferências ou distinções em razão da naturalidade, da sede ou domicílio dos licitantes ou de qualquer outra circunstância impertinente ou irrelevante para o específico objeto do contrato;"*

Vale lembrar que dentre os Princípios da Administração, o da Legalidade é o mais importante e do qual decorrem os demais, por ser essência ao Estado de Direito e ao Estado Democrático de Direito. **Note que na atividade administrativa permite-se a atuação do agente público, apenas se concedida ou deferida por norma legal**, ao passo que ao particular é permitido fazer tudo quanto não estiver proibido pela lei. Toda atividade administrativa vincula-se a tal princípio, que se encontra consagrado em nossa Constituição Federal (Art. 5o , II, XXXV e Art. 37).

Ora, mantida a restrição quanto ao formato da participação das empresas em consórcio, a Impugnante estará, juntamente com outras prestadoras de serviços de telecomunicações, prejudicada de participar desta competição! O licitante, nesta licitação, pode (e deve), com segurança, eficiência e vantajosidade, admitir a participação de empresas consorciadas, sem quaisquer limitações, como sempre o fez, **porque a associação de empresas pode representar a apresentação da melhor proposta para a Administração.**

Nesse sentido, cumpre trazer os seguintes entendimentos do TCU acerca da matéria:

> *"No entender da Unidade Técnica, não obstante constituir faculdade da*

Administração permitir ou não a participação de empresas em consórcio nas aludidas convocações, no presente caso, a vedação teria ocorrido sem a adequada motivação, o que teria inviabilizado a participação de mais licitantes, em prejuízo do princípio da ampla competição." (Acórdão 59/2006 - Plenário) "Não prospera também o argumento de que a possibilidade de formação de consórcio no Edital afastaria eventual restrição à competitividade da licitação. A constituição de consórcio visa, em última instância, a junção de 2 (duas) ou mais empresas para realização de determinado empreendimento, objetivando, sob a ótica da Administração Pública, proporcionar a participação de um maior número de empresas na competição, quando constatado que grande parte delas não teria condições de participar isoladamente do certame. (...)" (Acórdão n.º 1.591/2005, Plenário, rel. Ministro Guilherme Palmeira) (grifo nosso)

Nota-se, tanto do entendimento doutrinário quanto jurisprudencial, que a permissão de consórcios nas licitações tem aspecto bifronte, podendo gerar ou restringir a competitividade. Não obstante, conforme se demonstrou acima, a formação de consórcios é medida válida e necessária, que irá beneficiar a Administração com o aumento da participação de empresas na licitação, aumentando a competição entre elas e reduzindo, inevitavelmente, o preço final da contratação.

Da mesma forma, não deve haver restrições quanto ao consórcio de empresas que sejam coligadas, controladoras e controladas. Isso porque, decorrente das particularidades do mercado e da economia globalizada, é comum a existência no âmbito das telecomunicações conglomerados econômicos que necessitam dessa ferramenta jurídica para participarem das licitações. Frise-se que muitas das vezes a prestação do serviço por empresa isolada não é o suficiente, necessitando da atuação em conjunto para a consecução do objeto da licitação.

Ante o exposto, de forma a possibilitar a participação de um maior número de empresas no certame, garantindo a sua competitividade e a busca pela proposta mais vantajosa à Administração Pública requer seja excluído o item 5.6.5 do Edital **para que seja permitida a participação em consórcio de empresas,** nos termos do art. 33 da Lei n.º 8.666/93.

3. IMPEDIMENTO À PARTICIPAÇÃO DE EMPRESAS SUSPENSAS DE LICITAR COM A ADMINISTRAÇÃO PÚBLICA EM GERAL

O item 5.6.6 do Edital veda a participação de empresas que estejam cumprindo penalidade de suspensão do direito de licitar com a Administração Pública Direta ou Indireta Federal, Estadual, Municipal ou do Distrito Federal.

Com efeito, o art. 87, inciso III, da Lei n.º 8.666/1993 prevê, dentre as modalidades de penalidades em caso de inexecução total ou parcial do

contrato, a **suspensão temporária de participação em licitação e impedimento de contratar com a Administração.**

Diante do acima exposto, faz-se necessário esclarecer que os conceitos de Administração e Administração Pública são distintos, nos termos dos incisos XI e XII do art. 6º da Lei de Licitações, in verbis:

> *"Art. 6 o - Para os fins desta Lei, considera-se:*
>
> *XI - Administração Pública - a administração direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, abrangendo inclusive as entidades com personalidade jurídica de direito privado sob controle do poder público e das fundações por ele instituídas ou mantidas;*
>
> *XII - Administração - órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente;"*

Da análise dos dispositivos legais, verifica-se que as expressões "Administração Pública" e "Administração" são distintas.

Nesse sentido, importante citar a lição de Marçal Justen Filho a respeito do tema:

"Administração Pública: A expressão é utilizada em acepção ampla e não deve ser identificada com 'Poder Executivo'. Indica as pessoas de direito público que participam de uma contratação, ainda quando esta contratação se efetive através de órgãos do Poder Judiciário e do Poder Legislativo. Além da chamada 'Administração Direta' (União, Estados e Distrito Federal, Municípios), a expressão também abrange a 'Administração Indireta' (autarquias, empresas públicas e sociedades de economia mista). Além disso, as 'fundações' instituídas ou mantidas com recursos públicos ou outras pessoas de direito privado sob controle estatal estão abarcadas no conceito."

"Administração: A expressão isolada é utilizada para identificar a unidade específica que, no caso concreto, está atuando. A distinção entre Administração Pública e Administração é utilizada em algumas passagens na disciplina da Lei n.º 8.666. A hipótese de maior relevância encontra-se no art. 87, incs. III e IV, a propósito das sanções de suspensão temporária do direito de licitar ou de contratar e de declaração de inidoneidade."2

Da mesma forma entende Jessé Torres Pereira:

> *"A distinção, para os fins de aplicação desta lei, entre Administração e Administração Pública encontra importantes aplicações. Ilustre-se com a intrincada questão de estabelecer-se a extensão das penalidades de suspensão e de declaração de inidoneidade, ambas acarretando a supressão temporária do direito de*

participar de licitações e de contratar. Tratando-se de suspensão, a supressão se dá em face da Administração; na hipótese de inidoneidade, o cumprimento da punição é em face da Administração Público."3

Este entendimento foi ratificado em recentes decisões do Plenário do Tribunal de Contas da União, segundo o qual os efeitos jurídicos da referida sanção está adstrita ao órgão que a aplicou. Nesse sentido, destaca-se:

"- ACÓRDÃO Nº 266/2019 - TCU - Plenário

"9.3. dar ciência à Defensoria Pública da União, com fundamento no art. 7º da Resolução-TCU 265/2014, para que sejam adotadas medidas internas com vistas à prevenção de ocorrências semelhantes acerca da inabilitação, no Pregão Eletrônico 83/2018, da licitante Portal Turismo e Serviços EIRELI, em desconformidade com a legislação em vigor e o entendimento deste Tribunal (Acórdãos 3.243/2012, 3.439/2012, 2.242/2013, 3.645/2013, 504/2015 e 1.764/2017), no sentido de que a suspensão do direito de licitar prevista no inciso III do art. 87 da Lei 8.666/1993 produz efeitos apenas em relação ao órgão ou entidade contratante que aplicou a penalidade;"

"DATA: 13/02/2019

ASSUNTO: SANÇÕES ADMINISTRATIVAS

ACÓRDÃO 269/2019 - PLENÁRIO

Dar ciência à Financiadora de Estudos e Projetos – Finep, com fundamento no art. 7º da Resolução – TCU 265/2014, acerca das seguintes falhas (…), para que sejam adotadas medidas internas com vistas à prevenção de ocorrência de outras semelhantes:

1. a interpretação dada ao art. 7º da Lei 10.520/2002 afronta a jurisprudência do TCU, a qual é no sentido de que as sanções previstas nesse dispositivo se limitam ao ente federado sancionador (Acórdãos 2.242/2013, 2.081/2014 e 2.530/2015, todos do Plenário deste Tribunal, entre outros);

2. a interpretação dada ao art. 38, inciso II, da Lei 13.303/2016 está equivocada, uma vez que o impedimento de participar de licitações em razão desse dispositivo se refere tão somente a sanções aplicadas pela própria entidade, e não a sanções aplicadas por outra empresa pública ou sociedade de economia mista."

Vale mencionar que este já era o entendimento "histórico" do Tribunal de Contas da União, conforme se nota dos acórdãos nº 1.727/2006-1ª Câmara, nº 2.617/2010-2ª Câmara, nº 1.539/2010-Plenário e da Decisão nº 352/98-Plenário.

Assim, ao apresentar comparativo entre a sanção de suspensão do direito de licitar/impedimento de contratar e a declaração de inidoneidade, defende que a Administração é entendida, pela definição constante do inciso XI do art. 6º do diploma legal em comento, como sendo o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente – vale dizer, o órgão público. Já a Administração Pública é definida como sendo o universo de órgãos e entidades da União, dos Estados, do Distrito Federal e dos Municípios, nos termos do inciso XII do art. 6º da Lei n.º 8.666.

Portanto, requer seja alterado o item 5.6.6 do Edital, para que seja vedada a participação apenas das empresas suspensas de licitar e impedidas de contratar com este órgão público licitante, e não com a Administração Pública em geral.

4. DA EXIGÊNCIA DE EMISSÃO DE NOTA FISCAL COM CNPJ DA EMPRESA CONTRATADA

O Edital deste certame licitatório, no item 7.6 do Edital exige que: "O CNPJ da proponente, empresa cadastrada no SICAF e habilitada na licitação, deverá ser o mesmo para efeito de emissão das notas fiscais e posterior pagamento."

A mencionada exigência, no entanto, não encontra previsão legal e, além disso, se mostra ofensora a prescrições licitatórias e tributárias. Vejamos.

Inicialmente, vale destacar que o princípio da legalidade é elemento basilar do regime jurídicoadministrativo, considerado a "diretriz básica da conduta dos agentes da Administração" (CARVALHO FILHO, 2011, p. 18). Nesse sentido, é considerado aspecto indissociável de toda a atividade administrativa, vinculando as ações do administrador à lei, sendo decorrência direta do Estado Democrático de Direito.

Dessa forma, não pode o administrador furtar-se ao cumprimento da lei. Mais que isso, sua liberdade de ação deverá ser balizada inexoravelmente por texto legal. CELSO ANTÔNIO BANDEIRA DE MELLO (2011, p. 108) define com clareza que "o princípio da legalidade, no Brasil, significa que a Administração nada pode fazer senão o que a lei determina". Com isso, verifica-se que a liberdade administrativa diferencia-se da civil por ser positiva, ou seja, a lei define claramente os limites da atuação do administrador, enquanto a segunda é negativa, sendo legal todas as ações que não contrariem a lei.

Do ponto de vista licitatório, o artigo 29 da Lei n. 8.666/93 possibilita, ao participante da licitação, que comprove sua regularidade fiscal com documentação do domicílio ou da sede. Portanto, cabe à proponente a alternativa na apresentação de um ou outro, ou seja, tem a licitante a prerrogativa, autorizada em lei, de apresentar documentação da sua filial ou da matriz.

Sobre o tema, o Tribunal de Contas da União já se manifestou afirmando "[...] que, se a matriz participa da licitação, todos os documentos de regularidade fiscal devem ser apresentados em seu nome e de acordo com o seu CNPJ. Ao contrário, se a filial é que participa da licitação, todos os documentos de regularidade fiscal devem ser apresentados em seu nome e de acordo com o seu próprio CNPJ." (Acórdão n. 3.056/2008 - Plenário).

Vale salientar que matriz e filial não são pessoas jurídicas distintas. A matriz e a filial representam estabelecimentos diferentes pertencentes à mesma pessoa jurídica (TCU, Acórdão n. 3.056/2008 - Plenário). Por isso, não há óbice em o estabelecimento matriz ter sido habilitado e a filial entregar os produtos/serviços contratados.

Entretanto, no que concerne à questão tributária, a diferenciação matriz/filial assume relevância. Isto porque, sendo os serviços de telecomunicação tributados por ICMS (art. 155, II, da CF/88), imposto estadual, cada filial é contribuinte no Estado em que domiciliada.

Melhor explicando: não obstante o CNPJ da matriz conste da Fatura

apresentada, mensalmente, à Administração Pública, as notas fiscais, em atendimento à legislação que regula o recolhimento dos tributos incidentes sobre os serviços prestados (telecomunicação), são emitidas em cada local da prestação do serviço.

Assim, uma vez que o ICMS é incidente sobre a prestação de serviços de telecomunicações e sendo esse um tributo de competência estadual, em cada Estado onde o serviço de telecomunicações é prestado pela Oi, se dá a emissão da nota fiscal correspondente, razão pela qual as notas fiscais são emitidas pelas filiais.

Diante do exposto, ao emitir a nota fiscal com o CNPJ da filial, não obstante o contrato seja firmado pela Oi - Matriz, a Oi nada mais faz do que cumprir os pressupostos legais que regem a matéria tributária, sem prejuízo da Lei n. 8.666/93 que, como se vê aqui, igualmente encontra-se observada em sua íntegra

Assim, frise-se, não obstante a participação da proponente no certame licitatório se dê com apresentação de seus documentos da matriz OU da Filial, na forma do artigo 29 da Lei n. 8.666/93, as notas fiscais devem ser emitidas no CNPJ da filial do local onde é prestado o serviço, pois é este estabelecimento, nos termos do artigo 127, II, do Código Tributário Nacional, o contribuinte de ICMS para o Estado.

Diante do exposto, requer a alteração do item em comento para que, de forma a cumprir os pressupostos legais que regem a matéria tributária, sem prejuízo da Lei 8.666/93, seja emitida nota fiscal com o CNPJ da filial, não obstante o contrato possa ser firmado pela matriz na forma do art. 29 da Lei n. 8666/93.

5. PAGAMENTO VIA NOTA FISCAL COM CÓDIGO DE BARRAS

O item 19.2 do Edital estabelece que o pagamento deverá ser realizado por de crédito em conta corrente, mediante ordem bancária.

Ocorre que tal sistema de pagamento encontra-se em dissonância com o procedimento de pagamento adotado relativamente aos serviços de telecomunicações, uma vez que esses são pagos mediante apresentação de fatura (nota fiscal com código de barras), ou mediante SIAFI nos casos de órgãos vinculados à Administração Pública Federal, como é o caso da ANATEL.

Como é cediço, o SIAFI é um sistema informatizado que controla a execução orçamentária, financeira, patrimonial e contábil dos órgãos da Administração Pública direta federal, das autarquias, fundações e empresas públicas federais e das sociedades de economia mista que estiverem contempladas no orçamento fiscal e (ou) no orçamento da seguridade social da União.

Assim, as unidades gestoras registram seus documentos (empenho, ordem bancária etc.) e o SIAFI efetua automaticamente todos os lançamentos contábeis necessários para se ter conhecimento atualizado das receitas, despesas e disponibilidades financeiras do Tesouro Nacional. Com efeito, esse sistema de faturamento e cobrança, o qual permite o reconhecimento rápido e eficiente do pagamento, é baseado em código de barras.

Qualquer outra forma de pagamento, como o depósito em conta corrente previsto no Edital, causará transtornos ao sistema de contas a receber da empresa de telecomunicações contratada.

Ademais, a Oi utiliza o sistema de faturamento, por meio de Nota Fiscal/Fatura, emitida com código de barras para pagamento, em apenas uma via, modelo 22, em razão das várias vantagens que essa forma de pagamento proporciona.

Tal sistema proporciona vantagens à empresa prestadora dos serviços, haja vista que reduz a inadimplência e garante a satisfação do cliente.

Ante o exposto, para a melhor adequação do instrumento convocatório à realidade do setor de telecomunicações, requer a alteração do item 19.2 do Edital, a fim de permitir que o pagamento seja realizado mediante autenticação de código de barras, facilitando, assim, o reconhecimento eficiente do pagamento.

6. INDEVIDA APRESENTAÇÃO DE CERTIDÕES DE REGULARIDADE MENSALMENTE

O item 19.2.1 do Edital, os itens 9.1.1 e 9.2.1 do Termo de Referência e a Cláusula Décima Terceira, itens 1.1 e 2.1 da Minuta do Contrato estabelecem que a Contratante deverá apresentar os comprovantes de regularidade fiscal/social/trabalhista mensalmente, ou seja, no momento do pagamento junto com a nota fiscal/fatura.

Inicialmente é importante observar que tal obrigação não encontra guarida na Lei n.º 8.666/93, portanto, sem lastro legal.

Não obstante tal fato, é importante observar que a exigência de apresentação das certidões de regularidade juntamente com as notas fiscais não é razoável. Explica-se: as certidões de regularidade fiscal/social/trabalhista possuem um período de vigência que ultrapassa o período mensal (30 dias).

Assim, a apresentação mensal das referidas certidões foge dos padrões lógicos, visto que o prazo de validade das mesmas ultrapassa o período de trinta dias.

É de suma importância observar que não está se discutindo aqui a necessidade da manutenção dos requisitos de habilitação durante toda a execução do contrato. Tal fato é inquestionável! O que se discute nesta análise é a desproporcionalidade e ilegalidade em exigir a apresentação mensal desses requisitos, principalmente, pelos mesmos possuírem período de vigência superior à 30 (trinta) dias.

Vale corroborar, que a Administração Pública possui fé pública para certificar as informações apresentadas nas certidões. Se a certidão informa que seu prazo de validade é de 120 dias, porque a contratada deverá apresentar a certidão mensalmente?

Verifica-se a incongruência na aplicação da exegese do item 19.2.1 do Edital, dos itens 9.1.1 e 9.2.1 do Termo de Referência e da Cláusula Décima Terceira, itens 1.1 e 2.1 da Minuta do Contrato. Como se sabe, a atividade administrativa exige prestígio aos princípios da razoabilidade e proporcionalidade.

Carlos Ari Sundfeld, na obra "Fundamentos de Direito Público" afirma o seguinte acerca da proporcionalidade (fls. 165):

> *"A proporcionalidade é expressão quantitativa da razoabilidade. É inválido o ato desproporcional em*

relação à situação que o gerou ou à finalidade que pretende atingir."

Ora, o administrador está jungido ao Princípio da Legalidade, portanto, ao determinar obrigações que não possuem previsão legal, atua de forma desproporcional e irrazoável.

Para José dos Santos Carvalho Filho, "razoabilidade é a qualidade do que é razoável, ou seja, aquilo que se situa dentro dos limites aceitáveis, ainda que os juízos de valor que provocaram a conduta possam dispor-se de forma um pouco diversa"4 .

O princípio da regra da razão expressa-se em procurar a solução que está mais em harmonia com as regras de direito existentes e que, por isso, parece a mais satisfatória, em atenção à preocupação primária da segurança, temperada pela justiça, que é a base do Direito.

A Administração Pública está obrigada a adotar a alternativa que melhor prestigie a racionalidade do procedimento e de seus fins. Nesse sentido, Marçal Justen Filho ensina que:

> *"O princípio da proporcionalidade restringe o exercício das competências públicas, proibindo o excesso. A medida limite é a salvaguarda dos interesses públicos e privados em jogo. Incumbe ao Estado adotar a medida menos danosa possível, através da compatibilização entre os interesses sacrificados e aqueles que se pretende proteger."5*

Diante disso, requer a alteração do item 19.2.1 do Edital, dos itens 9.1.1 e 9.2.1 do Termo de Referência e da Cláusula Décima Terceira, itens 1.1 e 2.1 da Minuta do Contrato para que não exija a apresentação mensal das certidões de regularidade fiscal/trabalhista/sociais, sob pena de ferir os Princípios da Razoabilidade, da Proporcionalidade, da Legalidade e ainda, o da fé pública inerente aos documentos públicos (certidões).

7. RETENÇÃO DO PAGAMENTO PELA CONTRATANTE

O item 19.2.3 do Edital e a Cláusula Décima Terceira, parágrafo terceiro da Minuta do Contrato dispõem sobre hipóteses de retenção do pagamento que não encontram previsão legal.

Entretanto, o art. 87 da Lei de Licitações define rol taxativo de sanções aplicáveis à Contratada, prevendo a hipótese de advertência, multa, suspensão temporária de participação em licitação, impedimento de contratar com a Administração e declaração de inidoneidade para licitar ou contratar com a Administração Pública. Não obstante, não consta em nenhum momento a previsão de retenção dos pagamentos.

Nesse sentido, deve-se impedir que o Edital imponha à Contratada medidas que não estejam relacionadas ao art. 87 da Lei 8.666/1993, em obediência ao princípio da legalidade. Dessa forma, pode-se afirmar que a exigência editalícia em comento não tem razão de ser, sendo impossível promover a retenção dos pagamentos como sanção ao não cumprimento da regularidade fiscal.

Esse é entendimento recentemente esposado pelo Tribunal de Contas da União – TCU, no sentido de que a perda da regularidade fiscal no curso de contratos de execução continuada ou parcelada justifica a imposição de sanções à Contratada, mas não autoriza a retenção de pagamentos por serviços prestados:

> *"Consulta formulada pelo Ministério da Saúde suscitou possível divergência entre o Parecer da Procuradoria Geral da Fazenda Nacional (PGFN) 401/2000 e a Decisão nº 705/1994 – Plenário do TCU, relativamente à legalidade de pagamento a fornecedores em débito com o sistema da seguridade social que constem do Sistema de Cadastramento Unificado de Fornecedores (Sicaf). A consulente registra a expedição, pelo Ministério do Planejamento, Orçamento e Gestão de orientação baseada no Parecer 401/2000 da PGFN, no sentido de que "os bens e serviços efetivamente entregues ou realizados devem ser pagos, ainda que constem irregularidades no Sicaf". Tal orientação, em seu entendimento, colidiria com a referida decisão, por meio do qual o Tribunal firmou o entendimento de que os órgãos e as entidades da Administração Pública Federal devem exigir, nos contratos de execução continuada ou parcelada, a comprovação, por parte da contratada, da regularidade fiscal, incluindo a da seguridade social. O relator, ao endossar o raciocínio e conclusões do diretor de unidade técnica, ressaltou a necessidade de os órgãos e entidade da Administração Pública Federal incluírem, "nos editais e contratos de execução continuada ou parcelada, cláusula que estabeleça a obrigação do contratado de manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação", além das sanções resultantes de seu descumprimento. Acrescentou que a falta de comprovação da regularidade fiscal e o descumprimento de cláusulas contratuais "podem motivar a rescisão contratual, a execução da garantia para ressarcimento dos valores e indenizações devidos à Administração e a aplicação das penalidades previstas no art. 87 da Lei nº 8.666/93, mas não a retenção do pagamento". Caso contrário estaria a Administração incorrendo em enriquecimento sem causa. Observou, também, que a retenção de pagamento ofende o princípio da legalidade por não constar do rol do*

art. 87 da Lei nº 8.666/93. O Tribunal, então, decidiu responder à consulente que os órgãos e entidades da Administração Pública Federal devem: a) "... exigir, nos contratos de execução continuada ou parcelada, a comprovação, por parte da contratada, da regularidade fiscal, incluindo a seguridade social, sob pena de violação do disposto no § 3º do art. 195 da Constituição Federal"; b) "... incluir, nos editais e contratos de execução continuada ou parcelada, cláusula que estabeleça a obrigação do contratado de manter, durante a integral execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação, prevendo, como sanções para o inadimplemento a essa cláusula, a rescisão do contrato e a execução da garantia para ressarcimento dos valores e indenizações devidos à Administração, além das penalidades já previstas em lei (arts. 55, inciso XIII, 78, inciso I, 80, inciso III, e 87, da Lei nº 8.666/93)". (Acórdão n.º 964/2012-Plenário, TC 017.371/2011-2, rel. Min. Walton Alencar Rodrigues, 25.4.2012) (grifo nosso)

Na mesma esteira encontra-se a jurisprudência do STJ:

"ADMINISTRATIVO. CONTRATO. ECT. PRESTAÇÃO DE SERVIÇOS DE TRANSPORTE. DESCUMPRIMENTO DA OBRIGAÇÃO DE MANTER A REGULARIDADE FISCAL. RETENÇÃO DO PAGAMENTO DAS FATURAS. IMPOSSIBILIDADE

1. A exigência de regularidade fiscal para a participação no procedimento licitatório funda-se na Constituição Federal, que dispõe no § 3º do art. 195 que "a pessoa jurídica em débito com o sistema da seguridade social, como estabelecido em lei, não poderá contratar com o Poder Público nem dele receber benefícios ou incentivos fiscais ou creditícios", e deve ser mantida durante toda a execução do contrato, consoante o art. 55 da Lei 8.666/93.

2. O ato administrativo, no Estado Democrático de Direito, está subordinado ao princípio da legalidade (CF/88, arts. 5º, II, 37, caput, 84, IV), o que equivale assentar que a Administração poderá atuar tão somente de acordo com o

que a lei determina.

3. Deveras, não constando do rol do art. 87 da Lei 8.666/93 a retenção do pagamento pelos serviços prestados, não poderia a ECT aplicar a referida sanção à empresa contratada, sob pena de violação ao princípio constitucional da legalidade. Destarte, o descumprimento de cláusula contratual pode até ensejar, eventualmente, a rescisão do contrato (art. 78 da Lei de Licitações), mas não autoriza a recorrente a suspender o pagamento das faturas e, ao mesmo tempo, exigir da empresa contratada a prestação dos serviços.

4. Consoante a melhor doutrina, a supremacia constitucional 'não significa que a Administração esteja autorizada a reter pagamentos ou opor-se ao cumprimento de seus deveres contratuais sob alegação de que o particular encontra-se em dívida com a Fazenda Nacional ou outras instituições. A administração poderá comunicar ao órgão competente a existência de crédito em favor do particular para serem adotadas as providências adequadas. A retenção de pagamentos, pura e simplesmente, caracterizará ato abusivo, passível de ataque inclusive através de mandado de segurança.' (Marçal Justen Filho. Comentários à Lei de Licitações e Contratos Administrativos, São Paulo, Editora Dialética, 2002, p. 549).

5. Recurso especial a que se nega provimento."

(REsp 633.432/MG, Rel. Ministro LUIZ FUX, PRIMEIRA TURMA, julgado em 22/02/2005, DJ 20/06/2005, p. 141)

Assim, existindo na data de pagamento pendências fiscais, poderá a Administração, atendendo ao princípio da legalidade, aplicar uma das sanções definidas no art. 87 da Lei de Licitações, não sendo admissível a imposição de sanção que fuja ao rol taxativo do dispositivo legal citado. Frisese que o princípio da legalidade, sendo o elemento basilar do regime jurídico-administrativo, é considerado como aspecto indissociável de toda a atividade administrativa, vinculando as ações do administrador à lei, sendo decorrência direta do Estado Democrático de Direito. Dessa forma, impor sanção que extrapola a lei importa em desrespeito inexorável ao princípio da legalidade.

Diante disso, tendo em vista que a suspensão do pagamento pelos serviços prestados não consta no rol do art. 87 da Lei n.º 8.666/93, o qual elenca as sanções pela inexecução total ou parcial do contrato, requer a modificação do item 19.2.3 do Edital e da Cláusula Décima Terceira, parágrafo terceiro da Minuta do Contrato.

8. DAS PENALIDADES EXCESSIVAS

Os itens 20.1 do Edital, os itens 12.1.5, 12.1.6 e 12.1.7 do Termo de Referência e a Cláusula Décima Oitava, parágrafo terceiro, itens IV, V e VI da Minuta do Contrato determinam a aplicação de multas que extrapolam o limite de 10% (dez por cento) sobre o valor do contrato estabelecido pelo Decreto n.º 22.626/33, em vigor conforme Decreto de 29 de novembro de 1991. A fixação de multa nesse patamar também ofende a Medida Provisória n.º 2.172/01 (e suas reedições), aplicável a todas as modalidades de contratação, inclusive aquelas firmadas entre particulares e Administração Pública.

O art. 87, inciso III, da Lei de Licitações determina que na hipótese de inexecução total ou parcial do contrato a Administração poderá aplicar a sanção de "multa, na forma prevista no instrumento convocatório ou no contrato". Ocorre que não há no dispositivo em questão qualquer limite à aplicação da multa, o que gera, automaticamente, sua interpretação indissociável com o princípio da proporcionalidade, conforme se observa do entendimento de Marçal Justen Filho sobre o tema:

> *"Então, o instrumento jurídico fundamental para elaboração de uma teoria quanto às sanções atinentes à contratação administrativa reside na proporcionalidade. Isso significa que, tendo a Lei previsto um elenco de quatro sanções, dotadas de diverso grau de severidade, impõe-se adequar as sanções mais graves às condutas mais reprováveis. A reprovabilidade da conduta traduzir-se-á na aplicação de sanção proporcionada correspondente" 6 (grifo nosso)*

Nesse sentido, deve-se guardar a proporcionalidade entre o fato gerador da sanção e o quantum a ser exigido, como bem alinhava o art. 2º, parágrafo único, inciso VI, da Lei n.º 9.784/1999, por exigir "adequação entre meios e fins, vedada a imposição de obrigações, restrições e sanções em medida superior àquelas estritamente necessárias para o atendimento do interesse público".

Não é o que se observa no caso em questão. A multa definida no percentual acima exposto gera para a Contratada gravame completamente desproporcional, ferindo os princípios da proporcionalidade e da própria legalidade.

A doutrina alemã do princípio da proporcionalidade, amplamente aceita e praticada no sistema jurídico brasileiro, traz como método de sua aplicação a análise de seus três sub-princípios: adequação (Geeignetheit), necessidade (Notwendigkeit) e proporcionalidade em sentido estrito (Verhältnismäßig im engeren Sinn). O pressuposto da adequação determina que a medida aplicada deve guardar relação entre meio e fim, de modo que seja a mais adequada para a resolução da questão. A necessidade diz respeito à escolha da medida menos gravosa para atingir sua efetividade. E, por fim, a proporcionalidade em sentido estrito é a ponderação entre o meio-termo e a justa-medida da ação que se deseja perpetrar, verificando-se se a medida alcançará mais vantagens que desvantagens.

Tal princípio é reconhecido e definido por José dos Santos Carvalho Filho da seguinte forma:

"Segundo a doutrina alemã, para que a conduta estatal observe o princípio da proporcionalidade, há de revestir-se de tríplice fundamento: 1) adequação, significando que o meio empregado na atuação deve ser compatível com o fim colimado; 2) exigibilidade, porque a conduta deve ser necessária, não havendo outro meio menos gravoso ou oneroso para alcançar o fim público, ou seja, o meio escolhido é o que causa o menor prejuízo possível para os indivíduos; 3) proporcionalidade em sentido estrito, quando as vantagens a serem conquistadas superarem as desvantagens."7 (grifo nosso)

No presente caso, verifica-se que a sanção de multa fixada no referido percentual até se encaixam no primeiro pressuposto, sendo adequadas ao cumprimento de seu fim. No entanto, o mesmo não se pode dizer quanto à necessidade. A quantidade fixada à título de multa é medida completamente desnecessária para punir o descumprimento da regra do Edital, uma vez que poderia causar menor prejuízo para o particular e mesmo assim atingir o fim desejado. Entendese que a aplicação de multa com fito pedagógico pode ser entendida como razoável, mas a sua definição em patamares elevados torna a sanção desnecessária. Isso porque existem meios menos gravosos, mas mesmo assim a Administração optou pela escolha do pior método.

Por fim, verifica-se que a sanção aplicada à Contratada não preenche também o pré-requisito da proporcionalidade em sentido estrito. É flagrante que o presente percentual de multa pune a Contratada sobremaneira, excedendo-se desarrazoadamente quando se observa o fato que a ensejou. É perfeita a aplicação da metáfora de Jellinek que "não se abatem pardais disparando canhões"

Observa-se, portanto, que a Administração, ao fixar a penalidade em comento, descumpriu completamente o princípio da proporcionalidade, sendo necessária a revisão de tal medida. Cumpre ainda ressaltar que não quer a Contratada se eximir do cumprimento das sanções estabelecidas se de fato viesse a descumprir o contrato e dar ensejo a rescisão deste. Pede-se apenas que estas sejam aplicadas de forma proporcional ao fato que as ensejou.

Noutro giro, verifica-se que o próprio STJ reconheceu que diante do caráter vago do art. 87 da Lei de Licitações, a Administração deve-se balizar pelo princípio da proporcionalidade:

> *"Mandado de Segurança. Declaração de Inidoneidade. Descumprimento do Contrato Administrativo. Culpa da Empresa Contratada. Impossibilidade de Aplicação de Penalidade mais Grave a Comportamento que não é o mais Grave. Ressalvada a aplicação de Outra Sanção pelo Poder Público.*
>
> *Não é lícito ao Poder Público, diante da imprecisão da lei, aplicar os incisos do artigo 87 sem qualquer critério. Como se pode observar pela leitura do dispositivo, há uma gradação entre as sanções. Embora não esteja o administrador submetido ao princípio da pena específica, vigora no Direito Administrativo o princípio da proporcionalidade.*
>
> *Não se questiona, pois, a responsabilidade civil da empresa pelos danos, mas apenas a*

> *necessidade de imposição da mais grave sanção a conduta que, embora tenha causado grande prejuízo, não é o mais grave comportamento." (MS n.º 7.311/DF)*

Vê-se que tal entendimento corrobora o que fora acima alinhavado, demonstrando que a fixação da sanção, bem como o quantum referente à multa deve ocorrer tendo como base o princípio da proporcionalidade.

Por todo o exposto, requer a adequação do item 20.1 do Edital, dos itens 12.1.5, 12.1.6 e 12.1.7 do Termo de Referência e da Cláusula Décima Oitava, parágrafo terceiro, itens IV, V e VI da Minuta do Contrato, para que as multas aplicadas observem o limite de 10% (dez por cento) sobre o valor do contrato

9. VALOR DA GARANTIA

A Cláusula Décima Quinta da Minuta do Contrato estipula que a garantia a ser apresentada deverá corresponder ao percentual de 5% (cinco por cento) sob o valor do contrato.

Todavia, o artigo 56, § 2º, da Lei 8.666/1993 estipula que a garantia exigida não excederá a 5% (cinco por cento) do valor total do contrato.

Como se sabe, a atividade administrativa exige prestígio aos princípios da razoabilidade e proporcionalidade.

Para José dos Santos Carvalho Filho, "razoabilidade é a qualidade do que é razoável, ou seja, aquilo que se situa dentro dos limites aceitáveis, ainda que os juízos de valor que provocaram a conduta possam dispor-se de forma um pouco diversa8 ".

O princípio da regra da razão se expressa em procurar a solução que está mais em harmonia com as regras de direito existentes e que, por isso, parece a mais satisfatória, em atenção à preocupação primária da segurança, temperada pela justiça, que é a base do Direito.

A Administração Pública está obrigada a adotar a alternativa que melhor prestigie a racionalidade do procedimento e de seus fins.

Nesse sentido, Marçal Justen Filho ensina que:

> *"O princípio da proporcionalidade restringe o exercício das competências públicas, proibindo o excesso. A medida limite é a salvaguarda dos interesses públicos e privados em jogo. Incumbe ao Estado adotar a medida menos danosa possível, através da compatibilização entre os interesses sacrificados e aqueles que se pretende proteger9 ."*

O princípio da razoabilidade deve ser observado pela Administração Pública à medida que sua conduta se apresente dentro dos padrões normais de aceitabilidade. Se atuar fora desses padrões, algum vício estará, sem dúvida, contaminando o comportamento estatal. Não pode, portanto, existir violação ao referido princípio quando a conduta

administrativa é inteiramente revestida de licitude.

Com efeito, o princípio da razoabilidade se fundamenta nos princípios da legalidade e da finalidade, como ensina Celso Antônio Bandeira de Mello:

> *"A Administração Pública, ao atuar no exercício de discrição, terá que estabelecer critérios aceitáveis do ponto de vista racional, em sintonia com o senso normal de pessoas equilibradas e respeitosa das finalidades que presidiram a outorga da competência exercida.*
>
> *(...)*
>
> *Com efeito, o fato de a lei conferir ao administrador certa liberdade (margem de discrição) significa que lhe deu o encargo de adotar, ante a diversidade de situações a serem enfrentadas, a providência mais adequada a cada qual delas. Não significa como é evidente, que lhe haja outorgado o poder de agir ao sabor exclusivo de seu líbito, de seus humores, paixões pessoais, excentricidades ou critérios personalíssimos, e muito menos significa que liberou a Administração para manipular a regra de Direito de maneira a sacar dela efeitos não pretendidos nem assumidos pela lei aplicanda. Em outras palavras: ninguém poderia aceitar como critério exegético de uma lei que esta sufrague as providências insensatas que o administrador queira tomar; é dizer, que avalize previamente condutas desarrazoadas, pois isto corresponderia a irrogar dislates à própria regra de Direito10."*

Logo, quando se pretender imputar à conduta administrativa a condição de ofensiva ao princípio da razoabilidade, terá que estar presente a ideia de que a ação é efetiva e indiscutivelmente ilegal. Inexiste, por conseguinte, conduta legal vulneradora do citado princípio.

Assim, o princípio da razoabilidade acarreta a impossibilidade de impor consequências de severidade incompatível com a irrelevância de defeitos. Sob esse ângulo, as exigências da Lei ou do Edital devem ser interpretadas como instrumentais.

Desta feita, a apresentação de garantia equivalente ao percentual máximo permitido em Lei não é razoável, razão pela qual se requer a modificação da Cláusula Décima Quinta da Minuta do Contrato, para que a garantia exigida não corresponda ao limite máximo de 5% (cinco por cento).

10. DOS ITENS TÉCNICOS

10.1. POSSIBILIDADE DE SUBCONTRATAÇÃO DOS SERVIÇOS

O item 10.20.2 “A subcontratação total/parcial é permitida apenas para o Item 04 mantendo os critérios estabelecidos na seção 5.5 deste Termo; ”

Nesse sentido, cumpre trazer à colação a redação do artigo 72 da Lei n.º 8.666/93:

> *“Art. 72. O contratado, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar partes da obra, serviço ou fornecimento, até o limite admitido, em cada caso, pela Administração.” (grifo nosso)*

Ora, além da Lei prever que a Administração permita ao ente privado, que queira contratar consigo, subcontratar apenas partes dos serviços, tem-se que essas fases ou etapas devem se remeter à atividade meio do serviço licitado, sendo vedada a subcontratação do serviço todo ou a atividade fim que a Administração está a licitar, tendo em vista a análise dos critérios de habilitação para que a Administração contrate um ente privado realmente idôneo.

Nesse sentido é a lição de MARÇAL JUSTEN FILHO acerca da subcontratação:

> *“A hipótese torna-se cabível, por exemplo, quando o objeto licitado comporta uma execução complexa, em que algumas fases, etapas ou aspectos apresentam grande simplicidade e possam ser desempenhados por terceiros sem que isso acarrete prejuízo. A evolução dos princípios organizacionais produziu o fenômeno denominado de ‘terceirização’, que deriva dos princípios da especialização e da concentração das atividades. Em vez de desempenhar integralmente todos os ângulos de uma atividade, as empresas tornam-se especialistas em certos setores.”. [Comentários à Lei de Licitações e Contratos Administrativos, Dialética, 12ª edição, p.757] (grifamos)*

Assim, está ratificada a impossibilidade da subcontratação, pela Contratada, de serviço ou atividade fim.

Neste diapasão, cumpre colacionar jurisprudência do TCU com o mesmo entendimento:

> *“É ilegal e inconstitucional a sub-rogação da figura da contratada ou a divisão das responsabilidades por elas assumidas, ainda que de forma solidária, por contrariar os princípios constitucionais da moralidade e da eficiência.” (Acórdão nº 3.475/2006, 1ª C., rel.*

Min. Marcos Bemquerer)

> *"(...) firmar o entendimento de que, em contratos administrativos, é ilegal e inconstitucional a sub-rogação da figura da contratada ou a divisão das responsabilidades por elas assumidas, ainda que de forma solidária, por contrariar os princípios constitucionais da moralidade e da eficiência (art. 37, caput, da Constituição Federal), o princípio da supremacia do interesse público, o dever geral de licitar (art. 37, XXI, da Constituição) e os arts. 2º, 72 e 78, inciso VI, da Lei 8.666/96." (Acórdão nº 909/2003, Plenário, rel. Min. Augusto Sherman Cavalcanti)*

Todavia, deve-se solicitar a alteração dos em comento, para que seja permitida a subcontratação parcial dos serviços, cujo a característica seja de aplicação temporária, nos termos do art. 72 da Lei n.º 8.666/93, a fim de que seja garantida a ampliação da competitividade;

10.2. DOS PRAZOS DE ENTREGA

Os subitens "e", "f" e "g" do item 9.2 referente aos apontamentos da proposta vencedora temos:

e) Prazo entrega do plano de implementação: Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

f) Prazo início processo de migração/reunião alinhamento: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;

g) Prazo processo de migração: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

Os prazos apresentados nos subitens supracitados são extremamente curtos e não favorecem a ampla concorrência.

Para o subitem "E" O desenho da solução e todas as nuances características do objeto proposto, são deliberados na reunião de alinhamento com a equipe da contratante. Desta forma, 5 dias úteis não são suficientes para este fim.

Com base no exposto, solicitamos a ampliação do prazo para 10 dias úteis;

Com relação ao item "F" que define o início do processo de migração da solução, o prazo de 5 dias úteis é totalmente inexequível. Para que seja possível qualquer ação de migração, se faz necessário que os equipamentos pertencentes a solução tenha sidos entregue.

Com base no exposto, solicitamos a ampliação do prazo para 60 dias, considerando o atual momento que vivemos e as dificuldades de

deslocamento nos dias atuais;

Com relação ao item "G" que define o término do processo de migração da solução, o prazo de 60 dias necessita ser revisto.

Com base no exposto, solicitamos a ampliação do prazo para 90 dias, considerando o atual momento que vivemos e as dificuldades de deslocamento nos dias atuais;

10.3. DA SOLUÇÃO DE GERENCIAMENTO

A solução prevê uma gerência centralizada como descreve o item 5.2.7:

5.2.7 Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança;

Por questões de segurança e compliance com a ISO27001, não é fornecido senha de "ESCRITA" para nenhum item, appliance ou serviço.

Com base no exposto, entendemos que somente senha de LEITURA atende as necessidades da contratante para esta solução.

10.4. DA EXIGÊNCIA DE PROFISSIONAL

Para atendimento da solução contratada o item 5.8.19 exige:

5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da prestação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas;

Solicitamos que esta exigência possa ser substituída por uma declaração do fabricante que a empresa contratada é plenamente capaz de atender todos os itens do objeto desta contratação.

Pedido

Para garantir o atendimento aos princípios norteadores dos procedimentos licitatórios, a Oi, requer que V. Sª julgue motivadamente a presente Impugnação, no prazo de 24 horas, acolhendo-a e promovendo as alterações necessárias nos termos do Edital e seus anexos, sua consequente republicação e suspensão da data de realização do certame.

Obviamente, o segundo requisito apontado decorre dessa acepção de legitimidade, pois mesmo que não se trate de pretenso licitante com interesse concreto e pontualmente direcionado às regras do

cotejo, o interesse da parte legitimada pela regra sobredita pode estar revestido do mero e simples anseio de se satisfazer com o cumprimento estrito da lei.

Na verdade, cremos que a intenção do legislador foi justamente a de conferir ao procedimento licitatório o mais amplo, acessível e rigoroso sistema de fiscalização.

O terceiro ponto a ser observado decorre certamente da consequência lógica do instituto ora em estudo. É dizer, só se pode questionar, esclarecer ou impugnar algo que existe. *In casu,* um ato administrativo instrumentalizado sob a forma de um documento público.

Consequentemente, eventual objeção a um ato administrativo deve trazer consigo suas razões fundamentais específicas, mesmo que simplesmente baseada em fatos, de forma a evitar que a oposição seja genérica, vaga e imprecisa. A peça em análise preencheu, também, esse requisito ao indagar pontualmente o entendimento de determinada regra do edital.

Por derradeiro, há o pressuposto que condiciona o exercício dessa faculdade a determinado lapso temporal, de forma que, ultrapassado o limite de tempo em que se poderia interpor os questionamentos reputados necessários, deixa de existir o direito conferido pela Lei àquela particular situação.

No caso corrente, a manifestação partiu de pretensos licitantes e, por isso, o juízo de admissibilidade deve lastrear-se nas disposições do §2º, art. 41 da Lei Licitatória, levando-se em conta o prazo fixado no decreto regulamentador.

Com termos semelhantes dispõe, também, o item 22 e seus subitens do Edital, estipulando que:

> **22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO**
>
> 22.1. Até o dia 15/02/2021, 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital, mediante petição, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).
>
> 22.2. A impugnação poderá ser realizada por forma eletrônica (preferencialmente), pelo email licitacao@mpam.mp.br, no horário local de expediente da Instituição, até às 14 horas (horário local) da data limite fixada ou por petição dirigida ou protocolada no endereço constante do Rodapé, endereçado à Comissão Permanente de Licitação.
>
> 24.3. Caberá ao Pregoeiro decidir sobre a impugnação, no prazo de até 02 (dois) dias úteis contados da data de recebimento da petição, prorrogáveis desde que devidamente justificado, limitado ao dia anterior à data prevista de abertura, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos Anexos.
>
> [...]
>
> 22.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até o dia 15/02/2021, 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, no horário local de expediente da Instituição (até às 14 horas – horário local), preferencialmente por meio eletrônico via internet ou no endereço indicado no rodapé do Edital, mediante petição, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).
>
> 22.6. O pregoeiro responderá aos pedidos de esclarecimentos no prazo

> de até 02 (dois) dias úteis contados da data de recebimento do pedido, prorrogáveis desde que devidamente justificado, limitado ao dia anterior à data prevista de abertura, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos Anexos.
>
> 22.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame. 22.7.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.
>
> [...]
>
> 23.1. A COMISSÃO PERMANENTE DE LICITAÇÃO prestará todos os esclarecimentos solicitados pelos interessados nesta licitação, estando disponível para atendimento de segunda a sexta-feira, das 8 às 14 horas, na Av. Coronel Teixeira, 7.995, Nova Esperança, Manaus – AM, pelos telefones (92) 3655-0701, (92) 3655-0743 ou, ainda, pelo e-mail: licitacao@mpam.mp.br.

Faz-se mister, contudo, elucidar os critérios utilizados na contagem dos prazos estabelecidos no instrumento convocatório, valendo-se, para tanto, de lição do mestre Jorge Ulisses Jacoby Fernandes[1], cujo excerto segue abaixo:

> "A contagem do prazo para impugnação se faz com a observância da regra geral do art. 110 da Lei nº 8.666/93, tendo por termo inicial a data estabelecida para a apresentação da proposta"[2]. Para facilitar o entendimento, exemplifica-se a seguinte situação:
>
> O dia 16/01/2019 foi fixado para a realização da sessão e, na forma da contagem geral de prazos, não se computa o dia do início. O primeiro dia na contagem regressiva é o dia 15; o segundo, o dia 14; o terceiro dia 11. Portanto, até o dia 10, último minuto do encerramento do expediente no órgão, poderá qualquer pessoa solicitar esclarecimentos de dúvidas face o ato convocatório (...).
>
> Caso a impugnação ou pedido de esclarecimento seja oferecido fora do prazo, não deve ser conhecida com essa natureza, mas merece ser respondida, como qualquer documento que é dirigido à Administração.

Na mesma tônica, vejamos trecho do julgado exarado pelo Corte de Justiça do Estado do Acre em Agravo de Instrumento:

> (...) Em hipóteses como a da espécie em tela, a forma de contagem obedece à regra geral constante do CPC, segundo a qual exclui-se do cômputo o dia do início e inclui-se o do vencimento (art. 184, caput). O traço distintivo, porém, reside no fato de que durante o período de transcurso do prazo é proibida a prática do ato. (...) o prazo referido nos dispositivos legais em destaque é chamado de regressivo, ou inverso. Isso porque a respectiva contagem se dá para trás com a finalidade de impor um limite temporal na prática do ato que não seja dentro do período proibido. (...) No caso vertente, a abertura da sessão pública do Pregão Presencial nº 088/2008 foi aprazada para o dia 18 de dezembro de 2008, quinta-feira. Sendo assim, contando o prazo regressivamente a partir do dia 17, o último dia para impugnação do ato convocatório em questão seria o dia 15 de dezembro de 2008, isto porque o dia 16 de dezembro de 2008 foi o último dia proibido para a prática do ato. (TJ/AC, AI nº 2009.0000052,Rel. Des. Adair Longuini, j. em 12.05.2009.).

Vê-se, portanto, que, a partir de uma interpretação finalística do dispositivo legal ao norte especificado, a intenção do legislador foi justamente a de disponibilizar à Administração um tempo mínimo suficiente para a apreciação de eventuais recursos, neles inclusos impugnações e/ou pedidos de esclarecimentos, sendo assinalado para cada uma das hipóteses normativas prazos razoáveis para a tomada de decisões.

Destaca-se que a data de abertura das propostas do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ está prevista para ocorrer às 10:00 horas, hora de Brasília-DF, do dia 21 de fevereiro de 2022, conforme amplamente divulgado no Diário Oficial Eletrônico deste Ministério Público, Ed. 2306, de 04.02.2022, no Jornal do Comércio, Ed. 43.475, de 5 a 7/02/2022; no sítio do Comprasnet; no sítio do MPAM: https://www.mpam.mp.br/.

À luz dessas considerações, conforme já se disse alhures, os interessados interpuseram suas solicitações, respectivamente, empresa **SERVIX INFORMÁTICA LTDA (Horário: 08h36min - doc. 0768830)**, **PISONTEC SOLUTIONS (Horário: 14h31min - doc. 0769227), ARVVO TECNOLOGIA (Horário: 16h27min - doc. 0769228)** e **OI S.A., EM RECUPERAÇÃO JUDICIAL (Horário: 20h31min - doc. 0769297 e 0769298)**, todos no dia 15/02/2021**.** Logo, as indagações protocoladas via e-mail deixaram de obedecer o prazo, portanto, restaram **INTEMPESTIVAS,** bem como a forma requerida, exigências estas dispostos nos subitens 26.5, 26.6 e 27.1, todos do instrumento convocatório.

Neste sendo, reconhecem-se os requisitos de admissibilidade do ato de esclarecimento/impugnação, exceto o prazo, ao qual passa-se a apreciar o mérito para decisão dentro do prazo legal.

3. RAZÕES DE DECIDIR

Vale ressaltar, em caráter preliminar, que as disposições constantes do instrumento convocatório procuram alinhar-se, estritamente, aos auspícios dos princípios e regras legais que disciplinam o procedimento licitatório, estabelecidos quer na **Lei n.° 8.666/1993,** Estatuto Nacional de Licitações e Contratos Administrativos, como também na **Lei n.° 10.520/2002,** quer na **Constituição Federal de 1988,** bem como, frisa-se, seguindo-se os mais lúcidos preceitos da doutrina de escol e da jurisprudência majoritária.

Nesse sentido, é mister recordar que o dever administrativo de adotar critérios claros, objetivos e legais durante a análise das documentações dos concorrentes em uma licitação decorre da obrigação da Administração Pública manter plena transparência de seus atos, a fim de definir qual a licitante reúne condições de qualificação técnica e econômica indispensáveis à garantia do cumprimento de seus deveres, sem desviar-se da observância necessária do princípio da igualdade entre os licitantes, estimulando o caráter competitivo da licitação, constante no artigo 3.º da Lei n.º 8.666/93, abaixo disposto:

> "*A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da* ***legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório****, do julgamento objetivo e dos que lhes são correlatos." **(g.n.)***

Em outras palavras, no que tange às contratações realizadas mediante licitação, deve a Administração Pública, em observância ao disposto no art. 3º, caput, da Lei nº 8.666/93, garantir a igualdade na participação dos licitantes e a selecionar a proposta mais vantajosa, sem se afastar dos princípios básicos descritos no dispositivo supra.

Destarte, é certo que não deve a Administração, em nenhuma hipótese, fazer exigências que

frustrem o caráter competitivo do certame, sob pena de macular a garantia à ampla concorrência na disputa licitatória, de modo sim a possibilitar o maior número de concorrentes, desde que estes preencham todos os requisitos exigidos e necessários ao fiel cumprimento das obrigações, em especial, jurídico, econômico, fiscal e técnico.

Assim, destaca-se que a Administração tem o dever de precaução contra eventuais empresas que frustem a contratação futura por não se adequarem técnica e economicamente aptas à execução do serviço ou fornecimento de um bem. Logo, o Poder Público deve se valer do seu direito de discricionariedade para garantir que seja realizado o melhor procedimento aquisitivo adequando preço e qualidade.

Em face dos questionamentos lançados, as peças foram remetidas à análise e manifestação da **Diretoria de Tecnologia de Informação e Comunicação - DTIC/Setor de Infraestrutura e Telecomunicação - SIET** desta Instituição, órgão emissor do Termo de Referência, integrante do Edital ora questionado.

Via de consequência, aquele Setor se pronunciou no seguinte sentido, por meio das manifestações a seguir exposto de forma detalhada:

PARECER Nº 2.2022.SIET.0771082.2021.015252

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar pedido de esclarecimento interposto aos termos do Edital de **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, originados das empresas: **SERVIX INFORMÁTICA LTDA** (0768833), **PISONTEC SOLUTIONS** (0769231) e **ARVOO TECNOLOGIA** (0769231). Trata ainda, do pedido de imougação da empresa **OI S.A.** (0769299).

2. Análise

O presente parecer se baseia nas disposições do Termo de Referência n. 20.2021.DTIC.0720733.2021.015252, Anexo I ao Edital do certame, SEI 0763629, em seus diversos itens confome abaixo:

2.1 SERVIX INFORMÁTICA LTDA

Questionamento 01

Item - 5.2.15.6.6 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU ou memória do dispositivo.

Pergunta - A solução fornece gerenciamento apartado do plano de dados do restante da solução. Logo, quando utilizado toda a capacidade do hardware de NGFW, seu plano de gerência continua funcional sem que haja indisponibilidade do appliance ou necessidade de desativação da funcionalidade de IPS. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Sim, o entendimento está correto.

Questionamento 02

Item - 5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

Pergunta - A solução permite analisar os arquivos dentro dos fluxos de SMTP e POP3 e identificar se o conteúdo do email é maligno ou benigno e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Especificamente para o MTA (Message Transfer Agent), sim, o entendimento está correto. Não obstante, as demais topologias devem seguir sendo suportadas.

Questionamento 03

Item - 5.2.15.7.30 A solução, deve emular e eliminar malwares contidos em anexos de e-mail e documentos baixados da web.

Pergunta - A solução permite o emular os anexos contidos nos emails e documentos baixados da web, classificar esses anexos e documentos baixados como benigno e malignos e baseado em regras de NGFW aplicar as devidas regras, como por exemplo permitir ou negar o tráfego analisado. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Sim, o entendimento está correto.

Questionamento 04

Item - 5.2.15.9.39 Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados.

Pergunta - A solução permite o correlacionamento de eventos e logs, classificando em níveis de severidade, através de métricas de tempo, objetos, IP de origem e destino, usuários, nome do ataque, país de origem. A partir dessas métricas é possível visualizar graficamente as informações e correlacionar as evidências apresentadas. Compreendemos que esse método atende o item, está correto o entendimento?

Resposta - Sim, o entendimento está correto.

2.2 PISONTEC SOLUTIONS

Questionamento I

Item - Geral/Ambiente

Pergunta - O serviço está sendo executado ou já foi em algum momento?

Se a reposta for positiva:

a) qual empresa é ou foi responsável?

b) Quantos profissionais atuam atualmente no serviço?

Resposta - O serviço objeto deste certame hoje é executado internamente no órgão, por profissionais técnicos especializados que são servidores concursados efetivos.

Questionamento II

Item - Geral

Pergunta - Será necessário fornecimentos de peças e/ou materiais ou softwares?

Resposta – Sim, todos os itens necessários para o cumprimento total das exigências dispostas no Edital n. 4005/2022-CPL/MP/PGJ, seus anexos, bem como no Termo de Referência n. 20.2021.|DTIC.0720733.2021.015252, são de responsabilidade da CONTRATANTE, exceto disposição em contrário explícita nestes documentos.

Questionamento III

Item - Geral

Pergunta - O serviço poderá ser executado remotamente?

Resposta – Sim, o serviço poderá ser executado remotamente, exceto em casos que impeçam esta modalidade, como em defeitos de hardware, por exemplo. Entretanto, como dita o Edital e o Tremo de Referência, os equipamentos devem ser instalados nas dependências da CONTRATANTE. Indicamos a leitura minuciosa de todos os itens do Edital e do Termo de Referência, especialmente este último, que contém todas as especificações técnicas do serviço desejado, incluindo as previsões para as manutenções, SLA, formas de prestação do serviço, entre outros.

Questionamento IV

Item – 5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas.

Pergunta - A apresentação de Profissionais Certificados integrantes no quadro de funcionários da Licitante, deve ser realizada apenas no ato da assinatura do contrato, sendo aceitos profissionais certificados cuja contratação se dê por prestação de serviço, sem vínculo trabalhista com a Licitante.

Resposta - Deve-se atender plenamente o disposto no item 5.8.19 do Termo de Referência, não havendo vedação para comprovação do vínculo dos profissionais exigidos com a CONTRATANTE através de contrato de terceirização.

Questionamento V

Item - Não relacionado à DTIC

Pergunta - Qual o valor estimado?

Resposta - Não relacionado à DTIC

Questionamento VI

Item - Geral

Pergunta - Se existir serviços de manutenção de equipamentos, necessário disponibilizar a lista contendo as marcas e os modelos dos respectivos equipamentos.

Resposta - Todos os itens necessários para o cumprimento total das exigências dispostas no Edital n. 4005/2022-CPL/MP/PGJ, seus anexos, bem como no Termo de Referência n. 20.2021.|DTIC.0720733.2021.015252, são de responsabilidade da CONTRATANTE, exceto disposição em contrário explícita nestes documentos, ou seja, todas as manutenções nos equipamentos que fazem parte da solução integrante dos serviços objeto deste certame devem ser realizadas conforme exigências dos documentos supracitados. Indicamos a leitura minuciosa de todos os itens do Edital e do Termo de Referência, especialmente este último, que contém todas as especificações técnicas do serviço desejado, incluindo as previsões para as manutenções, SLA, formas de prestação do serviço, entre outros.

2.3 ARVOO TECNOLOGIA

Esclarecimento 01

Item - 5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.

Pergunta - Para a identificação dos usuários poderá ser utilizado o serviço agregado ao servidor de gerenciamento para integração ao base de usuários LDAP, nem a necessidade de instalação de agentes ou software de clientes nos servidores Active Directory?

Resposta - A função exigida pelos itens deve estar integrada à solução ofertada, não sendo aceitas instalações de servidores separados para suprir a funcionalidade desejada.

Esclarecimento 02

Item - 5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).

Pergunta - Após o bloqueio, serão aceitas soluções que a liberação e a continuação da navegação sejam permitidas após avaliação do responsável pela manutenção da solução ofertada?

Resposta - Não, a solução deve ser capaz de permitir que o usuário decida se continua o acesso a algo potencialmente perigoso, mesmo após um alerta/bloqueio, sem a intervenção da equipe técnica de gerenciamento da solução.

Esclarecimento 03

Item - 5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.

Pergunta - Entendemos que a topologia e arquitetura de implementação do sistema de IPS deve ser capaz de interceptar todo trafego e tomar as ações de inspeção assim estipuladas quando em modo Inline e apenas registrar em modo Mirror/TAP. A topologia de implementação MTA se faz equivocada neste sentido, visto que em modo In-line ou TAP "todo" o trafego será analisado e o modo MTA se faz necessário em soluções de proteção de messageria. Neste caso o conceito de IPS não faz uso dessa topologia de comunicação para analise de apenas do trafego de mensagens de e-mail. Esta correto nosso entendimento?

Resposta - Apesar de tecnicamente o entendimento estar correto para os conceitos de IPS/IDS de soluções tradicionais de firewall, como o objeto deste certame visa a contratação de firewall de próxima geração (NGFW), é padrão de mercado que o tratamento do fluxo de emails seja feito em conjunto com todo o fluxo de dados.

Esclarecimento 04

Item - 5.2.15.8.1 Deverá possuir certificação ICSA para Firewall

Pergunta - A certificação ICSA depende de contratação para ser emitida em ordem que, os testes realizados por outras empresas certificadoras, realizam os mesmos testes de performance com abrangência internacionais. Levando isto em consideração, entendemos que a solução ofertada pode ser certificada em outros laboratórios desde que atenda aos requisitos de testes submetidos de forma equivalente aos executados pela ICSA.

Resposta - O objetivo deste certame é obter uma solução que eleve o patamar da proteção do ambiente computacional em todos os sentidos possíveis, incluindo equipamentos de qualidade excepcional, de forma a

diminuir ao máximo o risco de prejuízos para o Ministério Público do Estado do Amazonas. A certificação solicitada é uma garantia do diferencial de qualidade desejado presente nos equipamentos dos melhores fabricantes do mercado, em diversas marcas, ou seja, não exigem contratação separada ou adicional para a CONTRATADA. Desta forma, sob pena de prejuízos advindos de soluções com qualidade inferior à necessária para o MPAM, todas exigências presentes no Termo de Referência devem ser atendidas, incluindo a certificação ICSA do item 5.2.15.8.1.

2.4 OI S.A.

Pedidos de impugnação dos capítulos:

"1. EXIGÊNCIA ABUSIVA"

"2. DA VEDAÇÃO DE PARTICIPAÇÃO DE LICITANTES EM REGIME DE CONSÓRCIO"

"3. IMPEDIMENTO À PARTICIPAÇÃO DE EMPRESAS SUSPENSAS DE LICITAR COM A ADMINISTRAÇÃO PÚBLICA EM GERAL"

"4. DA EXIGÊNCIA DE EMISSÃO DE NOTA FISCAL COM CNPJ DA EMPRESA CONTRATADA"

"5. PAGAMENTO VIA NOTA FISCAL COM CÓDIGO DE BARRAS"

"6. INDEVIDA APRESENTAÇÃO DE CERTIDÕES DE REGULARIDADE MENSALMENTE"

"7. RETENÇÃO DO PAGAMENTO PELA CONTRATANTE"

"8. DAS PENALIDADES EXCESSIVAS"

"9. VALOR DA GARANTIA"

Resposta: Não relacionado à DTIC

Pedido de impugnação do capítulo "10.1 POSSIBILIDADE DE SUBCONTRATAÇÃO DOS SERVIÇOS"

Resposta: Sob pena de degradação da qualidade final dos serviços prestados, bem como falta de conformidade entre os serviços prestados, além de desorganização, impossibilidades de padronização de todos os procedimentos e dificuldades de estabelecer escopos e responsabilidades com agilidade, os itens 01, 02, e 03 não devem ser prestados por empresas diferentes, o que inclui subcontratações. Soma-se ao exposto o fato dos itens 01, 02 e 03 serem serviços contínuos e, em conjunto, formarem o cerne da atividade que a CONTATANTE deseja contratar para execução. Como brevemente exposto no item 3.3, do Termo de Referência, os bens e serviços pretendidos estão intrinsecamente relacionados e a realização dos serviços por empresas diferentes pode resultar em soluções incompatíveis, o que acarretaria prejuízo ao CONTRATANTE. A descrição individualizada do objeto no caso dos itens 01, 02 e 03, dentro do Lote do certame, se deu única e exclusivamente para melhor entendimento e organização do Termo de Referência, bem como pela diferença das quantidades de cada um. Entretanto, estes itens são partes do único serviço desejado, que poderia ser descrito como o "serviço para prover o Ministério Público de uma solução, em todos os aspectos, de firewall de próxima geração em alta disponibilidade"

Pedido de impugnação do capítulo "10.2 DOS PRAZOS DE ENTREGA"

Item: 9.2, "e" - Prazo para entrega do plano de implementação

Resposta: O objetivo deste certame é a contratação de empresa especializada nos serviços descritos pelo objeto, pelo que se espera vasta experiência de seu corpo técnico, incluindo a execução de vários projetos como o que virá a ser executado pela CONTRATADA. Por

óbvio, um corpo técnico com a experiência necessária para projetos deste porte e complexidade já possui plano de implementação básico, com itens indispensáveis e comuns a todo serviço do tipo, para os equipamentos que utiliza prontos e formatados, restando apenas os pequenos ajustes decorrentes de cada cenário de seus clientes. Sendo assim, considera-se o prazo indicado pela alínea "e", da entrega do plano de implementação, de 05 (cinco) dias úteis após a reunião de alinhamento é perfeitamente exequível.

Além disto, conforme descrito nas justificativas deste certame, este é um serviço crítico, essencial e contínuo, ou seja, qualquer atraso pode gerar risco desnecessário para o MPAM.

Item: 9.2, "f" - Prazo para início do processo de migração/reunião de alinhamento

Resposta: Conforme disposto no Edital e Termo de Referência, o início da migração se dá com a reunião de alinhamento e não com a efetiva instalação e configuração de equipamentos. Desta forma, não há que se falar em distensão de prazo para entrega de equipamentos. O prazo apenas exige um tempo máximo para o acontecimento da reunião de alinhamento incial, que inclusive pode ser realizada via videoconferência. Sendo assim, considera-se o prazo indicado de 05 (cinco) dias úteis após assinatura do contrato perfeitamente exequível.

Item: 9.2, "g" - Prazo para finalizar o processo de migração

Resposta: Durante a pesquisa de mercado, que precede a confecção do Termo de Referência, foram consideradas todas as dificuldades do momento atual e de deslocamento, caracteríticas de nossa região. Mesmo com as dificuldades impostas pela pandemia, em todas as consultas a diversos fornecedores, dos mais diversos fabricantes, o prazo de 60 dias excede o indicado como necessário para este tipo de projeto por todos.

De toda forma, conforme Termo de Referência, o prazo de 60 dias só é contado enquanto há dependências por parte da CONTRATADA e fica suspenso em caso de dependências por parte da CONTRATANTE.

Além disto, conforme descrito nas justificativas deste certame, este é um serviço crítico, essencial e contínuo, ou seja, qualquer atraso pode gerar risco desnecessário para o MPAM. E, no caso da migração, pode significar uma parada completa do funcionamento do órgão.

Sendo assim, considera-se o prazo indicado pefeitamente exequível, não devendo ser alterado.

Pedido de impugnação do capítulo "10.3 DA SOLUÇÂO DE GERENCIAMENTO"

Item: 5.2.7

Resposta: A administração e gerenciamento da solução será realizada em conjunto pela equipe técnica da CONTRATANTE e da CONTRADA, sendo impraticável e ineficiente que os equipamentos da solução estejam indisponíveis para uma das equipes. A imposição por parte da CONTRATADA de não fornecer senhas que permitam escrita acabaria por gerar morosidade na resolução de problemas rotineiros e, por conseguinte, gerando prejuízos ao funcionamento eficiente do MPAM. Sendo assim, a exigência do item em questão deve permanecer inalterada.

Pedido de impugnação do capítulo "10.4 DA EXIGÊNCIA DE PROFISSIONAL"

Item: 5.8.19

Resposta: O objeto deste certame é um serviço crítico, essencial e contínuo para o funcionamento do MPAM e inclui manutenção preventiva e corretiva, com SLA bem definido. A exigência em questão visa garantir que o atendimento prestado pela CONTRATADA tenha a qualidade e a capacidade necessária, a qualquer momento, para manter

o funcionamento ininterrupto dos serviços do MPAM. Sendo assim, não é suficiente uma simples declaração do fabricante como solicitado, devendo ser mantida a exigência do Termo de Referência, sob pena de prejuízos ao MPAM.

Manaus, 18 de fevereiro de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ
Coordenador da Área de Redes

Com relação os demais questionamentos, apresentamos as razões e motivações, conforme individualmente elencado:

3.1. PEROLA PLETSCH, representando a empresa **PISONTEC SOLUTIONS (doc. 0769227):**

3.1.1. VALOR ESTIMADO

Considerando o pedido, este nos remete à possível apresentação do valor estimado pela Administração para a contratação do objeto em voga, o cerne da indagação da interessada é direto e simples e, portanto, reclama pronunciamento pontual e sem muita digressão, muito mais por se tratar de questão de pacífico entendimento no âmbito da Corte Máxima de Contas da União.

Bem se sabe que as contratações públicas são regidas por vários princípios e critérios, dentre os quais, certamente, o da publicidade. Ocorre que, no caso particular em apreço, há que se considerar, sobretudo, outros princípios de muito maior relevância, repisamos, *in casu,* já que, em abstrato, não se pode afirmar a sobrepujança de um princípio sobre o outro. Referimo-nos, assim, aos critérios da competitividade, impessoalidade e da igualdade entre os concorrentes.

I) Levando-se em conta a **competitividade** do certame, a experiência vivenciada pelo Órgão conduz à irrefutável conclusão de que a revelação do preço máximo a ser desembolsado com este tipo de contratação **faz com que as propostas dos licitantes orbitem em torno daquele valor**, o que prejudica a obtenção das melhores condições de contratação, em patente afronta ao princípio sob exame.

Em outras palavras, pela óptica da Administração Pública, restaria prejudicada a possibilidade de negociação do preço com o licitante vencedor preconizado no inciso XVII do artigo 4º da Lei 10520/2002[3].

Desse modo, com a divulgação do valor estimado o dispositivo supracitado tornar-se-ia letra morta, perdendo, portanto, sua finalidade. Ora, o licitante vencedor sabendo que sua proposta se encontra dentro do estimado, em tese, não se abriria a negociação, pois sabe que a Administração deve contratá-lo com o preço inicial ofertado, uma vez que está no limite da estimativa.

II) Considerando-se a **impessoalidade e isonomia entre os interessados**, à luz da solicitação em análise, **ambos os critérios seriam ofendidos** ao conceder-se, única e exclusivamente, à

empresa que pedisse, as informações alusivas à quantia máxima disponível para desembolso pela Administração. Dito de outra forma, não há como se garantir impessoalidade e, portanto, isonomia, se as regras aplicadas no certame não forem conhecidas por todos e pelos mesmos meios.

Tudo isso porque, lembramos, caso fosse admitida a consulta anterior à tal fase, além de se comprometer a livre disputa e a possível contratação mais vantajosa, estar-se-ia, flagrantemente, desrespeitando o princípio da isonomia.

Em ambos os sentidos (I e II), há farta jurisprudência recente do Tribunal de Contas da União corroborando com o que aqui se apregoa, tais como os Acórdãos 644/2006, 1925/2006, 114/2007, 1789/2009, todos do Plenário do TCU. Eis o trecho do voto do Relator, **Ministro José Jorge**, do Processo nº TC 033.876/2010-0, atinente ao **ACÓRDÃO Nº 392/2011 – TCU – Plenário**:

> "
>
> *[...]*
>
> *Portanto, nas licitações na modalidade de pregão, os orçamentos estimados em planilhas de quantitativos e preços unitários – e, se for o caso, os preços máximos unitários e global –* ***não constituem elementos obrigatórios do edital****, devendo, no entanto, estar inseridos nos autos do respectivo processo licitatório.* ***Caberá aos gestores/pregoeiros, no caso concreto, a avaliação da oportunidade e conveniência de incluir tais orçamentos*** *– e os próprios preços máximos, se a opção foi a sua fixação – no edital, informando nesse caso, no próprio ato convocatório, a sua disponibilidade aos interessados e os meios para obtê-los." .(g.n.)*

No julgamento do mesmo processo, decidiu o Plenário daquela Corte:

> "
>
> *[...]*
>
> *não seria obrigatória a fixação de preço máximo, tampouco a divulgação do valor orçado, por se tratar de pregão. Pelas razões já expostas,* ***ficaria a critério do órgão fixar o preço máximo, sendo igualmente discricionária a sua divulgação."*** *. (g.n.)*

Esse posicionamento foi reafirmado na sessão plenária do TCU, do dia 20 de agosto de 2014, decidindo-se que,

na licitação na modalidade pregão, o orçamento estimado em planilhas de quantitativos e preços unitários não constitui um dos elementos obrigatórios do edital, mas deve estar inserido obrigatoriamente no bojo do processo relativo ao certame. (BRASIL. Tribunal de Contas da União. Plenário. Acórdão n. 2.166/2014. Relator: min. substituto Augusto Sherman Cavalcanti. Sessão de 20 ago. 2014.)

Debatendo sobre o Regime Diferenciado de Contratações (RDC) no Tribunal de Contas do Estado do Rio de Janeiro, o **Ministro Benjamin Zymler**, à época presidente do Tribunal de Contas da União, ao comentar as inovações desse novo regime de licitações, destacou que "*o sigilo sobre o orçamento evitará que as propostas gravitem em torno do orçamento fixado pela Administração, ampliando-se a competitividade do certame.*"

Em outras palavras, a prática adotada pelo *Parquet*, é dizer, o sigilo sobre o orçamento, traduz a posição defendida pelo TCU, isto é, amplia a disputa e consagra a competitividade do certame,

culminando no princípio basilar da licitação: a busca da melhor proposta para a Administração Pública.

Vale destacar que, após a fase de lances, caso o valor ofertado pela licitante permaneça acima do valor estimado pela Administração, **este será informado pelo(a) Pregoeiro (a) com intuito de lograr melhor preço para o Órgão**. Isto significa valor igual ou menor que o estimado, caso contrário, a proposta não poderá ser aceita com fundamento no subitem 11.2.2. do instrumento convocatório.

Outrossim, cabe destacar que se trata de uma prática comumente adotada por esta Instituição há bastante tempo. Corroborando, temos que o novo decreto regulamentador do Pregão Eletrônico, qual seja, o Decreto nº 10.024 de 20 de setembro de 2019, **consagrou tal procedimento, afastando quaisquer entendimentos em sentidos contrários**:

> Art. 15. O valor estimado ou o valor máximo aceitável para a contratação, se não constar expressamente do edital, possuirá caráter sigiloso e será disponibilizado exclusiva e permanentemente aos órgãos de controle externo e interno.
>
> § 1º O caráter sigiloso do valor estimado ou do valor máximo aceitável para a contratação será fundamentado no § 3º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, e no art. 20 do Decreto nº 7.724, de 16 de maio de 2012.
>
> § 2º Para fins do disposto no **caput**, o valor estimado ou o valor máximo aceitável para a contratação será tornado público apenas e imediatamente após o encerramento do envio de lances, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias à elaboração das propostas.
>
> § 3º Nas hipóteses em que for adotado o critério de julgamento pelo maior desconto, o valor estimado, o valor máximo aceitável ou o valor de referência para aplicação do desconto constará obrigatoriamente do instrumento convocatório.

Vale ressaltar também que, após a fase de lances, será ampla a possibilidade de acesso, por parte dos licitantes, ao processo administrativo de onde constam os orçamentos estimados em planilhas de quantitativos e preços unitários.

Por derradeiro, ressalta-se que todos os procedimentos licitatórios de interesse desta PGJ/AM passam por uma rigorosa ***fase interna***, incluindo, pesquisa de preços para apuração do valor médio, a fim de refletir o real preço praticado no mercado.

3.2. RAUL LUIZ MARTINS PEREGRINO, representando a **OI S.A., EM RECUPERAÇÃO JUDICIAL (doc. 0769297 e 0769298):**

Inicialmente, permita-me utilizar das argumentações apresentadas pelo eminente Sr. ALBERTINO PIERRE DA COSTA, TÉCNICO JUDICIÁRIO/ ADMINISTRATIVA junto à JUSTIÇA FEDERAL NO RIO GRANDE DO NORTE quando da análise da IMPUGNAÇÃO ao ato convocatório do Pregão Eletrônico nº 09/2017 – JF/RN , que objetivava a contratação, em que pese não idêntica a presente, do Serviço de Telefonia Fixa Comutada – STFC (Fixo-Fixo e Fixo-Móvel), apresentada pela empresa TELEMAR NORTE LESTE S.A. (OI), CNPJ nº 33.000.118/0001 79, na Decisão proferida no Processo: SEI 00015304.2017:

> **5. Inicialmente, forçoso rechaçar a prática perpetrada pela empresa impugnante do exercício indiscriminado e abusivo do direito de impugnação previsto no ordenamento jurídico, o qual apresenta como**

finalidades, além da proteção dos direitos subjetivos dos particulares interessados, a de proteção aos próprios interesses públicos.

5.1. Com efeito, registrese que nas diversas vezes em que foram publicados certames licitatórios com o objetivando a contratação dos STFC – Serviços de Telefonia Fixa Comutada tivemos impugnações da OITELEMAR, de maneira que já estamos na terceira edição com **petição impugnatória baseada em tópicos, na sua maioria, idênticos a anteriores já afastadas fundamentadamente, por decisão definitiva da autoridade máxima do órgão.**

5.2. Isso demonstrar, sim, prática abusiva de direito e que precisa ser combatida pela Administração Pública. Ora, quando nada de novo se tem a arguir em relação a certo ponto já questionado e, fundamentadamente, considerado improcedente, resta juridicamente esgotada a via administrativa para tal discussão, com a consequente preclusão da matéria. Tratase de lição básica de direito processual. Consequência cara à segurança jurídica.

5.3. Não há como deixar de considerar, ademais, que **tal prática também leva a desperdícios de recursos públicos.** Desperdícios de tempo de trabalho do pessoal da área de licitação para analisar e fundamentar, reiteradas vezes, petições com argumentos já exaustivamente analisadas por diversas vezes pelo mesmo órgão julgador; desperdícios por tramitação desnecessária de processo para fins de decisão da autoridade superior em relação a fatos ou pontos do edital já fundamentadamente julgados improcedentes; desperdícios de recursos materiais diversas da Instituição.

5.4. **Por tanto, resta claramente prejudicial à tramitação do presente certame licitatório conhecer de impugnações já analisadas exaustivamente em ocasiões pretéritas, sem que existe qualquer fato ou argumento novo, e que já foram julgadas absolutamente improcedentes.**

6. Das Razões da Impugnação dos subitens 1.2, 1.5, 1.6, 1.7 e 1.8 do relatório:

6.1. Conforme já destacado, agrupamos neste tópico todos os itens da impugnação aqui analisada que já foram objeto de apreciação e julgamento por ocasião de impugnações formuladas anterioremente, pela própria empresa TELEMAR, em oposição às regras fixadas nos Pregões 10/2016 e 22/2016, conforme consta dos autos do Processo Administrativo nº 540/2016 (que foi migrado para o sistema SEI em março de 2017, recebendo o número SEI 00015304.2017).

6.2. A preclusão é instituto de direito processual que representa a perda do direito de agir nos autos em razão da efetiva perda da oportunidade, ou até mesmo de seu já exercício. Ela pode ser temporal, lógica ou consumativa. No presente caso, temse preclusão consumativa porque todos esses itens já foram analisados e acatados ou não, de forma fundamentada, por ocasião da primeira impugnação aduzida pela TELEMAR, em face dos editais dos pregões nºs 10/2016 e 22/2016.

6.3. Tratase de matéria prevista no art. 63, § 2º, da Lei do Processo Administrativo (Lei nº 9.784/1999), in verbis (sem grifos no original): Art. 63. O recurso não será conhecido quando interposto: I fora do prazo; II perante órgão incompetente; III por quem não seja legitimado; IV após exaurida a esfera administrativa. § 1 o Na hipótese do inciso II, será indicada ao recorrente a autoridade competente, sendolhe devolvido o prazo para recurso. § 2 o O não conhecimento do recurso não impede a Administração de rever de ofício o ato ilegal, desde que não ocorrida preclusão administrativa.

6.4. Percebam: não faz qualquer sentido lógicojurídico a rediscussão de tais matérias. Nenhum fato novo ocorreu e nem mesmo qualquer argumento diferente fora acrescido pela impugnante que pudesse justificar ou motivar o exercício do direito de impugnação do edital. É, reafirmamos, abuso do direito de impugnação previsto no art. 41 da Lei 8.666/93.

6.5. De mais a mais, por força do princípio da economia processual, e sobretudo da eficiência administrativa, remetemos o interessado às decisões anteriores para fins de compreensão dos fundamentos e do

posicionamento adotado por esta Instituição. Rogando pela definitiva pacificação de tais questões.

6.6. ANTE O EXPOSTO, propomos que não seja conhecida a presente impugnação em relação aos supracitados itens ou tópicos questionados na petição de impugnação.

Tecidas essas breves considerações, da análise da peça aviada, vê-se que a maioria das razões de impugnação da pretensa licitante já foram respondidas em ocasiões passadas, de certames de natureza correlata, de forma que este subscrevente não apresentará toda fundamentação e citação às decisões precedentes novamente, sobretudo, face à intempestividade do pleito.

Outrossim, convém destacar que o pretende a Requerente é a adequação das exigências fixadas pela Administração a sua realidade, quando na verdade o raciocínio correto é o inverso. A Administração elaborou **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252** com as especificações mínimas e prazos que entendeu salutar para a implementação do projeto.

Ademais, observa-se do **ITEM 2 - JUSTIFICATIVA** constante do aludido documento, da relevância da contratação ora pretendida em prol da Segurança da Informação desta Instituição, de forma que é plenamente justificável a previsão de prazos mais céleres e sanções nesses patamares.

Ademais, quanto às razões do pedido que giram em torno de aspectos técnicos da especificação do objeto e às obrigações deles acessórias, esclareça-se que as respostas aqui concedidas decorreram da análise e manifestação da **DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO-DTIC** desta Instituição, por intermédio do **Setor de Infraestrutura e Telecomunicações-SIET**, órgão emissor do Termo de Referência integrante do Edital ora objeto do questionamento.

À luz das razões ora delineadas, este Presidente, em cumprimento ao "**item 26**" do ato convocatório, considera esclarecidas as solicitações, reputando, portanto, desnecessária a retificação do edital, posto que em amplo respeito ao **Princípio da motivação**, dando prosseguimento ao certame até o seu desiderato.

4. CONCLUSÃO

Dessarte, resolvo **receber** e **conhecer** a solicitação feita pelo Senhor **JEFFERSON MATOS,** representando a empresa **SERVIX INFORMÁTICA LTDA**, todavia, **receber e NÃO conhecer** dos **PEDIDOS DE ESCLARECIMENTOS** interpostos pela Senhora **PEROLA PLETSCH,** representando a empresa **PISONTEC SOLUTIONS;** Senhor **CRISTIAN TELES**, representando a empresa **ARVVO TECNOLOGIA** e a **IMPUGNAÇÃO** apresentada pelo Senhor **RAUL LUIZ MARTINS PEREGRINO**, representando a **OI S.A., EM RECUPERAÇÃO JUDICIAL**, por ausência de pressusposto objeto da tempestividade. E, no mérito, **reputar esclarecidas,** fartamente refutado pelas razões de fato e direito exposta alhures.

Considerando que o teor da presente decisão não afeta a formulação das propostas por parte dos pretensos licitantes, conforme preleciona o artigo 21, § 4º, da Lei n.º 8.666/93, **mantém-se a realização do cotejo na data original, conforme publicação oficial, a fim de dar-se prosseguimento aos demais atos providenciais**.

É o que temos a esclarecer.

Manaus, 18 de fevereiro de 2022.

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Pregoeiro designado pela PORTARIA N° 229/2022/SUBADM

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 18/02/2022, às 18:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0771060** e o código CRC **1F14930B**.

2021.015252 v62

AO
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
PROCURADORIA GERAL DE JUSTIÇA
COMISSÃO PERMANENTE DE LICITAÇÃO – CPL
REF.: PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.015252

PROPOSTA DE PREÇOS, CONFORME MODELO DO ANEXO IV DO EDITAL

Proposta que faz a empresa Network Secure Segurança Da Informação Ltda, inscrita no CNPJ (MF) nº 05.250.796/0001-54, localizada Av. Pontes Vieira, 2340 - Dionísio Torres, UNO - Medical & Office - Sala 510 - 514 - 5º andar, na cidade de Fortaleza/CE, CEP 60135-238, fone (85) 3195-2200,e-mail licitacoes@networksecure.com.br, para a prestação do serviço abaixo relacionado, de acordo com todas as especificações e condições estabelecidas no **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ**, promovido pelo Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça:

PLANILHA DE FORMAÇÃO DE PREÇOS

LOTE ÚNICO					
ITEM	ESPECIFICAÇÃO	UNIDADE	QTD	VALOR UNITÁRIO (R$) (B	VALOR TOTAL (R$) (A * B)
1	Serviço de Firewall em Alta Disponibilidade – Fabricante Check Point – 2x NGFW - PNs: 2x CP-CPAP-SG66XX-PLUS-INV - 6600 Appliance Plus – Inventory + 2x CP-UPG-CPAP-SG6600-PLUS-SNBT - 6600 Plus appliance with SandBlast subscription package for 1 year + 2x CP-CPSB-SNBT-6600-PLUS-3Y - Next Generation Threat Prevention and Sandblast for additional 3 years for 6600 PLUS Appliance + 2x CP-CPSB-MOB-U - Mobile Access Blade unlimited + Suporte 24x7 e demais serviços conforme especificações técnicas do edital.	Meses	48	R$ 44.791,66	R$ 2.149.999,68
2	Serviço de Monitoramento da Solução – Fabricante Check Point – PNs: 1x CP-CPSM-NGSM5 - Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year) + 1x CP-CPSB-EVS-COMP-5-3Y - SmartEvent, SmartReporter and Compliance blades for 5 gateways (Smart-1 & open server) 3 year	Meses	48	R$ 5.208,33	R$ 249.999,84

	subscription + Suporte 24x7 e demais serviços conforme especificações técnicas do edital.				
3	Serviço de Migração do Ambiente Atual para a nova solução – Fabricante Check Point. Conforme especificações técnicas do edital.	Unidade	1	R$ 30.553,33	R$ 30.553,33
4	Serviço de Treinamento da Solução do Fabricante Check Point. Conforme especificações técnicas do edital.	Pessoas	5	R$ 9.500,00	R$ 47.500,00
VALOR TOTAL DA PROPOSTA = R$ 2.478.052,85 (dois milhões, quatrocentos e setenta e oito mil e cinquenta e dois reais e oitenta e cinco centavos)					

A Network Secure Segurança Da Informação Ltda declara que concorda com todas as especificações do Edital.

a) Prazo de validade da proposta: 90 (noventa) dias, a contar da data de sua apresentação.

b) Prazo entrega do plano de implementação: Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

c) Prazo início processo de migração/reunião alinhamento: A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato;

d) Prazo processo de migração: A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

e) Dados Bancários: Banco do Brasil nº 001 - Comercial Aldeota, AGÊNCIA: 3515-7 CONTA CORRENTE Nº 7028-9

f) Contato para fins de faturamento: Yure Leopoldo Sabino De Freitas, Diretor Comercial, Rua Barbara De Sousa Costa, 100 – Lagoa Redonda – Fortaleza/CE, CEP: 60831-083, (85) 3195-2200, licitacoes@networksecure.com.br

g) Dados dos 3 (três) principais integrantes do quadro societário da licitante, assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade.

Nome: JOSE MURILO CIRINO NOGUEIRA JUNIOR
CPF: 648.711.503-72
Nome: TATIANA RIBEIRO LEITE
CPF: 691.833.093-49
Nome: ALARICO ISAIAS DE SOUSA GUIMARAES
CPF: 620.143.313-91
Nome: YURE LEOPOLDO SABINO DE FREITAS
CPF: 525.285.023-20

DECLARAÇÕES:

1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6.**, para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores

ocupantes de cargo de direção, chefia ou assessoramento no âmbito **do Ministério Público do Estado do Amazonas** e de sua **CPL**;

2. Os documentos e declarações apresentados são fiéis e verdadeiros, bem como que a empresa recebeu o Edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

3. Estou ciente da obrigação de, caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhar os documentos necessários à CONTRATANTE, a fim de efetuar o referido cadastramento no prazo de cinco dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;

4. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

Fortaleza/CE 21 de Fevereiro de 2022.

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ Nº 05.250.796/0001-54
Yure Leopoldo Sabino De Freitas
Diretor Comercial
CPF Nº 525.285.023-20

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMÁTICA LTDA
AV: PONTES VIEIRA Nº 2340
DIONISIO TORRES SL 510/514
5º ANDAR CEP: 60.135-238
FORTALEZA CEARÁ

AO
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
PROCURADORIA GERAL DE JUSTIÇA
COMISSÃO PERMANENTE DE LICITAÇÃO – CPL
REF.: PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.015252

ESPECIFICAÇÕES TÉCNICAS;

5. DETALHAMENTO DO OBJETO

5.1 ESPECIFICAÇÕES GERAIS - PARA TODOS OS ITENS

5.1.1 São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

5.1.2 Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

5.1.3 Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a CONTRATANTE seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA);

5.1.4 O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 5.4.10, ou na exposição de ativos a riscos de segurança.

5.1.5 Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional MPAM.

5.1.6 A CONTRATADA deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

5.1.7 Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. Qualquer dano eventual de manuseio/transporte a CONTRATADA será obrigada a reparo imediato.

5.1.8 Quaisquer recursos materiais que tenham sido instalados nas dependências do CONTRATANTE pela CONTRATADA durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a CONTRATADA arcar com todos os custos referentes ao envio e transporte desses materiais.

5.1.9 Após o encerramento do contrato, caso haja a necessidade expressa pelo CONTRATANTE, a CONTRATADA deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada a prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do CONTRATANTE durante uma eventual transição para os serviços de outra contratada.

5.1.10 Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço será de propriedade do CONTRATANTE, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do CONTRATANTE.

5.1.11 A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

5.1.12 A CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

5.2 ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE

5.2.1 O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de "Firewall" provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do CONTRATANTE e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

5.2.2 Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

5.2.3 Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

5.2.4 O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web.

5.2.5 Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela CONTRATADA.

5.2.6 Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

5.2.7 Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

5.2.8 Os serviços de instalação e implantação da solução serão de responsabilidade da CONTRATADA, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos serviços especificados.

5.2.9 Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

5.2.10 Após a reunião de alinhamento, a CONTRATADA deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do CONTRATANTE.

5.2.11 O CONTRATANTE entregará à CONTRATADA, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de

acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do CONTRATANTE e configurados pela CONTRATADA quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o CONTRATANTE.

5.2.12 O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo appliance e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos appliances que compõem a solução, operando em alta disponibilidade.

5.2.13 Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo appliance, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 deste Termo, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

5.2.14 Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

5.2.15 A solução deve ser capaz de atender às seguintes especificações mínimas dos serviços, a serem ofertados em uma única plataforma:

5.2.15.1 VPN

5.2.15.1.1 Suportar VPN Site-to-Site e Client-To-Site.

5.2.15.1.2 Suportar IPSec VPN.

5.2.15.1.3 Suportar SSL VPN.

5.2.15.1.4 A VPN IPSEc deve suportar 3DES.

5.2.15.1.5 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

5.2.15.1.6 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.2.15.1.7 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

5.2.15.1.8 A VPN IPSEc deve suportar AES 128 e 256 (Advanced Encryption Standard).

5.2.15.1.9 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

5.2.15.1.10 Deverá ser suportado o uso de CA interna e CA externa de terceiros.

5.2.15.1.11 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

5.2.15.1.12 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

5.2.15.1.13 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

5.2.15.1.14 As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

5.2.15.1.15 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

5.2.15.1.16 Atribuição de DNS nos clientes remotos de VPN.

5.2.15.1.17 Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

5.2.15.1.18 Suportar autenticação via AD/LDAP, certificado e base de usuários local.

5.2.15.1.19 Suportar leitura e verificação de CRL (certificate revocation list).

5.2.15.1.20 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

5.2.15.1.21 Deverá manter uma conexão segura com o portal durante a sessão.

5.2.15.1.22 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 ou superior (64 bits) e Mac OS X (v10.14 ou superior).

5.2.15.2 GEOLOCALIZAÇÃO

5.2.15.2.1 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).

5.2.15.2.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.2.15.2.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas que as utilizem.

5.2.15.3 QOS E TRAFFIC SHAPPING

5.2.15.3.1 Suportar a criação de políticas de QoS por endereço de origem, por endereço de destino e por porta.

5.2.15.3.2 QoS deve possibilitar a definição de classes por banda garantida, banda máxima e fila de prioridade.

5.2.15.3.3 Disponibilizar estatísticas RealTime para classes de QoS.

5.2.15.3.4 Deve fazer controle de banda por aplicação, por usuário e por IP.

5.2.15.4 IDENTIFICAÇÃO DE USUÁRIOS

5.2.15.4.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.

5.2.15.4.2 A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários.

5.2.15.4.3 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single signon. Essa funcionalidade não deve possuir limites de usuários ou qualquer tipo de restrição de uso, como a utilização de sistemas virtuais ou segmentos de rede, mas não se limitando a estes.

5.2.15.4.4 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.2.15.4.5 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

5.2.15.4.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.2.15.4.7 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular.

5.2.15.4.8 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

5.2.15.4.9 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupo de usuários do sistema do Active Directory.

5.2.15.5 CONTROLE DE APLICAÇÃO E FILTRO URL

5.2.15.5.1 Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado
horário ou período (dia, mês, ano, dia da semana e hora).

5.2.15.5.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

5.2.15.5.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.

5.2.15.5.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
5.2.15.5.5 Possuir pelo menos 60 categorias de URLs.
5.2.15.5.6 Deve possuir a função de exclusão de URLs do bloqueio, por categoria.
5.2.15.5.7 Permitir a customização de página de bloqueio.
5.2.15.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site).
5.2.15.5.9 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.
5.2.15.5.10 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
5.2.15.5.11 Reconhecer pelo menos 2700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, e-mail e compartilhamento de arquivos.
5.2.15.5.12 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.
5.2.15.5.13 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.
5.2.15.5.14 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária.
5.2.15.5.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.
5.2.15.5.16 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.
5.2.15.5.17 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.
5.2.15.5.18 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação.
5.2.15.5.19 Identificar o uso de táticas evasivas via comunicações criptografadas.
5.2.15.5.20 Atualizar a base de assinaturas de aplicações automaticamente.
5.2.15.5.21 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.
5.2.15.5.22 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.
5.2.15.5.23 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo.
5.2.15.5.24 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
5.2.15.5.25 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
5.2.15.5.26 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

5.2.15.5.27 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, Emule, etc), possuindo granularidade de controle/políticas para cada um deles.
5.2.15.5.28 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (WhatsApp, AIM, Hangouts, Facebook Chat, etc), possuindo granularidade de controle/políticas para cada um deles.
5.2.15.5.29 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.
5.2.15.5.30 Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para cada uma delas.
5.2.15.5.31 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como a tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc).
5.2.15.5.32 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como o nível de risco da aplicação.
5.2.15.5.33 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como a categoria da aplicação.
5.2.15.5.34 Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto.
5.2.15.5.35 Deve possuir categoria específica para classificar domínios recém registrados, com menos de 32 (trinta e dois) dias.
5.2.15.6.36 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução.

5.2.15.6 PREVENÇÃO DE AMEAÇAS COM IPS, ANTIVÍRUS E ANTI-BOT

5.2.15.6.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.
5.2.15.6.2 Deve incluir assinaturas de prevenção de intrusão (IPS).
5.2.15.6.3 Deve incluir assinaturas de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
5.2.15.6.4 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por toda a vigência do contrato.
5.2.15.6.5 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.
5.2.15.6.6 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU ou memória do dispositivo.
5.2.15.6.7 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear.
5.2.15.6.8 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
5.2.15.6.9 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.
5.2.15.6.10 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.
5.2.15.6.11 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
5.2.15.6.12 Deve permitir o bloqueio de vulnerabilidades.
5.2.15.6.13 Deve permitir o bloqueio de exploits conhecidos.
5.2.15.6.14 Deve incluir proteção contra-ataques de negação de serviços.
5.2.15.6.15 Deverá possuir os seguintes mecanismos de inspeção de IPS: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

5.2.15.6.16 Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
5.2.15.6.17 Detectar e bloquear a origem de port scans.
5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos.
5.2.15.6.19 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.
5.2.15.6.20 Possuir assinaturas para bloqueio de ataques de buffer overflow.
5.2.15.6.21 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou antispyware, permitindo a criação de exceções com granularidade nas configurações.
5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.
5.2.15.6.23 Suportar bloqueio de arquivos por tipo.
5.2.15.6.24 Identificar e bloquear comunicação com botnets.
5.2.15.6.25 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.
5.2.15.6.27 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação através da console de gerência centralizada.
5.2.15.6.28 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
5.2.15.6.29 Os eventos devem identificar o país de onde partiu a ameaça.
5.2.15.6.30 A solução deve ter um mecanismo centralizado de correlação e relatório de evento para IPS, Antivírus e Anti-bot.
5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
5.2.15.6.33 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança.
5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox.

5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY

5.2.15.7.1 O relatório das emulações deve apresentar a listagem dos arquivos emulados.
5.2.15.7.2 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks.
5.2.15.7.3 Caso a Prevenção de Ameaças 0-Day seja ofertada no modelo de appliance, o hardware e software fornecido não podem constar, em momento algum durante a vigência do contrato, em listas de end-of-sale, end-ofsupport, end-of engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
5.2.15.7.4 Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS.
5.2.15.7.5 A solução deve ser capaz de inspecionar o tráfego criptografado SSL.
5.2.15.7.6 A solução de Emulação, deve possuir engine onde remove os conteúdos ativos e exploits a partir do documento inspecionado.
5.2.15.7.7 A solução deve possuir engine onde faça Mitigação DNS, sendo ela possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso.

5.2.15.7.8 Implementar e identificar existência de malware em anexos de e-mail e URLs conhecidas.
5.2.15.7.9 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.
5.2.15.7.10 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF.
5.2.15.7.11 A solução deve fornecer a capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, incluindo, no mínimo, as versões de Windows suportadas pela Microsoft.
5.2.15.7.12 A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
5.2.15.7.13 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.
5.2.15.7.14 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.
5.2.15.7.15 Implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle).
5.2.15.7.16 A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP.
5.2.15.7.17 A solução de emulação, deverá suportar a inspeção/bloqueio de malwares em tempo real para determinar o veredito e bloqueio de um malware.
5.2.15.7.18 Implementar atualização a base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização.
5.2.15.7.19 Deve realizar bloqueio de ameaças avançadas de dia zero independente do sistema operacional.
5.2.15.7.20 O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regra individualmente visando otimizar a performance do equipamento.
5.2.15.7.21 A solução deve apresentar informações comportamental incluindo listagem de módulos e processos utilizados pelo malware e/ou código malicioso de forma sequencial.
5.2.15.7.22 Toda análise poderá ser realizada em nuvem, desde que do mesmo fabricante da solução.
5.2.15.7.23 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador para solicitar a análise.
5.2.15.7.24 Todas as máquinas virtuais utilizadas na nuvem do fabricante devem estar integralmente instaladas e licenciadas pelo período do contrato, sem a necessidade de intervenções por parte do administrador do sistema, e, as atualizações deverão ser providas pelo fabricante.
5.2.15.7.25 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.
5.2.15.7.26 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.
5.2.15.7.27 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede, endereço IP.
5.2.15.7.28 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado.
A solução deve suportar a inspeção de, no mínimo, os seguintes tipos de arquivos: CAB, DOC, DOCX, DOCM, DOT, DOTM, DOTX, EXE, HWP, JAR, PDF, PIF, PPAM, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, RAR, RTF, Seven-Z, SLDM, SLDX, SWF, TAR, TGZ, XLA, XLAM, XLL, XLW, XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, ZIP.
5.2.15.7.29 Implementar sincronização de hora através de protocolo NTP.
5.2.15.7.30 A solução, deve emular e eliminar malwares contidos em anexos de e-mail e documentos baixados da web.

5.2.15.7.31 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções e gráfico da taxa de transferência de tráfego monitorado.
5.2.15.7.32 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro.
5.2.15.7.33 A solução deve permitir visualizar a quantidade de arquivos emulados pela solução.
5.2.15.7.34 A solução deve permitir a visualização da fila de arquivos que serão emulados.
5.2.15.7.35 O relatório das emulações deve conter todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos.
5.2.15.7.36 A solução de sandboxing deve possuir mecanismo independente onde sua ação não depende de engines externas como antivírus, anti-malware.
5.2.15.7.37 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados.
5.2.15.7.38 O sistema de emulação deve exibir percentual de arquivos escaneados.
5.2.15.7.39 A solução deve permitir a criação de White list baseado em hash de arquivo.
5.2.15.7.40 A solução deve possuir serviço web online para categorização atualizada de sites e para definições de Widget atualizadas. As respostas recebidas pelo gateway de segurança são armazenadas localmente para otimizar o desempenho. Quando um acesso não puder ser categorizado com os dados armazenados localmente, a solução deve possuir funcionalidade que bloqueia ou permite o tráfego até que a mesma seja classificada.

5.2.15.8 NEXT GENERATION FIREWALL

5.2.15.8.1 Deverá possuir certificação ICSA para Firewall.
5.2.15.8.2 Deve permitir controle de acesso à internet por períodos do dia, mês e ano, permitindo a aplicação de políticas por horários e por dia da semana.
5.2.15.8.3 Deve permitir realizar checagem de regras para conformidade e sombreamento de regras prioritárias top-down.
5.2.15.8.4 Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado.
5.2.15.8.5 O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance.
5.2.15.8.6 Deve suportar atuação como cliente NTP (Network Time Protocol) versões 1, 2, 3 e 4.
5.2.15.8.7 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.
5.2.15.8.8 Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-interfaces lógicas associadas a VLANs.
5.2.15.8.9 A comunicação entre a solução de gerência e os appliances de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada;
5.2.15.8.10 Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos.
5.2.15.8.11 A solução deve permitir que em caso de falha de comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do appliance de segurança.
5.2.15.8.12 Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas e degradação.
5.2.15.8.13 Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário.
5.2.15.8.14 Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP.

5.2.15.8.15 A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: TACACS, RADIUS e certificados digitais.
5.2.15.8.16 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora.
5.2.15.8.17 Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário, roteamento com base em prioridades.
5.2.15.8.18 Deve implementar roteamento multicast (PIM-SM e PIM-DM).
5.2.15.8.19 Possuir funcionalidade de DHCP Relay e DHCP Server.
5.2.15.8.20 Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras.
5.2.15.8.21 Possuir base de regras singular sem separação de regras orientadas à versão de endereço IP utilizada.
5.2.15.8.22 Implementar sub-interfaces ethernet lógicas.
5.2.15.8.23 Deve suportar os seguintes tipos de NAT:
5.2.15.8.23.1 Dinâmico Many-to-1.
5.2.15.8.23.2 Dinâmico Many-to-Many.
5.2.15.8.23.3 Estático 1-to-1.
5.2.15.8.23.4 Estático Many-to-Many.
5.2.15.8.23.5 Estático bidirecional 1-to-1.
5.2.15.8.23.6 NAT de Origem.
5.2.15.8.23.7 NAT de Destino.
5.2.15.8.24 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.
5.2.15.8.25 Deve implementar roteamento estático IPv4 e IPV6.
5.2.15.8.26 Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4.
5.2.15.8.27 Deve permitir a importação , criação e edição de regras SNORT.
5.2.15.8.28 Deve suportar aplicações multimídia como H.323 e SIP.
5.2.15.8.29 Deve permitir o funcionamento em modo transparente tipo "bridge".
5.2.15.8.30 Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing).
5.2.15.8.31 Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.
5.2.15.8.32 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.
5.2.15.8.33 Deve ter a capacidade de inspecionar e bloquear tráfego operando nos modos de camada 2 (L2) e de camada 3 (L3).
5.2.15.8.34 Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações.
5.2.15.8.35 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações.
5.2.15.8.36 Promover a integração com LDAP e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações.
5.2.15.8.37 Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS.
5.2.15.8.38 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.
5.2.15.8.39 A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports".

5.2.15.8.40 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria.
5.2.15.8.41 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora.
5.2.15.8.42 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando alterações simultaneamente.
5.2.15.8.43 Habilidade de realizar upgrade via SCP ou https via interface WEB.
5.2.15.8.44 A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços.
5.2.15.8.45 A solução deverá possuir uma ferramenta onde o fabricante disponibilize HotFixes de segurança e upgrades de versão para instalação simples e com downtime apenas no curto espaço de tempo de reinicialização.
5.2.15.8.46 Suportar a criação de políticas por geolocalização, permitindo que o(s) tráfego(s) de determinado(s) país(es) seja(m) bloqueado(s).
5.2.15.8.47 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
5.2.15.8.48 Deverá suportar controle de política de firewall:
5.2.15.8.48.1 Por zona de segurança.
5.2.15.8.48.2 Por porta e protocolo.
5.2.15.8.48.3 Por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
5.2.15.8.48.4 Por usuários, grupos de usuários, IPs, redes e zonas de segurança.
5.2.15.8.49 Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo, em modo transparente, tanto em Layer 2, como em Layer 3.
5.2.15.8.50 O serviço de alta disponibilidade (HA) deve sincronizar todas as sessões, certificados decriptografados, todas as Associações de Segurança das VPNs e todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS.
5.2.15.8.51 Deve possuir monitoração de falha de link.
5.2.15.8.52 A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces.
5.2.15.8.53 Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante.
5.2.15.8.54 Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). O fluxo mínimo de análise de regras legadas deve trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.
5.2.15.8.55 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
5.2.15.8.56 Deve suportar NAT64 e NAT46.

5.2.15.9 GERÊNCIA

5.2.15.9.1 Deve possuir solução de gerenciamento e administração centralizado possibilitando o gerenciamento de diversos equipamentos de proteção de rede.
5.2.15.9.2 Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a licença de maior capacidade do portfólio ou de capacidade ilimitada.
5.2.15.9.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.
5.2.15.9.4 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
5.2.15.9.5 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

5.2.15.9.6 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS).
5.2.15.9.7 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.
5.2.15.9.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.
5.2.15.9.9 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração.
5.2.15.9.10 Suportar backup das configurações e rollback de configuração para a última configuração salva.
5.2.15.9.11 Suportar validação de regras antes de serem aplicadas.
5.2.15.9.12 Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing).
5.2.15.9.13 Deve permitir a visualização dos logs de uma regra específica em tempo real.
5.2.15.9.14 Deve possibilitar a integração com outras soluções de Gerencamento e Correlação de Eventos de Segurança (SIEM) de mercado desde que não sejam software livre.
5.2.15.9.15 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.
5.2.15.9.16 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti- Malware) e similares.
5.2.15.9.17 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.
5.2.15.9.18 Deve ser possível exportar os logs em CSV.
5.2.15.9.19 Deve possibilitar a geração de relatórios de eventos no formato PDF.
5.2.15.9.20 Deve possibilitar rotação do log.
5.2.15.9.21 Deve suportar geração de relatórios com resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e AntiMalware), de rede vinculadas a este tráfego.
5.2.15.9.22 Deve permitir a criação de relatórios personalizados.
5.2.15.9.23 Suportar enviar os relatórios de forma automática via arquivo em formato PDF.
5.2.15.9.24 A solução de gerência centralizada poderá ser entregue como appliance virtual, devendo ser compatível/homologado para o Acropolis Hypervisor Virtualization and Software - Nutanix. Caso não haja compatibilidade/homologação a CONTRATADA deverá entregar uma infraestrutura de virtualização adequada ou entregar este item da solução na forma de appliance físico.
5.2.15.9.25 Deve consolidar logs e relatórios de todos os dispositivos administrados.
5.2.15.9.26 Deve possuir capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.
5.2.15.9.27 Deverá possuir mecanismo de detalhamento (Drill-Down) para navegação e análise dos logs em tempo real.
5.2.15.9.28 Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso.
5.2.15.9.29 Permitir a customização do padrão regulatório da própria instituição.
5.2.15.9.30 Permitir notificação instantânea ou emissão de relatório sobre mudanças de política de segurança que impactam negativamente a segurança.
5.2.15.9.31 Monitorar constantemente ou realizar emissão de relatório sobre o status de conformidade da solução aos padrões regulatórios informados.

5.2.15.9.32 Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade estabelecidas pelo CONTRATANTE ou de acordo com o padrão estabelecido pelo fabricante.
5.2.15.9.33 Gerar alertas ou emitir relatório de conformidade sobre o impacto de suas decisões na política de segurança trazendo as considerações regulatórias na gestão de segurança estabelecidas pelo CONTRATANTE ou de acordo com o padrão pré-determinado pelo fabricante.
5.2.15.9.34 Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.
5.2.15.9.35 Possuir alertas ou emitir relatório de políticas e as potenciais violações de conformidade.
5.2.15.9.36 Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.
5.2.15.9.37 Gerar relatórios diários com base nas configurações de segurança em tempo real.
5.2.15.9.38 Permitir que os relatórios possam ser salvos, enviados e impressos.
5.2.15.9.39 Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados.
5.2.15.9.40 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.
5.2.15.9.41 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
5.2.15.9.41.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação com principais eventos de segurança de acordo com a funcionalidade selecionada.
5.2.15.9.41.2 A solução deve possuir mecanismo para detectar login de administradores em horários irregulares.
5.2.15.9.41.3 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais.
5.2.15.9.41.4 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.
5.2.15.9.41.5 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius.
5.2.15.9.41.6 Permitir criações de políticas de acesso de usuários autenticada no Active Directory, que reconheçam os usuários de forma transparente.
5.2.15.9.41.7 Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados à solução.
5.2.15.9.41.8 Permitir a visualização de gráficos e mapa de ameaças.
5.2.15.9.41.9 Possuir mecanismo para que logs antigos sejam removidos automaticamente.
5.2.15.9.41.10 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
5.2.15.9.41.11 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.
5.2.15.9.41.12 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real.
5.2.15.9.41.13 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria.
5.2.15.9.41.14 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.
5.2.15.9.41.15 Caso necessite de licenciamento, a solução deverá vir totalmente licenciada para o nível mais alto de uso.

5.2.15.10 CAPACIDADES

5.2.15.10.1 Os valores mínimos e máximos a seguir servirão como margem para a CONTRATADA ofertar equipamentos que tenham capacidade compatível com os requisitos do CONTRATANTE durante o período de vigência do contrato.
5.2.15.10.2 A solução deve ser fornecida com kit para instalação em rack de 19".
5.2.15.10.3 Os equipamentos ofertados na solução deverão ser capazes de operar com todos os recursos habilitados, mantendo os níveis de operação descritos na seção 5.9 - ACORDO DE NÍVEL DE SERVIÇO (SLA), deste Termo de Referência.
5.2.15.10.4 A CONTRATADA deverá fornecer todos os transceivers de 10G SFP+ tanto para a solução de firewall, como para os switchs do CONTRATANTE, bem como os cordões de fibra óptica. Ou seja, todas as portas de comunicação, interfaces e afins, deverão estar habilitadas e operacionais, sem custos adicionais.
5.2.15.10.5 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
5.2.15.10.6 Para dimensionamento adequado da solução, a CONTRATADA deve levar em consideração a "Tabela de Capacidades" a seguir, que demonstra a demanda de recursos atual do CONTRATANTE, na coluna intitulada como "MÍNIMO", e a projeção de crescimento da demanda do CONTRATANTE, na coluna entitulada como "MÁXIMO". Cada conjunto da solução poderá ser entregue contemplando as capacidades mínimas da "Tabela de Capacidades", podendo ser expandida durante toda a vigência do contrato de forma que atenda às demandas dos limites máximos especificados.

Tabela de Capacidades

	DESCRIÇÃO DO REQUISITO	MÍNIMO	MÁXIMO
5.2.15.10.7	Interface 10/100/1000MbitEthernet	08	16
5.2.15.10.8	Interface 10Gbase-F SFP+	02	04
5.2.15.10.9	Interface de gerenciamento dedicada	01	01
5.2.15.10.10	Interface 10/100/1000MbitEthernetBaseTdedicada para alta disponibilidade	01	01
5.2.15.10.11	Interface Console Serial	01	01
5.2.15.10.12	Fonte de alimentação redundante bivolt 100-240 VAC Hot-Swappable	02	02
5.2.15.10.13	Disco de armazenamento de 500GB HDD e/ou 240GB SSD RAID 1	01	02
5.2.15.10.14	Firewalls virtuais	10	20
5.2.15.10.15	Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (emGbps)	05	10
5.2.15.10.16	Throughputde AES-128VPN(emGbps)	04	08
5.2.15.10.17	Throughputcom asfuncionalidadesdeFirewall, controledeAplicação, FiltroURL, IPS, Antivírus, Anti-Bot e controledeameaças avançadashabilitadas(emGbps)	2,5	05
5.2.15.10.18	Conexões simultâneas(em milhões)	02	04
5.2.15.10.19	Novas conexões por segundo(em milhares)	100	180
5.2.15.10.20	Suportar e estar licenciado para acesso remoto Client-to-site (VPN SSL)	200	400

* Baseado em amostras reais, ou seja, não serão aceitos testes usando UDP, HTTP 1M ou testes em laboratório.

5.3 ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO

5.3.1 Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

5.3.2 Deverá ser baseado em Dashboard, para fácil visualização.

5.3.3 Deve ser entregue com regras genéricas criadas pela CONTRATADA, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

5.3.4 O serviço da CONTRATADA deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo CONTRATANTE.

5.3.5 Deve possuir acesso WEB (HTTPS)

5.3.6 Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

5.3.7 Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

5.4 ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

5.4.1 O CONTRATANTE possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.2 O CONTRATANTE possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links "full-route" BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

5.4.3 A CONTRATADA deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

5.4.4 O CONTRATANTE possui infraestrutura hiper convergente, e para tanto usa o Acropolis Hypervisor Virtualization and Software - Nutanix. Assim, caso a CONTRATADA necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do CONTRATANTE.

5.4.5 A CONTRATADA deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

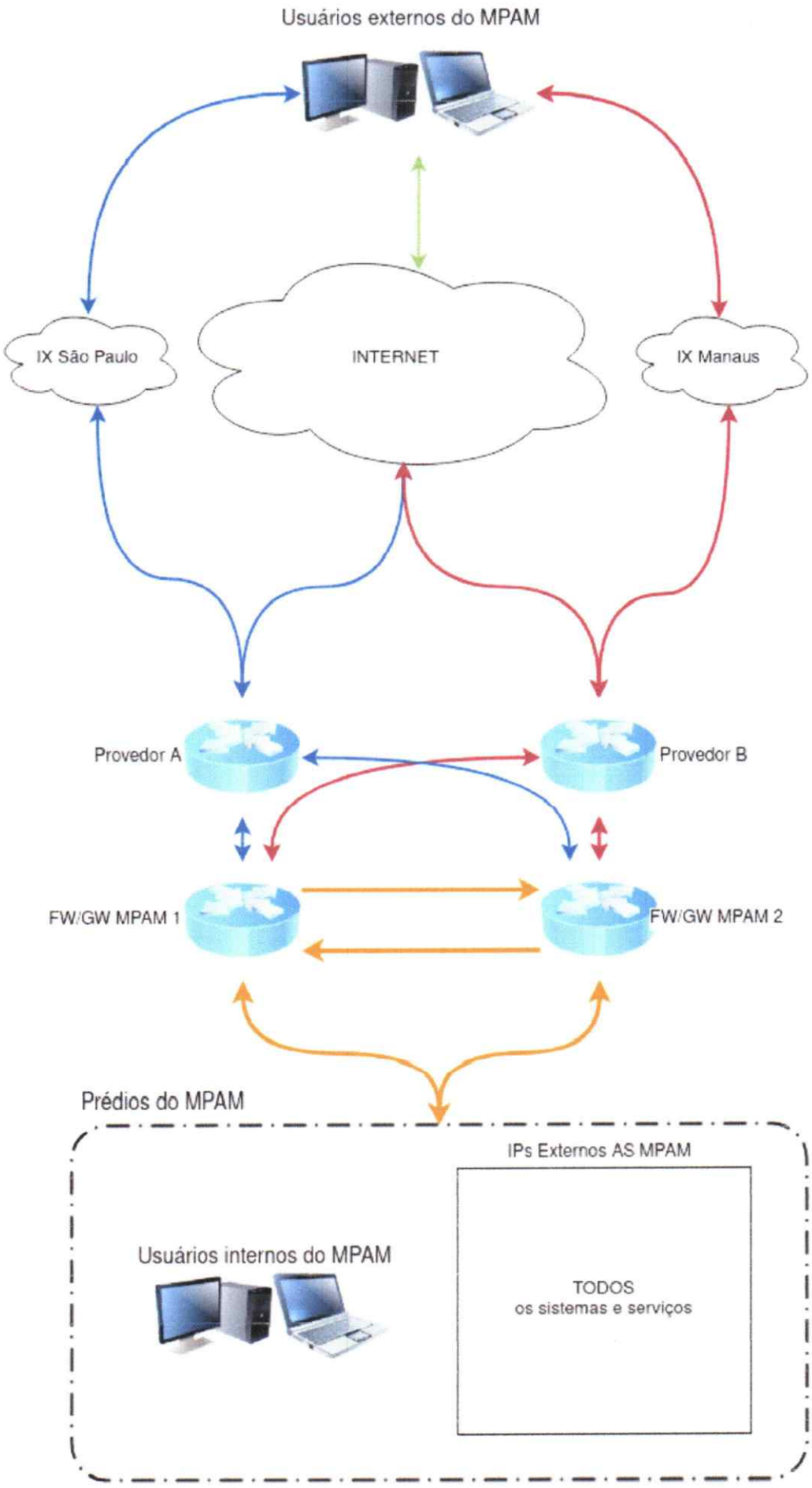
5.4.6 A CONTRATADA deverá finalizar o processo de migração após testes e aprovação pelo CONTRATANTE em até 60 (sessenta) dias após o seu início.

5.4.7 A CONTRATADA deverá evitar, durante o processo de migração, interromper os serviços de rede do CONTRATANTE, nos horários das 8hs às 18hs, em dias de expediente do CONTRATANTE.

5.4.8 É de responsabilidade da CONTRATADA a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do CONTRATANTE fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

5.4.9 A CONTRATADA deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CONTRATANTE, sendo vedada sua cessão, locação ou venda a terceiros.

5.4.10 A topologia da solução deve seguir conforme imagem a seguir:


Usuários externos do MPAM
IX São Paulo
INTERNET
IX Manaus
Provedor A
Provedor B
FW/GW MPAM 1
FW/GW MPAM 2
Prédios do MPAM
IPs Externos AS MPAM
Usuários internos do MPAM
TODOS
os sistemas e serviços

5.5 ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO

5.5.1 A CONTRATADA deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.5.2 A carga horária total para o treinamento deve ser de, no mínimo, 40 horas.

5.5.3 A CONTRATADA deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela FISCALIZAÇÂO.

5.5.4 O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fornecido em português do Brasil ou inglês.

5.5.5 O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do CONTRATANTE.

5.5.6 O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a CONTRATADA deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o CONTRATANTE. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.5.7 A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.5.8 A CONTRATADA deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.5.9 Caso o treinamento seja ofertado de forma presencial, o CONTRATANTE irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do CONTRATANTE.

5.5.10 O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a CONTRATADA deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do CONTRATANTE.

5.5.11 Será de responsabilidade da CONTRATADA prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.5.12 A CONTRATADA deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não

podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.5.13 Os instrutores designados pela CONTRATADA deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.5.14 A CONTRATADA deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.5.15 A CONTRATADA deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do CONTRATANTE e com finalidade de uso exclusivamente interno do CONTRATANTE, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela CONTRATADA.

5.6 SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS

5.6.1 A CONTRATADA deverá disponibilizar ao CONTRATANTE um número telefônico único, um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entendese por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS

5.6.2 No atendimento por meio de telefone a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

5.6.3 O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

5.6.4 Cada chamado deverá conter, no mínimo, as seguintes informações:

5.6.4.1 Número único do registro/ocorrência - a ser fornecido pela CONTRATADA.

5.6.4.2 Identificação do atendente.

5.6.4.3 Identificação do solicitante.

5.6.4.4 Data e hora de abertura do chamado/início da interrupção.

5.6.4.5 Descrição da ocorrência.

5.6.4.6 Designação do equipamento, quando for o caso.

5.6.4.7 Ações corretivas tomadas.

5.6.4.8 Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

5.6.5 O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

5.6.6 O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA.

5.6.7 Não deverá haver qualquer limitação para o número de solicitações de reparo.

5.6.8 O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a CONTRATADA deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

5.7 GARANTIA TÉCNICA

5.7.1 A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

5.7.2 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.
5.7.3 Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.
5.7.4 A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao CONTRATANTE.
5.7.5 Caso sejam detectadas falhas ou bugs nos produtos, a CONTRATADA deverá realizar as atualizações necessárias à correção do problema.
5.7.6 A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.
5.7.7 A CONTRATADA é a única responsável pelos produtos fornecidos ao CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.
5.7.8 A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas
adicionais àqueles apresentados pelo CONTRATANTE, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.
5.7.9 Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à CONTRATADA apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.
5.7.10 Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.
5.7.11 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o CONTRATANTE.
5.7.12 No que se refere a software, durante a vigência do Contrato, a CONTRATADA deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que
venham a substituí-lo no mercado, sem ônus adicional para o CONTRATANTE. Para fins desta especificação técnica, entendese como atualização o provimento de toda e qualquer evolução do produto, incluindo:
5.7.12.1 Patches, fixes, correções, updates e service packs.
5.7.12.2 Novas releases, builds e funcionalidades.
5.7.12.3 O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.
5.7.12.4 O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.
5.7.12.5 Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.
5.7.12.6 A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.
5.7.12.7 A CONTRATADA deverá fornecer tais atualizações independentemente de solicitação expressa do CONTRATANTE.

5.7.12.8 A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

5.7.12.9 As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

5.8 MANUTENÇÃO PREVENTIVA E CORRETIVA

5.8.1 Os serviços de manutenção on-site, serão prestados nas dependências do CONTRATANTE na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

5.8.2 O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do CONTRATANTE, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

5.8.3 A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

5.8.4 A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

5.8.5 Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

5.8.6 A CONTRATADA deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo CONTRATANTE ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser
realizada nas dependências do CONTRATANTE, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

5.8.7 O CONTRATANTE poderá determinar à CONTRATADA a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da CONTRATADA.

5.8.8 Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional ao CONTRATANTE.

5.8.9 A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do CONTRATANTE.

5.8.10 O serviço de suporte deverá ser efetuado on-site sempre que se fizer necessário ou quando for solicitado pelo CONTRATANTE, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o CONTRATANTE.

5.8.11 Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do CONTRATANTE, a CONTRATADA deverá desinstalar, embalar e

transportar o item defeituoso, instalar item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

5.8.12 Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar o CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

5.8.13 A CONTRATADA encaminhará mensagem de e-mail para o CONTRATANTE, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

5.8.14 Todos os custos diretos e indiretos para realização do atendimento presencial (on-site) serão de responsabilidade exclusiva da CONTRATADA.

5.8.15 Dentro do mesmo endereço, a ser executada pela CONTRATADA, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o CONTRATANTE.

5.8.16 Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

5.8.17 O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do CONTRATANTE, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

5.8.18 Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

5.8.19 A CONTRATADA deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da prestação dos serviços. Sempre que houver mudança na equipe técnica da CONTRATADA, deve haver comunicação formal ao CONTRATANTE, incluindo as comprovações exigidas.

5.9 ACORDO DE NÍVEL DE SERVIÇO (SLA)

5.9.1 Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos nesse Termo de Referência.

5.9.2 A CONTRATADA deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

5.9.3 A CONTRATADA deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

5.9.4 A realização de assistência técnica preventiva, caso não seja solicitada pelo CONTRATANTE, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do CONTRATANTE.

5.9.5 Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.6 Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

5.9.7 Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do CONTRATANTE, a solução será considerada como operando em Modo de Contingência.

5.9.8 Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

5.9.9 A CONTRATADA deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual. Este checkup faz parte da manutenção preventiva.
5.9.10 Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.
5.9.11 O Modo de Contingência se caracteriza por:
5.9.11.1 Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.
5.9.11.2 Funcionamento acima dos limiares de desempenho, conforme estabelecido nas cláusulas 5.9.5 e 5.9.6 acima.
5.9.11.3 Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineeringsupport ou end-of-life do fabricante ou fora de garantia.
5.9.11.4 Operação com funcionalidade ou performance abaixo dos mínimos exigidos neste Termo.
5.9.12 Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.
5.9.13 O estado de Inoperância Total se caracteriza por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do CONTRATANTE.
5.9.14 O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela CONTRATADA.

Fortaleza/CE 21 de Fevereiro de 2022.

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ Nº 05.250.796/0001-54
Yure Leopoldo Sabino De Freitas
Diretor Comercial
CPF Nº 525.285.023-20

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMÁTICA LTDA
AV: PONTES VIEIRA Nº 2340
DIONÍSIO TORRES SL 510/514
5º ANDAR CEP: 60.135-238
FORTALEZA CEARÁ

AO
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
PROCURADORIA GERAL DE JUSTIÇA
COMISSÃO PERMANENTE DE LICITAÇÃO – CPL
REF.: PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.015252

DECLARAÇÕES ANEXO III

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no **subitem 5.6**., para os devidos fins elencados no art. 9.º e seus incisos da Lei n.º 8.666/93, e quanto ao fato de que não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;
2. Os documentos e declarações apresentados são fiéis e verdadeiros, bem como que a empresa recebeu o Edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;
3. Estou ciente da obrigação de, caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM**, encaminhar os documentos necessários à CONTRATANTE, a fim de efetuar o referido cadastramento no prazo de cinco dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento apuratório por eventual retardamento da licitação;
4. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

Fortaleza/CE 21 de Fevereiro de 2022.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMÁTICA LTDA
AV: PONTES VIEIRA Nº 2340
DIONÍSIO TORRES SL 510/514
5º ANDAR CEP: 60.135-238
FORTALEZA CEARÁ

YURE LEOPOLDO SABINO DE FREITAS
CPF: 525.285.023-20
DIRETOR COMERCIAL

São Paulo, 18 de Fevereiro de 2022

Ao
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS – MP/AM
Ref.: PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ

DECLARAÇÃO

Declaramos para devidos fins, que a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., inscrita no CNPJ/MF nº 05.250.796/0001-54, situada na Avenida Pontes Vieira, 2340, UNO - MEDICAL & OFFICE - SALA 510 - 514, CEP 60.120-220 - Fortaleza/CE, é um integrador credenciado com a classificação 3 STARS da CHECK POINT SOFTWARE TECHNOLOGIES (BRAZIL) LTDA, inscrita sob CNPJ nº 04.260.390/0001-90, situada na Rua George Ohm, 230, Torre B, Conjunto 174, CEP 04576-020, São Paulo/SP, estando a mesma apta a comercializar, implementar e suportar as soluções desenvolvidas por este fabricante, garantindo assim a qualidade de entrega de nossas soluções.

Sem mais.

LUIZ HENRIQUE RODRIGUES BENTO:29775229804

Assinado de forma digital por LUIZ HENRIQUE RODRIGUES BENTO:29775229804
Dados: 2022.02.18 11:45:19 -03'00'

Luiz Bento
Representante Legal
Check Point Software Technologies

PROCURAÇÃO bastante que faz e assina, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, na forma abaixo:

Saibam quantos este público instrumento virem que, aos 13 (treze) dias do mês de outubro do ano de 2020 (dois mil e vinte), nesta cidade de Fortaleza, Capital do Estado do Ceará, República Federativa do Brasil, na Rua Capitão Melo, nº 3373, bairro Joaquim Távora, onde eu, Gisele Maria Tavares Pordeus de Vasconcelos, escrevente autorizada, vim em diligência, estava o sócio administrador, adiante qualificado, da ora outorgante, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.,** pessoa jurídica de direito privado, que tem o nome de fantasia NETWORK SECURE, com sede nesta Capital, na Rua Capitão Melo, nº 3373, bairro Joaquim Távora, inscrita no CNPJ sob o nº 05.250.796/0001-54, neste ato representada por seu sócio administrador JOSÉ MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado, empresário, nascido no dia 09/07/1981, filho de Jose Murilo Cirino Nogueira e Eluzia Peixoto da Silva, com endereço eletrônico: murilo@networksecure.com.br, residente e domiciliado nesta Capital, na Av. Coronel Miguel Dias, nº 1010, aptº 1301, T-A, bairro Guararapes, portador da CNH nº 1226678851-DETRAN-CE, registro nº 00809571455, emitida no dia 17/12/2015, onde consta a cédula de identidade nº 99010123694-SSP-CE, inscrito no CPF sob o nº 648.711.503-72, o presente reconhecido por mim, pela verificação dos documentos supraexibidos em seus originais, de cuja(s) identidade(s) e capacidade jurídica dou fé. Então pela outorgante NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA., me foi dito, representada como está, que nomeava e constituía seu bastante procurador, **YURE LEOPOLDO SABINO DE FREITAS,** brasileiro, casado, diretor comercial, nascido no dia 06/10/1978, filho de Jose Maria de Freitas e Claudete Sabino Ferreira, com endereço eletrônico: yure.sabino@networksecure.com.br, residente e domiciliado nesta Capital, na Rua Bárbara de Sousa Costa, nº 100, casa 08, bairro Lagoa Redonda, portador da CNH nº 1406940509-DETRAN-CE, registro nº 02054920750, emitida no dia 08/12/2016, onde consta a cédula de identidade nº 559056187-SSP-SP, inscrito no CPF sob o nº 525.285.023-20, a quem confere poderes amplos e ilimitados para praticar todos os atos relativos à contrato em geral, responder a repartições públicas e privadas, licitação, podendo formular ofertas escritas e verbais, negociar preços, assinar documentos de habilitação, atas e instrumentos de compromisso, interpor recursos e renunciar o direito de propô-los, retirar login e senha, preenchendo e assinando todas as formalidades legais para viabilidade do mesmo, praticar todos os demais atos pertinentes ao certame em nome da empresa outorgante, assistir a abertura de propostas, fazer impugnações, reclamações, protestos e recursos, assinar propostas, atas, documentos necessários, fazer novas propostas, rebaixos, descontos, receber em devolução documentos pertencentes a outorgante, assinar contratos, acordar, discordar, desistir de recursos, juntar e retirar documentos, prestar esclarecimentos, informações, assinar requerimentos e petições, podendo tudo requerer e assinar para o bom e fiel cumprimento do presente mandato, o que será dado por bom, firme e valioso e preencher todas as formalidades

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
Fortaleza, CE
16 OUT. 2020
ROBERTO FIUZA MAIA - TABELIÃO
FABRICIO GOULART DE AQUINO - ESC. AUTORIZADO
CLAUDIA CARNEIRO DA SILVA - ESC. AUTORIZADA
CONCEIÇÃO DE MARIA CORREIA MAIA - ESC. SUBST.
MARTHA MARY COSTA RIBEIRO - ESC. AUTORIZADA
3º OFÍCIO DE NOTAS - TABELIONATO PERGENTINO MAIA
Av. Pe. Antônio Tomás, 920 - Aldeota - Fortaleza-CE
Tel.: (85) 3304-9444
SELO DE AUTENTICIDADE
SELO DE AUTENTICIDADE
AUTENTICAÇÃO
N. IH 593185
OCR5

legais, **sendo vedado o substabelecimento. O PRESENTE INSTRUMENTO TEM VALIDADE DE 5 (CINCO) ANOS A CONTAR DESTA DATA. (FEITO SOB MINUTA). OS PODERES AQUI ELENCADOS ESTÃO SUJEITOS À OBSERVÂNCIA DAS RESTRIÇÕES CONTIDAS NO CONTRATO SOCIAL E ADITIVOS DA REFERIDA EMPRESA. O(s) nome(s) e dados do(s) procurador(es) e os elementos relativos ao objeto do presente instrumento foram fornecidos e conferidos pelo(s) outorgante(s), que por eles se responsabiliza(m)**. E como assim o disse, do que dou fé, lavrei este instrumento, que lido e achado conforme, aceita e assina. Eu, (a.) Gisele Maria Tavares Pordeus de Vasconcelos, escrevente autorizada, a lavrei. Eu, Rodrigo de Paula Pessoa Maia, escrevente substituto, a subscrevo. (a.a.) Rodrigo de Paula Pessoa Maia. **JOSÉ MURILO CIRINO NOGUEIRA JUNIOR**. Está conforme o original. Dou fé. Selo nº AAE245133-K2L9, AAE669928-D8I9. Trasladada em seguida. VÁLIDO SOMENTE COM SELO DE AUTENTICIDADE.

Subscrevo e assino

Em testemunho da verdade.

Gisele Maria Tavares Pordeus de Vasconcelos
Escrevente Autorizada

PODER JUDICIÁRIO Estado do Ceará
Selo Tipo 1
REGISTRAL DISTRIBUIÇÃO
Nº AAE669928-D8I9
SELO DIGITAL DE AUTENTICIDADE
Consulte a validade do Selo Digital em selodigital.tjce.jus.br/portal

PODER JUDICIÁRIO Estado do Ceará
Selo Tipo 6
SELO-6
Nº AAE245133-K2L9
SELO DIGITAL DE AUTENTICIDADE
Consulte a validade do Selo Digital em selodigital.tjce.jus.br/portal

CUSTAS E EMOLUMENTOS INCIDENTES

Nº do Atendimento:	100326
Total Emolumentos:	R$ 37,99
Total FERMOJU:	R$ 4,44
Total Selos:	R$ 6,23
Valor Total:	R$ 48,66

Base de Cálculo / Atos com Valor Declarado
Bem/Negócio 1. R$ 0,00

Detalhamento da cobrança / Listagem dos códigos da tabela de emolumentos evolvidos

Códigos: 2003 / 5023

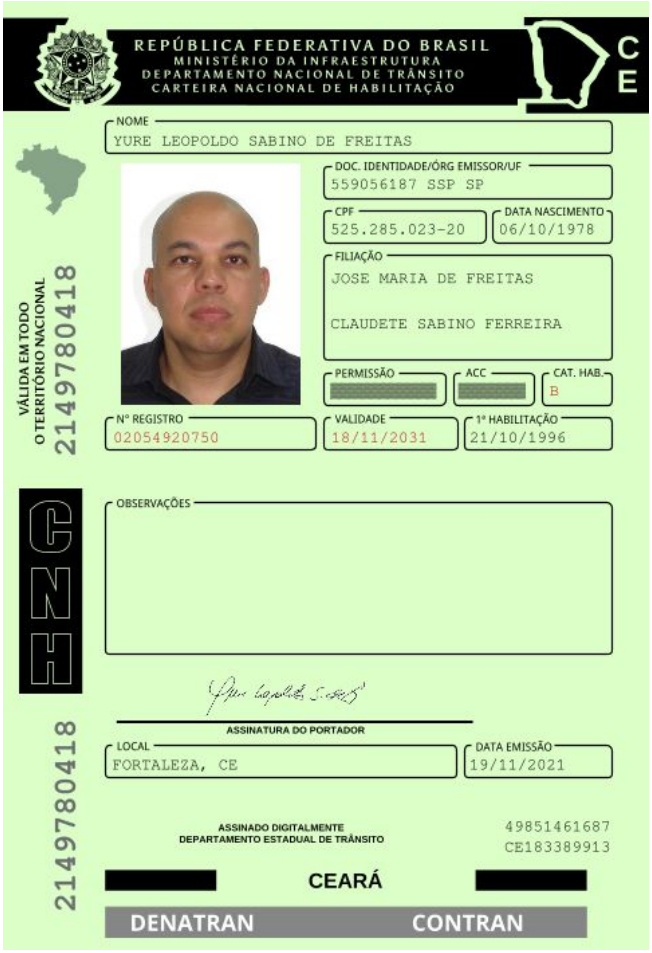
3º OFÍCIO DE NOTAS
Cartório MAIA
Av. Pe. Antônio Tomás, 920
Tel (085) 3304-9444
Aldeota - Fortaleza - CE
USO SOMENTE COM SELO DE AUTENTICIDADE

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
Fortaleza - CE.
16 OUT. 2020
ROBERTO FEIJA MAIA - TABELIÃO
FABRICIO GOMART DE MORAIS - ESC. AUTORIZ.
CLAUDIA CARNEIRO DA SILVA - ESC. AUTORIZ.
CONCEIÇÃO DE MARIA CORRÊA MAIA - ESC. SUBST.
MARIA MARLY MOTA RIBEIRO - ESC. AUTOR.

JHYK 03 AUTENTICAÇÃO N. IH 593192

CNH Digital

Departamento Nacional de Trânsito



QR-CODE

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua validade poderá ser confirmada por meio do programa Assinador Serpro.

As orientações para instalar o Assinador Serpro e realizar a validação do documento digital estão disponíveis em:
< http://www.serpro.gov.br/assinador-digital >, opção Validar Assinatura.

SERPRO / DENATRAN

VÁLIDA EM TODO O TERRITÓRIO NACIONAL

REGISTRO GERAL 96002206506 DATA DE EXPEDIÇÃO 17/03/2014

NOME
ALARICO ISAIAS DE SOUSA GUIMARÃES

FILIAÇÃO
LAWSON RIBEIRO GUIMARÃES
MARIA AMÉLIA DE SOUSA GUIMARÃES

NATURALIDADE
FORTALEZA - CE

DATA DE NASCIMENTO
23/04/1980

DOC. ORIGEM
CERT. CASAMENTO - CARTÓRIO:5 ZONA TERMO:10972 FOLHA:236 V
LIVRO:B-19 FORTALEZA - CE

CPF 620.143.313-91

2 VIA

ASSINATURA DO DIRETOR

P.: 1

LEI Nº 7.116 DE 29/08/83

Certifico que a presente cópia reprostática é a reprodução fiel do original. Dou fé.
Fortaleza - CE, 18 SET. 2015

3º OFÍCIO DE NOTAS
Av. Pe. Antônio Tomás, 920
Tel (85) 3394-9444
Aldeota - Fortaleza-CE
VÁLIDA COM SELO DE AUTENTICIDADE

ROBERTO [illegible] - TABELIÃO
PATRÍCIO [illegible] - ESC. AUTORIZADO
EMANUEL [illegible] - ESC. AUTORIZADO
[illegible] - ESC. AUTORIZADO
ANTÔNIO ALEXANDRE [illegible] - ESC. AUTORIZADO

Selo de Autenticidade
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ
5MQR 03
AUTENTICAÇÃO
Nº GP 175.272

REPÚBLICA FEDERATIVA DO BRASIL
ESTADO DO CEARÁ
SECRETARIA DA SEGURANÇA PÚBLICA E DEFESA SOCIAL
PERÍCIA FORENSE DO ESTADO DO CEARÁ
COORDENADORIA DE IDENTIFICAÇÃO HUMANA E PERÍCIAS BIOMÉTRICAS

Polegar Direito

ASSINATURA DO TITULAR

CARTEIRA DE IDENTIDADE

Selo de Autenticidade
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ
Z3FU 03
AUTENTICAÇÃO
Nº GP 175.273

Certifico que a presente cópia reprostática é a reprodução fiel do original. Dou fé.
Fortaleza - CE, 18 SET. 2015

3º OFÍCIO DE NOTAS
Av. Pe. Antônio Tomás, 920
Tel (85) 3394-9444
Aldeota - Fortaleza-CE
VÁLIDA COM SELO DE AUTENTICIDADE

ROBERTO [illegible] - TABELIÃO
PATRÍCIO [illegible] - ESC. AUTORIZADO
EMANUEL [illegible] - ESC. AUTORIZADO
[illegible] - ESC. AUTORIZADO
ANTÔNIO ALEXANDRE [illegible] - ESC. AUTORIZADO

CNH Digital

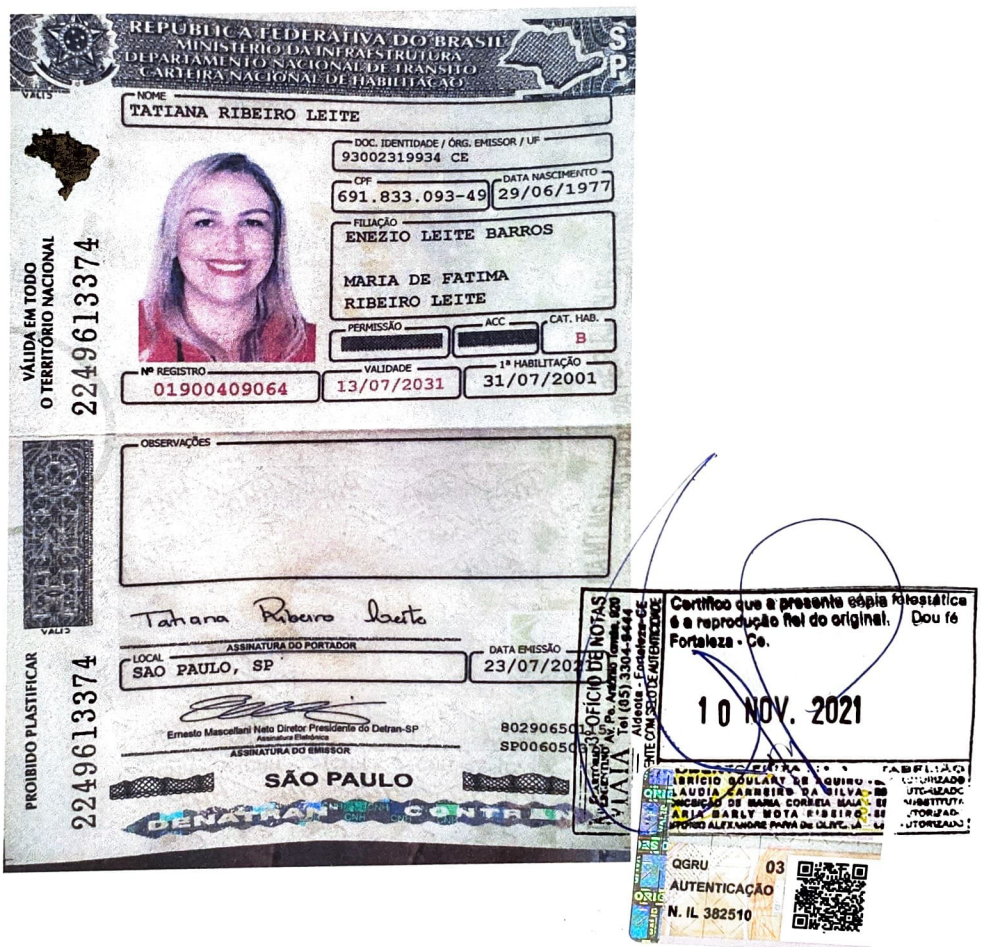
Departamento Nacional de Trânsito

QR-CODE

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua validade poderá ser confirmada por meio do programa Assinador Serpro.

As orientações para instalar o Assinador Serpro e realizar a validação do documento digital estão disponíveis em:
< http://www.serpro.gov.br/assinador-digital >, opção Validar Assinatura.

SERPRO / DENATRAN



REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA INFRAESTRUTURA
DEPARTAMENTO NACIONAL DE TRÂNSITO
CARTEIRA NACIONAL DE HABILITAÇÃO

SP

NOME
TATIANA RIBEIRO LEITE

DOC. IDENTIDADE / ÓRG. EMISSOR / UF
93002319934 CE

CPF
691.833.093-49

DATA NASCIMENTO
29/06/1977

FILIAÇÃO
ENEZIO LEITE BARROS
MARIA DE FATIMA RIBEIRO LEITE

PERMISSÃO

ACC

CAT. HAB.
B

Nº REGISTRO
01900409064

VALIDADE
13/07/2031

1ª HABILITAÇÃO
31/07/2001

VÁLIDA EM TODO O TERRITÓRIO NACIONAL

2249613374

OBSERVAÇÕES

Tatiana Ribeiro Leite
ASSINATURA DO PORTADOR

LOCAL
SAO PAULO, SP

DATA EMISSÃO
23/07/2021

Ernesto Mascellani Neto Diretor Presidente do Detran-SP
Assinatura Eletrônica
ASSINATURA DO EMISSOR

8029065
SP006050

SÃO PAULO

PROIBIDO PLASTIFICAR

2249613374

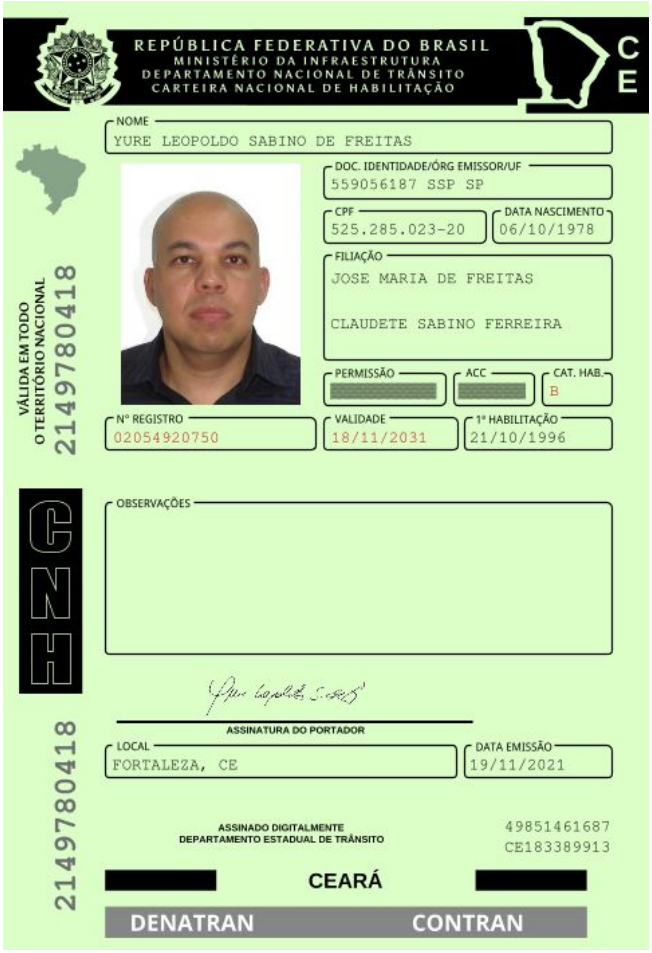
1º OFÍCIO DE NOTAS
Autenticação Digital
Tel (85) 3304-5444
Aldeota - Fortaleza - CE

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé
Fortaleza - Ce.
10 NOV. 2021

QGRU 03
AUTENTICAÇÃO
N. IL 382510

CNH Digital

Departamento Nacional de Trânsito



QR-CODE

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua validade poderá ser confirmada por meio do programa Assinador Serpro.

As orientações para instalar o Assinador Serpro e realizar a validação do documento digital estão disponíveis em:
< http://www.serpro.gov.br/assinador-digital >, opção Validar Assinatura.

SERPRO / DENATRAN

À
Diretoria de Orçamento e Finanças
Procuradoria-Geral de Justiça do Estado do Amazonas
Av. Coronel Teixeira, 7995 – Nova Esperança
69037- 473 MANAUS/AM

A empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, CNPJ nº 05.250.796/0001-54 e endereço na Av. Pontes Vieira, 2340 - Dionísio Torres, UNO - Medical & Office - Sala 510 - 514 - 5º andar - Fortaleza/CE, CEP: 60135-238, solicita a esse Setor o seu cadastro no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE – CADASTRAMENTO DE CREDORES – dessa **SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ.**

Assim sendo, acompanha esta carta de solicitação de cadastramento a documentação abaixo listada, exigida para a efetivação do registro:

a) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

b) Cópia legível do comprovante (por ex: extrato, cópia reprográfica de cartão bancário, etc.) dos seguintes dados bancários:

Banco Bradesco, 237

Agência: 0564-9

Conta: 78934-8

07 de Março de 2022

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMÁTICA LTDA
AV: PONTES VIEIRA Nº 2340
DIONÍSIO TORRES SL 510/514
5º ANDAR CEP: 60.135-238
FORTALEZA CEARÁ

YURE LEOPOLDO SABINO DE FREITAS
CPF: 525.285.023-20
DIRETOR COMERCIAL

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
05.250.796/0001-54 **MATRIZ**		**02/08/2002**

NOME EMPRESARIAL
NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
NETWORK SECURE	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
46.51-6-01 - Comércio atacadista de equipamentos de informática (Dispensada *)

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
46.15-0-00 - Representantes comerciais e agentes do comércio de eletrodomésticos, móveis e artigos de uso doméstico (Dispensada *)
46.18-4-99 - Outros representantes comerciais e agentes do comércio especializado em produtos não especificados anteriormente (Dispensada *)
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis (Dispensada *)
62.04-0-00 - Consultoria em tecnologia da informação (Dispensada *)
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação (Dispensada *)
70.20-4-00 - Atividades de consultoria em gestão empresarial, exceto consultoria técnica específica (Dispensada *)
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios (Dispensada *)
85.99-6-03 - Treinamento em informática (Dispensada *)
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos (Dispensada *)

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV PONTES VIEIRA	**2340**	**SALAS 510 A 514**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
60.135-238	**DIONISIO TORRES**	**FORTALEZA**	**CE**

ENDEREÇO ELETRÔNICO	TELEFONE
ANDREA@NETWORKSECURE.COM.BR	**(85) 3195-2200**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**03/11/2005**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

(*) *A dispensa de alvarás e licenças é direito do empreendedor que atende aos requisitos constantes na Resolução CGSIM nº 51, de 11 de junho de 2019, ou da legislação própria encaminhada ao CGSIM pelos entes federativos, não tendo a Receita Federal qualquer responsabilidade quanto às atividades dispensadas.*

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **24/02/2022** às **09:11:21** (data e hora de Brasília). Página: **1/1**

Comp	Banco	Agência		C1		Conta	DV	C2		Cheque Nº	C3	R$
018	237	0564	9	0	705	078934	8	5	TQ1959	001047	2	
018		0564	9	0	705	078934	8	5	TQ1959	001047	2	

Pague por este cheque a quantia de ________________

________________ e centavos acima

________________ ou à sua ordem

NULO

________________, ______ de ________________ de ______

Bradesco

Banco Bradesco S.A.

ALDEOTA-UFO-CE
AV. SANTOS DUMONT, 2.834

CLIENTE P. JURIDICA

NETWORK SECURE SEGURANCA DA INFORMACAO
CNPJ 05250796/0001-54

Cliente bancario
desde 12/2002

Bradesco

23705642 0180010475 381807893482

VALID 06/2017

Confecção: 08/2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

09 December 2021

MOBILE ACCESS

R80.40

Administration Guide

[Classification: Protected]

STEP UP TO
5TH GENERATION
CYBER SECURITY

Check Point Copyright Notice

Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R80.40
For more about this release, see the R80.40 home page.

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
09 December 2021	Updated *"User Authentication in Mobile Access" on page 158*
21 November 2021	Updated *"Native Applications for Client-Based Access" on page 101*
26 January 2020	First release of this document

Table of Contents

Glossary

A

Administrator
A user with permissions to manage Check Point security products and the network environment.

API
In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components.

Appliance
A physical computer manufactured and distributed by Check Point.

B

Bond
A virtual interface that contains (enslaves) two or more physical interfaces for redundancy and load sharing. The physical interfaces share one IP address and one MAC address. See "Link Aggregation".

Bonding
See "Link Aggregation".

Bridge Mode
A Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

CA
Certificate Authority. Issues certificates to gateways, users, or computers, to identify itself to connecting entities with Distinguished Name, public key, and sometimes IP address. After certificate validation, entities can send encrypted data using the public keys in the certificates.

Certificate
An electronic document that uses a digital signature to bind a cryptographic public key to a specific identity. The identity can be an individual, organization, or software entity. The certificate is used to authenticate one identity to another.

CGNAT
Carrier Grade NAT. Extending the traditional Hide NAT solution, CGNAT uses improved port allocation techniques and a more efficient method for logging. A CGNAT rule defines a range of original source IP addresses and a range of translated IP addresses. Each IP address in the original range is automatically allocated a range of translated source ports, based on the number of original IP addresses and the size of the translated range. CGNAT port allocation is Stateless and is performed during policy installation. See sk120296.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
A Security Gateway that is part of a cluster.

CoreXL
A performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
Also CoreXL FW Instance. On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

D

DAIP Gateway
A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the IP address of the external interface is assigned dynamically by the ISP.

Data Type
A classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

Database
The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

Distributed Deployment
The Check Point Security Gateway and Security Management Server products are deployed on different computers.

Domain
A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

Domain Log Server
A Log Server for a specified Domain, as part of a Multi-Domain Log Server. It stores and processes logs from Security Gateways that are managed by the corresponding Domain Management Server. Acronym: DLS.

E

Expert Mode
The name of the full command line shell that gives full system root permissions in the Check Point Gaia operating system.

External Network
Computers and networks that are outside of the protected network.

External Users
Users defined on external servers. External users are not defined in the Security Management Server database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

F

Firewall
The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restrictive shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for Check Point Gaia operating system.

H

Hotfix
A piece of software installed on top of the current software in order to fix some wrong or undesired behavior.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPv4
Internet Protocol Version 4 (see RFC 791). A 32-bit number - 4 sets of numbers, each set can be from 0 - 255. For example, 192.168.2.1.

IPv6
Internet Protocol Version 6 (see RFC 2460 and RFC 3513). 128-bit number - 8 sets of hexadecimal numbers, each set can be from 0 - ffff. For example, FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF.

L

Link Aggregation
Technology that joins (aggregates) multiple physical interfaces together into one virtual interface, known as a bond interface. Also known as Interface Bonding, or Interface Teaming. This increases throughput beyond what a single connection could sustain, and to provides redundancy in case one of the links should fail.

Log
A record of an action that is done by a Software Blade.

Log Server
A dedicated Check Point computer that runs Check Point software to store and process logs in Security Management Server or Multi-Domain Security Management environment.

M

Management High Availability
Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

Management Interface
Interface on Gaia computer, through which users connect to Portal or CLI. Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member.

Management Server
A Check Point Security Management Server or a Multi-Domain Server.

Multi-Domain Log Server
A computer that runs Check Point software to store and process logs in Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Security Management
A centralized management solution for large-scale, distributed environments with many different Domain networks.

Multi-Domain Server
A computer that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Acronym: MDS.

N

Network Object
Logical representation of every part of corporate topology (physical machine, software component, IP Address range, service, and so on).

O

Open Server
A physical computer manufactured and distributed by a company, other than Check Point.

R

Rule
A set of traffic parameters and other conditions in a Rule Base that cause specified actions to be taken for a communication session.

Rule Base
Also Rulebase. All rules configured in a given Security Policy.

S

SecureXL
Check Point product that accelerates IPv4 and IPv6 traffic. Installed on Security Gateways for significant performance improvements.

Security Gateway
A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

Security Management Server
A computer that runs Check Point software to manage the objects and policies in Check Point environment.

Security Policy
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Single Sign-On
A property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. Acronym: SSO.

SmartConsole
A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

SmartDashboard
A legacy Check Point GUI client used to create and manage the security settings in R77.30 and lower versions.

SmartUpdate
A legacy Check Point GUI client used to manage licenses and contracts.

Software Blade
A software blade is a security solution based on specific business needs. Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

SSO
See "Single Sign-On".

Standalone
A Check Point computer, on which both the Security Gateway and Security Management Server products are installed and configured.

T

Traffic
Flow of data between network devices.

U

Users
Personnel authorized to use network resources and applications.

V

VLAN
Virtual Local Area Network. Open servers or appliances connected to a virtual network, which are not physically connected to the same network.

VLAN Trunk
A connection between two switches that contains multiple VLANs.

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Introduction to Mobile Access

Mobile Access

Check Point Mobile Remote Access VPN Software Blade is the safe and easy solution to connect to corporate applications over the internet with your mobile device or PC. The solution provides enterprise-grade remote access with both Layer 3 VPN and SSL VPN. It gives you simple, safe and secure connectivity to your email, calendar, contacts and corporate applications. At the same time, it protects networks and endpoint computers from threats.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet.

Check Point Mobile Apps enables secure encrypted communication from unmanaged smartphones and tablets to your corporate resources.

Mobile Access Applications

Mobile Access provides the remote user with access to the various corporate applications, including, Web applications, file shares, Citrix services, Web mail, and native applications.

- A Web application is a set of URLs that are used in the same context and that are accessed through a Web browser. For example, an application for inventory management, or HR management.
- A file share is a collection of files, made available across the network through a protocol that enables actions on files, such as opening, reading, writing and deleting files across the network.
- Mobile Access supports Citrix client connectivity to internal XenApp servers.
- Mobile Access supports Web mail services including:
    - Built-in Web mail: Web mail services give users access to corporate mail servers via the browser. Mobile Access provides a front end for any email server that supports the IMAP and SMTP protocols.
    - Other Web-based mail services, such as Outlook Web Access (OWA) and IBM Lotus Domino Web Access (iNotes). Mobile Access relays the session between the client and the OWA server.
- Mobile device support:
    - Access to Web applications.
    - Access to email, calendar, and contacts.
    - Multi-factor authentication.
- Mobile Access supports IPv6 for access to:
    - The Mobile Access Portal.
    - Capsule Workspace.

  Notes:

    - SSL Network Extender is not supported with IPv6.
    - IPv6 is supported for inbound connections to the Security Gateway only. It is not supported for outbound connections from the Security Gateway, even with an external interface.
- SSL Network Extender support for macOS as part of Capsule Workspace Access.
- Mobile Access supports all native applications, through SSL Network Extender. A native application is an IP-based application that is hosted on servers within the organization. When a user is allowed to use a native application, Mobile Access launches SSL Network Extender and allows users to employ native clients to connect to native applications, while ensuring that all traffic is encrypted.

Remote users initiate a standard HTTPS request to the Mobile Access Security Gateway. The Security Gateway authenticates users based on one or more of the configured authentication methods, such as user name and password, certificates, or SecurID. Users have access to applications based on the Mobile Access policy.

For information about Web applications, file shares, Citrix services, Web mail see *"Mobile Access Applications" on page 58*.

For information about native applications, see *"Native Applications for Client-Based Access" on page 101*.

Mobile Access Management

- The Security Management Server that manages all Check Point Security Gateways, also manages Mobile Access Security Gateways.
- Configure Mobile Access from the Mobile Access tab of SmartDashboard and in the Access Control Rule Base.
- Mobile Access users and related network objects are shown in SmartConsole.
- See Mobile Access logs in SmartLog from the SmartConsole **Logs & Monitor** view.
- Mobile Access supports SNMP. See the *R80.40 Gaia Administration Guide* > Chapter *System Management* > Section *SNMP*.

Commonly Used Concepts

This section briefly describes commonly used concepts that you will encounter when dealing with Mobile Access.

Authentication

All remote users that access the Mobile Access Portal must be authenticated by one or more of the supported authentication methods. Multiple login options for users and multi-factor authentication are supported. See *"User Authentication in Mobile Access" on page 158*.

Authorization

Authorization determines how remote users access internal applications on the corporate LAN. If the remote user is not authorized, access to the services provided by the Mobile Access Security Gateway is not granted.

After authentication, the user can open an application based on the Mobile Access policy.

Endpoint Compliance Scanner

The Check Point Endpoint Security on Demand scanner scans the endpoint machine to see if it complies with the endpoint compliance policy. For example, an endpoint compliance policy can make sure that the endpoint clients have updated Anti-Virus signatures and an active Firewall. If the endpoint is compliant with the endpoint compliance policy, the user is allowed to access the portal.

Secure Workspace

End-users can utilize Check Point's proprietary virtual desktop that enables data protection during user-sessions, and enables cache wiping, after the sessions have ended. Secure Workspace protects all session-specific data accumulated on the client side. It uses protected disk space and file encryption to secure files created during the access session. Afterward, it cleans the protected session cache, eliminating any exposure of proprietary data that would have been inadvertently left on public PCs.

Protection Levels

Protection Levels maintain a balance between connectivity and security. The Protection Level is a security requirement that users must meet before they can access the resource. For example, an application can have a Protection Level that requires users to use a specified authentication method. Mobile Access has three pre-defined Protection Levels: Permissive, Normal, and Restrictive. You can edit Protection Level settings, and define new Protection Levels.

Session

After authentication, remote users are assigned a Mobile Access *session*. The session is the period of communication with the Security Gateway until the user logs out or the connection times out.

SSL Network Extender

The SSL Network Extender client makes it possible to access native applications through Mobile Access.

SSL Network Extender is downloaded automatically from the Mobile Access Portal to the endpoint machines, so that client software does not have to be pre-installed and configured on users' PCs and laptops. SSL Network Extender transports application traffic through a secure, encrypted, and authenticated SSL tunnel to the Mobile Access Security Gateway.

Server Side Security Highlights

Mobile Access Gateways are fully integrated with and benefit from the same security features as other Security Gateways. In addition, Mobile Access Gateways have numerous security features to enable secure remote access. These are some of the security features available on Mobile Access Gateways:

- **IPS** - Protects organizations from all known, and most unknown network attacks using intelligent security technology.

  The Web Intelligence component of IPS enables protection against malicious code transferred in Web-related applications: worms, various attacks such as Cross Site Scripting, buffer overflows, SQL injections, Command injections, Directory traversal, and HTTP code inspection.

- **IPS Service** - Downloads new defense mechanisms to the IPS console, and brings existing defense mechanisms up-to-date.

- **Anti-Virus** - Many Anti-Virus settings enabled on the Security Gateway also apply to Mobile Access traffic to prevent virus infection for end users and the enterprise.
- **Granular authorization policy** - Limits which users are granted access to which applications based on: authentication, encryption, and client security requirements.
- **Web Application support over HTTPS** - All traffic to Web-based applications is encrypted with HTTPS. Access is allowed for a specific application set rather than full network-level access.
- **Encryption** - SSL Network Extender, used by Mobile Access, encrypts traffic with the 3DES or the RC4 encryption algorithm.

Client Side Security Highlights

These are some of the security features available on the client side:

- **Endpoint Compliance for Mobile Access on the endpoint machine** - Prevents threats posed by endpoint clients that do not have updated protection, for example, updated Anti-Virus and Firewall *"Endpoint Security on Demand" on page 190*.
- **Secure Workspace protects all session-specific data, accumulated on the client side** - End-users can utilize Check Point's proprietary virtual desktop that prevents data leakage. It encrypts all files and deletes data from the computer at the end of the user session. The administrator can use Protection Levels to force end users to use Secure Workspace to access the user portal or sensitive *"Endpoint Security on Demand" on page 190*.
- **Controls browser caching** - You can disable browser caching or decide which web content can be cached by browsers when users access *"Mobile Access Applications" on page 58*.
- **Captures cookies sent to the remote client by the internal Web server** - In most configurations, Mobile Access captures cookies and keeps them on the Security Gateway. Mobile Access attaches the cookie information, stored on Mobile Access, to the request that Mobile Access makes to the internal Web server to simulate user or web server cookie transmission.
- **Supports multi-factor authentication methods and multiple log-in options** - For example, use SecurID tokens, or SSL client certificates in combination with a one-time DynamicID password.

Check Point Remote Access Solutions

Secure Remote Access

In today's business environment, it is clear that workers require remote access to sensitive information from a variety of locations and a variety of devices. Organizations must also make sure that their corporate network remains safe and that remote access does not become a weak point in their IT security.

Types of Solutions

All of Check Point's Remote Access solutions provide:

- Enterprise-grade, secure connectivity to corporate resources.
- Strong user authentication.
- Granular access control.

Factors to consider when choosing remote access solutions for your organization:

- **Client-Based vs. Clientless** - Does the solution require a Check Point client to be installed on the endpoint computer or is it clientless, for which only a web browser is required. You might need multiple solutions within your organization to meet different needs.
- **Secure Connectivity and Endpoint Security** - Which capabilities does the solution include?
  - **Secure Connectivity** - Traffic is encrypted between the client and VPN Security Gateway. After users authenticate, they can access the corporate resources that are permitted to them in the Access Control Policy. All Check Point solutions supply this.
  - **Endpoint Security** - Endpoint computers are protected at all times, even when there is no connectivity to the corporate network. Some Check Point solutions supply this.

Client-Based vs. Clientless

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. The client supplies access to most types of corporate resources according to the access privileges of the user.
- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

Secure Connectivity and Endpoint Security

You can combine secure connectivity with additional features to protect the network or endpoint computers.

- **Secure Connectivity** - Traffic is encrypted between the client and VPN Security Gateway and strong user authentication is supported. All Check Point solutions supply this.

  These solutions require licenses based on the number of users connected at the same time.

- **Security Verification for Endpoint computers** - Makes sure that devices connecting to the Security Gateway meet security requirements. Endpoint machines that are not compliant with the security policy have limited or no connectivity to corporate resources. Some Check Point solutions supply this.

- **Endpoint Security**:

  - **Desktop Firewall** - Protects endpoint computers at all times with a centrally managed security policy. This is important because remote clients are not in the protected network and traffic to clients is only inspected if you have a Desktop Firewall. Some Check Point solutions supply this

  - **More Endpoint Security Capabilities** - Check Point solutions can include more Endpoint Security capabilities, such as Anti-Malware, disk encryption and more.

  These solutions require licenses based on the number of clients installed.

Remote Access Solution Comparison

Details of the newest version for each client and a link for more information are in sk67820.

SSL VPN Portal and Clients	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6 Support
Capsule Workspace for iOS (previously Mobile Enterprise)	iOS	Client	SSL	✓ Jailbreak & Root Detection MDM Cooperative Enforcement (sk98201)		✓
Capsule Workspace for Android (previously Mobile Enterprise)	Android	Client	SSL	✓ Jailbreak & Root Detection MDM Cooperative Enforcement (sk98201)		✓

Layer 3 VPN Tunnel Clients	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6 Support
Capsule Connect for iOS (previously Mobile VPN)	iOS	Client	IPsec / SSL	MDM Cooperative Enforcement (sk98201)		
Capsule VPN for Android (previously Mobile VPN)	Android	Client	IPsec/SSL	MDM Cooperative Enforcement (sk98201)		
Check Point VPN Plugin for Windows 8.1	Windows 8.1	Pre-installed client	SSL			
Check Point Capsule VPN for Windows 10	Windows 10	Client	SSL			
Check Point Mobile for Windows	Windows	Client	IPsec	✓		

Layer 3 VPN Tunnel Clients Integrated with Endpoint Security	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6 Support
Endpoint Security VPN for Windows	Windows	Client	IPsec	✓	✓	
Endpoint Security VPN for Mac	macOS	Client	IPsec		✓	

Layer 3 VPN Tunnel Clients Integrated with Endpoint Security	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6 Support
Endpoint Security Suite Remote Access VPN Blade	Windows, macOS	Client	IPsec	✓	✓	

Additional Remote Access Solutions	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6 Support
SecuRemote	Windows	Client	IPsec			

Summary of Remote Access Options

Below is a summary of each Remote Access option that Check Point offers. All supply secure remote access to corporate resources, but each has different features and meets different organizational requirements.

Details of the newest version for each client and a link for more information are in sk67820.

Capsule Connect for iOS

Capsule Connect is a full Layer 3 tunnel app that gives users network access to all mobile applications. It supplies secure connectivity and access to all types of corporate resources. It was previously called Mobile VPN.

Required Licenses - Mobile Access Software Blade on the Security Gateway and a mail license on the Security Management Server

Supported Platforms - iOS 6.0 +

Where to Get the Client - Apple App Store

Capsule VPN for Android

Capsule VPN for Android devices is an Layer 3 VPN client. It supplies secure connectivity and access to corporate resources using Layer 3 IPSec/SSL VPN Tunnel. It was previously called Mobile VPN.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Android 4 + (ICS+)

Where to Get the Client - Google Play Store

Check Point VPN Plugin for Windows 8.1

Check Point VPN Plugin for Windows 8.1 is an Layer 3 VPN client. It supplies secure connectivity and access to corporate resources using Layer 3 SSL VPN Tunnel.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Windows 8.1

Where to Get the Client - Pre-installed with Windows.

Check Point Capsule VPN for Windows 10

Check Point Capsule VPN for Windows 10 is an Layer 3 VPN client. It supplies secure connectivity and access to corporate resources using Layer 3 SSL VPN Tunnel.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Windows 10

Where to Get the Client - Microsoft Software & Apps store.

Check Point Mobile for Windows

Check Point Mobile for Windows is an IPsec VPN client. It is best for medium to large enterprises that do not require an Endpoint Security policy.

The client gives computers:

- Secure Connectivity
- Security Verification

Required Licenses - IPsec VPN and Mobile Access Software Blades on the Security Gateway.

Supported Platforms - Windows

Where to Get the Client - Check Point Support Center - sk67820.

Endpoint Security VPN

Endpoint Security VPN is an IPsec VPN client that replaces SecureClient. It is best for medium to large enterprises.

The client gives computers:

- Secure Connectivity
- Security Verification
- Endpoint Security that includes an integrated Desktop Firewall, centrally managed from the Security Management Server.

Required Licenses - The IPsec VPN Software Blade on the Security Gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

Supported Platforms - Windows

Where to Get the Client - Check Point Support Center - sk67820.

Note - Endpoint Security VPN on macOS includes a Desktop Firewall, but not Security Verification.

Endpoint Security VPN for Mac

Endpoint Security VPN combines Remote Access VPN with Endpoint Security in a client that is installed on endpoint computers. It is recommended for managed endpoints that require a simple and transparent remote access experience together with Desktop Firewall rules. It includes:

- Enterprise Grade Remote Access Client that replaces SecureClient for Mac.
- Integrated Desktop Firewall, centrally managed from the Security Management Server.

Required Licenses - The IPsec VPN Software Blade on the Security Gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

Supported Platforms for Users - macOS

Where to Get the Client - Check Point Support Center - sk67820.

Endpoint Security Suite

The Endpoint Security Suite simplifies endpoint security management by unifying all endpoint security capabilities in a single console. Optional Endpoint Security Software Blades include: Firewall, Compliance Full Disk Encryption, Media Encryption & Port Protection, and Anti- Malware & Program Control. As part of this solution, the Remote Access VPN Software Blade provides full, secure IPsec VPN connectivity.

The Endpoint Security suite is best for medium to large enterprises that want to manage the endpoint security of all of their endpoint computers in one unified console.

Required Licenses - Endpoint Security Container and Management licenses and an Endpoint VPN Software Blade on the Security Management Server.

Supported Platforms - Windows, macOS

Where to Get the Client - Check Point Support Center - sk67820.

SecuRemote

SecuRemote is a secure, but limited-function IPsec VPN client. It provides secure connectivity.

Required Licenses - IPsec VPN Software Blade on the Security Gateway. It is a **free** client and does not require additional licenses.

Supported Platforms - Windows

Where to Get the Client - Check Point Support Center - sk67820.

Getting Started with Mobile Access

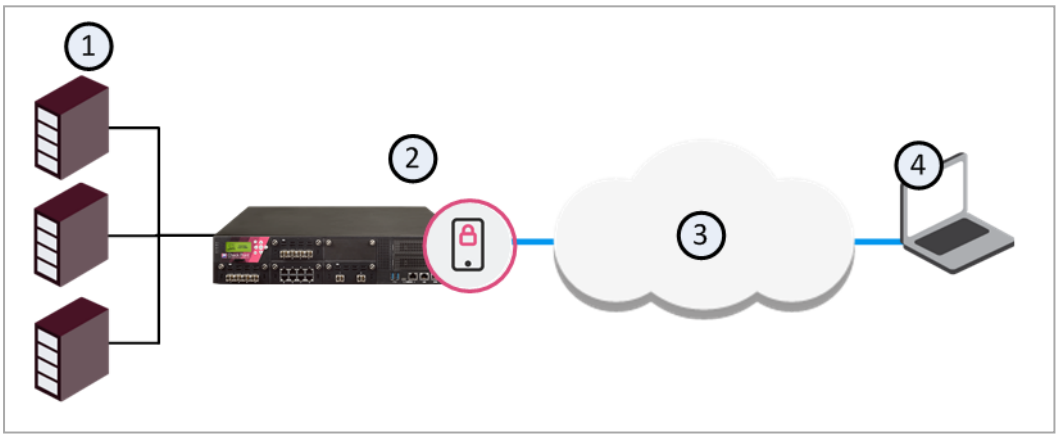
Recommended Deployments

Mobile Access can be deployed in a variety of ways depending on an organization's system architecture and preferences.

Simple Deployment

In the simplest Mobile Access deployment, one Mobile Access enabled Security Gateway inspects all traffic, including all Mobile Access traffic. IPS and Anti-Virus can be active on all traffic as well. The Security Gateway can be on the network perimeter.

This is the recommended deployment. It is also the least expensive and easiest to configure as it only requires one Security Gateway machine for easy and secure remote access.



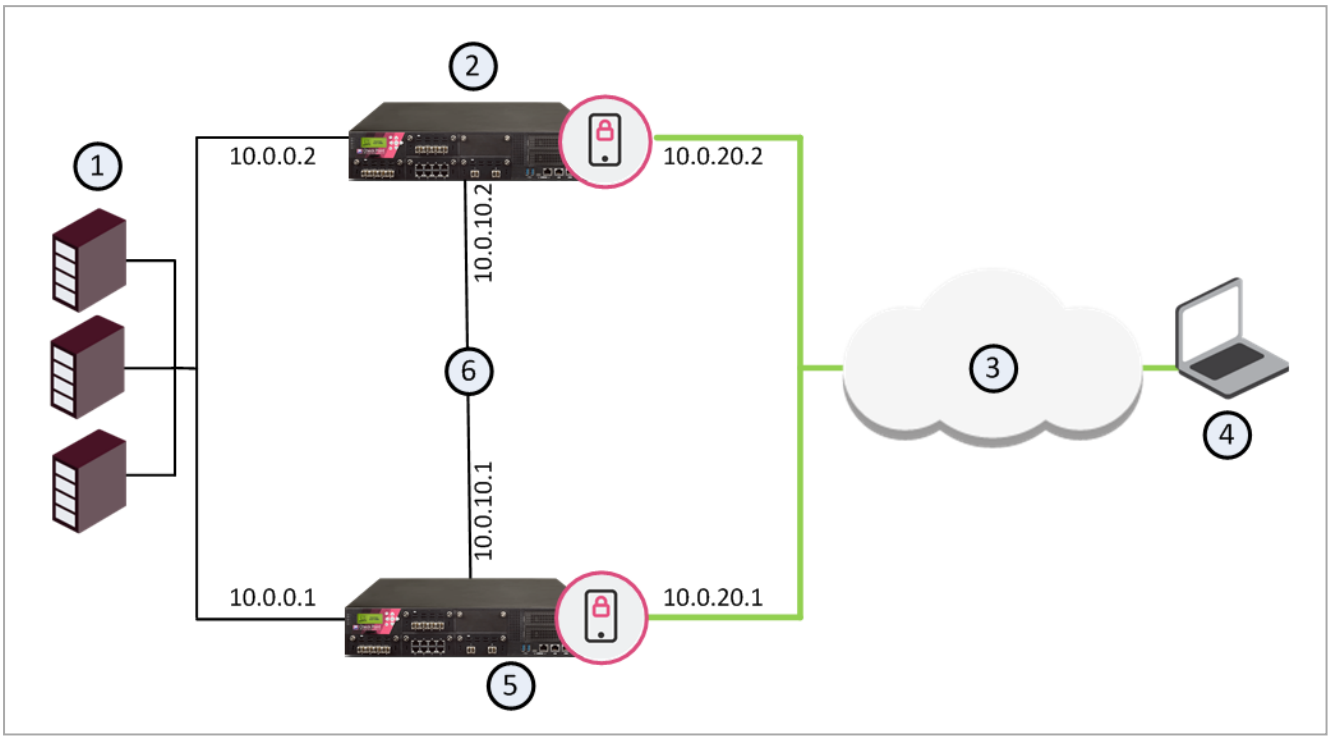
Item	Description
1	Internal servers
2	Security Gateway with Mobile Access enabled
3	SSL Tunnel through Internet
4	Remote User

Deployment in the DMZ

When a Mobile Access enabled Security Gateway is put in the DMZ, traffic initiated both from the Internet and from the LAN to Mobile Access is subject to Firewall restrictions. By deploying Mobile Access in the DMZ, the need to enable direct access from the Internet to the LAN is avoided. Remote users initiate an SSL connection to the Mobile Access Security Gateway. You must configure the Access Control Policy to allow traffic from the user to the Mobile Access server, where SSL termination, IPS and Anti-Virus inspection, authentication, and authorization take place. The Security Gateway forwards requests to the internal servers.

Cluster Deployment

If you have large numbers of concurrent remote access users and continuous, uninterrupted remote access is crucial to your organization, you may choose to have Mobile Access active on a cluster. A cluster can be deployed in any of the deployments described above.



Item	Description
1	Internal servers
2	Mobile Access enabled cluster member B
3	Internet
4	Remote User making SSL connection through Internet
5	Mobile Access enabled cluster member A
6	Secure Network (Sync)

Each cluster member has three interfaces: one data interface leading to the organization, a second interface leading to the internet, and a third for synchronization. Each interface is on a different subnet.

In a simple deployment with the Mobile Access cluster in the DMZ, two interfaces suffice; a data interface leading to the organization and the internet, and a second interface for synchronization.

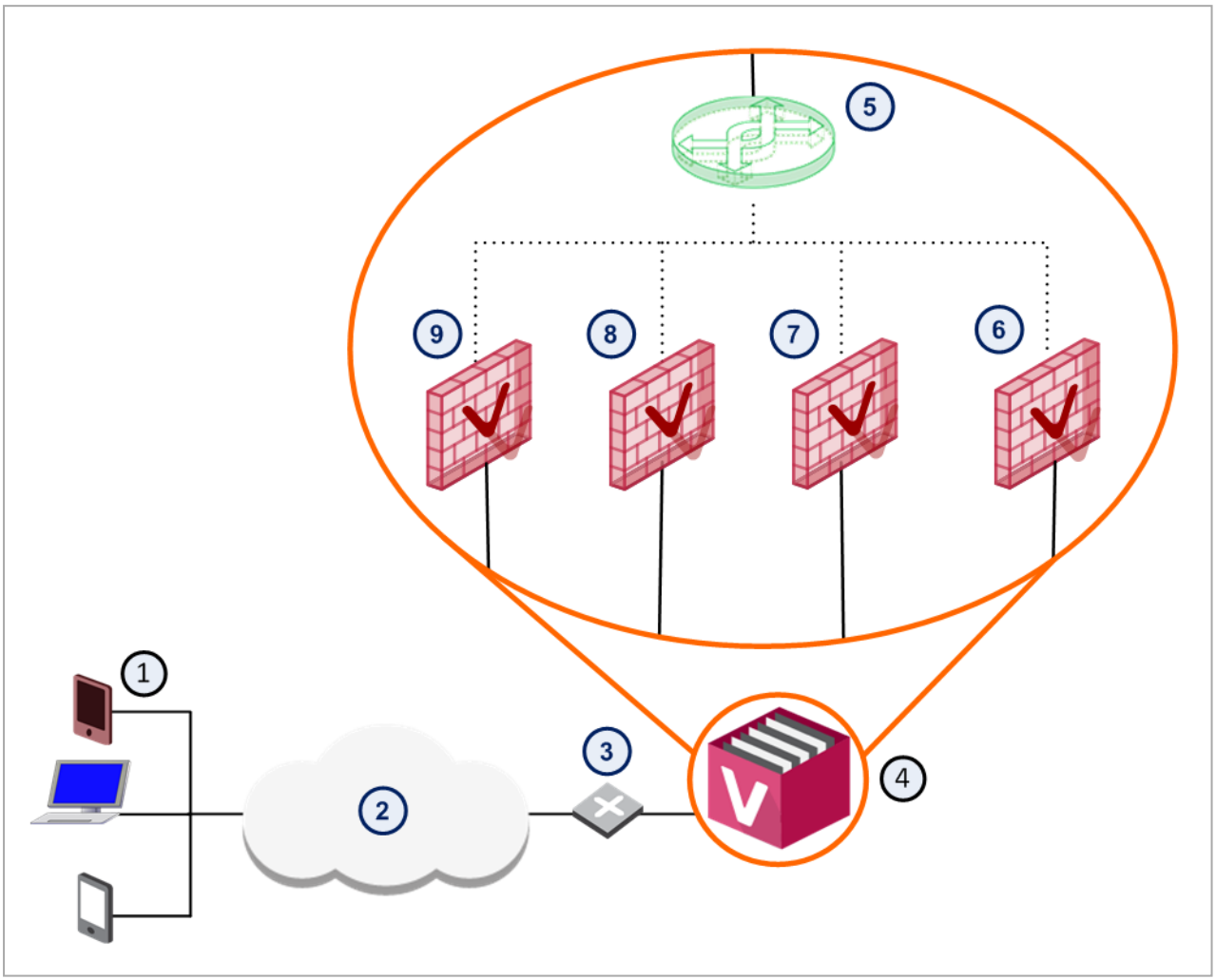
Deployments with VSX

You can enable the Mobile Access Software Blade on VSX Virtual Systems.

This feature is supported in R77.10 and above.

You can use a VSX deployment to support different Mobile Access scenarios. Each Virtual System can have a Mobile Access Portal with different applications, access policies, authentication requirements, and mobile clients.

For example, in the picture below, a VSX Gateway has four Virtual Systems with Mobile Access enabled. Each Virtual System has Mobile Access configured with different settings to meet the company's needs for different users.



Item	Description	Example Mobile Access Portal URL
1	Remote Users	
2	Internet	
3	Router	
4	VSX Gateway	
5	Virtual Switch	
6	Virtual System 4 with Mobile Access enabled	https://guest.company.com/sslvpn
7	Virtual System 3 with Mobile Access enabled	https://finance.company.com/sslvpn

Item	Description	Example Mobile Access Portal URL
8	Virtual System 2 with Mobile Access enabled	https://sales.company.com/sslvpn
9	Virtual System 1 with Mobile Access enabled	https://dev.company.com/sslvpn

This table shows an example of different settings that you can have on each Virtual System.

Virtual System	Users	Clients Allowed	Authentication Schemes	Endpoint Health Checks	Applications Configured
Virtual System 9	Development team	Mobile Access Portal, SSL Network Extender, Capsule Workspace	Certificate + AD Password	Mobile Access Portal ESOD check for company Endpoint Security requirements Jail broken or rooted devices not allowed	Development applications
Virtual System 8	Sales team	Capsule Workspace, Capsule Connect	SecurID + AD password	Jail broken or rooted devices not allowed	Sales applications
Virtual System 7	Finance team	Mobile Access Portal, Capsule Workspace	SecurID + AD password	Cooperative enforcement with company MDM server	Finance applications
Virtual System 6	Contractors	Mobile Access Portal	Certificate that expires after 30 days	Mobile Access Portal ESOD check for commercial AV solution and recent AV signature updates	Contractor internal applications

Deployment as a Reverse Proxy

You can configure a Mobile Access Security Gateway to be a reverse proxy for Web Applications on your servers, using Mobile Access. Reverse Proxy users browse to an address (URL) that is resolved to the Security Gateway IP address. Then the Security Gateway passes the request to an internal server, according to the Reverse Proxy rules. You control the security level (HTTP or HTTPS) of connections between users and resources.

See *"Reverse Proxy" on page 224*.

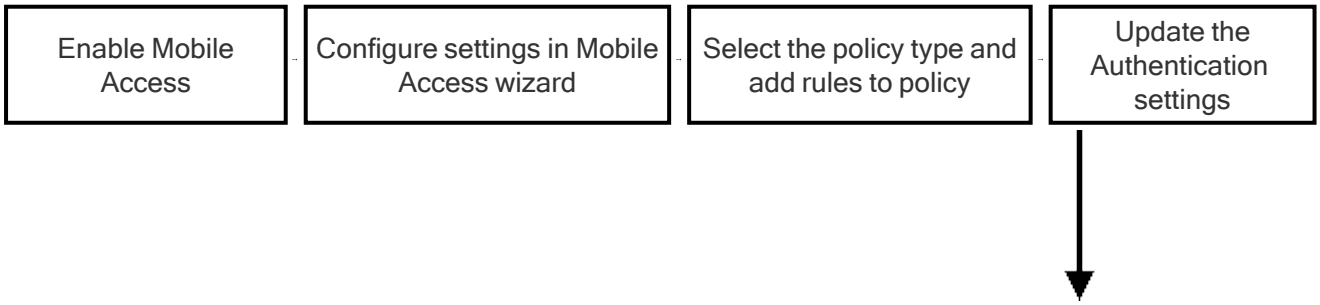
You can also enable Single Sign-on for Capsule Workspace with Capsule Docs users. See the *R80.40 Endpoint Security Server Administration Guide* for details.

Sample Mobile Access Workflow

This is a high-level workflow to configure remote access to Mobile Access applications and resources.

1. Use SmartConsole to enable the Mobile Access Software Blade on the Security Gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
    a. Select mobile clients.
    b. Define the Mobile Access Portal.
    c. Define applications, for example Outlook Web App.
    d. Connect to the AD server for user information.
3. Select the policy type:
    - The default is to use the Legacy Policy, configured in the **Mobile Access** tab in SmartConsole.
    - To include Mobile Access in the **Unified Access Policy**, select this in **Gateway Properties** > **Mobile Access**.
4. Add rules to the Policy:
    - For Legacy Policy: Add rules in SmartConsole. Select **Security Policies** > **Shared Policies** > **Mobile Access** > **Open Mobile Access Policy in SmartConsole**.
    - For Unified Access Policy: Add rules in SmartConsole > **Security Policies Access Control Policy**.
5. Configure the authentication settings in **Gateway Properties** > **Mobile Access** > **Authentication**.
6. Install the Access Control Policy on the Security Gateway.

    Users can access mobile applications through the configured Mobile Access Portal with the defined authentication method.
7. Optional: Give secure access to users through the Capsule Workspace app with certificate authentication.
    a. In the Security Gateway, **Mobile Access** > **Authentication**, click **Settings**, and select **Require client certificate**.
    b. Use the Certificate Creation and Distribution Wizard (in the **Security Policies** view > **Client Certificates** > **New**.
    c. Users download the Capsule Workspace app.
    d. Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.



Users can access internal resources	Users download app, open it, and enter settings	Generate a certificate for the clients	Install the Access Control Policy

Mobile Access Wizard

The Mobile Access Wizard runs when you enable the Mobile Access blade on a Security Gateway. It lets you quickly allow selected remote users access to internal web or mail applications, through a web browser, mobile device, or remote access client.

See *"Check Point Remote Access Solutions" on page 32* to understand more about the remote access clients mentioned in the wizard. Many of the settings in the wizard are also in **Gateway Properties** > **Mobile Access**.

Mobile Access

Select from where users can access the Mobile Access applications:

- **Web** - Through a browser on any computer. SSL Network Extender can be downloaded by users when necessary to access native applications.
- **Mobile Devices** - Through an iOS or Android Mobile device. Devices must have a Check Point app installed.
  - **Capsule Workspace** - Use Check Point Capsule Workspace app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.
- **Desktops/Laptops** - Check Point clients for PCs and Macs that use a Layer 3 tunnel to provide access to internal network resources.

Web Portal

Enter the primary URL for the Mobile Access Portal. The default is the `https://<IP address of the Security Gateway>/sslvpn`. You can use the same IP address for all portals on the Security Gateway with a variation in the path. You can import a p12 certificate for the portal to use for SSL negotiation. All portals on the same IP address use the same certificate.

Applications

Select the applications that will be available to web or mobile device users:

- **Web Applications** - Select the web applications to show on the Mobile Access Portal.
  - **Demo web application (world clock)** - Select while testing Mobile Access, to have a web application show as it will when you are in production.
  - **Custom web application** - Enter the URL of the web application that you want users to be able to open when they connect with Mobile Access. For example, you can set the home page of your intranet site.
- **Mail/Calendar/Contacts** - Enter the Exchange server that mobile devices work with and select which applications mobile device users can access.

- **Mobile Mail**
- **ActiveSync Applications**
- **Outlook Web App**

Active Directory Integration

Select the AD domain, enter your credentials and test connectivity. If you do not use AD, select **I don't want to use active directory now**.

Authorized Users

Select users and groups from Active Directory or internal users. You can also create a test user that will get access to the configured applications.

What's Next?

This window helps you understand steps that are required to complete the automatic configuration done by the Mobile Access wizard. Depending on the selections you made, you might see these steps:

- **Edit the Access Control policy and add a rule for Remote Access Community** - To work with Desktop Remote Access Clients or Capsule Connect clients, the Mobile Access Wizard automatically includes this Security Gateway in the Remote Access VPN community. Remote Access Clients get access rules from the Firewall Rule Base.
- **Install policy on this security gateway** - When you install policy, the changes made by the Mobile Access Wizard become active.
- **Log in to the Web portal (usually https://<ip address>/sslvpn)** - This is the web portal that you configured. Log in to see and use it.

  Each Mobile Access-enabled Security Gateway leads to its own Mobile Access user portal. Remote users log in to the portal using an authentication scheme configured for that Security Gateway.

  Remote users access the portal from a Web browser with `https://<Gateway_IP>/sslvpn`, where *<Gateway_IP>* is one of these:

  - FQDN that resolves to the IP address of the Security Gateway
  - IP address of the Security Gateway

  Remote users that use HTTP are automatically redirected to the portal using HTTPS.

  Note - If Hostname Translation is the method for link translation, **FQDN** is required.

  Set up the URL for the first time in the Mobile Access First Time Wizard.
- **Install Check Point Capsule Workspace App and Desktop VPN client** - Install an App or VPN client to start using it. Prepare for mobile devices and for desktop clients (see the "Preparing for Capsule Workspace" section).
- **Easily deploy client certificates to your users with the new client certificates tool** - If you use authentication with client certificates, configure the client certificates (see the "Managing Client Certificates" section).

Setting up the Mobile Access Portal

Each Mobile Access-enabled Security Gateway leads to its own Mobile Access user portal. Remote users log in to the portal using an authentication scheme configured for that Security Gateway.

Remote users access the portal from a Web browser with `https://<Gateway_IP>/sslvpn`, where *<Gateway_IP>* is one of these:

- FQDN that resolves to the IP address of the Security Gateway
- IP address of the Security Gateway

Remote users that use HTTP are automatically redirected to the portal using HTTPS.

Note - If Hostname Translation is the method for link translation, **FQDN** is required.

Set up the URL for the first time in the Mobile Access First Time Wizard.

Customizing the User Portal

To change the IP address used for the user portal:

From the properties of the Security Gateway object, select **Mobile Access > Portal Settings**.

To configure the look and feel of the portal:

From the properties of the Security Gateway object, select **Mobile Access > Portal Customization**.

Configuring Mobile Access Policy

Users can access Mobile Access applications remotely as defined by the policy rules.

On Security Gateways R80.10 and higher, there are different policy options:

- **Unified Access Policy** - Configure all rules for the Security Gateway in the Unified Access Policy. This option is only available for Security Gateways R80.10 and higher. See *"Mobile Access and the Unified Access Policy" on page 49*.
- **Legacy Policy** - Configure all rules for the Security Gateway in the shared Mobile Access Policy in the SmartDashboard. This option is available for Security Gateways of all versions and is the default for all Security Gateways.

For Security Gateways R77.30 and lower, use the Legacy Mobile Access Policy in the **Policy** page of the **Mobile Access** tab in SmartDashboard.

For all policy types, rules include these elements:

- Users and User Groups - In the Unified Access Policy, these are included in Access Roles.
- Applications that the users can access.
- The Security Gateways, to which the rule applies.

You can also include VPN and Remote Access clients in rules to define which client users can use to access the application.

The Mobile Access policy applies to the Mobile Access Portal and Capsule Workspace. It does not apply to Desktop clients or Capsule Connect.

Settings related to what users can access from mobile devices are also defined in the Mobile Profile: SmartDashboard > **Mobile Access** tab > **Capsule Workspace**.

Including Mobile Access in the Unified Access Policy

To make an R80.x Mobile Access Security Gateway use the Unified Access Policy:

1. In SmartConsole, from the left navigation panel, click **Gateways & Servers** and double-click the Mobile Access Security Gateway object.
2. From the tree, select **Mobile Access**.
3. In the **Policy Source** area, select **Unified Access Policy**.
4. Click **OK**.
5. Install policy.

To create rules for Mobile Access in the Unified Access Policy:

See *"Mobile Access and the Unified Access Policy" on page 49*.

Creating Mobile Access Rules in the Legacy Policy

The order of the rules in the Legacy Policy is not important.

To create rules in the Mobile Access Rule Base:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Policy**.
3. Right-click the rule and select **New Rule > Below**.
4. In the **Users** column, right-click the cell and select **Add Users**.
5. In the User Viewer that opens, you can:
   - Select a user directory, either internal or an Active Directory domain.
   - Search for and select individual users, groups, or branches.
6. In the **Applications** column, right-click the cell and select **Add Applications**.
7. In the Application Viewer that opens, you can:
   - Select an application from the list.
   - Click **New** to define a new application.
8. If you create a New application:
   a. Select the type of application.
   b. In the window that opens enter a **Display Name** to show to end-users. For example,

"Corporate Intranet".

c. Enter the URL or path to access the application according to the example shown.

9. In the **Install On** column, right-click the cell and select **Add Objects** and select the Security Gateways for the rule.
10. Click **Save** and then close SmartDashboard.
11. In SmartConsole, install policy.

Preparing for Capsule Workspace

To enable devices to connect to the Security Gateway with Capsule Workspace:

1. In SmartConsole, enable and configure Mobile Access on the Security Gateway.
2. From the **Gateway Properties**, click **Mobile Access**, and select **Mobile Devices** and **Capsule Workspace**.
3. In **Gateway Properties** > **Mobile Access** > **Authentication**, select how users authenticate to the mobile device.

   If necessary, manage certificates for authentication between the devices and the Security Gateway (see the "Configuring Client Certificates" section).
4. **Optional:** Configure ESOD Bypass for Mobile Applications (see the "ESOD Bypass for Mobile Apps" section).
5. Make sure you have rules in the Access Control Policy that allow traffic for mobile devices. For example, access to Exchange and application servers from the Security Gateway.
6. Download a Capsule Workspace App from the App Store or Google Play to mobile devices.
7. Give users instructions to connect, including the:
   - Site Name
   - Registration key (if you use certificate authentication)

   If you use certificate authentication, we recommend that you include this information in the client certificate distribution email.

Configuring Client Certificates

If you use certificates for mobile and desktop clients, use the **Client Certificates** page in SmartConsole to manage certificates for authentication between the devices and the *"Mobile Access for Smartphones and Tablets" on page 131*.

To configure client certificates:

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. In the **Client Certificates** pane, click **New**.

   The **Certificate Creation and Distribution** wizard opens
3. From the navigation tree click **Client Certificates**.

4. Create and distribute the certificates.
5. Install Policy.

For more details see *"Mobile Access for Smartphones and Tablets" on page 131*.

Mobile Access and the Unified Access Policy

Overview of Mobile Access in the Unified Policy

When you include Mobile Access in the Unified Policy, you configure all rules related to the Mobile Access Portal, Capsule Workspace, and on-demand clients in the Access Control Policy.

In the Access Control Rule Base, you can configure rules that:

- Apply to all Mobile Access Security Gateways, or some of them.
- Apply to one or more Mobile Access clients, such as the Mobile Access Portal or Capsule Workspace.

Mobile Access features such as Protection Levels, Secure Workspace, and Endpoint Compliance also apply.

Note that when you use the **Unified Access Policy**, some Mobile Access features and settings are still configured in the SmartDashboard > **Mobile Access** tab.

Configuring Mobile Access in the Unified Policy

- You can include Mobile Access rules in Policy Layers and Inline Layers. You must enable Mobile Access on each Layer that contains rule with Mobile Access applications.

  See the *R80.40 Security Management Administration Guide* for more about layers.
- To make a Mobile Access application show in the Mobile Access Portal or in Capsule Workspace, you must put the application in the **Services & Applications** column.
  - If you put **Any** in the **Services & Applications** column, the application does not show in the portal but it is allowed. You can open it from the Mobile Access Portal if you manually enter the URL, but not from Capsule Workspace. You can change this behavior. See sk112576 for details.
  - If you put an application's service, such as HTTPS, in the **Services & Applications** column, it does not match Mobile Access https applications.
- In the **Services & Applications** column, you must use Mobile Access Application objects in rules to match Mobile Access traffic. You can define these applications in:
  - In SmartConsole: **CustomApplications/Sites** > **Mobile Access and the Unified Access Policy**
  - In SmartDashboard > **Mobile Access** tab > define an application

  Application objects defined for Application Control, for example, are not supported in Mobile Access rules.
- When you enable Mobile Access on a Security Gateway, the Security Gateway is automatically added to the **RemoteAccess** VPN Community. Include that Community in the **VPN** column of the rule or use **Any** to make the rule apply to Mobile Access Security Gateways. If the Security Gateway was removed from the VPN Community, the **VPN** column must contain **Any**.

- Use Access Roles as the **Source** or **Destination** for a rule to make the rule apply to specified users or networks. You can also use an Access Role to represent Mobile Access or other remote access.

  You must enable Identity Awareness on each Security Gateway that is an installation target for rules with Access Roles.

Creating Mobile Access Rules in the Unified Access Policy

Create Mobile Access rules in the Access Control Policy with these requirements:

Column	Value	Explanation
No	Make sure that the rule position is logical.	The order of rules in the Rule Base is important. The first rule that matches the traffic is enforced.
Name	All	We recommend that you use a descriptive name.
Source	Access Role	Create an Access Role that includes the Users, User Groups, or Mobile/Remote Access Client that the rule applies to. See the "Mobile Access and the Unified Access Policy" section.
Destination	The internal server on which the Mobile Access application is set.	Mobile Access Applications are defined in the **Services & Applications** column.
VPN	**Any** or a Remote Access Community that includes the Mobile Access Security Gateway	When you enable the Mobile Access or IPsec Software Blade on a Security Gateway, the Security Gateway is automatically added to the default **RemoteAccess** VPN Community. By default the community also contains a user group that contains all users. If you remove the Security Gateway from the VPN Community, you must select **Any**.
Services & Applications	Mobile Applications Do not include applications or service objects that are not specified as Mobile Access.	To create a Mobile Application: Click + > click ✳ > **Mobile Applications** > select an application type and define it. To select an existing Mobile Application: Click + > ***All** > **Mobile Applications** and select one. Mobile Applications only show in the list if Mobile Access is enabled on the Layer
Content	**Any**	Content Awareness is not relevant for Mobile Access rules.

Column	Value	Explanation
Action	**Accept** or **Drop**	Only **Accept** and **Drop** are supported. **Reject** is also supported but acts the same as **Drop**. You can also select **Inline Layer** to send all traffic that matches the rule to a "Mobile Access and the Unified Access Policy".
Track	All log options	Right-click in the cell and select **More** > **Extended log**
Install On	One or more Security Gateways	Each Security Gateway must have Mobile Access and Identity Awareness enabled and have **Unified Access Policy** selected as the **Policy Source**.

Mobile Access Applications in the Unified Access Policy

To use a Mobile Access application in the Unified Access Policy, you must define it as a **Mobile Application** from the SmartConsole or define it in the in SmartDashboard > **Mobile Access** tab.

Other application objects, such as URL Filtering applications, are not relevant for Mobile Access. For example: To authorize Facebook as a web application in Mobile Access, you must create a new Web Application and specify Facebook's URL. You cannot use the URL Filtering Facebook application, because it is not for Mobile Access.

Creating Mobile Applications for the Access Control Policy

To create a Mobile Application object to use in the Access Control Policy:

1. In SmartConsole, expand the **Objects** pane.
2. Select **New** > **More** > **Custom Application/Site** > **Mobile Application**.
3. Select a type of Mobile Application.
4. Define the **General Properties** and **Authorized Locations**.
5. Optional: Define more settings for the Application.
6. Click **OK**.

Access Roles for Remote Access

Create a rule in the Access Control Rule Base that handles remote access connections.

1. Go to **Security Policies** and right-click the cell in the VPN column.
2. Select **Specific VPN Communities**.
3. Choose the community and click **+**.
4. Close the VPN community window.
5. Define **Services & Applications** and **Actions** columns.
6. Install the policy.

Example:

To allow remote access users to access the organization's SMTP server, called SMTP_SRV, create the following rule:

Source	Destination	VPN	Service	Action	Track
Any	SMTP_SRV	Remote_Access_Community	SMTP	Accept	Log

Including Mobile Access in the Unified Policy

After you configure rules for Mobile Access in the Unified Access Policy, configure the Security Gateway to use the **Unified Access Policy**.

To make an R80.x Mobile Access Security Gateway use the Unified Access Policy:

1. In SmartConsole, click **Gateways & Servers** and double-click the Mobile Access Security Gateway object.
2. From the tree, select **Mobile Access**.
3. In the **Policy Source** area, select **Unified Access Policy**.
4. Click **OK**.
5. Install policy.

Enabling Access Control Features on a Layer

To enable Mobile Access on an Ordered Layer:

1. In SmartConsole, click **Security Policies**.
2. Under **Access Control**, right-click **Policy** and select **Edit Policy**.
3. Click options  for the Layer.
4. Click **Edit Layer**.

   The **Layer Editor** window opens and shows the **General** view.
5. Select **Mobile Access**.
6. Click **OK**.

To enable Mobile Access on an Inline Layer:

1. In SmartConsole, click **Security Policies**.
2. Select the Ordered Layer.
3. In the parent rule of the Inline Layer, right-click the **Action** column, and select **Inline Layer** > **Edit Layer**.

4. Select **Mobile Access**.
5. Click **OK**.

Best Practices for Mobile Access in the Unified Policy

When you include Mobile Access in the Unified Access Policy, these are some factors that you need to be aware of:

- How to use layers
- How the content of rules affects your policy
- How rule order can affect your policy

Best Practices with Layers

We recommend that you make an Inline Layer for Mobile Access rules, to easily manage the Mobile Access policy.

To use an Inline Layer effectively, define a parent rule in the main layer. The parent rule matches all Mobile Access traffic and sends the traffic to the Inline Layer. It requires an Access Role that includes all Mobile Access client types or traffic in the **Source** column.

When a rule contains **Inline Layer** in the **Action** column, an Inline Layer is automatically created below it and it becomes a parent rule.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Network rules	My_network	GW	Any	Any	Accept	Log
2	Mobile Access Inline Layer Entry Point	All Mobile Access traffic	Any	Any	Any	Mobile Access Inline Layer	Extended Log
2.1	Capsule Workspace rule	Capsule Workspace traffic	Any	Any	Business Mail Corporate Ordering	Accept	Extended Log
2.2	Special access rule	Managers	Any	Any	Internal App	Accept	Extended Log
2.3	Mobile Access Inline Layer Cleanup rule	Any	Any	Any	Any	Drop	Extended Log

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
3	Cleanup rule	Any	Any	Any	Any	Drop	Log

To make a rule that sends all Mobile Access traffic to a Mobile Access Inline Layer:

1. From the **Source** column of a rule in the Access Control Policy, create a new Access Role that includes all Mobile Access client types:
    a. In the New Access Role window, click **Remote Access Clients**.
    b. Select **Specific Client** and create a **New > Allowed Client** for all Mobile Access Portals or clients that are used in your environment. These can include: Capsule Workspace, Mobile Access Portal, ActiveSync, and SSL Network Extender.
2. Make sure the **VPN** column contains **Any** or the **RemoteAccess** VPN Community that contains your Mobile Access Security Gateways.
3. In the **Action** column, select **Inline Layer** > **New Layer**.
4. In the **Layer Editor**:
    - Enter a name for the layer, such as **Mobile Access Inline Layer**.
    - In the **Blades** area, select Mobile Access.
    - Optional: To use this Mobile Access Inline Layer in multiple policies, in the **Sharing** area, click **Multiple policies and rules can use this layer**.

To configure rules in the Inline Layer:

1. Click the **Cleanup** rule in the Inline Layer that was created automatically and the click the **Add Rule Above** icon.
2. Configure rules for the Mobile Access policy as required. See the "Mobile Access and the Unified Access Policy" section.
3. Make sure that the Cleanup rule stays at the end of the layer and that the Action is Drop.
4. Right-click in the **Track** cell and select **More** > **Extended log**.

Mobile Access with Ordered Layers

If you work with Ordered Layers, you can configure a Mobile Access Inline Layer in any Ordered Layer.

Make sure to create a *bypass* rule for Mobile Access traffic in all layers that come before the Mobile Access layer. For example, if your Mobile Access Inline Layer is in the third layer, you must create a bypass rule in the first and second Ordered Layers.

The bypass rule matches the Mobile Access traffic in the layer and allows the traffic. The traffic then moves to the next layer, until it gets to the Mobile Access Inline Layer.

To create a bypass rule, use the Access Role for all Mobile Access users in the **Source** column and **Accept** in the **Action** column.

Best Practices for Rules

- Do not use a Security Gateway as the **Destination** in a Mobile Access rule. The rules authorize a user's access to an internal resource. Use **Any** or the internal hosts of relevant applications in the **Destination** column.
- Do not use **Any** in the **Services & Applications** column. To make an application show in the Mobile Access Portal or Capsule Workspace, it must be Mobile Access application object that is used explicitly in the Rule Base.

  If you do use **Any** to represent all Mobile Access applications, configured Mobile Access applications are authorized, but they do not show in the portal or Capsule Workspace. Users can enter the URL of the App in the **Address** field of the Mobile Access Portal.

  To change the behavior when **Any** is used to represent Mobile Access applications, see sk112576.

Best Practices for Rule Order

In the Unified Access Policy, put Mobile Access rules that authorize applications above rules that contain a related service. For example, put a rule to allow a web application above a rule that allows or blocks HTTP/HTTPS. If the HTTP/HTTPS rule is first, the user will not see the Mobile Access Web application in the portal or in Capsule Workspace and will not be able to access it.

For example, this Rule Base allows Outlook Web Access (OWA), a web-based Mobile Access application. It also allows HTTPS traffic:

Correct way to allow the HTTPS service and also Mobile Access HTTPS applications:

No	Name	Source	Destination	Services & Applications	Action	Track
1	Network rule	My_network	GW_1	Any	Accept	Log
2	Mobile Access Inline Layer	All Mobile Access traffic	Any	Any	Mobile Access Inline Layer	Log
2.1	Mobile Access applications	All Mobile Access traffic	Any	Internal App OWA Business Mail	Accept	Log
2.2	Cleanup rule	Any	Any	Any	Drop	Log
3	Allow HTTPS	Any	Any	https	Accept	Log
4	Cleanup rule	Any	Any	Any	Drop	None

Rule **2.1**, that allows access to Mobile Access applications, including Outlook Web Access (OWA) on HTTPS, is above rule **3**, which allows all HTTPS traffic.

If you put rule **3** to allow HTTPS above the Mobile Access rules, the user will not see the OWA Web application in the portal or in Capsule Workspace and will not be able to access it. To authorize a Mobile Access application, you must use a Mobile Access application in the **Services & Applications** column.

You *can* use HTTPS in the parent rule of the Mobile Access Inline Layer, but specify the Mobile Access application inside the Inline Layer. That way, the HTTPS traffic for OWA, for example, will match on the HTTPS rule, and will also match on the OWA App inside the Inline Layer.

Native Applications

In this scenario with a Native application:

- The Native application is in an Inline Layer in the rule base.
- And the Native application configuration includes **Any** in the **Authorized Locations** tab.

Then the parent rule of the Inline Layer must include one of these in the Services & Applications column:

- **Any** service
- **HTTPS** service
- The Native Application

Mobile Access Behavior in the Rule Base

- In a policy with Policy Layers, for the traffic to be approved, it needs to be accepted in all layers. It is only authorized when accepted in the last layer. The policy keeps going to the next layer until the Mobile Access traffic is matched with a **Drop** rule or it is accepted in all layers.
- In Inline Layers, like in multi-layered policies: Mobile Access is matched on the Inline Layer parent rule and then on the inner rule inside the Inline Layer. The matched application for Mobile Access is taken from the last rule matched with a Mobile Access application. If the matched rule inside the Inline Layer has no Mobile Access application, the policy looks for a Mobile Access application in the parent rule of the Inline Layer.

Limitations for Mobile Access in the Unified Policy

- Mobile Access cannot work with Content Awareness or URL Filtering. Do not use Content Awareness or URL Filtering objects in rules with Mobile Access.
- These limitation apply for Access Roles in Mobile Access rules in the Unified Access Policy:
  - In the **Source** column - Access Roles can include **Networks**, **Users**, and **Remote Access Clients**.
  - In the **Destination** column - Access Roles can include **Networks** and **Users**.
- The Native Applications **Connect** button always shows in the Mobile Access Portal when SSL Network Extender is enabled.
- If users do not meet the defined Protection Level requirements for an application, the application does not show for them. This is true in the Mobile Access Portal and Capsule Workspace. (In the Legacy Mobile Access policy, the applications show but are disabled).
- If the Mobile Access Security Gateway was removed from the **RemoteAccess** VPN Community, the **VPN** column must contain **Any**.

- If you configure Unified Policy, you must include the authorized location (the range of IP addresses) for each application inside the encryption domain for remote access.

Note - The range of IP addresses for an application must not overlap with the range for another application. Users with access to the first application have access to other applications within the same range.

Mobile Access Applications

Introduction to Applications for Clientless Access

Giving remote users access to the internal network exposes the network to external threats. A balance needs to be struck between connectivity and security. In all cases, strict authentication and authorization is needed to ensure that only the right people gain access to the corporate network. Defining an application requires deciding which internal LAN applications to expose to what kind of remote user.

Mobile Access provides the remote user with access to the various corporate applications, including, Web applications, file shares, Citrix services, Web mail, and native applications.

File Shares

A file share is a collection of files, made available across the network by means of a protocol that enables actions on files, including opening, reading, writing, and deleting files across the network.

Configuring File Shares

To create a new File Share Application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > File Share**.

   The **File Share Application** window opens.

File Share Application - General Properties Page

Go to the **General Properties** page of the **File Share Application** object. **Name** is the name of the SmartDashboard object.

File Share Application - Authorized Locations Page

1. Go to the **Authorized Locations** page of the **File Share Application** object.

   This page lets you configure the file shares that users are authorized to access. These settings take effect whenever a user attempts access, no matter what interface is used, whether by manually typing a path in the portal, browsing using the file viewer, clicking a user-defined file favorite, or clicking the predefined file favorite path defined by the administrator in the **Link in Portal** page.
2. Fill in the fields on the page:
   - **Servers** are the machine(s) or DNS Name(s) on which the file server is hosted. Choose either a single **Host or DNS name**, or **Multiple hosts**.

- **Allow access to any file share** gives the users access to all locations on the file server defined in **Servers**.
- **Allow access to specific file shares** restricts user access to specific shares. For example `My_Share`. Use only the name of a share, such as `My_share`, `$$user`, or `My_share$`, without any slashes. Do not specify a sub-directory inside a share. The `$$user` variable represents the name of the currently logged-in user. This variable provides personalized authorization for users. If `$$user` is defined as a file share, then if the user currently logged-in is `alice`, she will be allowed access to the share called `alice` that was defined on the server, such as `\\myserver\alice`.

If you configure two or more overlapping file share applications (for example, one for Any Share and one for a specific share on the same host), the application settings that are in effect are undefined.

File Share Application - Link in Portal Page

This page allows you to configure one predefined favorite link. This link is displayed in the Mobile Access Portal. By clicking the link the user is able to directly access the specified path. Note that you must authorize access to this location in the **Authorized Locations** page.

1. Go to the **Link in Portal** page of the **File Share Application** object.
2. Fill in the fields on the page:
   - **Add a link to this file share in the Mobile Access Portal** - If you do not enter a link, users will be able to access the application by manually typing its link in the portal, but will not have a pre-configured link to access it.
   - **Link text (multi-language)** - Shows in the Mobile Access Portal. It can include `$$user`, which represents the user name of the currently logged-in user. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.
   - **Path** - The full file path that the link will attempt to access, specified using UNC syntax. It can be either a location of a share, or any path under the share. Can include `$$user`, which represents the user name of the currently logged-in user. For example, a path that is defined as `\\host\Pub\users\$$user` appears for user `alice` as `\\host\Pub\users\alice` and for user `Bob` as `\\host\Pub\users\Bob`.

     Note - The `host` defined here is the same host that is defined in the **Authorized Locations** page. The IP address of the host is resolved by the DNS Server that is defined on Mobile Access (not by the Mobile Access management).
   - **Tooltip (multi-language)** - Gives additional information. It can include `$$user`, which represents the user name of the currently logged-in user. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

File Share Application - Single Sign-On Page

To configure Single Sign On:

1. Go to the **Single Sign On** page of the **File Share Application** object.
2. Select **Turn on single Sign On for this application**.
3. Configure the sign on method for the application. The default option is:

   Prompt the users for their credentials and store them for future use

File Share Application - Protection Level Page

1. Go to the **Protection Level** page of the **File Share Application** object.
2. Fill in the fields on the page:

   Security Requirements for Accessing this Application allows you to:

   - Allow access to this application to any endpoint machine that complies with the security requirements of the Security Gateway
   - Make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile

Completing the Configuration of the File Share Application

1. Go to the **Policy** page of the Mobile Access tab.
2. In the **Policy** page, make rules to associate:
   - *User groups*.
   - *Applications* that the users in those user groups are allowed to access.
   - *Install On* are the Mobile Access Security Gateways and Clusters that users in those user groups are allowed to connect to.
3. Click **Save** and then close SmartDashboard.
4. In SmartConsole, install the policy.

Using the $$user Variable in File Shares

You can configure personalized user locations that use the login name of the currently logged in user. To do this, use the Mobile Access Applications wherever you need to specify the name of the user. The `$$user` variable is resolved during the Mobile Access session to the login name of the currently logged-in user.

For example, a UNC file path that is defined as `\\host\Pub\$$user` is resolved for user Alice as `\\host\Pub\Alice` and for user Bob as `\\host\Pub\Bob`.

Protection Levels

Protection Levels are predefined sets of security settings that offer a balance between connectivity and security. Protection Levels allow Mobile Access administrators to define application protections for groups of applications with similar requirements.

Mobile Access comes with three default Protection Levels - Normal, Restrictive, and Permissive. You can create additional Protection Levels and change the protections for existing Protection Levels.

Using Protection Levels

You can include Protection Levels in the definition of most Mobile Access application types. Each application can have a Protection Level associated with it. A single Protection Level can be assigned for all native applications.

When you define an application, in the **Protection Level** page of the application object, you can choose:

Security Requirements for Accessing this Application:

- **This application relies on the security requirements of the gateway**
  Rely on the Security Gateway security requirement. Users who have been authorized to the portal, are authorized to this application. This is the default option.
- **This application has additional security requirements specific to the following protection level**
  Associate the Protection Level with the application. Users are required to be compliant with the security requirement for this application in addition to the requirements of the portal.

Defining Protection Levels

To access the Protection Level page from the Mobile Access tab:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > Protection Levels** page from the navigation tree.
3. Click **New** to create a new Protection Level or double-click an existing Protection Level to modify it.

   The **Protection Levels** window opens, and shows the **General Properties** page.

To access the Protection Level page from a Mobile Access application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E). Or in SmartDashboard, **Mobile Access** tab, go to **Applications** > Application type.
2. Search for the Mobile Access application.
3. Double-click the application.
4. From the navigation tree, select **Additional Setting > Protection Level**.
5. To create a new Protection Level, select **Manage > New**.
6. To edit the settings of a Protection Level, select the Protection Level from the drop down list and then select **Manage > Details**.

   The **Protection Levels** window opens, and shows the **General Properties** page.

To configure the settings for a Protection Level:

1. From the **General Properties** page in the **Protection Level** window, enter the **Name** for the Protection Level (for a new Protection Level only).
2. In the navigation tree, click **Authentication** and select one or more authentication methods from the available choices. Users accessing an application with this Protection Level must use one of the selected authentication schemes.
3. If necessary, select **User must successfully authenticate via SMS**.
4. In the navigation tree, click **Endpoint Security** and select one or both of these options:
   - **Applications using this Protection Level can only be accessed if the endpoint machine complies with the following Endpoint compliance policy**. Also, select a policy. This option gives access to the associated application only if the scanned client computer complies with the selected policy.

- **Applications using this Protection Level can only be accesses from within Secure Workspace**. This option requires Secure Workspace to be running on the client computer.

5. Click **OK** to close the Protection Level window
6. Install the policy.

Web Applications

A Web application can be defined as a set of URLs that are used in the same context and are accessed via a Web browser, for example, inventory management or human resource management.

Mobile Access supports browsing to websites that use HTML and JavaScript.

Browsing to websites with VBScript, Java, or Flash elements that contain embedded links is supported using SSL Network Extender, by defining the application as a native application.

Additionally, some sites will only work through a default browser, and therefore cannot be defined as a Web application. If that is the case, use a native application.

Web Applications of a Specific Type

It is possible to configure a Web Application with a specific type as iNotes (Domino Web Access) application or as an Outlook Web Access application.

iNotes

IBM iNotes (previously called Lotus Domino Web Access) is a Web application that provides access to a number of services including mail, contacts, calendar, scheduling, and collaboration services.

Domino Web Access requires its files to be temporarily cached by the client-side browser. As a result, the endpoint machine browser caching settings of the Mobile Access Protection Level do not apply to these files. To allow connectivity, the cross site scripting, command injection and SQL injection Web Intelligence protections are disabled for Domino Web Access.

Note - To make iNotes work through the Mobile Access Portal, you must work with Mobile Access Applications.

These iNotes features are not supported:

- Working offline
- Notebooks with attachments.
- Color button in the Mail Composition window.
- Text-alignment buttons in the Mail Composition window.
- Decline, Propose new time and Delegate options in meeting notices.
- Online help- partial support is available.

Outlook Web Access

Outlook Web Access (OWA) is a Web-based mail service, with the look, feel and functionality of Microsoft Outlook. Mobile Access supports Outlook Web Access versions 2000, 2003 SP1, 2007, 2010, 2013, and 2016.

Configuring Mobile Applications

You can use SmartConsole to create and configure the settings for all the Mobile Access application objects. However, there are some Mobile Access settings that you can configure only from SmartDashboard.

To create a new Mobile application in SmartDashboard:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartConsole opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Applications**.
3. Click the applicable application category.
4. Click **New**.

To create a new Mobile application in SmartConsole:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New > Custom Application/Site > Mobile Application** and select the Mobile application type.

   The Mobile application window opens.

Web Application - General Properties Page

Use the **General Properties** page to configure the basic settings for the Web Application.

Domino Web Access requires its files to be temporarily cached by the client-side browser. As a result, the endpoint machine browser caching settings of the Mobile Access Endpoint Compliance Profile do not apply to these files.

To allow connectivity, the cross site scripting, command injection and SQL injection Web Intelligence protections are disabled for Domino Web Access.

- **Name** is the name of the application. Note that the name of the application that appears in the user portal is defined in the **Link in Portal** page.
- **This application has a specific type** - Select this option if the Web application is of one of the following types:
  - **Domino Web Access** is a Web application that provides access to a number of services including mail, contacts, calendar, scheduling, and collaboration services.
  - **Outlook Web Access** (OWA) is a Web-based mail service, with the look, feel and functionality of Microsoft Outlook. OWA functionality encompasses basic messaging components such as email, calendaring, and contacts.

Web Application - Authorized Locations Page

Use the **Authorized Locations** page to define the locations that can access the Web Application.

For an application that is defined as an Outlook Web Access application, the following are set as the allowed directories:

- Private Mailboxes: /exchange/
- Graphics and Controls: /exchweb/
- Client access: /owa/
- Public Folders: /public/

When two or more overlapping applications are configured (for example, one for any directory and one for a specific directory on the same host), it is undefined which application settings take effect. If one of the overlapping applications is OWA or iNotes, it will take precedence.

- **Host or DNS name** on which the application is hosted.
- **Allow access to any directory** gives the user access to all locations on the application server defined in **Servers**.
- **Allow access to specific directories** restricts user access to specific directories. For example `/finance/data/`. The pathscan include $$user, which is the name of the currently logged-in user.
- **Application paths are case sensitive** improves security. Use this setting for UNIX-based Web servers that are case sensitive.
- **Services** that are allowed are typically HTTP for cleartext access to the Web application, and HTTPS for SSL access.

  On Security Gateways R77.20 and higher, you can select which SSL version to use with HTTPS. Select an option from the list. The default is **Automatic**.
- **Advanced** lets you select multiple services.

Web Application - Link in Portal Page

Use the **Link in Portal** page to configure a link to the Web Application in the Mobile Access user portal.

- **Add a link to this Web application in the Mobile Access Portal** - If you do not enter a link, users will be able to access the application by typing its URL in the user portal, but will not have a pre-configured link to access it.
- **Link text (multi-language)** - Shows in the Mobile Access Portal. Can include `$$user`, which represents the user name of the currently logged-in user. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.
- **URL** - The link to the location of the application. Can include `$$user`, which represents the user name of the currently logged-in user. For example, a URL that is defined as `http://host/$$user` appears for user `aa` as `http://host/aa` and for user `bb` as `http://host/bb`.
- **Tooltip (multi-language)** - Gives additional information. It can include `$$user`, which represents the user name of the currently logged-in user. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

Web Application - Protection Level Page

Use the **Protection Level** page to choose the protection level for Web applications, and configure how browser caching is configured.

Security Requirements for Accessing this Application:

- **This application relies on the security requirements of the gateway**

  Rely on the Security Gateway security requirement. Users who have been authorized to the portal, are authorized to this application. This is the default option.

- **This application has additional security requirements specific to the following protection level**

  Associate the Protection Level with the application. Users are required to be compliant with the security requirement for this application in addition to the requirements of the portal.

Browser Caching on the Endpoint Machine - Control caching of web application content in the remote user's browser.

- **Allow caching of all content** - Recommended setting for Hostname Translation, method of Link Translation. ActiveX and streaming media will use Hostname Translation.
- **Allow caching of these content types** - Select type of web application content to cache: images, scripts, HTML.
- **Prevent caching of all content** - Improves security for remote users who access a Web Application from a workstation that is not under their full control. Personal data is not stored on the workstation. **Be aware!** This setting prevents files that require an external application (for example, MS Office files) from opening. It can cause some applications to malfunction, if the application requires caching.

Configuring Web Content Caching

Protection Levels let administrators prevent browsers from caching Web content. The caching feature in most browsers presents a security risk because cache contents are easily accessible to hackers.

When the **Prevent caching of all content** option is enabled, users may not be able to open files that require an external viewer application (for example, a Word or PDF file). This requires the user to first save the file locally.

To let users open external files:

1. Set the Protection Level to **Allow caching of all content**.
2. Add Microsoft Office documents to the HTML caching category.
   a. Run: `cvpnstop`
   b. Backup the Apache configuration file: `$CVPNDIR/conf/http.conf`
   c. In this file, uncomment the `CvpnCacheGroups` directives related to Microsoft Office documents.
   d. In cluster setups, repeat these steps for all cluster members.
   e. Run: `cvpnstart`
3. Install Policy.

Web Application - Link Translation Page

Use the **Link Translation** page to configure how the Web Application converts the internal URLs to valid links for the Internet.

- **Use the method specified on the gateway through accessing this application** - Uses the method configured in the: **Additional Settings > Link Translation** page, in the **Link Translation Settings on Gateways** section.
- **Using the following method** - Select the Mobile Access Applications that this application uses:

- **Path Translation** - Default for new installations.
- **URL Translation** - Supported by the Mobile Access Security Gateway with no further configuration
- **Hostname Translation** - Mobile Access Applications.

Using the Login Name of the Currently Logged in User

Mobile Access applications can be configured to differ depending on the user name of the currently logged-in user. For example, portal links can include the name of the user, and a file-share can include the user's home directory. For this purpose, the `$$user` directive is used. During a Mobile Access session, `$$user` resolves to the login name of the currently logged-in user.

For such personalized configurations, insert the `$$user` string into the relevant location in the definitions of Web applications, file shares, and native applications.

For example, a Web application URL that is defined as `http://host/$$user` appears for user `aa` as `http://host/aa` and for user `bb` as `http://host/bb`.

If the user authenticates with a certificate, `$$user` resolves during the user's login process to the user name that is extracted from the certificate and authorized by the directory server.

For its use in configuring File Shares, see the "Mobile Access Applications" section.

Completing the Configuration of the Web Application

To complete the configuration, add the Web application to a policy rule and install policy from SmartConsole.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 49*.

For legacy policy, see *"Getting Started with Mobile Access" on page 38*.

Configuring a Proxy per Web Application

It is possible to define an HTTP or HTTPS proxy server per Web application. This configuration allows additional control of access to Web resources allowed to users. For configuration details see sk34810.

Configuring Mobile Access to Forward Customized HTTP Headers

For proprietary Web applications that do not support a standard HTTP authentication method, the `CvpnAddHeader` directive can be used to forward end-user credentials (user name and IP address) that are carried in the HTTP header.

To configure Mobile Access to automatically forward a customized HTTP header, with a specified value, such as the user name or the client IP address:

1. Edit `$CVPNDIR/conf/http.conf`. For a Mobile Access cluster, edit all members.
2. Add or edit the line containing `CvpnAddHeader` according to the following syntax:

   ```
   CvpnAddHeader "customized_header_name" "customized_header_value"
   ```

You can use the following two macros for the `customized_header_value` string:

- `$CLIENTIP`, which is resolved to the actual IP address of the end-user's client machine.
- `$USER NAME`, which is resolved to the user name entered as a credential in the login page.

Examples:

- `CvpnAddHeader "CustomHTTPHeaderName" "MyCustomHTTPHeaderValue"`
- `CvpnAddHeader "CustomIPHeader" "$CLIENTIP"`
- `CvpnAddHeader "CustomUsernameHeader" "$USER NAME"`

Web Application Features

Mobile Access contains various features to make working with Web Applications efficient and secure. Some of these are described in the following sections.

Reuse TCP Connections

The Reuse TCP Connections feature enhances performance by letting the network reuse TCP connections that would otherwise be closed. To enable Reuse TCP Connections, make a change to the Security Gateway configuration files.

> **Best Practice** - We strongly recommend that you back up configuration files before you make changes.

In the **General Properties** page of a Web application, there is a section called Application Type. In this section, you can define the application as having a specific type, either Domino Web Access or Outlook Web Access.

In previous versions, if you chose one of these Application Type options, the TCP connections for the application are closed after each request. However, if you enable Reuse TCP Connections, the connections are reused. This leads to a boost in performance as the three-way handshake does not have to be renewed and the optimized authorization cache feature can be fully utilized.

By default, Reuse TCP Connections is enabled.

To turn off Reuse TCP Connections:

1. Change this line in the `$CVPNDIR/conf/http.conf` configuration file:

   from:

   ```
   CvpnReuseConnections On
   ```

   to:

   ```
   CvpnReuseConnections Off
   ```

2. Save the changes.
3. Run the `cvpnrestart` command to activate the settings.

If your Mobile Access Security Gateway is part of a cluster, make the same changes on each cluster member.

Website Certificate Verification

Mobile Access lets you validate website security certificates, and either warn the user about problems, ignore any problems, or block websites with certificate problems.

By default, Website Certificate Verification is set to "monitor" this means that a record is entered in SmartLog and there is no effect on end-users. The setting can also be set to "warn" so that users are alerted to any potential security issues and can then decide what steps to take. The setting can also be set to "block," which blocks any website that has a problem with its SSL server certificate, or "ignore", to ignore any issues with a website's security. All settings create a record in SmartLog except for "ignore".

You must restart Mobile Access services after changing the website certificate verification setting.

You can configure Website Certificate Verification per Security Gateway and per application.

Website Certificate Verification is configured in GuiDBedit Tool (see sk13009).

To change the Website Certificate Verification default behavior for Web applications on the Security Gateway:

1. In GuiDBedit Tool, go to the **Network Objects > network_objects** > the Security Gateway object
2. In the bottom pane, go to the **Connectra_settings** section.
3. Search for:

   certificate_verification_policy
4. Enter **block**, **warn**, **monitor**, or **ignore** as the value.

   The default setting is monitor.

If your internal web servers do not use a commonly known certificate (such as an internal CA), then either change the default setting, or add a trusted Certificate Authority for Website certification to Mobile Access.

If the Mobile Access Security Gateway is part of a cluster, be sure to make the same changes on the cluster object table.

To change the Website Certificate Verification default behavior per Web application:

1. In GuiDBedit Tool, go to the **Network Objects > network_objects** > the Web application object
2. In the bottom pane, search for **certificate_verification_policy**.
3. Type **block**, **warn**, or **ignore** as the value.
4. For the **use_gateway_settings** parameter:
   - Enter **true** to use the Security Gateway settings.
   - Enter **false** to use the setting configured for the application.
5. Save the changes in GuiDBedit Tool and close it.
6. Install policy on the Security Management Server.

Adding a Trusted Certificate Authority for Website Certification

You can add specific Certificate Authorities that Mobile Access does not recognize by default, such as your organization's internal CA, to your trusted certificates. The list of default Certificate Authorities recognized by Mobile Access is the same as the list recognized by common browsers. To add CAs to this list, copy the certificate to a `.pem` file and then move the file to your Mobile Access Security Gateway. If your Mobile Access Security Gateway is part of a cluster, be sure to make the same changes on each cluster member.

Saving a Trusted Certificate in .pem Format

The procedure for saving a trusted certificate as a .pem file is similar for all browsers and versions with slight differences. Below is an example procedure, using Internet Explorer 7.0.

To save a trusted certificate in .pem format using Internet Explorer 7.0:

1. Using your browser, **View** the certificate of a website that uses the Certificate Authority you want to add. Be sure to choose the Certificate Authority certificate: In the **Certification Path** tab, choose the CA and click View Certificate.
2. Select the **Details** tab and click **Copy to File**.

   The **Certificate Export Wizard** opens.
3. In the **Export File Format** page, select Base-64 encoded.
4. In the **File to Export** page, type the File name under which you want to save the certificate information with a .pem file extension.
5. Click **Finish**.

Moving the CA Certificate to the Mobile Access Security Gateway

To move the CA Certificate to the Mobile Access Security Gateway:

1. Move the .pem file to your Mobile Access Security Gateway, into a directory called:

   `$CVPNDIR/var/ssl/ca-bundle/`
2. Run the following command: `rehash_ca_bundle`

   The Certificate Authority should now be accepted by the Mobile Access Security Gateway without any warnings. You do not need to restart Mobile Access services for the change to take effect.

Deleting a Certificate Authority from a Trusted List

To delete a Certificate Authority from your trusted Certificate Authorities:

1. Delete the .pem file from the `$CVPNDIR/var/ssl/ca-bundle/` file of the Mobile Access Security Gateway.
2. Run the following command: `rehash_ca_bundle`

   You do not need to restart Mobile Access services for the change to take effect.

Link Translation

Link Translation is the process by which Mobile Access converts internal URLs to public URLs that are valid on the Internet. In this way internal resources become accessible through all internet browsers.

Mobile Access converts HTTP requests into secure HTTPS requests and changes the port to 443. To accomplish this, Mobile Access translates the source URL into an HTTPS URL that routes traffic to its destination through the Mobile Access Security Gateway. The translated URL is returned to the browser and is shown to users.

Mobile Access supports different methods of Link Translation:

- **Path Translation (PT)** - The default method that works with most web applications.
- **URL Translation (UT)** - The original link translation method, maintained for backward compatibility.
- **Hostname Translation (HT)** - This method is faster and supports a wider range of Web applications than PT. It requires additional configuration and a certificate.
- **Client-side Link Translation** - Works on the end user's browser through the Mobile Access browser plugin OR on a Wrapped Mobile application. It translates each request sent through Mobile Access on the client side.

How Translated URLs Appear in a Browser

A translated URL appears to users in their browser differently, for the different Link Translation methods.

Method	Translated `http://www.example.com/path`
UT	`https://ssl.example.com/Web/path,CVPNHost=www.example.com,CVPNProtocol=http`
HT	`https://c-ds1q-itfgppae7oq.ssl.example.com/path` Note that the seemingly random character string, `c-ds1q-itfgppae7oq`, represents the destination URL.
PT	`https://ssl.example.com/PT/http://www.example.com/path`
Client-side	`https://ssl.example.com/PT/http://www.example.com/path`

SmartDashboard Configuration of Link Translation

You can configure Link Translation to meet the requirements of the application (a web application or a Citrix service) or of the Security Gateway through which the applications are accessed. For example, you can configure one Mobile Access application to work with URL Translation, while all other applications supplied by the Security Gateway use Path Translation.

- You can set the default Link Translation method for all applications of a Security Gateway - Only applications that have a different method configured will not use the default method.
- You can set the default Link Translation method for an application - This Web application uses the selected method, even if another method is default on the Security Gateways.
- You can configure which domains are translated.

Configuring PT

Path Translation (PT) is selected by default for newly installed Security Gateways.

To configure PT as default method for Security Gateways:

1. In SmartConsole, right-click the Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Link Translation**.

3. Under **Supported Translation Methods**, make sure that **Path Translation (always supported)** is selected.
4. Under **Default Translation Method**, select **Path Translation**.
5. Click **OK**.

To configure PT as default method for an application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The Web Application window opens.
4. Click **Additional Settings > Link Translation**.

   The **Link Translation** page of the Mobile Access application opens.
5. Select **Use the following method > Path Translation**.
6. Click **OK** and close the Web Application window
7. Install the policy.

Configuring UT

URL Translation is supported by all versions of Security Gateways.

To configure UT as default method for Security Gateways:

1. In SmartConsole, right-click the Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Link Translation**.
3. Under **Supported Translation Methods**, make sure that **URL Translation (always supported)** is selected.
4. Under **Default Translation Method**, select **URL Translation**.
5. Click **OK**.

To configure UT as default method for an application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The **Web Application** window opens.
4. Click **Additional Settings > Link Translation**.

   The **Link Translation** page of the Mobile Access application opens.
5. Click **URL Translation**.

6. Click **OK**.
7. Install the policy.

Using Hostname Translation

Hostname Translation enhances security by replacing the destination host name with a seemingly random character string in the URL, as it appears in the client browser.

You must configure the DNS server to resolve wildcard hostnames, to enable HT.

Important - If the DNS server is not configured to resolve wildcard Mobile Access host names, users will be unable to connect to Mobile Access, because the portal changes to a sub-domain: `portal.ssl.example.com`.
If you use Hostname Translation as your method for link translation, users must enter an FQDN as the portal URL and not an IP address.

Configuring HT

To configure the DNS server for HT:

1. Add a record to the DNS server, to resolve Mobile Access sub-domains to the Mobile Access IP address: `*.domain`

   For example, assume `ssl.example.com` is the Security Gateway. Configure the DNS to resolve `*.ssl.example.com` to the Security Gateway IP address. This wildcard includes all sub-domains of the parent domain, such as `a.ssl.example.com` and `b.ssl.example.com`.
2. Define the parent domain (`ssl.example.com`) as a separate DNS record, to resolve Mobile Access IP address.

   This lets users access the Mobile Access Portal directly, with its FQDN.
3. *"Server Certificates" on page 232*.

To configure HT as default method for Security Gateways:

1. In SmartConsole, right-click the Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.

   If this message appears, clear **Hostname Translation**, for now:

   ```
   Hostname Translation requires Portal URL to be defined in the following
   format: 'https://hostname/'
   ```
3. In **Main URL**, enter the portal URL of the Mobile Access Security Gateway.
4. From the navigation tree, click **Link Translation**.
5. Under **Supported Translation Methods**, click **Hostname Translation**.
6. Under **Default Translation Method**, select **Hostname Translation**.
7. Click **OK**.
8. Install the policy.

To configure HT as default method for an application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The **Web Application** window opens.
4. Click **Additional Settings > Link Translation**.

   The **Link Translation** page of the Mobile Access application opens.
5. Select **Use the following method > Hostname Translation**.
6. Click **Advanced Hostname Translation Settings**.
7. Select the **HTTP Cookies Handling** mode:
   - **On the gateway** - Default. All HTTP cookies that are sent to clients by internal Web servers are stored on Mobile Access, and are not passed on to the client's browser.
   - **On the endpoint machine** - If the default setting causes the JavaScript (from the internal servers that run on the client browser) that handles HTTP cookies to fail, select this option. Mobile Access passes HTTP cookies to the browser.
8. Click **OK** and close the Web Application window.
9. Install the policy.

Configuring Link Translation Domains in SmartDashboard

A Link Translation domain for Web applications:

- Improves connectivity to external sites. For example, links to external sites displayed in emails are not broken, because they are not translated by Mobile Access.
- Reduces the load on the Mobile Access machine, thereby increasing performance.
- Saves the administrator the trouble of defining all external content as Web applications.

Configure which domains use link translation in SmartDashboard > **Mobile Access** tab > **Additional Settings** > **Link Translation > Link Translation Domains**.

For Security Gateways R77.30, to enable this feature, you must install the R77.30 Add-on.

This option is not supported in Security Gateways lower than R77.30.

To manually configure domains to translate:

1. In the **Mobile Access** tab > **Additional Settings** > **Link Translation > Link Translation Domains** area, select **Manually configure domains to translate**.
2. Click **Add Domain** to add a whole domain or host (URL) to be translated.
3. Click **Add Exception** to configure a part of a domain or host within a domain that will not be translated.
4. Install policy.

Link Translation Domains

The options are:

- **Translate all domains** - This is the default behavior. Link translation is active for all traffic.
- **Manually configure domains to translate** - Add internal domains to the list. Only domains on the list are translated. You can also add exceptions from within a domain. We recommend that you use this setting to improve performance. To keep communication secure, make sure all internal domains are on the list.
- **Do not translate any domain** - This is relevant for companies that do not have internal domains.

Link Translation with Wrapped Applications

With *Client-Side Link Translation with wrapped applications*, Check Point Mobile App clients are responsible for link translation for specified, *wrapped applications*. These applications are *wrapped* in a security container that gives them secure access to network resources and prevents data leakage.

Wrapped applications are only available with mobile devices and do not show in the Mobile Access Portal.

To use Client-Side Link Translation with wrapped applications, see the App Wrapping Guide.

Link Translation Issues

These Link Translation configuration tips apply to Web applications.

- For Web sites that use ActiveX and streaming media, configure Mobile Access Web applications to Allow caching of all content. This is configured in the **Protection Level** page of the Web application.
- Domain cookies created in JavaScript are not supported. For example, if you create a cookie with this JavaScript code:

  document.cookie=Name=Value; domain=.example.com,

  The client browser cannot send the cookie to Mobile Access and the Web server if Mobile Access is not located under the domain .example.com.

  Note that domain cookies created in HTTP headers are supported, if they are not manipulated by JavaScript code.
- With Hostname Translation, the URL shown in the client browser is:

  `https://<Obscured Destination Host Name>.<Mobile Access FQDN>/path`

  The maximum number of characters in each part of the host name (between https:// and the /path) is limited to 63 (see RFC 1034). Therefore, the entire internal host name, including the protocol and the port, Mobile Access Applications.
- Hostnames displayed in client browsers appear as a seemingly random character string, instead of the complete destination path.
- If you sign out from Outlook Web Access, Domino Web Access (iNotes), or Microsoft SharePoint, the Mobile Access session can become disconnected.

Citrix Services

Citrix Deployments Modes - Unticketed and Ticketed

Unticketed Mode

In the recommended Unticketed Mode scenario:

- The remote access user logs into the Mobile Access user portal
- Using the Mobile Access Web interface, the user is directed to the Citrix Web Interface server and then has access to the Presentation server.

Ticketed Mode

In the Ticketed Mode scenario:

- The remote access user logs into the Mobile Access user portal.
- Using the Mobile Access Web interface, the user is directed to the Citrix Web Interface server.

The user logs into the Citrix Web Interface server and is assigned a secure ticket by the Secure Ticket Authority. This ticket allows the user to access the Presentation server once it is verified by the Mobile Access Web Security Gateway.

You do not need to use Secure Ticketing authority (STA) servers because Mobile Access implements its own STA engine.

Configuring Citrix Services

To configure a new Citrix Service:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Citrix Services**.

   The **Citrix Services** window opens.

Before Configuring Citrix Services

The server certificate for Mobile Access must be based on a FQDN (Fully Qualified Domain Name) and issued to the Mobile Access FQDN. For example www.sample.com.

Before you configure Citrix Services, change the Mobile Access server certificate to one that was issued to the FQDN. This is necessary to comply with the Citrix standards for server certificates. Additionally, end-users must browse to Mobile Access using the FQDN that is routable from their network.

Note - Make sure that the certificate is *"Server Certificates" on page 232*.

If your Web Interface server is configured to deploy ICA Web clients and the Mobile Access server certificate is issued by a private CA, the certificate's public key must be installed on the client side browser for the ICA Web Client to function properly. The Mobile Access certificate public key is located under:
`$CVPNDIR/var/ssl/server.crt`

Citrix Service ? Web Interface page

1. Go to the **Web Interface** page of the **Citrix Service** object.
2. Fill in the fields on the page:
   - **Servers** are the machine(s) or DNS Name(s) on which the Web Interface server is hosted. Choose either a single **Host or DNS name**, or **Multiple hosts**. In order to keep the environment simple, it is recommended to configure a single Web Interface server per Citrix Application.

- **Services** must match the settings on the Web Interface server. Select `http` or `https`, as required. Other services are NOT supported.

Citrix Service ? Link in Portal Page

1. Go to the **Link In Portal** page of the **Citrix Service** object.
2. Fill in the fields on the page:
   - **Link text (multi-language)** - Shows in the Mobile Access Portal. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.
   - **URL** - The link to the location of the application, or to a sub-directory of the application.
   - **Tooltip (multi-language)** - Gives additional information. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

Citrix Service ? STA Servers Page

1. Go to the **STA servers** page of the **Citrix Service** object.
2. Get the Host from the current settings on the Web Interface (WI) server.
3. Get the STA ID from the Secure Ticketing Authority (STA) servers.

Note - Mobile Access implements its own Secure Ticketing authority (STA) engine. STA servers are not necessary.

To get the host name or IP address:

1. Login to the Web Interface Citrix administration page.
2. Click **Server-Side Firewall**.
3. Scroll to the **Secure Ticket Authority list**.
   - If the field is blank, you are in unticketed mode and you do not need to define any STA Servers on Mobile Access.
   - If the field contains entries, you are in ticketed mode. Each entry in this list is a URL containing the IP or FQDN of a Citrix server. Every entry in the Secure Ticket Authority list must be separately entered into Mobile Access.

To get the STA ID:

1. Login to the STA server.
2. From the Windows **Start** menu, select **Programs > Citrix > Citrix Secure Gateway > Secure Ticket Authority Configuration**.
3. Click **Next**.

The STA ID is shown in the **Enter the STA ID** field.

Citrix Service - MetaFrame Servers Page

Go to the **MetaFrame servers** page of the **Citrix Service** object. In this page you can allow access to all Presentation Servers, or restrict access to defined MetaFrame servers.

If you select **Restrict access to these servers only**:

- Define the servers using an IP address or Fully Qualified Domain Name (FQDN).
- Make sure that the definition matches the configuration made on the XenApp server farm. If you do not, Mobile Access may not authorize the connection. The Presentation server configuration affects one of the parameters in the ICA file that is received by the client.

Citrix Service - XenApp Servers Page

Use the **XenApp Servers** page to configure access to the XenApp Servers.

Note - If you select **Restrict access to these servers only**,

1. Define the servers using an IP address or Fully Qualified Domain Name (FQDN).
2. Make sure that the definition matches the configuration made on the Metaframe server farm.

   If you do not, Mobile Access may not authorize the connection. (The XenApp server configuration affects one of the parameters in the ICA file that is received by the client).

Citrix Service - Single Sign On Page

Single Sign On increases application security.

To configure Single Sign On:

1. Go to the **Single Sign On** page of the **File Share Application** object.
2. Select **Turn on single Sign On for this application**.

   Configure the sign on method for the application.

Citrix Service - Protection Level Page

1. Go to the **Protection Level** page of the **Citrix Service** object.
2. Enter data in these fields:

   Security Requirements for Accessing this Application lets you:

   - Allow access to this application to any endpoint that complies with the security requirements of the Security Gateway,
   - OR make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.

   Note - The Citrix architecture requires ICA files and ActiveX executables to be temporarily cached by the client-side browser. As a result, Mobile Access's Protection Level settings do not apply to these files.
3. Get the Host and the STA ID of the Secure Ticketing Authority (STA) servers from the current settings on the Web Interface (WI) server.

   Note - Mobile Access implements its own Secure Ticketing authority (STA) engine. STA servers are not necessary.

To get the hostname or IP address:

1. Login to the Web Interface Citrix administration page.
2. Click **Server-Side Firewall**.

3. Scroll to the **Secure Ticket Authority list**.
   - If the field is blank, you are in unticketed mode and you do not need to define any STA Servers on Mobile Access.
   - If the field contains entries, you are in ticketed mode. Each entry in this list is a URL containing the IP or FQDN of a Citrix server. Every entry in the Secure Ticket Authority list must be separately entered into Mobile Access.

To get the STA ID:

1. Login to the STA server.
2. From the Windows **Start** menu, select **Programs > Citrix > Citrix Secure Gateway > Secure Ticket Authority Configuration**.
3. Click **Next**.

   The STA ID is shown in the **Enter the STA ID** field.

Completing the Configuration of the Citrix Service

To complete the configuration, add the Citrix Service to a policy rule and install policy from SmartConsole.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 49*.

For legacy policy, see *"Getting Started with Mobile Access" on page 38*.

Web Mail Services

Mobile Access supports built-in Web mail. Web mail provides a simple way for remote users, through a web browser interface, to access their email. Employees can access their email from any computer that has access to the Internet, such as a computer in a library, or Internet cafe. There is no need to install special email or remote access software. This is helpful for employees who work outside the office on a regular basis.

Note - The traffic log does not show actions done by the user through the Web mail interface.

Mobile Access also supports the IBM Lotus Domino Web Access (DWA, formerly known as iNotes) and Outlook Web Access (OWA). DWA and OWA are configured in Mobile Access as Web Applications.

Web Mail Services User Experience

Remote users login to Mobile Access and authenticate themselves in order to gain access to the portal. They can then click a link to access the Web mail application. Mobile Access can be configured to reuse the login credentials when authenticating to the IMAP account on the mail server. If the reused credentials are incorrect, Mobile Access again presents the user with a login page. Valid credentials are saved for future logins.

Once authenticated to the mail application, users can:

- Compose, send and receive email.
- Create, delete, rename, and manipulate mail folders.
- Index messages in various ways.
- Stores addresses.

- Search emails according to various criteria, such as body text, subject and sender's address.
- Highlight messages with different background colors, enabling quick differentiation.
- Display preferences.

Incoming (IMAP) and Outgoing (SMTP) Mail Servers

Mobile Access provides a Web front-end for any email application that uses the IMAP protocol for incoming mail, and SMTP for outgoing mail.

Email stored on the IMAP server is manipulated through the browser interface without having to transfer the messages back and forth. Users can connect to several mail servers depending on their authorization.

Configuring Web Mail Services

To configure a new Web Mail application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Mail Service**.

   The **Web mail service** window opens.

Web Mail Service - General Properties Page

1. Go to the **General Properties** page of the **Web mail service** object.
2. Fill in the fields on the page:
   - **Name** for the mail service, for example, my_mail_server
   - **Outgoing Mail Server (SMTP)**
     - **Host or DNS Name**, for example, smtp.example.com
     - **Service** is normally the standard predefined SMTP service.
   - **Incoming Mail Server**
     - **IMAP server type**
     - **Host or DNS Name**, for example, smtp.example.com
     - **Service** is normally the standard predefined IMAP service.

Web Mail Service - Link in Portal Page

1. Go to the **Link In Portal** page of the **Web mail service** object.
2. Fill in the fields on the page:
   - **Link text (multi-language)** - Shows in the Mobile Access Portal. If more than one link is configured with the same (case insensitive) text, only one of them will be shown in the portal.
   - **Tooltip (multi-language)** - Gives additional information. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

Web Mail Service - Single Sign-On Page

Configure the *"Single Sign On" on page 84* settings for the Web Mail Service.

1. Go to the **Single Sign On** page of the **Web mail service** object.
2. Select the sign on method for the application.

Web Mail Service - Protection Level Page

1. Go to the **Protection Level** page of the **Web mail service** object.
2. Fill in the fields on the page:

   Security Requirements for Accessing this Application lets you:

   - Allow access to this application to any endpoint machine that complies with the security requirements of the Security Gateway,
   - Give access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.

Completing the Configuration of the Web Mail Service

To complete the configuration, add the Web Mail application to a policy rule and install policy from SmartConsole.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 49*.

For legacy policy, see *"Getting Started with Mobile Access" on page 38*.

Enabling LDAP Contacts Search in Web Mail Applications

By default, the contact search in Web Mail applications works only for internal users that are defined on the Mobile Access Security Gateway. To enable search on contacts that are defined on an LDAP server, see sk34997.

Native Applications

"Native Applications for Client-Based Access" on page 101 are not clientless. They require the SSL Network Extender client on the endpoint machine.

DNS Names

If an internal application is hosted on a server inside the organization, using a DNS Name object in the definition of the Mobile Access application makes it possible to change the IP address of the server without having to change the definition of the host object in the Mobile Access application.

For example, if "myhost.example.com" is used in the definition of a Mobile Access application, Mobile Access resolves the IP address of "myhost" when authorizing access to the application.

If an internal application is hosted on multiple replicated servers, a single DNS Name object can be used in the definition of the Mobile Access application, instead of having to individually define each host.

The DNS server that is specified on Mobile Access resolves the DNS names. To set or change the DNS server, use the `sysconfig` command.

DNS Names and Aliases

A DNS name can have a number of aliases. For example, `www.example.com`, `www.example.co.uk` and `www.example.co.fr` could be aliases of the same DNS name.

In the definition of the DNS Name object, use the format "`a.b? x.y.z`", where each section of the DNS name is demarcated by a period. For example, `mail.example.com` or `www.example.co.uk`.

Wildcards can be used at the beginning of a domain name, but not at the end. For example, `*.example.com` includes `www.example.com` and `mail.example.com`. On the other hand, `www.example.*` is NOT valid.

Where DNS Name Objects are Used

DNS objects are used when defining hosts for Mobile Access Web applications, file share applications, Citrix services, and Web mail services. They are also used when configuring support for Hostname Translation.

DNS Name objects cannot be used in the Security Rule Base.

Defining the DNS Server used by Mobile Access

The DNS server that resolves the IP addresses of the DNS Name objects must be defined in one of these locations:

- In SmartDashboard:

  On the Mobile Access tab, go to the **Additional Settings > Network Accessories > Name Resolution** page.

- On the Mobile Access Security Gateway:

  For instructions, see the *R80.40 Gaia Administration Guide* - Chapter *Network Management* - Section *Hosts and DNS*.

Configuring DNS Name Objects

To create a new DNS Name object:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > DNS Names**.
3. Click **New**.
4. Enter a **Name** for the DNS Name object.
5. Click **DNS Names**.
6. Click **Add**.
7. Type the DNS name.
8. Click **OK**.

9. Click **Save** and then close SmartDashboard.
10. In SmartConsole, install policy.

Using the Login Name of the Currently Logged in User

Mobile Access applications can be configured to differ depending on the user name of the currently logged-in user. For example, portal links can include the name of the user, and a file-share can include the user's home directory. For this purpose, the `$$user` directive is used. During a Mobile Access session, `$$user` resolves to the login name of the currently logged-in user.

For such personalized configurations, insert the `$$user` string into the relevant location in the definitions of Web applications, file shares, and native applications.

For example, a Web application URL that is defined as `http://host/$$user` appears for user `aa` as `http://host/aa` and for user `bb` as `http://host/bb`.

If the user authenticates with a certificate, `$$user` resolves during the user's login process to the user name that is extracted from the certificate and authorized by the directory server.

For its use in configuring File Shares, see the "Mobile Access Applications" section.

WebSockets

WebSockets support in the Mobile Access Software Blade gives remote terminal access from a browser, without a pre-installed RDP/VDI client.

This feature is supported in R77.10 and above.

For WebSockets system requirements, see sk95311.

Check Point appliances can support hundreds of concurrent WebSocket users. The amount depends on the power of the appliance and their deployment (Load Sharing an appliance cluster can support more users). To get the best appliance that best suits your needs, contact your Check Point sales engineer.

Using WebSockets

To use WebSockets support:

Create a regular Web application to the WebSocket server.

- Make sure to include the port used for the WebSocket connection in the **Authorized Locations** of the Web application.
- The Web applications related to the WebSocket application must use **Path Translation** as their Link Translation method. It can be inherited from the Security Gateway setting or configured in the Web application.

Monitoring WebSockets

To monitor WebSocket connections:

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Run:

   ```
   PingerAdmin report type ws
   ```

   Alternatively, to see all connections currently handled by the Pinger daemon (such as ActiveSync push), run:

   ```
   PingerAdmin report all
   ```

Single Sign On

Introduction to Single Sign On

Single Sign On (SSO) eliminates the need for users to re-authenticate to an application when they access it for a second time, during a Mobile Access session, or between sessions. The authentication credentials used to log in to the Mobile Access Portal can be re-used automatically to authenticate to multiple applications accessed through Mobile Access. You can also record other credentials for the application, and store them for future use. SSO user credentials are securely stored on Mobile Access and therefore remain valid even if the user logs in from a different client machine.

Supported SSO Authentication Protocol

Mobile Access supports Single Sign On for authentication to internal Web and other application servers. The supported authentication protocols are:

- Basic Access - RFC enhancement. Not recommended because of security implications.
- Digest Access - RFC enhancement.
- Integrated Windows Authentication - RFC enhancement. Supports: NTLMv1, NTLMv2, and Kerberos.
- Credential forwarding in HTTP headers - Ad hoc solution. Not recommended because of security implications.
- Web form (HTML) based.

Certificate Attribute Forwarding

Certificate attribute forwarding is a Single Sign-on method that transfers details from a user's certificate to internal servers without the need for a username and password. It forwards the certificate attributes as HTTP headers to the internal servers when a user logs in with a certificate. Users can then log in to other applications automatically with Single Sign-on.

Configuring Certificate Attribute Forwarding

Configure Certificate attribute forwarding in the Mobile Access configuration file: `$CVPNDIR/conf/cvpnd.C`

Important! After every change to `cvpnd.C`, you *must* restart the cvpn services: `cvpnrestart`

To:	Parameter=value in the `$CVPNDIR/conf/cvpnd.C`
Enable	`:EnableCertHeadersForwarding (true)`
Disable	`:EnableCertHeadersForwarding (false)`

To configure which attributes of the certificate are forwarded in the HTTP headers:

Add parameters to the `CertHeaders` section in the `$CVPNDIR/conf/cvpnd.C`.

To forward:	Parameter=value in the `$CVPNDIR/conf/cvpnd.C`
Complete certificate, encoded in base 64	"*<header_name>*: *<Certficate in Base64>*"
Certificate Issuer DN	"*<header_name>* : *<DN of Certficate Issuer>*"
Serial number of the certificate	"*<header_name>* : *<Certficate Serial>*"
Subject DN	"*<header_name>* : *<DN of Certficate Subject>*"
Alternative subject DN	"*<header_name>* : *<DN of Certficate Alternative Subject>*"
Valid start date, before which the certificate cannot be used	"*<header_name>* : *<Certficate Validity Start Date>*"
Certificate expiration date	"*<header_name>* : *<Certficate Validity End Date>*"

Example:

To forward the certificate Issuer DN, edit the `cvpnd.C` file (where **X-Cert-IssuerDN** is the header name):

```
:EnableCertHeadersForwarding (true)
:CertHeaders (
    : ("X-Cert-IssuerDN : <DN of the Certificate Issuer>")
)
```

HTTP Based SSO

For applications that perform authentication at the HTTP level, HTTP-based SSO is available, in which the credentials are forwarded in HTTP headers. This applies to the Basic, Digest, Integrated Windows Authentication, and Credential forwarding in HTTP headers authentication protocols.

When the user attempts to access these sites, a browser-specific form opens:

The user must enter his/her user name and password for that application, and click OK.

HTTP Based SSO Limitation

Single Sign On is not supported if:

- The Web server requests authentication for a POST request in either the digest or Integrated Windows Authentication methods,
- And the server does not support sending of "100 Continue" responses.

Web Form Based SSO

Most Web applications have their own Web forms for authentication. For these applications, Mobile Access supports Web form (HTML) based SSO.

The advantage of Web form based SSO authentication over HTTP authentication is that users are presented with the login page of the application itself, rather than a more obtrusive browser-specific page.

A typical Web form is shown below, for Outlook Web Access, together with a Mobile Access SSO popup that assists the user.

It is recommended to use the Web form based SSO for every application that is configured to work with Web form authentication. Do not enable Web form SSO for other applications, in order to maintain performance and connectivity.

Application Requirements for Easy Configuration

Web form based SSO in its default configuration can be configured by selecting a single check box in SmartDashboard. In order for the default settings to work, the application must:

- Present the login form as the first form seen by the user.
- Redirect (status 301 or 302) on login success.

Web Form Based SSO Limitations

Web form based SSO does not support:

- Password remediation forms.
- Forms that contain 'old/new/confirm' password fields. These fields are not recognized correctly, and wrong credentials might be recorded or forwarded.
- Forms that use Ajax requests instead of the usual 'ACTION' attribute for form submission.

Configuring SSO Name Format

This feature prevents problems with SSO caused by different formats of credentials required by different applications. You configure the credential format for each application, and the Mobile Access Security Gateway sends the credentials to the organizational server in the correct format. This applies to Web, Mobile Mail, and ActiveSync applications and works with Web Form based SSO.

Note - This feature is for LDAP users who connect to the Mobile Access Portal. Internal users who connect to web applications though the portal with SSO authentication use a default of **$$user**.For example, SSO can apply to both of these applications:

- Web application A that uses the format domain\username
- ActiveSync application B that uses the format username@domain

This feature is supported in R77.20 and higher. In R80.10 and higher you can configure it in SmartConsole.

To configure the format of credentials required for an application:

1. In SmartConsole, open a mobile application.
2. Select **Additional Settings** > **Single Sign-on**.

3. In the **Credential Formats** area, select an option.
4. Install Policy.

Application and Client Support for SSO

The following table shows which SSO methods are available for each Mobile Access application:

Mobile Access Application	Supports HTTP Based SSO	Supports Web Form Based SSO
Web applications	Yes	Yes
File shares	Yes	Not relevant
Citrix services	Yes	Yes
Web Mail	Simplified	No
Native applications	No	Not relevant
Mobile Mail	Yes	Not relevant
ActiveSync	Yes	Not relevant

Most Mobile Access Web Applications and Citrix Services support Web Form SSO, with either no configuration, or minimal configuration required. Some applications have been tested and found to require manual configuration (of the HTTP Post details). Some applications do not support Web Form SSO at all.

For a list of common applications that are certified by Check Point to work with Web Form SSO, see SecureKnowledge solution sk35080.

Basic SSO Configuration

To configure a basic SSO for a web application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.
4. From the navigation tree click **Additional Settings > Single Sign On**.
5. Select **Turn on Single Sign On for this application**.
6. Configure the sign on method for the application. These are the default options:

   For Web applications, File Shares and Citrix Services:

   Prompt the users for their credentials and store them for future use

   For Web Mail applications this same option is called:

   Prompt user for credentials

With this option, the application credentials are stored and reused. The portal credentials are not used to authenticate to applications.

7. Install the policy.

Basic Configuration of Web Form SSO

Web form SSO is supported only for Mobile Access Web applications and Citrix services.

In the default settings, Web Form Single Sign On automatically analyzes the sign-in Web page of the application. The default settings assume:

- HTTP redirect (301, 302) upon authentication success.
- No redirect upon authentication failure.

To configure Web Form SSO with default settings:

- In the **Single Sign On** page of the Mobile Access application, select **This application uses a Web form to accept credentials from other users**

  Note - Only enable Web form SSO for applications that use a Web form to accept user credentials, in order to maintain performance and connectivity.

SSO for Native Applications

Native applications that you access with SSL Network Extender can use Single Sign-On (SSO) functionality. With SSO support, users connect automatically to native applications that require login. The native application gets the Mobile Access Portal login username and password parameters from the internal server.

This feature is supported in R77.20 and higher. It requires a SSL Network Extender client upgrade.

Configuring SSO for Native Applications

Use the dynamic parameters $$user and $$password to configure SSO for a native application. These parameters are resolved to the actual username and password of the logged-in user when the Security Gateway sends the parameters to the native application.

These instructions show you how to configure the new $$password parameter in for a Simple native application. You can also use the $$password parameter in the application parameters in Advanced native applications.

Note - When SSO is configured for a native application, it sends the end-user's password back to the client side.

To configure SSO for a native application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.
4. Select **Endpoint Applications** from the navigation tree of the object.

5. Select **Simple (Application is installed on the endpoint machine)** and enter information for these fields:
   - **Path and executable name** - Enter the path of the native application.
     For example for Remote Desktop Plus: `D:\rdp.exe`
   - **Parameters** - Enter this syntax for the username, password, and target remote host to connect to.
     For example: `/u:acme\$$user /p:$$password /v:192.0.2.2 /f`

     This setting defines how the Security Gateway sends the username and password of a locally logged-in user to the native application.
6. Install the policy.

Upgrading the SSL Network Extender Client to use SSO

Users must have an upgraded SSL Network Extender client on their computer to use SSO with native applications. To upgrade users' clients, make sure the **Client upgrade** setting is set to one of these:

- **Always upgrade** -Clients are upgraded automatically when users connect for the first time after the Security Gateway upgrade.
- **Ask user** -Users are prompted before installation starts. If you use this option, make sure to let users know that they must confirm the upgrade.

Upgraded SSL Network Extender clients can still connect to Security Gateways of earlier versions.

To change the Client upgrade settings:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > VPN Clients**.
3. In **Advanced Settings for SSL Network Extender**, click **Edit**.

   The **SSL Network Extender - Advanced Settings** window opens.
4. In the **Deployment options** section, make sure that **Client upgrade upon connection** is configured for **Always upgrade** or **Ask user**.
5. Click **OK**.
6. Click **Save**
7. Close SmartDashboard.
8. Install the policy.

Advanced Configuration of SSO

The following configuration instructions apply to both HTTP based SSO and to Web form based SSO. The advanced configuration options are supported for Web applications, file shares, and Citrix services.

For configuration options that are specific to Web form SSO, see the "Single Sign On" section.

Configuring Advanced Single Sign On

There are a number of Single Sign On methods. The different options allow you to configure how to handle portal credentials, and how to handle other credentials used to authenticate to the application.

To configure the Single Sign On methods:

1. Go to the **Single Sign On** page of the Mobile Access application.
2. For the **Advanced** options, click **Edit**.

These are the available single sign on methods.

SSO Method	Single Sign On is On/Off	Forward portal credentials	Learn other credentials
Turn on Single Sign On for this application is cleared	Off. Users are always prompted.	No	No
Prompt users for their credentials, and store them for future use	On. Default method.	No	Yes
This application reuses the portal credentials. Users are not prompted.	On. Advanced method.	Yes	No
This application reuses the portal credentials. If authentication fails, Mobile Access prompts users and stores their credentials.	On. Advanced method.	Yes	Yes

Configuring Login Settings

Login settings allow you to configure the default Windows domain (if Windows authentication is being used), to notify users that their credentials will be stored, and to specify a hint to help users supply the correct credentials.

To configure the login settings for Single Sign On:

1. Go the **Single Sign On** page of the Mobile Access application.
2. In the **Login Settings** section, click **Edit**.

   The **Login Settings** window opens.
3. Fill in the fields according to the explanations below.

Windows Domain

- **The user of this application belongs to the following Windows domain**:

  Specify the Windows domain or workgroup (for example "LOCALDOMAIN") if Windows authentication is used. Integrated Windows authentication requires the domain to be forwarded with the user name and password.

  If **Accept the portal credentials from the gateway** Single Sign On method is used, Mobile Access does not know the domain, because the user does not supply it with the portal credentials. The domain is fetched from the one specified here.

User Notification

- **Notify the users that their credentials for this application are going to be stored**

  When users access the application login page for the first time, they see a message that their credentials will be stored for future access.

- **Allow the users to specify that their credentials for this application will not be stored**

  When users access the application login page for the first time, they see a message from which they can select not to record their credentials.

Administrator Message

- **Show the following message together with the credentials prompt**

  Show a hint to the user about the credentials they must supply. for example, whether or not they should supply the domain name and user name (for example: AD/user) or just the user name (for example: user). After clicking the **Help me choose credentials** link, the user sees the hint. The message can include ASCII characters only.

Advanced Configuration of Web Form SSO

Use the advanced Single Sign On settings for Web form credentials to configure an application for Web form SSO if there is one of these:

- *No* HTTP redirect (301, 302) upon authentication success
- *No* redirect upon authentication failure.

You can specify different criteria for:

- Sign In Success or Failure Detection
- Credential Handling

Configuring Sign In Success or Failure Detection

To configure Sign In success or failure criteria:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

The Web Application window opens.

4. From the navigation tree, click **Additional Settings > Single Sign On**.
5. In the **Web Form** section, click **This application uses a Web form to accept credentials from users**.
6. Click **Edit**.
7. Click **Specify a criterion for success or failure** and then select one of these options:
   - **Mobile Access regards the authentication as successful, if after signing in, this application creates a cookie with the following name:**
     The application places a session cookie upon success. To obtain the exact name of the session cookie, install a sniffer or browser plug-in (such as the Fiddler HTTP debugging proxy)
   - **Mobile Access regards the authentication as a failure, if after signing in, this application redirects to the following URL:**
     The application redirects on failure. To find the target URL, install a sniffer or browser plug-in (such as the Fiddler HTTP debugging proxy). Use this URL format:
     `<protocol>://<host>/[<path>][?< query>]`
8. Click **OK** and close the Web Application window.
9. Install the policy.

Credential Handling

By default, Mobile Access looks for the user name and password fields at the application URL. If the default settings do not work, you can either configure an automatic credential detection method, or you can manually hard-code the POST details.

To configure automatic credential handling:

1. In the **Single Sign On** page of the Mobile Access application, in the **Web Form** section, click **Edit**.
2. In the **Credentials Handling** section, click **Edit**.
3. Select **Automatically handle the credentials**.
4. Under **Sign in Web Form Detection Settings**, select:

   Mobile Access regards the following URL as the sign in Web form:

   If the application presents a Web form that requires credentials, before the actual login form, so that Mobile Access is unable to automatically analyze the sign-in Web page, you can specify the URL of the actual login form.

   Syntax:
   `<protocol>://<host>/[<path>][?< query>]`
5. Under **Password Validation Settings**, select:

   Mobile Access sends the following password:

   Clients need to submit the sign on Web form with a user name and password. However, it is not secure to store the password on the client for future SSO use. Mobile Access therefore generates a dummy password that it sends to the client, and replaces it upon sign on with the real password. Some applications check the dummy password on the client side. If the Mobile Access dummy password is not compatible with the application, you can define a different one.

   Note - This password cannot include special characters. Use ASCII characters only.

Manually Defining HTTP Post Details

If automatic Web form SSO does not work, you can define HTTP POST details.

To manually specify how to handle credentials:

1. From the **Credentials Handling** window, select **Manually specify how to handle the credentials**.
2. Fill in the fields for **When the following sign in URL is requested**:
   - **post to the following URL**
     In this and the previous field, the URL must be absolute. Use the URL format `<protocol>://<host>/[<path>][?< query>]`
   - **the following POST data**, which must include:
     - $USERNAME resolves to the user name stored on Mobile Access.
     - $PASSWORD resolves to the password stored on Mobile Access.
     - $DETAILS resolves to the Windows domain stored on Mobile Access

When manual credential handling is configured for Web form SSO, the HTTP authentication request window appears, when credentials are requested for the first time.

Kerberos Authentication Support

Kerberos is a network protocol that lets people and computers securely authenticate over a non-secure network. In Windows 2000 and higher, Kerberos is the default authentication protocol.

- Kerberos Authentication is supported for Web Applications (HTTP and HTTPS). Mobile Access can authorize against Kerberos servers on behalf of users.
- Microsoft IIS and other web servers employ Kerberos using the *Negotiate* method in HTTP authentication headers.
- Kerberos is sensitive to time differences between the Security Gateway and Domain Controller. Make sure clocks on the Mobile Access Security Gateway and on the domain controller(s) are synchronized to within 1 minute. The best way to ensure this is to use an NTP time server.
- By default, NTLM authentication is preferred as the authentication method over Kerberos authentication. To prefer Kerberos over NTLM, follow the instructions in sk106848.

To use Kerberos with Mobile Access:

- If Microsoft Active Directory is configured, the Security Gateway automatically updates with the relevant settings from the AD Account Unit and Kerberos enabled. You can review the Kerberos settings in `$CVPNDIR/var/krb5.auto.conf`

  Warning: Do not manually edit `krb5.auto.conf`.
- If you must make a change to `krb5.auto.conf`, do it in the template file, `krb5.auto.conf.template`. The template is used to create the `krb5.auto.conf` file.

  To edit `krb5.auto.conf.template`:

1. Edit the `$CVPNDIR/var/krb5.auto.conf.template` file and add your changes.

   The file contains Kerberos conf file information and place holders for the Account Unit settings - the place holders are in the form of `<++PlaceHolderName++>`.

   Important - Do not change the place holder names.

2. On the Security Gateway, run:

   ```
   cvpnd_admin policy
   ```

   Example of the template file `krb5.auto.conf.template`:

   ```
   [libdefaults]
   <++libdefaults++>
   rdns = false
   [realms]
   <++realms++>
   [domain_realm]
   <++domain_realm++>
   ```

   Example of how it looks in `krb5.auto.conf`:

   ```
   [libdefaults]
   default_realm = EXAMPLE.COM
   rdns = false
   [realms]
   EXAMPLE.COM = {
    kdc = 192.168.1.1
   }
   [domain_realm]
   ```

- If Microsoft Active Directory is not yet configured for Mobile Access, but you want to use it:
  1. Use the Mobile Access wizard to configure your AD.
  2. Edit the SmartDashboard Network Objects for the AD server and for the Single Sign On.
- If you do not want to use Microsoft Active Directory, manually configure Kerberos for your Single Sign On.

Configuring Microsoft Active Directory for Mobile Access

These steps assume you defined the Microsoft AD server as a Check Point LDAP Account Unit object. If that object does not exist, create one: **Objects > New > More > Server > LDAP Account Unit**.

To make sure Microsoft Active Directory is configured for the default settings:

1. In the SmartConsole, go to **Objects > Servers > LDAP Account Units**.
2. Right-click the LDAP AD server and select **Edit**.

   In the **General** tab of the **LDAP Account Unit Properties** window, the value of **Profile** is **Microsoft_AD**.
3. Make sure the value of **Domain** is correct for the AD Domain.
4. Click **OK**.
5. Publish the SmartConsole session.

To configure Microsoft Active Directory server priorities:

1. Open the object for the Security Gateway with Mobile Access enabled.

   If there is more than one, do these steps for each.

2. Open **Other** > **User Directory**.

   By default, the Security Gateways use all Domain Controllers of the AD. If there is a connectivity issues (no or poor connectivity) from a Security Gateway to a Domain Controller, adjust the priorities.

3. Make sure that **Selected Account Units List** is selected.

   When this is selected, the **Selected AUs** list is available. If the list is empty, click **Add** to add an **LDAP Account Unit** defined for **Microsoft_AD**.

4. Select the Microsoft AD server.

   The **Servers priorities for selected AU** is available.

5. Clear **Use default priorities**.

6. Select a host of the AD server.

   The **Priority** field is available.

7. Set the priority of the host with connectivity issues to be lower than a different host.

   For example: Priority **1** is highest. Priority **5** is lower.

8. Click **Set**.

9. Click **OK**.

Manual Configuration for Kerberos

If you are working with a directory that is not Microsoft AD, or experiencing problems with automatic configuration, manually configure Kerberos authentication.

To manually configure Kerberos:

1. Create `$CVPNDIR/var/krb5.manual.conf`.

2. Populate `krb5.manual.conf` with values that specify your domain addresses and domain controllers.

   Use this format:

```
[libdefaults]
      default_realm = YOUR.AD.NAME
[realms]
      YOUR.AD.NAME = {
            admin_server = your.domain.controller.name
            default_domain = your.dns.domain
      }
[domain_realm]
      .your.dns.domain = YOUR.AD.NAME
      your.dns.domain = YOUR.AD.NAME
```

   In the file:

- `YOUR.AD.NAME` is the Windows domain name.
- To configure more than one Windows domain (also known as a "Realm"), add more domains to the `[realms]` section and to `[domain_realm]` section.
- If each realm has more than one domain controller, instead of the `admin_server` statement use several statements of the type:

```
[realms]
<DOMAIN_NAME> = {
    kdc = <1st domain controller address>
    kdc = <2nd domain controller address>
}
```

Important: If you specify multiple domain addresses (realms) and domain controllers in `krb5.manual.conf` , you must also add them to the Mobile access configuration in the `$CVPNDIR/conf/cvpnd.C`.

To add them, use these `cvpnd_settings` commands:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd kerberosRealms YOUR.AD.NAME
cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd kerberosRealms
YOUR.OTHER.AD.NAME
```

1. Test the manual configuration:
   a. Set `KRB5_CONFIG` as an environment variable in the shell to point to the relevant configuration file:
      - In the Expert mode (Bash shell), run:

        ```
        export KRB5_CONFIG=$CVPNDIR/var/krb5.manual.conf
        ```

      - In the Tcsh or Csh shell, run:

        ```
        setenv KRB5_CONFIG $CVPNDIR/var/krb5.manual.conf
        ```

   b. From the Mobile Access Security Gateway command line, run in the Expert mode (Tcsh, or Csh):

      ```
      kinit your-ad-username
      ```

      - If there are several realms, the `kinit` syntax applies to the default realm.
      - For other realms, use the syntax:

        ```
        kinit your-ad-username@YOUR.OTHER.AD.NAME
        ```

      You should get a prompt similar to:

      ```
      Password for your-ad-username@YOUR.DOMAIN:
      ```

   c. Enter the password.
   d. Run:

      ```
      klist
      ```

      The `Ticket cache` list shows one ticket.

e. Delete the list by running:

`kdestroy`.

2. Open `$CVPNDIR/conf/cvpnd.C` for editing.
3. Change the value of the `kerberosConfigMode` attribute from `auto` to `manual`.

   Alternatively, run:

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd.C set kerberosConfigMode manual
   ```

   Note - If you assign the value `none` to `kerberosConfigMode`, it disables Kerberos SSO.
4. Run:

   ```
   cvpnrestart
   ```

Important - In a cluster environment, repeat steps 1 to 6 on each cluster member.

Kerberos Constrained Delegation

Kerberos constrained delegation is a Single Sign-on method that uses Kerberos authentication for users to access internal resources without the need to enter a password. It is supported for the Mobile Access Portal and Capsule Workspace.

To enable Kerberos constrained delegation:

1. On the Mobile Access Security Gateway, run:

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd_internal_settings.C set EnableKCD true
   ```
2. Run:

   ```
   cvpnrestart
   ```
3. In a cluster environment, repeat the steps on all cluster members.

Configuring Kerberos Constrained Delegation

Before you begin, make sure:

- That your site supports Kerberos authentication.
- The Mobile Access Security Gateway is configured to support Kerberos. .
- The date and time on the Security Gateway and Active Directory server are the same.
- You must use FQDN and not an IP address with your internal server name. Make sure that the FQDN resolves both on the Security Gateway and on the Kerberos server.

The configuration includes:

- Configuring a Delegate User on the AD Server.
- Configuring Kerberos Constrained Delegation support on the Mobile Access Security Gateway.

Configuring a Delegate User on the AD Server

A delegate user can have specified permissions without being part of a higher privileged group. For Kerberos Constrained Delegation, the delegate user can allow access to other users for specified services.

To configure a delegate user on the Active Directory (AD) server:

1. Add a new user to the AD server.
2. Open the command prompt on the AD server and run the command:

   ```
   setspn -A HTTP/<user name> <domain name>\<user name>
   ```

   - <user name> - The user name for the user that was created.
   - <domain name> - The domain name that the created user belongs to.
3. From the **Users and Computers** tree, right-click the user to open the **User Properties** of the new user.
4. Click the **Delegation** tab.
5. Select: **Trust this user for delegation to specified services only**.
6. Select: **Use any authentication protocol**.
7. In the **Services to which this account can present delegated credentials** table, click **Add** to add http on the server that the user is allowed to access.
8. Click **OK**.

Configuring Kerberos Constrained Delegation Support

Kerberos Constrained Delegation is supported with Web Applications and Mobile Mail applications.

To configure Kerberos Constrained Delegation in SmartDashboard:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application for which you want to configure Kerberos Constrained Delegation.

   The Web Application window opens.
4. From the navigation tree click **Additional Settings > Single Sign On**.
5. Configure these settings:
   - Select **Turn on Single Sign On for this application**
   - Select **Advanced**
6. Click **Edit**.
7. In the **Advanced** window, select **This application reuses the portal credentials. Users are not prompted**.
8. Click **OK** and close the Web Application window.
9. Install the policy.

Troubleshooting

If you have issues with Kerberos Constrained Delegation:

1. Connect to the command line on the Mobile Access Security Gateway.
2. Make sure that the value of **EnableKCD** in `$CVPNDIR/conf/cvpnd_internal_settings.c` is **true**.
3. Run the `cvpnrestart` command.
4. See if there is a **Kerberos Constrained Delegation failure** entry in the Mobile Access logs in SmartLog.
5. Make sure that the account unit credentials have delegate privileges.
6. Make sure that the date and time of the Security Gateway and Active Directory server are synchronized.
7. Make sure that the DNS server is configured correctly and the Security Gateway can resolve the web application host name and the Active Directory server.

Certificate Attribute Forwarding

Certificate attribute forwarding is a Single Sign-on method that transfers details from a user's certificate to internal servers without the need for a username and password. It forwards the certificate attributes as HTTP headers to the internal servers when a user logs in with a certificate. Users can then log in to other applications automatically with Single Sign-on.

Configuring Certificate Attribute Forwarding

Configure Certificate attribute forwarding in the Mobile Access configuration file: `$CVPNDIR/conf/cvpnd.C`

Important! After every change to `cvpnd.C`, you *must* restart the cvpn services: `cvpnrestart`

To:	Parameter=Value in the `$CVPNDIR/conf/cvpnd.C`
Enable	`:EnableCertHeadersForwarding (true)`
Disable	`:EnableCertHeadersForwarding (false)`

To configure which attributes of the certificate are forwarded in the HTTP headers:

Add parameters to the `CertHeaders` section in the `$CVPNDIR/conf/cvpnd.C` file.

To forward:	Parameter=value in the `$CVPNDIR/conf/cvpnd.C`
Complete certificate, encoded in base 64	"*<header_name>*: *<Certficate in Base64>*"
Certificate Issuer DN	"*<header_name>* : *<DN of Certficate Issuer>*"
Serial number of the certificate	"*<header_name>* : *<Certficate Serial>*"

To forward:	Parameter=value in the `$CVPNDIR/conf/cvpnd.C`
Subject DN	"*<header_name>* : *<DN of Certficate Subject>*"
Alternative subject DN	"*<header_name>* : *<DN of Certficate Alternative Subject>*"
Valid start date, before which the certificate cannot be used	"*<header_name>* : *<Certficate Validity Start Date>*"
Certificate expiration date	"*<header_name>* : *<Certficate Validity End Date>*"

Example:

To forward the certificate Issuer DN, edit the `cvpnd.C` file (where **X-Cert-IssuerDN** is the header name):

```
:EnableCertHeadersForwarding (true)
:CertHeaders (
    : ("X-Cert-IssuerDN : <DN of the Certificate Issuer>"
)
```

Native Applications for Client-Based Access

Introduction to Native Applications

A native application is any IP-based application that is hosted on servers within the organization, and requires an installed client on the endpoint. The client is used to access the application and encrypt all traffic between the endpoint and Mobile Access.

SSL Network Extender automatically works with Mobile Access to support native applications.

Microsoft Exchange, Telnet, and FTP, are all examples of native application servers. Authorized users can use their native clients (for example, telnet.exe, ftp.exe, or Outlook) to access these internal applications from outside the organization.

A native application is defined by the:

- Server hosting applications.
- Services used by applications.
- Connection direction (usually client to server, but can also be server to client, or client to client).
- Applications on the endpoint (client) machines.

  These applications are launched on demand on the user machine when the user clicks a link in the user portal.

  They can be one of these:

  - Already installed on the endpoint machine
  - Run via a default browser
  - Downloaded-from-Mobile Access

SSL Network Extender for Accessing Native Applications

The SSL Network Extender client makes it possible to access native applications via Mobile Access. SSL Network Extender can operate in two modes: Network Mode and Applications Mode.

SSL Network Extender with Mobile Access

The SSL Network Extender client lets users access native applications using Mobile Access.

- If the Mobile Access blade is enabled on the Security Gateway, SSL Network Extender works through Mobile Access only. Configure its policy in the **Policy** page of the **Mobile Access** tab.
- If the Mobile Access blade is disabled and the IPsec VPN blade is enabled, SSL Network Extender works through the IPsec VPN blade. Configure its policy in the main security rule base.

Note - If SSL Network Extender was configured through IPsec VPN, and now you enabled the Mobile Access blade on the Security Gateway, you must reconfigure the SSL Network Extender policy in the Mobile Access tab of SmartDashboard. SSL Network Extender rules in the main security rule base are not active if the Mobile Access tab is enabled.

SSL Network Extender is downloaded automatically from the Mobile Access Portal to the endpoint machines, so that client software does not have to be pre-installed and configured on users' PCs and laptops. SSL Network Extender tunnels application traffic using a secure, encrypted and authenticated SSL tunnel to the Mobile Access Security Gateway.

SSL Network Extender requires *"The Mobile Access Portal" on page 184*.

SSL Network Extender Network Mode

The SSL Network Extender Network Mode client provides secure remote access for all application types (both Native-IP-based and Web-based) in the internal network via SSL tunneling. To install the Network mode client, users must have administrator privileges on the client computer.

After installing the client, an authenticated user can access any authorized internal resource that is defined on Mobile Access as a native application. The user can access the resource by launching the client application, either directly from the desktop or from the Mobile Access Portal.

SSL Network Extender Application Mode

The SSL Network Extender Application Mode client provides secure remote access for most application types (both Native (IP-based) and Web-based) in the internal network via SSL tunneling. Most TCP applications can be accessed in Application mode. The user does not require administrator privileges on the endpoint machine.

After the client is installed, the user can access any internal resource that is defined on Mobile Access as a native application. The application must be launched from the Mobile Access Portal and not from the user's desktop.

If an application is defined in the Mobile Access tab in SmartDashboard as one that can be used in Application Mode, a user that connects in Application Mode will be able to see it and launch it. If the application is not supported in Application Mode, a user who connects with Application Mode will not see it in the list of applications. While Application Mode is designed to work with most applications, only OPSEC-certified applications have been tested and verified to work with SSL Network Extender in Application mode.

Note - UDP based applications are not supported with SSL Network Extender in Application mode.

Supported Application Mode Applications

Most TCP applications work with SSL Network Extender in the Application Mode. If an application is defined in the Mobile Access tab in SmartDashboard as one that can be used in Application Mode, a user that connects in Application Mode will be able to see it and launch it. If the application is not supported in Application Mode, a user who connects with Application Mode will not see it in the list of applications.

The following applications have been tested and are Check Point OPSEC-certified for use with Mobile Access SSL Network Extender in Application mode. Note that this mode is different from SSL Network Extender in Network mode which supports any IP-based application. While Application Mode is designed to work with most applications, only OPSEC-certified applications have been tested and verified to work with SSL Network Extender in Application mode. Only specified versions are guaranteed to work and are fully supported. However, in most cases other versions of the same client and most other applications that are TCP based will work.

Note - Some Anti-Virus applications do not scan email when Microsoft Outlook is launched with SSL Network Extender Application mode, because the mail is encrypted in SSL before scanning begins.

Configuring SSL Network Extender as a VPN Client

To configure SSL Network Extender as a VPN client

1. From the **Gateways & Servers** tab, right-click the Mobile AccessSecurity Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.

2. From the navigation tree, click **Mobile Access > SSL Clients**.

   SSL Network Extender is automatically enabled when the Mobile Access blade is turned on.

3. Select an option:

   - **Automatically decide on client type according to endpoint machine capabilities** downloads the SSL Network Extender Network Mode client if the user on the endpoint machine has administrator permissions, and downloads the Application Mode client if the user does not have administrator permissions.
   - **Application Mode only** specifies that the SSL Network Extender Application Mode client is downloaded to the endpoint machines - irrespective of the capabilities of the endpoint machine.
   - **Network Mode only** specifies that the SSL Network Extender Network Mode client is downloaded to the endpoint machines - irrespective of the capabilities of the endpoint machine. The user on the endpoint machine must have administrator permissions in order to access Native Applications.

4. Click **OK**.

5. Install the policy.

   If you had SSL Network Extender configured through IPsec VPN and now you enabled the Mobile Access blade on the Security Gateway, you must reconfigure the SSL Network Extender policy in the Mobile Access tab of SmartDashboard. Rules regarding SSL Network Extender in the main security rule base are not active if the Mobile Access tab is enabled.

Office Mode

When working with Office Mode, Remote Access clients receive an IP address allocated for them by the VPN administrator. These addresses are used by the clients in the source field of the IP packets they build. Since the IP packets are then encrypted and encapsulated, the packets appear to the Internet with their original IP address. To the organization's internal network, after decapsulation and decryption, they appear with the allocated IP address. The clients seem to be on the internal network.

For more about Office Mode, see the *R80.40 Remote Access VPN Administration Guide*.

Configuring Office Mode

Configure Office Mode in **Gateway Properties > Mobile Access > Office Mode**. The settings configured here apply to Mobile Access clients and IPsec VPN clients.

Office Mode Method

Choose the methods used to allocate IP addresses for Office Mode. All of the methods selected below will be tried sequentially until the office mode IP addresses are allocated.

- **From $FWDIR/conf/ipassignment.conf** - You can over-ride the Office Mode settings created on Security Management Server. Edit the plain text file `ipassignment.conf` in the `$FWDIR/conf/` directory on the Check Point Security Gateway. The Security Gateway uses these Office Mode settings and not those defined for the object in Security Management Server.

  The `ipassignment.conf` file can specify:

  - An IP per user/group, so that a particular user or user group always receives the same Office Mode address. This allows the administrator to assign specific addresses to users, or particular IP ranges/networks to groups when they connect using Office Mode.
  - A different WINS server for a particular user or group.
  - A different DNS server.
  - Different DNS domain suffixes for each entry in the file.
- **From the RADIUS server used to authenticate the user** - A RADIUS server can be used for authenticating remote users. When a remote user connects to a Security Gateway, the user name and password are passed on to the RADIUS server, which checks that the information is correct, and authenticates the user.
- **Using one of the following methods**
  - **Manually (IP pool)** - Create a Network Object with the relevant addresses. The allocated addresses can be illegal but they have to be routable within the internal network.
  - **Automatically (Using DHCP)** - Specify the machine on which the DHCP server is installed. In addition, specify the virtual IP address to which the DHCP server replies. The DHCP server allocates addresses from the appropriate address range and relates to VPN as a DHCP relay agent. The virtual IP address must be routable to enable the DHCP send replies correctly.

    DHCP allocates IP addresses per MAC address. When VPN needs an Office Mode address, it creates a MAC address that represents the client and uses it in the address request. The MAC address can be unique per machine or per user. If it is unique per machine, then VPN ignores the user identity. If different users work from the same Remote Access client they are allocated the same IP address.

Multiple Interfaces

If the Security Gateway has multiple external interfaces, there might be a routing problem for packets whose destination address is a client working in Office Mode. The destination IP address is replaced when the packet is encapsulated and thus previous routing information becomes irrelevant. Resolve this problem by setting the Security Gateway to **Support connectivity enhancement for gateways with multiple external interfaces**. Do not select this option if your Security Gateway has only one external interface, as this operation affects the performance.

Anti-Spoofing

If this option is selected, VPN verifies that packets whose encapsulated IP address is an Office Mode IP address are indeed coming from an address of a client working in Office Mode.

If the addresses are allocated by a DHCP server, VPN must know the range of allocated addresses from the DHCP scope for the Anti-Spoofing feature to work. Define a Network object that represents the DHCP scope and select it here.

IP Pool Optional Parameters

Configure additional optional parameters for how office mode addresses are assigned by clicking **Optional Parameters**. If the office mode addresses are allocated from an IP pool, this window allows you to you specify the DNS and WINS addresses by selecting the appropriate Network Objects. In addition, specify the backup DNS and WINS servers and supply the Domain name.

If the office mode addresses are allocated by a DHCP server, DNS and WINS addresses are set on the DHCP server.

These details are transferred to the Remote Access client when a VPN is established.

IP Lease Duration

Specify the amount of time after which the Remote Access client stops using the allocated IP address and disconnects. By default, the duration is 15 minutes. The client tries to renew the IP address by requesting the same address after half of the set time has elapsed. When this request is granted, the client receives the same address until the lease expires. When the new lease expires, it must be renewed again.

Configuring SSL Network Extender Advanced Options

To configure SSL Network Extender advanced options

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > VPN Clients**.
3. From the **Advanced Settings for SSL Network Extender section**, click **Edit**.
4. Configure the applicable options.
5. Click **OK**.
6. Click **Save** and then close SmartDashboard.
7. In SmartConsole, install policy.

Deployment Options

- **Client upgrade upon connection** specifies how to deploy a new version of the SSL Network Extender Network Mode client on endpoint machines, when it becomes available.

  Note - Upgrading requires Administrator privileges on the endpoint machine.
- **Client uninstall upon disconnection** specifies how to handle the installed SSL Network Extender Network Mode client on the endpoint machine when the client disconnects.

- *Do not uninstall* allows the user to manually uninstall if they wish to.
- *Ask User* allows the user to choose whether or not to uninstall.
- *Always uninstall* does so automatically, when the user disconnects.

Encryption

- **Supported Encryption methods** define the strength of the encryption used for communication between SSL Network Extender clients and all Mobile Access Security Gateways and Clusters that are managed by the Security Management Server.
  - **AES, 3DES** - This is the default setting. The 3DES encryption algorithm encrypts data three times, for an overall key length of 192 bits.
  - **AES, 3DES or RC4** - to configure the SSL Network Extender client to support the RC4 encryption method, as well as AES and 3DES. RC4 is a variable key-size stream cipher. The algorithm is based on the use of a random permutation. It requires a secure exchange of a shared key that is outside the specification. RC4 is a faster encryption method than 3DES.

Launch SSL Network Extender Client

These settings define the behavior of the SSL Network Extender clients when launched on the endpoint machines.

- **On demand, when user clicks 'Connect" on the portal** - SSL Network Extender only opens when the user clicks "Connect" from the Mobile Access Portal.
- **Automatically, when user logs on** - When users log in to the Mobile Access Portal, SSL Network Extender launches automatically.
- **Automatically minimize client window after client connects** - For either of the options above, choose to minimize the SSL Network Extender window to the system tray on the taskbar after connecting. This provides better usability for non-technical users.

Endpoint Application Types

When defining a Native Application, you can define applications on endpoint machines. These applications launch on the endpoint machine when the user clicks a link in the Mobile Access Portal. You do not have to configure endpoint applications for users using SSL Network Extender in Network Mode, as they will be able to access them using their native clients.

Application Installed on Endpoint Machine

These endpoint applications are already installed on the endpoint machines.

Application Runs Via a Default Browser

Run via default browser is used to define a link to any URL. The link appears in the Mobile Access Portal, and launches the current Web browser (the same browser as the Mobile Access Portal). The link can include $$user, which represents the user name of the currently logged-in user.

This option has a user experience similar to a Web Application with a URL: The application is opened in a Web browser. However, Mobile Access Web applications perform Link Translation on the URL and encrypt the connection over SSL, while the "Run via default browser" option with SSL Network Extender does not perform link translation, and encrypts using SSL Network Extender. You may prefer to define a Native Application rather than a Web Application for convenience, or because some websites have problems working with Link Translation.

Applications Downloaded-from-Gateway

Downloaded-from-Gateway applications let you select applications that download from Mobile Access to the endpoint computer when the user clicks a link in the Mobile Access Portal.

These applications allow end users to securely use client-server applications, without requiring a native client to be installed on their machines.

Mobile Access has built-in applications that the administrator can configure. Downloaded-from-Gateway applications are either Java-based applications or single-executable applications (including batch files). All the applications that are available by default, other than the Terminal (PuTTY) client, are Java based applications, and are therefore multi-platform applications. The PuTTY client can only be used on Windows machines.

You can add Native Applications for Client-Based Access, in addition to the built-in applications.

The Downloaded-from-Gateway applications are third-party applications, which are supplied as-is, and for which Check Point provides limited support.

Some of these packages are not signed by Check Point, and when they are downloaded by end- users a popup warning informs the user that the package is not signed.

Downloaded-from-Gateway Applications

Application	Description
Remote Desktop (RDP)	Downloaded-from-Gateway Client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services. Communicates using Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required. Runs on Java 1.1 up (optimized for 1.4), and works on Linux, Windows and Mac.
Terminal (PuTTY)	An implementation of Telnet and SSH for Win32 platforms, including an Xterm terminal emulator.
Jabber	Downloaded-from-Gateway Jabber Client is an instant messenger based on the Jabber protocol. Runs on every computer with at least Java 1.4.
FTP	Graphical Java network and file transfer client. Supports FTP using its own FTP API and various other protocols like SMB, SFTP, NFS, HTTP, and file I/O using third party APIs, includes many advanced features such as recursive directory up/download, browsing FTP servers while transferring files, FTP resuming and queuing, browsing the LAN for Windows shares, and more.
Telnet	Telnet terminal. Provides user oriented command line login sessions between hosts on the Internet.

Application	Description
SSH	Secure Shell (SSH) is designed for logging into and executing commands on a networked computer. It provides secure encrypted communications between two hosts over an insecure network. An SSH server, by default, listens on the standard TCP port 22.
TN3270	IBM 3270 terminal emulator tailored to writing screen-scraping applications. TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.
TN5250	IBM 5250 terminal emulator that interprets and displays 5250 data streams.

Notes:

- You can also use Native Applications for Client-Based Access.
- When users are connected to the Mobile Access Gateway with SSL Network Extender in Application Mode, the Downloaded-from-Gateway applications do not work inside Endpoint Security On Demand Secure Workspace.

Configuring Authorized Locations per User Group

The authorized locations (hosts or address ranges) of a Native application are defined in the **Authorized Locations** page of the Native Application. However, it is also possible to configure authorized locations per user group. Users who belong to two or more groups can access the union of the authorized locations of the groups.

For configuration details, see sk32111.

Ensuring the Link Appears in the End-User Browser

If an endpoint application is defined by the administrator, but is not available on the endpoint machine, the link to the application will not be shown in the Mobile Access Portal.

For example, the link will not be shown if:

- An endpoint application that is pre-installed on the endpoint machine (of type "Already Installed") is configured, and the application is in fact not installed on the endpoint machine.
- A Downloaded-from-Gateway (Embedded) application requires Java, but Java is not installed on the endpoint machine.

Configuring a Simple Native Application

To configure a simple Native Application

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Native Applications**.
3. Click **New**.

   The **Native Application** window opens.

General Properties

In the **General Properties** page, define the name of the Native Application.

Authorized Locations

1. Go to the **Authorized Locations** page.

   An authorized location ensures users of the Native Application can only access the specified locations using the specified services.

2. Fill in the fields:

   - **Host or Address Range** is the machine or address range on which the application is hosted.
   - **Service** is the port on which the machine hosting the application listens for communication from application clients.

Applications on the Endpoint Computer

1. Go to the **Endpoint Applications** page.
2. Fill in the fields:

   - **Add link in the Mobile Accessportal** must be selected if you want to make endpoint application (s) associated with the Native Applications available to users.
   - **Link text** can include $$user, a variable that represents the user name of the currently logged-in user.
   - **Tooltip** for additional information. Can include `$$user`, which represents the user name of the currently logged-in user.
   - **Path and executable name** must specify one of the following:

     Note - If the endpoint application is not available on the endpoint machine, the link to the application will not be shown in the end user's browser.

     - Full path of the application on the endpoint machines. For example:
       `c:\WINDOWS\system32\ftp.exe`
     - The location of the application by means of an environment variable. This allows the location of the application to be specified in a more generalized way. For example:
       `%windir%\system32\ftp.exe`
     - If the application is listed in the Windows **Start > Programs** menu, only the application name need be entered, as it appears to the user in the Start menu. For example **HyperTerminal**.
     - If the location of the application is in the `path` of the endpoint computer, only the application name need be entered. For example:
       `ftp.exe`
   - **Parameters** are used to pass additional information to applications on the endpoint computer, and to configure the way they are launched.

Using the $$user Variable in Native Applications

You can use the `$$user` variable to define customized login parameters for native applications. To do this, enter the `$$user` variable wherever you need to specify a user name.

For example, you can use the `$$user` variable to return the user name as a part of the login string for Remote Desktop. In this example, `$$user.example.com` (in the **Parameters** field) resolves to the login string `ethan.example.com` for Ethan or `richard.example.com` for Richard.

Completing the Native Application Configuration

To complete the configuration, add the Native application to a policy rule and install policy from SmartConsole.

If necessary, configure the Native Applications for Client-Based Access.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 49*.

For legacy policy, see *"Getting Started with Mobile Access" on page 38*.

Configuring an Advanced Native Application

To configure an advanced Native Application

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Applications > Native Applications**.
3. Click **New**.

   The **Native Application** window opens.

Configuring Connection Direction

1. In the **General Properties** page of the Native Application object, click **Connection direction**.

   The **Advanced** window opens.
2. Select an option for the **Direction of communication from the connection initiator**:
   - **Client to server:** (For example, Telnet.) This is the default option. When you create a client to server application and assign it to a user group, you enable users of the group to initiate a connection to the specified server.
   - **Server to client:** (For example, X11.) When you create a server to client application, the specified server can initiate a connection to all SSL Network Extender or Secure Client Mobile users currently logged on to the Mobile Access Security Gateway, regardless of their group association.
   - **Client to client:** (For example, running Remote Administration from one client to another.) When you create a client to client Native Application and assign it to a user group, you enable users of that group to initiate a connection to all of the SSL Network Extender or Secure Client Mobile users currently logged on to Mobile Access, regardless of their user group association.

Note - A Client to Client Native Application does not require configuration of a destination address.

Multiple Hosts and Services

The native application can reside on a range of hosts, which can be accessed by the native application clients. You can also specify more than one service that clients may use to communicate with the application.

Users of the native application can only access the specified locations using the specified services.

To define a native application with multiple hosts and services

1. Define a **Native Application**.
2. In the **Authorized Locations** page of the Native Application object, select **Advanced**.
3. Click **Edit**.

   The **Native Application - Advanced** window opens.
4. Click **Add** or **Edit**.

   The **Native Application Hosts** window opens.
5. Configure the hosts.
6. Click **OK**.

Configuring the Endpoint Application to Run Via a Default Browser

To configure the Endpoint Application to run via a default browser

1. Define a Native Application.
2. In the **Endpoint Applications** page of the Native Application object, select **Add link in the Mobile Access Portal**.
3. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
4. Click **Add**.

   The **Edit Endpoint Application** window opens.
5. Select **Run via default browser**. This is used to define a link to any URL. The link appears in the Mobile Access Portal, and launches the current Web browser (the same browser as the Mobile Access Portal). The link can include `$$user`, which represents the user name of the currently logged-in user.

   This option has a similar user experience to a Web Application with a URL: The application is opened in a Web browser. However, Mobile Access Web applications perform Link Translation on the URL and encrypt the connection over SSL, while the "Run via default browser" option with SSL Network Extender does not perform link translation, and encrypts using SSL Network Extender. You may prefer to define a Native Application rather than a Web Application for convenience, or because some Web sites have problems working with Link Translation.

Automatically Starting the Application

To configure the Endpoint Application to start automatically:

1. Define a Native Application.
2. In the **Endpoint Applications** page of the Native Application object, select **Add link in the Mobile Access Portal**.
3. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
4. Click **Add** or **Edit**.

   The **Edit Endpoint Application** window opens.
5. Click **Advanced**.
   - **Automatically Start this Application** - Configure a Native Application to run a program or command automatically, after connecting to or disconnecting from SSL Network Extender (either Network mode or Application mode). When more than one Native Application is defined for automatic connection or disconnection, the applications run in the alphabetical order of the names of the Native Applications.
   - **When SSL Network Extender is disconnected** - Do not use this option to launch applications that require connectivity to the organization - SSL Network Extender Application Mode. In Network Mode, automatic start of applications when SSL Network Extender is disconnected, works correctly.

Making an Application Available in Application Mode

To make an application available in Application Mode

1. Define a Native Application.
2. In the **Endpoint Applications** page of the Native Application object, select **Add link in the Mobile Access Portal**.
3. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
4. Click **Add** or **Edit**.

   The **Edit Endpoint Application** window opens.
5. Click **Advanced**.
6. Select **Show link to this application in SSL Network Extender Application Mode**. The option **SSL Network Extender application mode compatibility** lets you make an application available to Application Mode clients. Users that connect using the SSL Network Extender Application Mode client are able to see a link to the application and launch it. Use this option if the application works well in Application Mode.

Note - If this option is NOT selected users who connect with Application Mode, do not see it in their list of applications.

Automatically Running Commands or Scripts

It is possible to configure a Native Application to run a program or command automatically, after connecting to or disconnecting from SSL Network Extender (either Network mode or Application mode).

Note - The user must have the appropriate privileges on the endpoint machine to run the commands.

One example of how automatically running a command can be useful is to mount or unmount a network drive. Giving users access to network drives is a convenient way of providing access to internal resources. A drive can be mapped by configuring an application that invokes the Windows `net use` command.

Note - When more than one Native Application is defined for automatic connection or disconnection, the applications run in the alphabetical order of the names of the Native Applications.

For configuration details, see the "Native Applications for Client-Based Access" section.

It is possible to extend this ability by defining a dynamic add-on Downloaded-from-Gateway application that runs a script (batch file) containing a sequence of commands to execute on the endpoint machine. This script can be launched manually when the user clicks a link, or it can launch automatically after connecting to or disconnecting from SSL Network Extender.

For configuration details, see the "Native Applications for Client-Based Access" section.

How to Automatically Map and Unmap a Network Drive

A drive can be mapped by configuring an application that invokes the Windows "`net use`" command.

Note - The "`net use`" command is available for SSL Network Mode only.

To automatically map (mount) and unmap (unmount) a network drive, create a Native Application that automatically maps the network drive when SSL Network Extender is launched:

1. Define a Native Application.
2. In the **Endpoint Applications** page of the Native Application object, select **Add link in the Mobile Access Portal**.
3. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
4. Click **Add** or **Edit**.

   The **Edit Endpoint Application** window opens.
5. Configure the **Edit Endpoint Application** page as follows:
   - **Already installed**.
   - **Path and executable name**: `net.exe`
   - **Parameters**: `use drive_letter: \\server name\share name`
6. Click **Advanced**.
7. Check **When SSL Network Extender is launched**.
8. Create another Native Application that automatically unmaps the network drive when SSL Network Extender is disconnected. Configure these settings in the **Edit Endpoint Application** page:

- **Already installed**
- **Path and executable name**: `net.exe`
- **Parameters**: `use /DELETE drive_letter:`

9. Click **Advanced**.
10. Check **When SSL Network Extender is disconnected**.
11. Click **OK**.

How to Automatically Run a Script (Batch File)

It is possible to define a new Downloaded-from-Gateway Endpoint Application (embedded application) that runs a script (batch file) automatically after connecting to or disconnecting from SSL Network Extender.

To automatically run a script

1. Create a batch (script) file containing a sequence of commands.
2. Define the batch file as a new Native Applications for Client-Based Access.
3. Define a Native Application.
4. In the **Endpoint Applications** page of the Native Application object, select **Add link in the Mobile Access Portal**.
5. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
6. Click **Add** or **Edit**.

   The **Edit Endpoint Application** window opens.
7. Click **Advanced**.
8. In the **Automatically start this application** section, select **When SSL Network Extender is launched**.

Protection Levels for Native Applications

You can define a protection level for each native application. Configure this in the Properties window of each native application in **Additional Settings** > **Protection Level**.

The options are:

- **This application relies on the security requirements of the gateway**
  Rely on the Security Gateway security requirements. Users authorized to use the portal are also authorized to use this application. This is the default option.
- **This application has additional security requirements specific to the following protection level**
  Associate the Protection Level with the application. Users must be compliant with the security requirement for this application in addition to the requirements for the portal.

Defining Protection Levels

To access the Protection Level page from the Mobile Access tab

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree click **Additional Settings > Protection Levels** page from the navigation tree.

3. Click **New** to create a new Protection Level or double-click an existing Protection Level to modify it.

   The **Protection Levels** window opens, and shows the **General Properties** page.

To access the Protection Level page from a Mobile Access application

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E). Or in SmartDashboard, **Mobile Access** tab, go to **Applications** > Application type.

2. Search for the Mobile Access application.

3. Double-click the application.

4. From the navigation tree, select **Additional Setting > Protection Level**.

5. To create a new Protection Level, select **Manage > New**.

6. To edit the settings of a Protection Level, select the Protection Level from the drop down list and then select **Manage > Details**.

   The **Protection Levels** window opens, and shows the **General Properties** page.

To configure the settings for a Protection Level

1. From the **General Properties** page in the **Protection Level** window, enter the **Name** for the Protection Level (for a new Protection Level only).

2. In the navigation tree, click **Authentication** and select one or more authentication methods from the available choices. Users accessing an application with this Protection Level must use one of the selected authentication schemes.

3. If necessary, select **User must successfully authenticate via SMS**.

4. In the navigation tree, click **Endpoint Security** and select one or both of these options:

   - **Applications using this Protection Level can only be accessed if the endpoint machine complies with the following Endpoint compliance policy**. Also, select a policy. This option gives access to the associated application only if the scanned client computer complies with the selected policy.
   - **Applications using this Protection Level can only be accesses from within Secure Workspace**. This option requires Secure Workspace to be running on the client computer.

5. Click **OK** to close the Protection Level window

6. Install the policy.

Adding Downloaded-from-Gateway Endpoint Applications

You can add Downloaded-from-Gateway applications to Mobile Access, in addition to the built-in applications. This section explains how, and gives detailed examples.

Downloaded-from-Gateway Application Requirements

Downloaded-from-Gateway applications are either Java-based applications or single-executable applications (including batch files).

Java applications have the following requirements:

- Application must be packaged into a JAR file
- The JVM of a version required by the application must be installed on the endpoint machine.
- The application must have a `Main` class.

Single-executable applications have the following requirements:

- Must not require installation.
- Must be platform-specific for Windows, Linux, or macOS.

Adding a New Application

To add a new Downloaded-from-Gateway application, first put the application in the relevant directory on the Security Gateway. Then use GuiDBedit Tool (see sk13009) to set its properties.

To add a new downloaded-from-gateway endpoint application:

1. Compress your downloaded-from-gateway application file into CAB file with the same name as the original file but with a `.cab` extension.

   To compress a file into a CAB file, you can use the Microsoft Cabinet Tool `cabarc.exe` (which can be downloaded from the Microsoft Web site).

   For example:

   ```
   cabarc.exe -m LZX:20 -s 6144 N ssh2.cab ssh2.jar
   ```

2. Copy both your downloaded-from-gateway application file and the `.cab` file you created to the Security Gateway machine at:

   ```
   $CVPNDIR/htdocs/SNX/CSHELL
   ```

3. Change the application file permissions to read, write and execute.
4. Run the GuiDBedit Tool - see sk13009.
5. Log in to the Security Management Server.
6. Select **Table** > **Other** > **embedded_applications**.
7. In the right side pane, right-click and select **New**.

8. In the **Object** field, enter a name for the new downloaded-from-application.
9. Specify the characteristics of the new downloaded-from-gateway application.

Field Name	Description
`display_name`	The application name, which will appear in the drop-down list of downloaded-from-gateway applications in SmartDashboard, in the **Edit Endpoint Application** window.
`embedded_application_type`	The type of downloaded-from-gateway application. Choose one of the options in the **Valid Values** list (*java_applet*, *linux_executable*, *mac_executable*, *windows_executable*).
`file_name`	The name of the file you placed in `$CPVNDIR/htdocs/SNX/CSHELL` (not the .cab version).
`server_name_required_params`	Indicate if the new downloaded-from-gateway application requires the server name to be configured in the Parameters field of the new downloaded-from-gateway application, in the SmartDashboard **Edit Endpoint Application** window.
`pre_custom_params`	Parameters concatenated before the `server_name_required_params` field. Usually used when configuring a new downloaded-from-gateway Java application. In that case, specify the Main Class name of the application.
`post_custom_params`	Parameters concatenated after the `server_name_required_params` field. Can be left blank.
`type`	Leave as `embedded_application`.

You can see and configure the new downloaded-from-gateway application in SmartDashboard, just as you do with the built-in downloaded-from-gateway applications. The downloaded-from-gateway applications appear in the **Edit Network Application** page of the Native Application object (Getting there: **Native Application object** > **Endpoint applications page** > **Advanced: Edit > Add/Edit**.

Example: Adding a New SSH Application

This example adds two applications to Mobile Access as new downloaded-from-Mobile Access applications:

1. SSH2 Java application:
   - JAR file name: `ssh2.jar`
   - Main class name: `ssh2.Main`
   - The application gets its server name as a parameter.
   - Name in SmartDashboard: `Jssh2 Client`.
2. SSH2 Windows executable:
   - Executable file name: `WinSsh2.exe`
   - The application gets its server name as parameter.
   - Name in SmartDashboard: `Essh2 Client`.

To add these applications:

1. Compress the `ssh2.jar` and `WinSsh2.exe` application files into `ssh2.cab` and `WinSsh2.cab`

   ```
   # cabarc.exe -m LZX:20 -s 6144 N ssh2.cab ssh2.jar
   # cabarc.exe -m LZX:20 -s 6144 N WinSsh2.cab WinSsh2.exe
   ```

2. Assuming the IP address of the SSH2 server is 1.1.1.1, save the files `ssh2.jar` and `WinSsh2.exe` to `$CVPNDIR/htdocs/SNX/CSHELL` with the proper permissions.
3. Put the application files in `$CVPNDIR/htdocs/SNX/CSHELL` with the proper permissions.
4. Use GuiDBedit Tool (see sk13009) or dbedit (see skI3301) to configure the two new downloaded-from-Mobile Access applications.

   SSH2 Java Application

Field Name	Value
`display_name`	Jssh2 Client
`embedded_application_type`	java_applet
`file_name`	ssh2.jar
`post_custom_params`	Empty
`pre_custom_params`	ssh2.Main
`server_name_required_params`	true
`type`	embedded_application

   SSH2 Windows Executable

Field Name	Value
`display_name`	Essh2 Client
`embedded_application_type`	windows_executable
`file_name`	WinSsh2.exe
`post_custom_params`	Empty
`pre_custom_params`	Empty
`server_name_required_params`	true
`type`	embedded_application

When you configure one of these new downloaded-from-Mobile Access applications (*Jssh2 Client* and *Essh2 Client*) in SmartDashboard, the **Parameters** field will be: 1.1.1.1 (the SSH2 server IP in this example).

Example: Adding a New Microsoft Remote Desktop Profile

This example demonstrates how to configure Mobile Access to work with Microsoft Remote Desktop, with a predefined profile. It also shows how to configure the profile per user group.

1. **Create the Remote Desktop Profile**

   Create the RDP profile file (with an .rdp extension) using Microsoft Remote Desktop Connection, found at `%SystemRoot%\system32\mstsc.exe`.

   When creating the profile, you can define the address, the settings, applications that should run at log in, and more.

   In this example, the profile file has the name of the relevant user group. For a user group called `mygr1`, save a profile file called `mygr1.rdp`.

2. **Create a CAB Package from the Profile**

   a. Compress the profile file into CAB file with the same name as the original file.

      You can use the Microsoft Cabinet Tool `cabarc.exe` (which can be downloaded from the Microsoft Web site).

      For this example, run the command:

      ```
      cabarc.exe -m LZX:20 -s 6144 N mygr1.cab mygr1.rdp
      ```

      This produces the output file `mygr1.cab`

   b. Copy both `mygr1.rdp` and `mygr1.cab` to the Mobile Access machine at `$CVPNDIR/htdocs/SNX/CSHELL`.

   c. Change their permissions to read, write and execute.

3. **Configure the Package Downloaded-from-Gateway Application**

   a. Run the GuiDBedit Tool - see sk13009.

   b. Enter the administrator user name and password.

   c. In the top left pane, go to **Table > Other > embedded_applications**.

      The **embedded_applications** table opens.

   d. In the top right pane, right-click and select **New...**.

   e. In the **Object** field, enter a name for the new downloaded-from-gateway application. Give it the name of the relevant user group. In this example: **mygr1**

   f. Specify the characteristics of the new downloaded-from-gateway application as follows:

      - **display_name**: **mygr1_RDP_Policy**
      - **embedded_application_type**: **windows_executable**
      - **file_name**: **mygr1.rdp**

      You can now see and configure the new downloaded-from-gateway application in SmartDashboard, just as for the built-in downloaded-from-gateway applications.

   g. Save the changes (**File** menu > **Save All**).

   h. Close the GuiDBedit Tool.

i. Open the SmartDashboard.

4. **Configure the Link to the Remote Desktop Application**

   Configure the link to Microsoft Remote Desktop that will appear in the SSL Network Extender window. Define it as an Already Installed endpoint application.

   a. Define a Native Application.

   b. In the **Endpoint Application** page of the Native Application, select **Add a Link to the application in the Mobile Access Portal**.

   c. Select **Advanced**, and click **Edit**.

      The **Endpoint Applications - Advanced** window opens.

   d. Click **Add**. The **Edit Endpoint Application** window opens.

   e. In the **Edit Endpoint Application** window, use the following settings, as shown in the screen capture:

      - **Link text (Multi-language):** `MS-RDP` (or any other name).
      - **Path and executable name:** `%SystemRoot%\system32\mstsc.exe`
      - **Parameters:** `%temp%\mygr1.rdp`

   f. Click **OK**.

5. **Configure the Remote Desktop Profile to Start Automatically**

   In the same Native Application, add another endpoint application for the Remote Desktop Profile. Define it as a Downloaded-from-Mobile Access endpoint application, which is downloaded to the user desktop as soon as SSL Network Extender is launched.

   a. In the **Endpoint Applications - Advanced** window, click **Add**.

      The **Edit Endpoint Application** window opens.

   b. Configure the Remote Desktop profile package with the following settings.

      - **Add link to the application in the Mobile Access Portal** must be *cleared*.
      - **Name: mygr1_RDP_Policy** (as configured in the GuiDBedit Tool).

   c. Click **Advanced**.

   d. Select **Automatically Start this Application: When SSL Network Extender is launched**.

   e. Click **OK** three times to save and close the Native Application.

6. **Assign the Native Application to the User Group**

   Assign the Native Application to the relevant user group.

Repeat for every new Microsoft Remote Desktop Connection.

Configuring Downloaded-from-Gateway Endpoint Applications

In the **Endpoint Applications** page of the Native Application object:

1. Select **Add link in the Mobile Access Portal**.
2. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
3. Click **Add**.

   The **Edit Endpoint Application** window opens.
4. Select **Downloaded-from-Gateway**.
5. From the **Name** drop-down list, select the applicable downloaded-from-gateway application.
6. Specify the **Parameters** for the downloaded-from-Security Gateway application. The parameters field is used to pass additional information to the downloaded-from-gateway applications on the endpoint machine, and to configure the way they are launched.

   The `$$user` variable can be used here to dynamically change according to the login name of the currently logged in user.

   See the configuration sections below for details of the required parameters:

Note - In the configuration sections for certified and add-on applications, below:
- `parameter` is a compulsory parameter,
- `[parameter]` is an optional parameter,
- `|` indicates a required choice of one from many.

- **Configuring the Telnet Client (Certified Application)**

Supported Platforms	All
Parameters field	Server name or IP address. Default port is 23.
Parameters usage	`server [port]`
Description	Telnet terminal. Provides user oriented command line login sessions between hosts on the Internet.
Home page	http://javassh.org

- **Configuring the SSH Client (Certified Application)**

Supported Platforms	All
Parameters field	Server name or IP address.
Parameters usage	`server`
Description	Secure Shell (SSH) is designed for logging into and executing commands on a networked computer. It provides secure encrypted communications between two hosts over an insecure network. An SSH server, by default, listens on the standard TCP port 22.
Home page	http://javassh.org

- **Configuring the TN3270 Client (Certified Application)**

Supported Platforms	All. Requires Java 1.3.1 or higher.
Parameters field	Ignored
Description	IBM 3270 terminal emulator tailored to writing screen-scraping applications. TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.
Home page	http://jagacy.com

- **Configuring the TN5250 Client (Certified Application)**

Supported Platforms	All endpoint machines must have Java 1.4 or higher.
Parameters field	Optional. Can use the Configure button on the application instead. For the full list of options that can be used in the parameters field, see the Quick Start Guide http://tn5250j.sourceforge.net/quick.html.
Parameters usage	`[server [options]]`
Description	IBM 5250 terminal emulator that interprets and displays 5250 data streams. You will be presented with a Connections screen for defining sessions. Select the configure button to define sessions when the session selection window opens. On first invocation of the emulator there are some console warning messages. These inform you that defaults files are being set up for the first run.
Home page	http://tn5250j.sourceforge.net/index.html
Quick Start Guide	http://tn5250j.sourceforge.net/quick.html

Configuring the Remote Desktop Client (Add-On Application)

Supported Platforms	All platforms. Endpoint machines must have Java 1.4 or higher.
Parameters field	Must contain the server name or its IP address.
Parameters usage	`[options] server[:port]` For example: `-g 800x600 -l WARN RDP_Server` Options: • `-b` - Bandwidth saving (good for 56k modem, but higher latency). This option clears the TCP 'no delay' flag. • `-d` - Windows domain you are connecting to. • `-f` - Show the window full-screen (requires Java 1.4 for proper operation). • `-g` - The size of the desktop in pixels (width x height). • `-m` - Keyboard layout on terminal server for languages (for example, en-us). • `-l {DEBUG, INFO, WARN, ERROR, FATAL}` - Amount of debug output (otherwise known as the logging level). • `-lc` - Path to a log4j configuration file. • `-n` - Override the name of the endpoint machine. • `-u` - Name of the user to connect as. • `-p` - Password for the above user. • `-s` - Shell to launch when the session is started. • `-t` - Port to connect to (useful if you are using an SSH tunnel, for example). • `-T` - Override the window title.
Description	Downloaded-from-Mobile Access Client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services. Communicates using Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required. Runs on Java 1.1 up (optimized for 1.4), and works on Linux, Windows and Mac.
Home page	http://properjavardp.sourceforge.net

Configuring the PuTTY Client (Add-On Application)

Supported Platforms	Windows only
Parameters field	Optional. Leaving the Parameters field empty leads PuTTY Client to open in full graphical mode.
Parameters usage	`[[-ssh | -telnet | -rlogin | -raw] [user@]server [port]]`
Description	An implementation of Telnet and SSH for Win32 platforms, including an Xterm terminal emulator.
Home page	http://www.eos.ncsu.edu/remoteaccess/putty.html

- **Configuring the Jabber Client (Add-On Application)**

Supported Platforms	All platforms. Endpoint machines must have Java 1.4 or higher.
Parameters field	Ignored
Description	Downloaded-from-Gateway Jabber Client is an instant messenger based on the Jabber protocol Runs on every computer with at least Java 1.4.
Home page	http://jeti.jabberstudio.org

- **Configuring the FTP Client (Add-On Application)**

Supported Platforms	All endpoint machines must have Java 1.4 or higher.
Parameters field	Ignored
Description	Graphical Java network and file transfer client. Supports FTP using its own FTP API and various other protocols like SMB, SFTP, NFS, HTTP, and file I/O using third party APIs, includes many advanced features such as recursive directory up/download, browsing FTP servers while transferring files, FTP resuming and queuing, browsing the LAN for Windows shares, and more.
Home page	http://j-ftp.sourceforge.net

7. Configure Native Applications for Client-Based Access.

Exchange Mail Applications for Smartphones and Tablets

Introduction to Exchange Mail Applications

Mobile Mail and Active Sync Applications are applications for smartphone and tablet users to connect to email, calendar, contacts, and notes through an Exchange server. Web applications and File shares can also be available on smartphones and tablets.

Mobile Mail Applications

Mobile Mail Applications work with Exchange servers to make business email available on mobile devices with a Capsule Workspace App. The application is in a secure area on the Mobile Device that is usually protected with a passcode. All data in Capsule Workspace is encrypted.

During the Mobile Access Wizard, if you select **Mobile Devices > Capsule Workspace**, and enter an Exchange server, a Mobile Mail Application is automatically created. Make sure that users have access to the Mobile Mail Application in your Mobile Access policy.

Configuring Mobile Mail Applications

To create and configure a new Mobile Mail application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Business Mail**.

   The **Mobile Mail Application** window opens.
3. In the **General Properties** page:
   - Enter a **Name** for the application in SmartDashboard
   - Enter the name of the **Exchange Server** that communicates with the Security Gateway and the **Port**. For example, **ad.example.com**
4. In the **Exchange Access** page, in the **Define access settings** area:
   - **Use encryption (https)** - By default, traffic to the Exchange server works with HTTPS.
   - **Use non-default path** - If the Exchange Web Services path on the Exchange server to the application is not the default, enter the path here.

     The default path is `EWS/Exchange.asmx` and the URL is `https://<IP address of the Exchange Server>/EWS/Exchange.asmx`
   - **Use specific domain** - If you want users to authenticate to a specified domain on the Exchange server, enter it here.
5. In the **Exchange Access** page, in the **Proxy Settings** area, if there is a proxy server between the Exchange Server and the Security Gateway, configure these settings:

- **Use gateway proxy settings** - By default the proxy settings configured for the Security Gateway are used.
- **Do not use proxy server** - Select if no proxy server is required.
- **Use specific proxy server** - Configure a proxy server that the Security Gateway communicates with to reach the Exchange Server.

a. Select the **Host** and **Service**.

b. If credentials are required to access the proxy server, select **Use credentials for accessing the proxy server** and enter the **Username** and **Password**.

6. In the **Display Link** page:
   - **Title** - The name of the application that users will see on their mobile devices.
   - **Description** - The description of the application that users will see on their mobile devices.
7. In the **Single Sign On** page, select the source of the credentials used for Single Sign-On for this application:
   - **Login to Exchange with the application credentials** - By default, use the same credentials that users use to log in to the Business Secure Container. This only applies if the authentication method configured for them on the Security Gateway is Username/Password (**Gateway Properties** > **Mobile Access** > **Authentication**).
   - **Prompt for user credentials and store them locally for reuse** - Use different credentials for the Business Secure Container.
     - **Show the user the following message on the credentials prompt** - Select this and enter a message that users see when prompted to enter the credentials required for the Business Secure Container.
8. In the **Periodic Test** page, select which tests are run regularly on the Security Gateways to make sure they can connect to the Exchange server. If there is a connectivity problem, a System Alert log generated.
   - **Run periodic test from gateways that have access to this application** - A test makes sure there is connectivity between the Security Gateway and Exchange server. The test runs at the interval that you enter.
   - **Perform extensive test using the following account** - Periodically run a test to make sure that a user can authenticate to the Exchange server. To run this test you must enter a valid **Username** and **Password**.

   Note - If the account password changes, you must enter the new password here.
9. Click **OK**.
10. Install the policy.

ActiveSync Applications

An ActiveSync application is an email application that works with ActiveSync, which is native in most Mobile devices. Mobile devices that can use the ActiveSync protocol and connect to an Exchange server can access ActiveSync applications.

As opposed to Mobile Mail applications, ActiveSync applications are not located in the Business Secure Container and are not protected. If you use the ActiveSync application, make sure that your mobile device is protected in other ways so that your sensitive business data and Exchange user credentials stay safe.

Make sure to give users access to the ActiveSync application in your Mobile Access policy.

Configuring ActiveSync Applications

To create a new ActiveSync application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > ActiveSync Application**.

   The ActiveSync Application window opens.

To configure an ActiveSync application:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The **ActiveSync Application** window opens.
4. In the **General Properties** page:
   - Enter a **Name** for the application in SmartDashboard
   - Enter the name of the **Exchange Server** that will communicate with the Security Gateway and the **Port**. For example, **ad. example.com**
5. In the **Exchange Access** page, in the **Define access settings** area:
   - **Use encryption (https)** - By default, traffic to the Exchange server works with HTTPS.
   - **Use non-default path** - If the ActiveSync path on the Exchange server to the application is not the default, enter the path here.
   - **Use specific domain** - If you want users to authenticate to a specified domain on the Exchange server, enter it here.
6. In the **Exchange Access** page, in the **Proxy Settings** area, if there is a proxy server between the Exchange Server and the Security Gateway, configure the settings here.
   - **Use gateway proxy settings** - By default the proxy settings configured for the Security Gateway are used.
   - **Do not use proxy server** - Select if no proxy server is required.
   - **Use specific proxy server** - Configure a proxy server that the Security Gateway communicates with to reach the Exchange Server.

   a. Select the **Host** and **Service**.

   b. If credentials are required to access the proxy server, select **Use credentials for accessing the proxy server** and enter the **Username** and **Password**.
7. In the **Display Link** page:
   - **Title** - The name of the application that users will see on their mobile devices.
   - **Description** - The description of the application that users will see on their mobile devices.

8. In the **Periodic Test** page, select which tests are run regularly on the Security Gateways to make sure they can connect to the Exchange server. If there is a connectivity problem, a System Alert log generated.
    - **Run periodic test from gateways that have access to this application** - A test makes sure there is connectivity between the Security Gateway and Exchange server. The test runs at the interval that you enter.
    - **Perform extensive test using the following account** - Periodically run a test to make sure that a user can authenticate to the Exchange server. To run this test you must enter a valid **Username** and **Password**.

    Note - If the account password changes, you must enter the new password here.
9. Click **OK**.
10. Install the policy.

Configuring a TLS/SSL Version for an Application

You can configure which SSL protocol to use on the internal server for Web applications and Exchange Mail applications. For example, you can configure that a Mobile Mail application always uses TLS 1.0. If you do not configure this, Mobile Access uses the default version that the organizational server recommends.

Configure the feature for each application in GuiDBedit Tool (see sk13009).

To configure an SSL version for an application:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with GuiDBedit Tool to the Management Server.
3. Go to **Other** > **network_applications** > **APPLICATION NAME** > **internal_resource_ssl_version**.
4. Select a version. The options are:
    - auto (default) - Uses the version that the organizational server recommends
    - SSLv3 (SSL 3.0)
    - TLSv1 (TLS 1.0)
    - TLSv1.1 (TLS 1.1)
    - TLSv1.2 (TLS 1.2)
5. Save the changes and close GuiDBedit Tool.
6. Connect with SmartConsole to the Management Server.
7. Install policy.

Policy Requirements for ActiveSync Applications

- To access ActiveSync, users must belong to a user group that is allowed to access ActiveSync applications.
- Each user must have an email address defined the **Email Address** field in the properties of an internal user object, or on an LDAP server (for LDAP users).
- If users are internal, their Check Point client passwords must be the same as their Exchange passwords, otherwise ActiveSync will not work.

Mobile Access for Smartphones and Tablets

Overview of Mobile Access for Smartphones and Tablets

To manage your users and their access to resources, make sure to:

- For email, calendar, and contact access, configure Mobile Mail or ActiveSync applications.

  This can be done automatically in the Mobile Access Wizard.
- Configure Web applications, if necessary.
- Make sure users have the information and credentials required to authenticate to the Security Gateway.

  For client certificates, use the Certificate Creation and Distribution Wizard (see the "Creating Client Certificates" section).
- Make sure users' Mobile Settings meet your organization's needs (see the "Managing Mobile Settings" section).
- Tell users which App to install.
- Make sure smartphone and tablet users are included in your Mobile Access Policy.

Certificate Authentication for Handheld Devices

For handheld devices to connect to the Security Gateway, these certificates must be properly configured:

- If the configured authentication methods is Personal Certificate, generate client certificates for users (see the "Managing Client Certificates" section).
- A server certificate signed by a trusted third-party Certification Authority (for example, Entrust) is strongly recommended. If you have a third-party certificate, make sure the CA is trusted by the device. If you do not have a third-party certificate, a self-signed (ICA) certificate, is already configured on the server.

Managing Client Certificates

Check Point Mobile Apps for mobile devices can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

Manage client certificates in **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**..

The page has two panes.

- In the **Client Certificates** pane:
  - Create, edit, and revoke client certificates.
  - See all certificates, their status, expiration date and enrollment key. By default, only the first 50 results show in the certificate list. Click **Show more** to see more results.
  - Search for specified certificates.
  - Send certificate information to users.
- In the **Email Templates for Certificate Distribution** pane:
  - Create and edit email templates for client certificate distribution.
  - Preview email templates.

Creating Client Certificates

Note - If you use LDAP or AD, creation of client certificates does not change the LDAP or AD server. If you get an error message regarding LDAP/AD write access, ignore it and close the window to continue.

To create and distribute certificates with the client certificate wizard

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. In the **Client Certificates** pane, click **New**.

   The **Certificate Creation and Distribution** wizard opens.
3. In the **Certificate Distribution** page, select how to distribute the enrollment keys to users. You can select one or both options.
   a. **Send an email containing the enrollment keys using the selected email template** -Each user gets an email, based on the template you choose, that contains an enrollment key.
      - **Template** - Select the email template that is used.
      - **Site** - Select the Security Gateway, to which users connect.
      - **Mail Server** - Select the mail server that sends the emails.

      You can click **Edit** to view and change its details.

   b. **Generate a file that contains all of the enrollment keys** - Generate a file for your records that contains a list of all users and their enrollment keys.
4. **Optional:** To change the expiration date of the enrollment key, edit the number of days in **Users must enroll within x days**.
5. **Optional:** Add a comment that will show next to the certificate in the certificate list on the **Client Certificates** page.
6. Click **Next**.

   The **Users** page opens.
7. Click **Add** to add the users or groups that require certificates.

- Type text in the search field to search for a user or group.
- Select a type of group to narrow your search.

8. When all included users or groups show in the list, click **Generate** to create the certificates and send the emails.
9. If more than 10 certificates are being generated, click **Yes** to confirm that you want to continue.

   A progress window shows. If errors occur, an error report opens.
10. Click **Finish**.
11. Click **Save**.
12. In SmartConsole, install the Policy.

Revoking Certificates

If the status of a certificate is Pending Enrollment, after you revoke it, the certificate does not show in the **Client Certificate** list.

To revoke one or more certificates

1. Select the certificate or certificates from the **Client Certificate** list.
2. Click **Revoke**.
3. Click **OK**.

After you revoke a certificate, it does not show in the **Client Certificate** list.

Creating Templates for Certificate Distribution

To create or edit an email template

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. To create a new template: In the **Email Templates for Certificate Distribution** pane, select **New**.

   To edit a template: In the **Email Templates for Certificate Distribution** pane, double-click a template.

   The **Email Template** opens.
3. Enter a **Name** for the template.
4. **Optional:** Enter a **Comment**. Comments show in the Mail Template list on the **Client Certificates** page.
5. **Optional:** Click **Languages** to change the language of the email.
6. Enter a **Subject** for the email. Click **Insert Field** to add a predefined field, such as a Username.
7. In the message body add and format text. Click **Insert Field** to add a predefined field, such as Username, Registration Key, or Expiration Date.
8. Click inside the E-mail Template body.

9. Click **Insert Link** and select the type of link to add (link or QR code).

   - **Site and Certificate Creation**

     For users who already have a Check Point app installed.

     When users scan the QR code or go to the link, it creates the site and registers the certificate.

     Select the client type that will connect to the site- Select one client type that users will have installed:

     - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
     - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.

   - **Download Application**

     Direct users to download a Check Point App for their mobile devices.

     Select the client device operating system:

     - **iOS**
     - **Android**

     Select the client type that will connect to the site- Select one client type that users will have installed:

     - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
     - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.

   - **Custom URL**

     Lets you configure your own URL.

   For each link type, you can select which elements are added to the mail template

   - **Link URL** - Enter the full link address.
   - **QR Code** - When enabled, users scan the code with their mobile devices.
   - **HTML Link** - When enabled, users tap the link on their mobile devices.

     You can select both **QR Code** and **HTML Link** to include both in the email.
   - **Display Text** - Enter the text for the link title.

10. Click **OK**.
11. **Optional:** Click **Preview in Browser** to see a preview of how the email will look.
12. Click **OK**.
13. Publish the changes

Cloning a Template

Clone an email template to create a template that is similar to one that already exists.

To create a clone of an email template

1. Select a template from the template list in the **Client Certificates** page.
2. Click **Clone**.
3. A new copy of the selected template opens for you to edit.

Remote Wipe

Remote Wipe removes the offline data cached on the user's mobile device.

When the administrator revokes the internal CA certificate, a Remote Wipe push notification is sent, if the Remote Wipe configuration for the client enables **Remote Wipe by Push Notification**. Remote Wipe is triggered when the device gets the push notification.

Note: Remote Wipe by Push Notification works by best effort. There is no guarantee that the Security Gateway will send the notification, or that the client will get it successfully.

If the device does not get the Remote Wipe push notification, Remote Wipe is triggered when the client does an activity that requires connection to the Security Gateway while using a revoked internal CA certificate.

Remote Wipe send logs:

- If a Remote Wipe Push Notification is sent.
- When a Remote Wipe process ends successfully.

This feature is supported in R77.10 and above.

To configure Remote Wipe

1. Run the command on the Security Gateway.

   Syntax: `cvpnd_settings <conf_file_path> {set|listAdd|listRemove} <name> <value>`

   - To enable or disable Remote Wipe:

     ```
     [Expert@HostName:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C set
     RemoteWipeEnabled {true|false}
     ```

     Remote Wipe is enabled by default.

   - To enable or disable Remote Wipe by Push Notification (wipe is done if client gets notification):

     ```
     [Expert@HostName:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C set
     RemoteWipePushEnabled {true|false}
     ```

     The Remote Wipe Push Notifications feature is enabled by default. For supported clients, see sk95587.

- To set supported devices for Remote Wipe Push Notifications, based on operating system:

  ```
  [Expert@HostName:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd
  RemoteWipePushSupportedClientOS {iOS | Android}
  ```

2. Run:

   ```
   [Expert@HostName:0]# cvpnrestart
   ```

   You must restart the cvpn service to apply the changes.

To see that your changes are applied, open the `$CVPNDIR/conf/cvpnd.C` file in Read-Only mode.

To trigger Remote Wipe on a device

1. Make sure that the `cvpnd.C` file is configured for Remote Wipe and, if you want, for Push Notifications.

   If you change the file, run: `[Expert@HostName:0]# cvpnrestart`

2. Revoke the client certificate:
   a. Open **Mobile Access** tab > **Client Certificates**.
   b. Select certificates.
   c. Click **Revoke**.
   d. Click **OK**.

To see Remote Wipe logs

1. Open SmartLog.
2. Query for:

   ```
   "Remote Wipe" AND blade:"Mobile Access" action:"Failed Log In".
   ```

   You can filter these results for user DN, device ID, or certificate serial number.

Managing Mobile Settings

For Capsule Workspace, many settings that affect the user experience on mobile devices come from the **Mobile Profile**.

Each Mobile Access user group has an assigned Mobile Profile. By default, all users get the Default Profile.

The settings in the Mobile Profile include:

- Passcode Settings
- Mail, Calendar, and Contacts availability
- Settings for offline content
- Where contacts come from

Manage the Mobile Profiles in **Mobile Access** tab > **Capsule Workspace Settings**.

- In the **Mobile Profiles** pane:
  - See all Mobile Profiles.
  - Create, edit, delete, clone, and rename Mobile Profiles.
- In the **Mobile Profile Policy** pane:
  - Create rules to assign Mobile Profiles to user groups.
  - Search for a user or group within the policy rules.

Creating and Editing Mobile Profiles

To create or edit a Mobile Profile

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Capsule Workspace**.
3. **Optional:** Create a new Mobile Profile, click **New**.
4. In the **Mobile Profiles** pane select the profile and click **Edit**.
5. Change settings. See the *Capsule Workspace Settings in the Mobile Profile* section below.
6. Click **Save** and then close SmartDashboard.
7. In SmartConsole, install the policy.

Capsule Workspace Settings in the Mobile Profile

Instructions

1. In the **Access Settings** area, configure:
   - **Session timeout** - After users authenticate with the authentication method configured in **Gateway Properties** > **Mobile Access** > **Authentication**, configure how long they stay authenticated to the Security Gateway.
   - **Activate Passcode lock** - Select to protect the Business Secure Container area of the mobile device with a passcode.
     - **Passcode profile** - Select a passcode profile to use. The profile includes the passcode complexity, length, expiration, and number of failed attempts allowed.
     - **Allow storing user credentials on the device for single-sign on** - If username and password authentication is used, store the authentication credentials on the device. Then users are only prompted for their passcode not also for their username and password.
   - **Report jail-broken devices** - Create a log if a jail-broken device connects to the Security Gateway.
     - **Block access from jail-broken devices** - Block devices that are jail-broken from connecting to the Security Gateway.

- **Track user's GPS location** (upon user's approval) - Tracks devices connecting to the Security Gateway.

2. In the **Allowed Items** area, select which Exchange features are available on devices:
   - **Mail**
   - **Calendar**
   - **Contacts**
   - **Notes** (iOS only)
3. In the **Offline Content** area, configure what data is saved and for how long when the Check Point App cannot reach the Security Gateway.
   - **Mail from the last x days** - Select the length of time from which emails are saved.
     - **Cache Mail** - Select which parts of the email are saved in the offline cache.
   - **Calendar from the last x months and the following x months** - Select which parts of the calendar are saved: the length of time in the past and length of time in the future.
     - **Cache Calendar** - Select which parts of the calendar entry are saved in the offline cache.
   - **Synchronize contacts** - Synchronize contacts so they are available offline.
4. In the **Push Notifications** area, select if you allow push notifications on devices and which notification templates to use.

   See the *Push Notifications* section below for details.

   To use this, push notifications must be enabled for Capsule Workspace on the Security Gateway that users connect to.
5. In the **Mail** area, select **Allow copy paste of mail content** if you allow contents of emails to be pasted into other apps.
6. In the **Calendar** area, select **Allow business calendar to sync to the device's native calendar** if you want to sync both calendars on the device. Events from Capsule Workspace will show in the device's calendar, outside of Capsule Workspace.
7. In the **Contacts** area, select which additional contacts to show on the device:
   - **Global Address List**
   - **Local Phone**
8. In the **Check Point Capsule Docs** area, select the Capsule Docs information that is stored in Capsule Workspace:
   - **Allow caching Check Point Capsule Docs credentials** - The credentials are required to open Capsule Docs protected documents are cached on the device. If they are not cached, users must enter their credentials each time they open a document for the first time.
   - **Allow caching Check Point Capsule Docs keys** - The Capsule Docs keys are cached on the device. If they are cached users can open a previously opened document with no need to enter credentials.

Managing Passcode Profiles

A passcode lock protects Capsule Workspace in mobile devices. In each Mobile Profile, configure which Passcode Profile it uses. The profile includes the passcode requirements, expiration, and number of failed attempts allowed. The default passcode profiles are Normal, Permissive, and Restrictive. You can edit the default profiles and create new profiles.

To manage Passcode Profiles

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Additional Settings > Passcode Profile**.
3. To create a new Passcode Profile, click **New**.
4. Configure the settings for the profile.
5. Click **Save**
6. Close SmartDashboard.
7. Publish the SmartConsole session.

Passcode Profile Settings

A Passcode Profile includes these settings:

- **Passcode Requirements** - The complexity requirements. When you configure this, remember that users usually have a small on-screen keyboard.
  - **Simple Passcode (4 digits)** - Users create a simple password of 4 numbers.
  - **Custom passcode strength** - Select from the requirements below.
    - **Minimum passcode length** - Enter the minimum number of characters.
    - **Require alphanumeric characters** - Show an alphanumeric keyboard and require at least one character to be a letter.
    - **Minimum complex characters** - Enter the number of characters that must be a special character.
- **Force passcode expiration** - Enter the number of days after which user's passcodes expires and must be replaced.
- **Allow grace period for entering passcode** - Select to let users access the Business Secure Container for a specified period of time without re- entering their passcode. Enter the quantity of time in minutes.
- **Exit after a few failures in passcode verification** - Select to lock users out after a specified number of failed attempts. After the failed attempts, users must re-authenticate. If the authentication method includes username and password, users must enter them. If the authentication is certificate-only, users need a new certificate.
- **Enforce passcode history** - When selected, users cannot use a passcode that is the same as earlier passcodes. Select the number of earlier passcodes that users cannot use.

Push Notifications

This feature sends push notifications for incoming emails and meeting requests on handheld devices, while the Mobile Mail app is in the background. The app icon shows the number of new, unhandled notifications. One user can get notifications for multiple devices.

Push notifications are disabled by default, but enabled when you run the Mobile Access First Time Wizard.

To use push notifications, the Security Gateway must have connectivity to these URLs on ports 443 and 80:

- https://push.checkpoint.com (209.87.211.173 and 217.68.8.71)
- http://SVRSecure-G3-crl.verisign.com/SVRSecureG3.crl
- http://crl.verisign.com/pca3-g5.crl

Notes:

- Users must enable notifications for the Mobile Mail app on iOS devices
- Push notifications can increase Exchange server CPU usage if many users are connected
- The Exchange server must have access to the Mobile Access Portal.
- If you change the URL or IP address of the Mobile Access Portal after you enable push notifications, you must update the Push Portal attributes with GuiDBedit Tool:
  1. In GuiDBedit Tool (see sk13009), go to the **Portals** section of your Security Gateway > **portal_name** > **ExchangeRegistration**.
  2. Change **main_url** and **ip_address** to match the URL of the Mobile Access Portal.
  3. Save the changes and close GuiDBedit Tool.
  4. In SmartDashboard, install policy on the Security Gateway.

Configuring Push Notifications

To enable push notifications

Enable push notifications from the Mobile Access Wizard or from the Security Gateway Properties of each Security Gateway.

- From the Mobile Access Wizard:
  - If you enable Mobile Mail in the Mobile Access Wizard, push notifications are automatically enabled for the Security Gateway.
  - If you enable Mobile Mail from the Mobile Access tab, push notifications are NOT enabled.
- From the Security Gateway Properties:
  1. Open a Security Gateway object that has Mobile Access enabled.
  2. Select **Mobile Access** > **Capsule Workspace** from the tree.
  3. Select **Enable Push Notifications**.
  4. Click **OK**.

Customizing Push Notifications

Customize push notifications from the mobile profile in the **Mobile Access** tab > **Capsule Workspace Settings**.

You can customize templates for Mail and Meeting notifications.

To see the default notifications or change the notifications

1. From SmartDashboard > **Mobile Access** tab > **Capsule Workspace Settings**, open a **Mobile Profile**.
2. Under **Push Notifications**, click **Manage**.

Exchange Server and Security Gateway Communication

Make sure that the Exchange server can access the Mobile Access Portal.

On R77.20 and higher Security Gateways, all confidential information between the Exchange server and the Security Gateway uses encrypted SSL tunnels. Non-confidential information can use unencrypted HTTP connections.

You can configure all push notification communication to use SSL tunnels.

By default, Kerberos authentication is not enabled for Push Notification registration to the Exchange server. To enable it, follow the instructions in sk110629.

To force all push notification communication to go through SSL tunnels

1. Install a trusted server certificate on the Mobile Access Security Gateway. See sk98203.
2. Close all SmartConsole windows connected to the Management Server.
3. Connect with GuiDBedit Tool (sk13009) to the Management Server.
4. Search for the field **main_url** (Ctrl +F).
5. Press F3 to see next **main_url** until you find **main_url** that contains the value **ExchangeRegistration**.
6. Double-click the **ExchangeRegistration main_url** field and edit the value to be **https://** and not **http://**.
7. Save the changes and close GuiDBedit Tool.
8. Connect with SmartConsole to the Management Server.
9. Open the Mobile Access Security Gateway object.
10. Click **OK**.
11. Install policy.

On Security Gateways R77.10, if the certificate on the Security Gateway is not trusted, import the certificate to the Exchange Server. This is not necessary on Security Gateways R77.20 and higher. For details about how to get the Security Gateway certificate, see sk98203.

To import a certificate to the Exchange server

1. Download the certificate to the Exchange server.
2. Double-click the certificate file, and follow the Windows certificate installation wizard steps.
3. Run the **Microsoft Management Console**.
4. In the window that opens, click **File > Add/Remove Snap-in**.

   Add or Remove Snap-ins window opens.
5. Select **Certificates** from the Available snap-ins, and click **Add**.
6. Select **My user account**.
7. Click **Finish**.
8. Select **Certificates** and click **Add** again.
9. Select **Computer account**.
10. Click **Next**.
11. Click **Finish**.
12. Click **OK**.

    The certificate is stored in **Local computer** and in **Current user** stores.

Push Notification Status Utility

Use the *Push Notification Status Utility* to understand if your environment is configured correctly for push notifications.

Intructions

Run the `$CVPNDIR/bin/PushReport` command to generate a report that contains this data:

1. **License** - Shows if the license is valid or if you have an evaluation license.
2. **Configuration** - Shows if push notifications are configured and enabled in the database.
3. **Connectivity** - Shows if you have a connection to the Check Point Cloud and CRLs list.
4. **Callback URL** - Shows the configured callback URL. If it is an https URL, the utility shows that a certificate is needed.

Output Example

```
[admin@gw-105 bin]# PushReport
This is your configuration status:
==================================
Topic               Status              Description
-------------------------------------------------------------------------
----
License             OK                  You are not using an evaluation
license
Configuration       OK                  Push is enabled in configuation
Connectivity        OK                  You have connectivity to cloud
Callback URL        OK                  Your callback push url is:
http://198.51.100.2/ExchangeRegistration. Make sure you have internal
connectivity to this URL.
```

Monitoring Push Notification Usage

Use the *"fwpush" on page 264* commands to monitor, debug, and troubleshoot push notification activity.

Note - Users must first install the latest version of the Capsule Workspace app from the app store and connect to the site created on the Security Gateway.

To see failed batches, expired push notifications, and delayed push notifications, see:
`$FWDIR/log/pushd_failed_posts`

Legal disclaimer on product functionality

Check Point uses Apple and Google services to deliver push notifications to iOS and Android devices. This is consistent with industry practice and similar to other applications vendors. Accordingly, Check Point assumes no liability in the event a notification is not sent or is not successfully pushed.

Information which is sent as a push notification passes through Check Point's push service and the Apple or Google push service (according to the user's device). Check Point does not keep, filter, or read any information that passes through. Check Point may review basic information to determine if a push notification reached its destination.

Check Point provides configuration options for the information sent as a push notification. The administrator can choose whether to set the subject, the sender, or the importance of any email, and can send the meeting location for meeting invitations.

Check Point will not be held liable for any loss of information that may result during the push notification process.

ESOD Bypass for Mobile Apps

Hand-held devices cannot run Endpoint Security on Demand (ESOD) components. By default, ESOD is disabled for smartphones and tablets.

If your organization has ESOD enabled, mobile apps cannot access ESOD enforced applications.

Note - Mobile apps are not recognized by their HTTP User-Agent header.

To change the ESOD setting on the Security Gateway

1. On the Security Gateway run:

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd.C set MobileAppBypassESODforApps
   "true"
   ```

   or

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd.C set MobileAppBypassESODforApps
   "false"
   ```

   - **true** - Bypasses ESOD for mobile apps (default).
   - **false** - Does not bypass ESOD.

2. Restart the Mobile Access services: `cvpnrestart`
3. If you use a cluster, copy the `$CVPNDIR/conf/cvpnd.C` file to all cluster members and restart the services on each.

MDM Cooperative Enforcement

Support for Mobile Device Management (MDM) through third-party vendors enforces a unified security policy for devices that access internal resources. Only managed devices that comply with the organizational security policy can successfully connect and access your business resources.

This feature is supported in R77.10 and above.

Check Point Apps establish a secure VPN connection to the corporate network through a Check Point Security Gateway. The Security Gateway queries the policy of the MDM server. The MDM server verifies the compliance level of employees' mobile devices when the VPN connection is established. The Security Gateway uses the MDM results to allow or block access, according to the device security and the user's permissions.

This feature is supported by Check Point Capsule Connect and Capsule Workspace clients.

For the most updated vendor information see sk98201.

To configure MDM Cooperative Enforcement with iOS 7, see sk98447.

Overview of the MDM Enforcement workflow

1. Before you start you must have:
   - An MDM account set up with required vendor license, if necessary
   - Necessary licenses for Capsule Connect or Capsule Workspace
   - Users with supported iOS or Android devices
2. Configure MDM on the Mobile Access Security Gateway. Edit the global options and vendor options.
3. For iOS 7 only: Configure settings and policy for your MDM vendor. See sk98447.
4. Make sure that the MDM functionality works - from a mobile device or Security Gateway console.

Configuring MDM on the Security Gateway

Enable MDM Enforcement in a configuration file on the Security Gateway. Then define global options and vendor-specific options.

To configure Mobile Device Management on a Security Gateway

1. Connect to the command line ine the Security Gateway.
2. Log in to the Expert mode mode.
3. Edit the `$FWDIR/conf/mdm.conf` file.
4. Edit the global options.

   #### Description

   MDM is disabled by default. You must change the value of the `enabled` parameter to `1`.

mdm.conf Options	Description
`enabled`	`0` - MDM disabled `1` - MDM enabled
`monitor_only`	`0` - Full enforcement: non-compliant mobile devices cannot log in. `1` - Monitor only: non-compliant devices can log in and attempts are logged.
`fail_open`	Defines behavior for cases of uncertainty, when an error occurs while checking MDM status. `0` - Drop VPN connections when an error occurs while checking MDM compliance status. `1` - Allow VPN connections when an error occurs while checking MDM compliance status.
`session_timeout_in_sec`	Maximum seconds allowed to determine device compliance status between the Security Gateway and the MDM cloud service. Starts at device login. If passed, the action of `fail_open` starts. Recommended: keep default.
`active_vendor`	Name of active third-party vendor, to test MDM compliance. You can configure multiple MDM vendors, but only one can be active. See the *Advanced Vendor Support* section below.

mdm.conf Options	Description
`password_ is_obscured`	`0` - `password` parameters in **mdm.conf** show in clear text. `1` - `password` parameters in **mdm.conf** show strings. Recommended: keep default (1). If the global property **password_is_obscured** is enabled, you cn obscure all parameters named `password` in the **Vendor Configuration** blocks. **To get an obscured password string from your password:** a. Run in the Expert mode: `# obfuscate_password <Your Expert mode Password>` The output is a string. For example: `33542b323a3528343640` b. Copy the string to the **mdm.conf file**, as the `password` value. c. Save the file. d. Install policy.
`verify_ssl_ cert`	`0` - SSL certificates not verified when Security Gateway accesses MDM cloud services. `1` - SSL certificates verified. Prevents some DNS poisoning, spoofing, man-in-the-middle attacks against Security Gateway. Recommended: keep default (1). If the MDM server is in a cloud, this parameter must be `1`. If you change it, the devices will be vulnerable to MITM attacks. (This risk is lower if the MDM server is local.)
`ssl_ca_ bundle_path`	Local path on Security Gateway of known CA certificate files. You can add more certificates to those that come with installation. Recommended: keep default.
`ssl_cipher_ list`	Allowed ciphers for HTTPS between Security Gateway and MDM cloud services. Recommended: keep default.
`ssl_use_ tls_v1`	To use TLSv1 or SSL for HTTPS between Security Gateway and MDM cloud services. Recommended: keep default.

5. Edit the vendor options.

   Description

   You can add more, if you have an understanding of the vendor's API and expertise with PHP programming.

   See the *Advanced Vendor Support* section below.

   For the most updated vendor information see sk98201.

6. Save the `$FWDIR/conf/mdm.conf` file.
7. Install policy.
8. Test the configuration.

Advanced Vendor Support

You can add more vendors. This requires PHP programming skills and an understanding of the third-party MDM vendor's cloud API.

Instructions

In these steps, we use "BestMDM" as the name of a fictional MDM vendor.

BestMDM's API requires an XML request to be sent to their URL that includes credentials and the ID of the device.

It returns an XML response with the device status and reason.

Example Request:

```
<request>
      <username>api_username</username>
      <password>api_password</password>
      <device>device_id</device>
</request >
```

Example Response:

```
<response>
      <status>compliance_status_code</status>
      <reason>reason</reason>
</response >
```

Example URL:

`https://bestmdm.com/api`

We use these examples in the steps below.

To add support for a new third-party vendor:

1. Edit the `$CVPNDIR/phpincs/MDMVendors.php` file.
2. Search for the text: **to add another vendor**
3. Remove the comment for a **case** branch.
4. Enter your MDM vendor name.

   For example:

   ```
   case "BestMDM":
         BestMDM($mdm_data);
         break;
   ```

5. At the end of the file, add a new PHP function. It must access the vendor's cloud API, and return a status and reason array.

   For example:

```
function BestMDM($mdm_data) {
      // Build the request XML
      $request_xml = new
      SimpleXMLElement
("<request><username/><password/><device/></request>");
      // Fill its fields with data from $mdm_data.
      // Note that "username", "password" and "device_id" always in
$mdm_data.
      $request_xml ->username = $mdm_data["username"];
      $request_xml->password = $mdm_data["password"];
      $request_xml->device = $mdm_data["device_id"];
      // Make POST request using the supplied class URLRequest
      // (The class URLRequest is defined in the same .php file).
      $url = "https://bestmdm.com/api";
      $conn = new URLRequest(); // open HTTP/HTTPS request session
      $resp_data = $conn->Request( $url, $post_body = $xml->asXML()
);
      // Handle possible network error.
      If ($resp_data === FALSE)
            return array("status"=>MDM_ERROR, "reason"=> $conn->get_
error_message());
      // Now $resp_data is raw string returned by the cloud API.
Parse it as XML:
      $resp_xml = new SimpleXMLElement($resp_data);
      // Check the status codes returned by the vendor's API.
      $status = MDM_ERROR;
      switch ($resp_xml->status) {
            case "not_managed":
                  return array("status"=>MDM_NOT_MANAGED,
"reason"=>"");
            case "compliant":
                  return array("status"=>MDM_COMPLIANT,
"reason"=>"");
            case "not_compliant":
                  return array("status"=>MDM_NOT_COMPLIANT,
"reason"=>$resp_xml->reason);
            default:
                  return array("status"=>MDM_ERROR,
"reason"=>"unknown status");
      } // end switch
} // end BestMDM compliance protocol handler
```

Status Codes:

- MDM_ERROR - Error occurred while accessing the MDM vendor's Cloud API.
- MDM_NOT_MANAGED - The device is not registered in the vendor's database.
- MDM_NOT_COMPLIANT - The device is known to the vendor as "not compliant with its policy".
- MDM_COMPLIANT - The device is known to the vendor as "compliant with its policy".

6. Define `$mdm_data` as an array of data from mdm.conf and the device ID.

```
Array(
"device_id"=><MAC address of device, or other ID known by the
vendor>,
"username"=><username to access the API of the MDM vendor>,
"password"=><password to access the API of the MDM vendor>
)
```

Important Notes:

- Global parameters and vendor parameters are merged in one list.
- If a vendor parameter is the same name as a global parameter, the vendor parameter overrides the global parameter.
- If **$mdm_data** includes a `password` parameter, and `password_is_obscured=1`, the password is decrypted automatically. The function gets the clear text password.

Example of $mdm_data:

With mdm.conf:	$mdm_data value:
(:enabled (1) :monitor_only (0) :fail_open (0) :active_vendor (BestVendor) :BestVendor (:username (MyUser) :auth_key (12345)))	Array("enabled"=>1, "monitor_only"=>0, "fail_open"=>0, "active_vendor"=>"BestVendor", "username"=>"MyUser", "auth_key"=>"12345", "device_ id"=>"12:34:56:78:9A:BC:DE:F0")

7. Save the `$CVPNDIR/phpincs/MDMVendors.php` file.
8. Edit the `$FWDIR/conf/mdm.conf` file.
9. Add a section after the last block for the new vendor.

   For example:

   ```
   :BestMDM (
         :username (MyUserName)
         :password (123456)
   )
   ```

10. Change the value of **active_vendor** to be the name of the new vendor.

    For example: `:active_vendor (BestMDM)`
11. Save the `$FWDIR/conf/mdm.conf` file.
12. Install policy.

Testing MDM

To make sure that MDM functionality is configured correctly

1. On a mobile device, launch the Check Point Mobile app.
2. Connect to the Security Gateway.
3. Look for Mobile Access login logs in SmartLog.

   The **Compliance Check**, **Information**, and **Reason** values in the details of the device login, show data about MDM compliance status and requirements.

Advanced Testing

You can make sure the MDM configuration works without a device in hand, but it requires expert knowledge. You log in to a test web page and enter the WiFi MAC address of a real device. For security, the MDM test page is disabled by default.

To enable the test page

1. Connect to the command line on the Security Gateway and log in the Expert mode.
2. Back up the `$CVPNDIR/conf/includes/Login.location.conf` file.
3. Edit the `$CVPNDIR/conf/includes/Login.location.conf` file.
4. Search for **test your integration**, and carefully follow the instructions there.
5. After you make required changes, save the file and run:

   ```
   [Expert@HostName:0]# cvpnrestart
   ```
6. Open the Mobile Access Portal with the `/Login/MDMProxy` path.

   For example: `https://<Security Gateway Hostname>/sslvpn/Login/MDMProxy`
7. Enter the device MAC address.
8. Click **Submit**.

   If there are issues for that device to access the third-party MDM vendor, the page shows diagnostics.
9. Revert `Login.location.conf` to the backup file.
10. Run:

    ```
    [Expert@HostName:0]# cvpnrestart
    ```

To prevent security risks, always revert and close the test page.

Example Diagnostics

- Parameters for the MDM vendor's cloud service (such as `Username` or `Password`) are not configured correctly in `$FWDIR/conf/mdm.conf`.
- There is a network problem accessing MDM vendor's cloud service.
- There is a problem with SSL certificates, which prevents the Security Gateway from accessing the MDM vendor's cloud service.

System Specific Configuration

This section describes system specific configuration required for iPhones, iPads, and Android devices. In some instances, end-user configuration is also required.

iPhone and iPad Configuration

Connecting iPhone/iPad Clients to ActiveSync Applications

When you allow access to an ActiveSync application, users see the **ActiveSync Setup** item and can install the ActiveSync profile. This gives users access to their corporate email.

Note - If your ActiveSync application requires a client certificate to connect, the ActiveSync profile will work only if a client certificate is also required for Capsule Workspace.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users.

To connect to corporate email:

1. Sign in to the Mobile Access site.
2. Tap **Mail Setup**.
3. Do the on-screen instructions.

Getting Logs from iPhones or iPads

To resolve issues with client devices, tell the users to send you the logs. The iPhone or iPad must have an email account set up.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users.

To configure logs:

1. Tap the **i** icon.

   Before login, this is on the top right. After login, this is on the bottom right.

2. Tap **Report a Problem** on the navigation bar.

   If you do not have an email account configured on the iPhone, a message shows that one must be configured. After this is done, you must open Check Point Mobile Access again.

   When an email account is configured, the email page opens. The logs are attached.

   Note - The email account that the iPhone uses to send the email is the default account. This might not be your organization's ActiveSync account.

   If the iPhone is not configured for a destination email address for logs, the email that opens has an empty **To** field. You can enter the destination address now, or set up a default destination address for Check Point Mobile logs.

Disabling Client SSO

Single Sign On (SSO) lets users in a session connect to the Mobile Access Security Gateway, without authenticating when the client starts. If a user cannot access the Security Gateway while SSO is enabled, disable it.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users.

To disable SSO on a client:

1. Tap **Settings**.
2. Scroll down to the **Check Point Mobile** icon and tap it.
3. In the **Mobile** global settings, tap the **Single Sign On** > **Enabled** switch.

Android Configurations

Browsing to Servers with Untrusted Server Certificates

When browsing from the Android app to a server with an untrusted server certificate, you are denied access and you get this message:

"Some resources on this page reside on an untrusted host."

In some cases, such as in a staging or demo environment, you can enable browsing to servers with untrusted certificates.

Important - Disabling the server certificate validation in the client app is forbidden for production setups since it allows any 3rd-party to intercept the SSL traffic.

Session Timeout for Android Devices

For Androids, idle timeout cannot be modified or enforced by the device or the Security Gateway.

The only timeout setting that applies to the device is the active session timeout. It is configured in SmartDashboard: **Mobile Access Software Blade > Additional Settings > Session > Re-authenticate users every x minutes** option. This setting indicates the maximum session length. When this period is reached, the user must log in again. For example, if re-authentication is set to 120 minutes, a user will need to log in again after 2 hours in an active session.

Getting Logs from Android Clients

To resolve issues with client devices, tell the users to send you the logs.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users.

To send logs:

1. Open the Check Point application.
2. Tap **About**.
3. Press the **Menu** button on the device.

4. Tap **Send Logs**.
5. Select a way to send the logs.

Instructions for End Users

Give these instructions to end users to configure their mobile devices to work with Mobile Access.

iPhone/iPad End User Configuration

Do these procedures on your iPhone/iPad so you can work with Mobile Access.

Before you start, make sure that your administrator gives you:

- The name of the site you will connect to.
- The required Registration key (also called Activation key).
- **Important** - Do only the procedures that your network administrator has instructed you to do.

To connect to the corporate site:

1. Get Check Point Capsule Workspace from the App Store.
2. When prompted, enter the:
   - Site Name
   - Registration key

To connect to corporate email:

1. Sign in to the Mobile Access site.
2. Tap **Mail Setup**.
3. Do the on-screen instructions.
4. When asked for the password, enter the Exchange password.

To configure logs:

1. Tap **Information**.

   Before login, this is on the top right. After login, this is on the bottom right.
2. Tap **Report a Problem** on the navigation bar.

   If you do not have an email account configured on the iPhone, a message shows that one must be configured. After this is done, you must open Check Point Mobile Access again.

   When an email account is configured, the email page opens. The logs are attached.

   Note - The email account that the iPhone uses to send the email is the default account. This might not be your organization's ActiveSync account.

   If the iPhone is not configured for a destination email address for logs, the email that opens has an empty **To** field. You can enter the destination address now, or set up a default destination address for Check Point Mobile logs.

To disable SSO on a client:

1. Tap **Settings**.
2. Scroll down to the **Capsule Workspace** icon and tap it.
3. In the **Mobile** global settings, tap the **Single Sign On** > **Enabled** switch.

Android End User Configuration

To disable the server certificate validation for Web applications

1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. Enable **Allow connection to untrusted servers**.

To disable the server certificate validation for Web applications

1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. Enable **Allow connection to untrusted servers**.

Do these procedures on your Android device so you can work with Mobile Access.

Before you start, make sure that your administrator gives you:

- The name of the site you will connect to.
- The required Registration key (also called Activation key).

Important - Do only the procedures that your network administrator has instructed you to do.

To connect to the corporate site

1. Get the Check Point Mobile app from the Android Market.
2. When prompted, enter the:
    - Site Name
    - Registration key

To send logs

1. Open the Check Point application.
2. Tap **About**.
3. Press the **Menu** button on the device.
4. Tap **Send Logs**.
5. Select a way to send the logs.

To transfer the client certificate to the 3rd party mail client

1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. From the **Export Certificate** option, tap **Export**. The Export Certificate window opens.

   If the Export Certificate option is disabled, contact the system administrator.
5. Select the certificate format appropriate for your mail client: P12 or PFX.
6. Select the location to save the certificate.
   The default path is /sdcard (for devices that have an SD card) or an external resource folder (for devices that do not have an SD card).
7. Tap **OK** to save the certificate to the selected location.

   A window shows: Export succeeded. Certificate password is: _____
8. You can copy the password to the clipboard. You will need the password when you import the certificate to the third party mail app.

Advanced Security Gateway Configuration for Handheld Devices

You can customize client authentication, device requirements, certificate details, and ActiveSync behavior. Use the CLI commands explained here to change the configuration file:
`$CVPNDIR/conf/cvpnd.C`

Note - Disable Link Translation Domain on Mobile Access Security Gateways before you connect to them with the Android client. To apply changes:

Restart the Mobile Access services: `cvpnrestart`

If you use a cluster, copy the `$CVPNDIR/conf/cvpnd.C` file to all cluster members and restart the services on each.

To set Mobile Access attributes:

```
cvpnd_settings set <attribute_name> "<value>"
```

To get the current value of an attribute:

```
cvpnd_settings get <attribute_name>
```

Attributes

Attribute	Description
ActiveSyncAllowed (true)	If access to ActiveSync applications is allowed.

Attribute	Description
ActiveSyncExchangeServerAuthentication Method (basic)	Method of forwarding authentication from the Mobile Access Security Gateway to the internal Exchange server. Valid values: `basic`, `digest`, `ntlm`
MobileAppAllowActiveSyncProfileConfig (true)	Make the automatic ActiveSync Profile configuration for iPhones and iPads available to users. If true, only users with authorization to access ActiveSync applications see this feature. If false, no user sees this feature.
MobileAppMinRequiredClientOSVersion (3.1)	Minimum operating system version for iPhones and iPads. If a client fails this requirement, user sees `Your OS version must be upgraded`
MobileAppAndroidMinRequiredClient OSVersion (2.1)	Minimum operating system version for Android. If a client fails this requirement, user sees `Your OS version must be upgraded`
MobileAppMinRecommendedClient OSVersion (3.1)	Recommended operating system version for iPhones and iPads. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than **Required** value, or Mobile Access will not start.
MobileAppAndroidMinRecommendedClient OSVersion (2.1)	Recommended operating system version for Android. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than **Required** value, or Mobile Access will not start.
MobileAppMinRequiredClientAppVersion (1.3)	Minimum App version required for iPhones and iPads. If a client fails this requirement, user sees `Application Update Required`
MobileAppAndroidMinRequiredClient AppVersion (1.0)	Minimum App version required for Android. If a client fails this requirement, user sees `Application Update Required`
MobileAppMinRecommendedClient AppVersion (1.3)	Recommended App version for iPhones and iPads. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than **Required** value, or Mobile Access will not start.

Attribute	Description
MobileAppAndroidMinRecommendedClientAppVersion (1.0)	Recommended App version for Android. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than **Required** value, or Mobile Access will not start.
MobileAppMinClientOSVersionForProfileConfig (3.1)	Minimum operating system version for iPhone and iPad to configure ActiveSync with the app. If you want data encryption, change this value from the default to `4.0`. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption.
MobileAppAndroidMinClientOSVersionForProfileConfig (2.1)	Minimum operating system version for Android to configure ActiveSync with the app. If you want data encryption, change this value from the default to `3.0`. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption.
MobileAppBypassESODforApps (false)	When true, mobile apps are allowed access to Mobile Access applications whose protection level requires Endpoint Security on Demand compliance. Mobile apps can always access the Mobile Access Portal.
MobileAppAllowClientCertExport (false)	When true, allows mobile app clients to export their client certificates to other apps and devices. See Using 3rd Party Android Mail Clients.

User Authentication in Mobile Access

User Authentication to the Mobile Access Portal

To enter the Mobile Access Portal and get access to its applications, users defined in SmartDashboard must authenticate to the Security Gateway. Authentication ensures that a user is who he or she claims to be. Users authenticate using one or more of these authentication schemes:

- **Username and password** - Users enter a user name and password.
- **Client Certificates** - Digital Certificates are issued by the Internal Certificate Authority or by a third party OPSEC certified Certificate Authority.
- **RADIUS Server** - Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme. The Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users. The RADIUS protocol uses UDP for communications with the Security Gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartDashboard.

  For more about configuring a Security Gateway to use a RADIUS server, see the *R80.40 Security Management Administration Guide*.
- **SecurID** - SecurID is a proprietary authentication method of RSA Security. An external SecurID server manages access by changing passwords every few seconds. Each user carries a SecurID token, a piece of hardware or software that is synchronized with the central server and displays the current password. The Security Gateway forwards authentication requests by remote users to the RSA Authentication Manager.

  For more about configuring a Security Gateway to use SecurID, see the *R80.40 Security Management Administration Guide*.
- **DynamicID One Time Password** - DynamicID One Time Password can be required as a secondary or later authentication method (not the first). When this is configured, users who successfully complete the first-phase or phases of authentication are challenged to enter an additional credential: a DynamicID One Time Password (OTP). The OTP is sent by email or text message to a mobile phone, or other mobile communication device.
- **Defined on user record (Legacy Authentication)** - The authentication method for each user is defined on the user record. For internal users, it is in the **Authentication** page of the User Properties. For LDAP users, it is on the user record in LDAP.

A user who tries to authenticate with an authentication scheme that is not configured for the Mobile Access Security Gateway will not be allowed to access resources through the Security Gateway.

Configuring Authentication for Security Gateways R77.30 and lower

Permitted authentication schemes must be configured for each Security Gateway.

On the Security Gateway, configure authentication in the **Gateway Properties** window of a Security Gateway in **Mobile Access** > **Authentication**. If you select an authentication method on this page, that is the method that all users must use to authenticate to Mobile Access. You can configure other authentication methods that users must use for different blades on different pages.

The default authentication scheme is **Username and Password**.

In the **Mobile Access** tab in SmartDashboard, select **Authentication** to show an overview of the Mobile Access Security Gateways and their authentication schemes.

On this page you can also configure settings for Two- Factor Authentication with a DynamicID One Time Password. Configure settings for the Security Gateway or global settings that are used for all Security Gateways that do not have their own DynamicID settings.

Requiring Certificates for Mobile Devices on Security Gateways R77.30 and lower

To require client certificates for mobile devices:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Authentication**.
3. Make sure that the Authentication Method is one of these options:
   - **Username and password**
   - **RADIUS**
   - **SecurID**
4. From the **Certificate Authentication for mobile devices** section, click **Require client certificate when using ActiveSync applications or Mobile Mail**.
5. Click **OK**.
6. Install the policy.

Image-Based RADIUS Authentication

Use Image-based RADIUS as a secondary authentication factor to authenticate to the Mobile Access Portal. It allows Mobile Access to integrate with third-party authentication services.

The images in this authentication factor are patterns of random numbers in a grid. During authentication, the user selects the numbers in the positions that correspond to a pre-selected pattern.

Configuring Image-Based RADIUS

To use image-based RADIUS as an authentication factor in Mobile Access, you have to configure RADIUS authentication with SmartConsole.

To configure Mobile Access authentication factors in SmartConsole:

1. In SmartConsole, from the **Gateways & Servers** tab, double-click the Security Gateway.

   The Check Point Security Gateway window shows.

2. From the menu, click **Mobile Access > Authentication**.
3. In the **Multiple Authentication Client Settings** table, add a new login option.
   a. Click **Add > New**.

      The **Multiple Login Options** window shows.
   b. In the **Authentication Methods** table, click **Add** to create **Authentication Factors**.
   c. When the **Authentication Factor** window opens, click **RADIUS**.
   d. Under **Customize Display**, add an appropriate description to the **Headline**.

      Note - When you return to the **Authentication Methods** table, make sure RADIUS authentication is not the first factor.

Enabling Image-Based RADIUS on Security Gateways

To enable Image-based RADIUS, edit the configuration file, `$CVPNDIR/conf/cvpnd.C` on each Mobile Access Security Gateway that uses Image-based RADIUS as an authentication factor.

Important - After every change to `cvpnd.C`, you must restart the cvpn services: `cvpnrestart`

```
:isImageBasedRadiusEnabled (false)
:ImageBasedRadiusRealmNames (
)
:ImageBasedRadiusURL ("")
```

Fields	Description	Example
`:isImageBasedRadiusEnabled (true)` `:isImageBasedRadiusEnabled (false)`	Enter **true** to enable. Enter **false** to disable. If set to true, the Security Gateway treats every RADIUS authentication factor found in `:ImageBasedRadiusRealmNames` as an Image-based RADIUS authentication factor.	
`:ImageBasedRadiusRealmNames`	List that has authentication realm names that are configured in SmartConsole, that contain Image-based RADIUS authentication as a secondary factor. If empty, all the authentication realms with RADIUS as a secondary authentication factor, are treated as an Image-based RADIUS authentication factor.	`(: ("realm name as configured")` `: ("another realm with Image-based RADIUS"))`

Fields	Description	Example
`:ImageBasedRadiusURL`	The URL from the third-party authentication service to get the user grid. Use `$$username` as a placeholder for the username.	`("https://<authentication_provider_url>?<query_string>&username=$$username")`

Google reCAPTCHA Challenge

The reCAPTCHA service uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities. It prevents malicious logins and at the same time allows authenticated users to pass through easily.

Configure your Security Gateway with Google reCAPTCHA v2 to challenge a user upon multiple, incorrect login attempts. reCAPTCHA appears as a challenge when a user reaches the maximum number of failed attempts.

The reCAPTCHA challenge is compatible with ClusterXL and VSX.

The reCAPTCHA challenge is not supported in the Capsule Workspace.

For supported browsers, see the Google documentation.

Registering Mobile Access for reCAPTCHA on Google

To use Mobile Access with reCAPTCHA, you have to register the Mobile Access Portal FQDN with reCAPTCHA.

Go to the Google reCAPTCHA site for instructions.

Adding reCAPTCHA to the Mobile Access Portal

You have to configure the Security Gateway manually to add reCAPTCHA. To enable reCAPTCHA, the Security Gateway needs:

- Internet connectivity
- A DNS configured
- Portal URL configuration with an FQDN and not an IP addres

  If you browse to the Portal with an IP address rather than an FQDN, you are redirected to the FQDN link.

  Note - In a cluster environment, each Security Gateway has to be configured identically.

To configure the Security Gateway manually, edit the `$CVPNDIR/conf/cvpnd.C` file.

Important - After every change in the `cvpnd.C` file, you must restart the CVPN services with the `cvpnrestart` command.

This shows:

```
:isCaptchaEnabled (false)
:isCaptchaEnabledForRelogin (false)
:captchaFailOpen (false)
:captchaPenaltyTimeInSeconds (1800)
:captchaFailedAttemptsThreshold (2)
:reCaptchaSiteKey ()
:reCaptchaSecret ()
:isCaptchaSettingsVerifierEnabled (false)
```

Fields	Description
`:isCaptchaEnabled (true)` `:isCaptchaEnabled (false)`	Enter **true** to enable. Enter **false** to disable.
`:IsCaptchaEnabledForRelogin(true)` `:IsCaptchaEnabledForRelogin(false)`	Determines if reCAPTCHA shows on a re-login flow. Enter **true** to enable. Enter **false** to disable.
`:captchaFailOpen(true)` `:captchaFailOpen(false)`	Entrance to the Portal. Enter **true** to enable. Enter **false** to disable. This determines when to block users: ■ No connectivity from the Security Gateway to Google ■ Invalid or missing a secret key ■ Invalid or missing a validation response from Google ■ Portal URL is not configured with an FQDN **False** - User is not allowed access to the Portal. See the login log for more information. **True** - User is allowed access to the Portal. A warning that the reCAPTCHA challenge was not verified shows. See the login log for more information.
`:captchaPenaltyTimeInSeconds (1800)`	The amount of time in seconds that the user in penalty is challenged with reCAPTCHA on each login until the user succeeds to log in. The default is 1800 seconds.
`:captchaFailedAttemptsThreshold (2)`	This is the number of times a user tries to log in unsuccessfully before reCAPTCHA shows. The default is two failed login attempts within the pre-determined time frame. Failures within that time frame are counted. If the time frame passes, the failure counter is set to zero again. If the field is set to zero, there is a reCAPTCHA challenge on every login attempt.
`:reCaptchaSiteKey ()`	The site key from Google.
`:reCaptchaSecret ()`	The secret from Google.

Fields	Description
`:isCaptchaSettingsVerifierEnabled (true)` `:isCaptchaSettingsVerifierEnabled (false)`	A utility page that checks the reCAPTCHA configuration and the connectivity from the Security Gateway. Enter **true** to enable the page. Enter **false** to disable the page. To see this page, go to: `https://<Portal URL>/Login/verifyCaptchaSettings`

Best Practice - If you enable and configure reCAPTCHA, make sure the Capsule Workspace uses certificate authentication. reCAPTCHA is not supported in the Capsule Workspace.

When you are challenged with reCAPTCHA, some Java scripts are downloaded to your browser.

Multiple Login Options for Security Gateways R77.30 and lower

On Security Gateways R80.10 and higher, you can configure multiple login options for Mobile Access and IPsec VPN.

The options can be different for each Security Gateway and each supported Software Blade, and for some client types. Users select one of the available options to log in with a supported client.

By default, all clients connect with the method for R77.30 and lower. When you create new login options, newer clients can see them in addition to the option of R77.30 and lower, but older clients cannot.

To see which clients support the new multiple login options, see sk111583.

Each configured login option is a global object that can be used with multiple Security Gateways and the Mobile Access and IPsec VPN Software Blades.

Compatibility with Older Clients

Older clients connect with the same login options available on Security Gateways R77.30 and lower. If you upgrade all or most clients to versions that support multiple login options, you can block older clients from connecting. After you do this, only clients that support multiple login options can connect to the Security Gateway.

By default, **Allow older clients to connect to this gateway** is selected in **Mobile Access** > **Authentication**. If you clear the option, older clients are blocked.

You can choose if newer clients that support multiple login options can connect with the authentication settings defined for older clients.

Configuring the Authentication Method for Newer Clients

To block newer clients from using the authentication method defined for older clients:

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. In the **Compatibility with Older Clients section**, click **Settings**.

The **Single Authentication Clients Settings** window opens.

3. Clear **Allow newer clients that support Multiple Login Options to use this authentication method**.
4. Click **OK**.
5. Install policy.

To let newer clients connect to the Security Gateway with the authentication settings defined for older clients:

Select **Allow newer clients that support Multiple Login options to use this authentication method**.

Configuring Authentication Settings for Older Clients

To let older clients connect to the Security Gateways R80.10 and higher:

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. Select **Allow older clients to connect to this gateway**.

   If this is not selected, older clients cannot connect to the Security Gateway.

To change the authentication method for older clients:

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. In the **Compatibility with Older Clients** section, click **Settings**.

   The **Single Authentication Clients Settings** window opens.
3. Change the **Display Name** to change the way the authentication method is shown in SmartConsole.
4. Select an **Authentication method**.
5. Click **Customize** to change the description of fields that are shown to users in the **login** window. See the "Customize Display Settings" section.
6. To require DynamicID with the selected authentication method, select **Enable DynamicID**. After you select this, you must configure the DynamicID settings for the Security Gateway from **Authentication** > **DynamicID Settings** > **Edit**.
7. Define the settings for **Capsule Workspace**:
   - Select **Require client certificate** to require **Capsule Workspace** to always use client certificates.
   - Select Allow DynamicID to require DynamicID in addition to the selected authentication method. After you select this, you must configure the DynamicID settings for the Security Gateway from **Authentication** > **DynamicID Settings** > **Edit**.
8. Click **OK**.
9. Click **OK**.
10. Install policy on the Security Gateway.

To configure global DynamicID settings that all Security Gateways use:

1. For each Security Gateway, in **Gateway Properties** > **Mobile Access** > **Authentication** > **DynamicID Settings**, select **Use Global Settings**.
2. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
3. Configure the global settings in **Mobile Access** tab > **Authentication** > **Two-Factor Authentication with DynamicID**.
4. Close SmartDashboard
5. In SmartConsole, install policy on the Security Gateway.

Configuring Multiple Log-in Options

You can configure login options from:

- **Gateway Properties** > **Mobile Access** > **Authentication**
- **Gateway Properties** > **VPN Clients** > **Authentication**
- SmartDashboard > **Mobile Access** tab > **Authentication**

The login options selected for Mobile Access clients, such as the Mobile Access Portal and Capsule Workspace, show in the **Mobile Access** > **Authentication** page in the **Multiple Authentication Client Settings** table.

The login options selected for VPN clients, such as Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote, show in the **VPN Clients** > **Authentication** page in the **Multiple Authentication Client Settings** table.

To configure multiple login options for Mobile Access Clients:

1. From the **Gateway Properties** tree of a Security Gateway, select **Mobile Access** > **Authentication**.
2. In the **Multiple Authentication Clients Settings** table, see a list of configured login options.

   The default login options are:

   - Personal_Certificate - Require a user certificate.
   - Username_Password - Require a username and password.
   - Cert_Username_Password - Require a username and password and a user certificate.
3. Click **Add** to create a new option or **Edit** to change an option. Each configured login option is a global object that can be used with multiple Security Gateways and Software Blades.
4. For each login option select one or more **Authentication Factors** and relevant **Authentication Settings**.

   For example, if you select **SecurID**, select the SecurID **Server** and **Token Card Type**. If you select **Personal Certificate**, select which certificate field the Security Gateway uses to fetch the username. See the "Certificate Parsing" section.
5. Select **Customize Display** to configure what users see when they log in with this option. See the "Customize Display Settings" section.

6. Click **OK**.
7. Use the **Up** and **Down** arrows to set the order of the login options.
   - If you include **Personal Certificates**, it must be first.
   - If you include **DynamicID**, it cannot be first.
8. On each **Login Option** > **Usage in Gateway**, select if the login option is available from:
   - The **Mobile Access Portal**
   - **Capsule Workspace**
9. Click **OK**.

Selecting a Client for a Login Option

For login options created from the **Mobile Access** > **Authentication** page, you can select if the login option is available for the Mobile Access Portal, Capsule Workspace, or both.

The login option will only be visible for the clients that you select.

Customize Display Settings

Enter descriptive values to make sure that users understand what information to input. These fields must all be the same language but they do not need to be in English.

- **Headline** - The title of the login option, for example, **Log in with a Certificate** or **Log in with your SecurID Pinpad**.
- **Username label** - A description of the username that users must enter, for example, **Email address** or **AD username**.
- **Password label** - A description of the password that users must enter, for example, **AD password**.

Certificate Parsing

When you select **Personal Certificate** as a Login option, you can also configure what information the Security Gateway sends to the LDAP server to parse the certificate. The default is the DN. You can configure the settings to use the user's email address or a serial number instead.

To change the certificate parsing:

1. In the **Multiple Authentication Clients Settings** table on the **Authentication** page, select a **Personal_Certificate** entry and click **Edit**.

   The **Authentication Factor** window opens.
2. In the **Authentication Settings area** in the **Fetch Username from** field, select the information that the Security Gateway uses to parse the certificate.
3. Click **OK**.
4. Install policy.

Deleting Login Options

To permanently delete a Login option:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.
2. In SmartDashboard go to the **Mobile Access** tab > **Authentication** page.
3. From the list of login options, select an option and click **Delete**.

Viewing all Authentication Settings

To see all Security Gateways and their authentication settings:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.
2. In SmartDashboard go to the **Mobile Access** tab.
3. From the tree, select **Gateways**.
4. Click a Security Gateway to see its authentication settings.

Multi-Factor Authentication with DynamicID

Multi-factor authentication is a system where two or more different methods are used to authenticate users. Using more than one factor delivers a higher level of authentication assurance. DynamicID is one option for multi-factor authentication.

Users who successfully complete the first-phase authentication can be challenged to provide an additional credential: a DynamicID One Time Password (OTP). The OTP is sent to their mobile communications device (such as a mobile phone) via SMS or directly to their email account.

On Security Gateways R80.10 and higher, DynamicID is supported for all Mobile Access and IPsec VPN clients.

How DynamicID Works

When logging in to the Mobile Access Portal, users see an additional authentication challenge such as:

Please type the verification code sent to your phone.

Users enter the one time password that is sent to the configured phone number or email address and they are then admitted to the Mobile Access Portal.

On the User Portal sign in screen, the **I didn't get the verification code** link shows. If the user does not receive an SMS or email with the verification code within a short period of time, the user can click that button to receive options for resending the verification code.

Administrators can allow users to select a phone number or email address from a list. Only some of the phone number digits are revealed. Users can then select the correct phone number or email address from the list and click **Send** to resend the verification code. By default, users can request to resend the message three times before they are locked out of the Portal.

Match Word

The Match Word feature ensures that users can identify the correct DynamicID verification code in situations when they may receive multiple messages. Users are provided with a match word on the Login page that will also appear in the correct message. If users receive multiple SMS messages, they can identify the correct one, as it will contain the same match word.

The SMS Service Provider

In Security Gateways R77.30 and lower, proxy settings for the SMS service provider were configured in **Gateway Properties** > **Mobile Access** > **HTTP Proxy**.

In Security Gateways R80.10 and higher, this is configured in **Gateway Properties** > **Network Management** > **Proxy**.

To access the SMS service provider, configure the proxy settings on the Security Gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Network Management** > **Proxy**.
3. Define the Proxy settings.

   If no proxy is defined on this page, no proxy is used for the SMS provider.

Whichever provider you work with, in order for the SMS messages to be sent to users, valid account details must be obtained from the provider and be configured in Mobile Access.

DynamicID Authentication Granularity

You can make multi-factor authentication with DynamicID a requirement to log in to the Security Gateway. Alternatively, you can make DynamicID a requirement to access specified applications. This flexibility gives you different security clearance levels.

To make multi-factor authentication with DynamicID a requirement to access specified applications, configure a Protection Level to require multi-factor authentication, and associate the Protection Level with Mobile Access applications (see the "Two-Factor Authentication per Application" section).

In an environment with multiple Mobile Access Security Gateways, make multi-factor authentication a requirement for a specified Security Gateway, configure multi-factor authentication for that Security Gateway.

On Security Gateways R80.10 and higher, DynamicID authentication can be part of a login option that is required for the Mobile Access Portal or Capsule Workspace, or both.

Basic DynamicID Configuration for SMS or Email

The workflow for basic configuration of two-factor authentication via DynamicID is:

1. **Obtain the SMS provider credentials and/or email settings.**

   Get these required SMS service provider settings from your SMS provider.

- A URL in the format specified by the SMS provider or a valid email address.
- Account credentials:
  - User name
  - Password
  - API ID (optional and may be left empty)

    Note - If DynamicID is configured to work with email only, an SMS Service Provider is not necessary.

2. **Configure the Phone Directory**

   The default phone number and email search method is that the Security Gateway searches for phone numbers or email addresses in user records on the LDAP account unit, and then in the phone directory on the local Security Gateway. If the phone number configured is actually an email address, an email will be sent instead of an SMS message. The phone number and email search method can be changed in the **Phone Number or Email Retrieval** section of the **Two-Factor Authentication with DynamicID - Advanced** window.

   ### Configuring Phone Numbers or Email Addresses in LDAP

   If users authenticate via LDAP, configure the list of phone numbers on LDAP by defining a phone number or email address for each user. By default, Mobile Access uses the **Mobile** field in the **Telephones** tab. If the phone number configured is actually an email address, an email will be sent instead of an SMS message.

   ### Configuring Phone Numbers or Email Addresses on Each Security Gateway

   Configure the list of phone numbers or email addresses on each Mobile Access Security Gateway. For a Mobile Access cluster, configure the directory on each cluster member.

   To configure a list of phone numbers on a Security Gateway:

   a. Connect to the command line on the Mobile Access Security Gateway using a secure console connection.

   b. Log in to the Expert mode.

   c. Back up the `$CPDIR/conf/dynamic_id_users_info.lst` file.

      Note - If this file does not yet exist, create it.

   d. Edit the `$CPDIR/conf/dynamic_id_users_info.lst` file.

   e. Add a list of user names and phone numbers, and/or email addresses.

      The list must be followed by a blank line. Use this syntax:

      ```
      <Username or Full DN> <Phone number or Email address>
      ```

Parameter	Meaning
<Username> or *<Full DN>*	Either a user name or, for users that log in using a certificate, the full DN of the certificate.
<Phone number>	All printable characters can be used in the phone number, excluding the space character, which is not allowed. Only the digits are relevant.
<Email address>	A valid email address in the format user@domain.com

Example of acceptable ways to enter users and their phone numbers or email addresses in `$CPDIR/conf/dynamic_id_users_info.lst`

```
bob +044-888-8888
jane.tom@domain.com
CN=tom,OU=users,O=example.com +044-7777777
CN=mary,OU=users,O=example.com +mary@domain.com
```

Configuring Multiple Phone Numbers

You can let users choose from multiple phone numbers when resending the verification code.

To configure choice of numbers:

Edit the configuration file `$CPDIR/conf/dynamic_id_users_info.lst` on the Security Gateway.

- Enter one number in the LDAP directory in the **Mobile** field and one or more phone numbers in configuration file.
- Enter multiple phone numbers separated by white space in the configuration file.

  For example: `user_a 917-555-5555 603-444-4444`

Note - If the configuration file `$CPDIR/conf/dynamic_id_users_info.lst` does not yet exist, create it.

3. **Perform basic configuration of DynamicID in SmartDashboard**

   Configure the **Authentication** settings to make two-factor authentication necessary for all mobile devices.

   This table explains parameters used in the SMS Provider and Email Settings field. The value of these parameters is automatically used when sending the SMS or email.

Parameter	Meaning
$APIID	The value of this parameter is the API ID.
$USERNAME	The value of this parameter is the username for the SMS provider.

Parameter	Meaning
$PASSWORD	The value of this parameter is the password for the SMS provider.
$PHONE	User phone number, as found in Active Directory or in the local file on the Security Gateway, including digits only and without a + sign.
$EMAIL	The email address of the user as found in Active Directory or in the local file on the Security Gateway - `$CPDIR/conf/dynamic_id_users_info.lst`. If the email address should be different than the listed one, it can be written explicitly. if the file does not exist, create it.
$MESSAGE	The value of this parameter is the message configured in the Advanced Two-Factor Authentication Configuration Options in SmartDashboard.
$RAWMESSAGE	The text from `$Message`, but without HTTP encoding.

Configuring DynamicID settings in SmartDashboard for all Security Gateways

a. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access**.

   Click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

b. From the navigation tree, click **Authentication**.

c. From the **Dynamic ID Settings** section, click **Edit**.

d. Select **Challenge users to provide the DynamicID one time password**.

e. Fill in the **SMS Provider and Email Settings** field using one of these formats:

   i. To let the DynamicID code to be delivered by SMS only, use the following syntax:

   ```
   https://api.example.com/http/sendmsg?api_id=$APIID&user=$USERNAME&password=$PASSWORD&to=$PHONE&text=$MESSAGE
   ```

ii. To let the DynamicID code to be delivered by email only, without an SMS service provider, use the following syntax:

- For SMTP protocol:

```
mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvpn@
example.com;BODY=$RAWMESSAGE
```

- For SMTPS protocol on port 465:

```
mail:TO=$EMAIL;SMTPSERVER=smtps://username:password@smt
p.example.com;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
```

- For SMTP protocol with START_TLS:

```
mail:TO=$EMAIL;SSL_
REQUIRED;SMTPSERVER=smtp://username:password@smtp.examp
le.com;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
```

- For SMTP protocol on port 587 with START_TLS:

```
mail:TO=$EMAIL;SSL_
REQUIRED;SMTPSERVER=smtp://username:password@smtp.examp
le.com:587;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
```

iii. To let the DynamicID code to be delivered by SMS or email, use the following syntax:

```
sms:https://api.example.com/sendsms.php?username=$USERNAME&
password=$PASSWORD&phone=$PHONE&smstext=$MESSAGE
mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvpn@exam
ple.com;BODY=$RAWMESSAGE
```

Note - If the SMTP username and password contain special characters, use these:

!	#	$	%	&	'	(
%21	%23	%24	%25	%26	%27	%28
)	*	+	,	/	:	;
%29	%2A	%2B	%2C	%2F	%3A	%3B
=	?	@	[	]		
%3D	%3F	%40	%5B	%5D		

f. In the **SMS Provider Account Credentials** section, enter the credentials received from the SMS provider:

- **Username**
- **Password**
- **API ID** (optional)

g. For additional configuration options, click **Advanced**.

h. Click **OK**.

i. Click **Save** and then close SmartDashboard.

j. In SmartConsole, install policy.

Configuring the Mobile Access Security Gateway to let computers and devices use DynamicID

a. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

The Security Gateway window opens and shows the **General Properties** page.

b. From the navigation tree, click **Mobile Access > Authentication**.

c. In the **Two-Factor Authentication** section, configure these settings:

- For a Security Gateway that uses the global authentication settings, select **Global settings**.
- For a Security Gateway that uses different authentication settings, select **Custom settings**.
- For mobile devices, select **Allow DynamicID for mobile devices**.

d. Click **OK**.

e. Install the policy.

4. **Test DynamicID Two-Factor Authentication**

a. Browse to the URL of the Mobile Access Portal.

b. Log in as a user.

c. Supply the Security Gateway authentication credentials.

d. Wait to receive the DynamicID code on your mobile communication device or check your email.

e. Enter the DynamicID code in the portal.

Make sure that you are logged in to the Mobile Access Portal.

Advanced Two-Factor Authentication Configuration

To configure settings for a specified Security Gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Authentication**.
3. From the **Two-Factor Authentication with DynamicID** section, click **Custom settings for this gateway**.
4. Click **Configure**.

   The **Two-Factor Authentication with DynamicID** window opens.

To configure global settings for all the Security Gateways:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Authentication**.
3. From the **DynamicID Settings** section, click **Edit**.
4. Click **Advanced**.

   The **Two-Factor Authentication with DynamicID** window opens.

DynamicID Message

- **Message text to be sent to the user**

  By default, the text of the message is "**Mobile Access DynamicID one time password:**". The message can contain the template fields shown in the following table to include the user's name and prompt users to use enter a One Time Password.

  For example, the message could say: **$NAME, use the verification code $CODE to enter the portal**.

Parameter	Meaning
`$NAME`	User name used in the first phase of authentication to the portal.
`$CODE`	Replaced with the One Time Password. By default, `$CODE` is added to the end of the message.

DynamicID Settings

- **Length of one time password** - By default, it is 6 digits.
- **One time password expiration (in minutes)** - By default, it is 5 minutes. Ensure there is a reasonably sufficient time for the message to arrive at the mobile communication device or email account, for the user to retrieve the password, and to type it in.
- **Number of times users can attempt to enter the one time password before the entire authentication process restarts** - By default, the user has 3 tries.

Display User Details

- **In the portal, display the phone number or email address that received the DynamicID** - By default, the phone number to which the SMS message was sent is not shown.

Country Code

- **Default country code for phone numbers that do not include country code** - The default country code is added if the phone number stored on the LDAP server or on the local file on the Security Gateway starts with 0.

Phone Number or Email Retrieval

- **Active Directory and Local File**

  Try to retrieve the user details from the Active Directory user record. If unsuccessful, retrieve from the local file on the Security Gateway.

  The LDAP account unit is defined in the **Users and Authentication > Authentication > LDAP Account Units** page of the SmartDashboard Mobile Access tab.

  The local phone directory on the Security Gateway is in the `$CPDIR/conf/dynamic_id_users_info.lst` file.

  Note - If this file does not exist yet, create it.

- **Active Directory Only**

  Retrieve phone numbers from Active Directory user record without using the local file on the Security Gateway.

  The LDAP account unit is defined in the **Users and Authentication > Authentication > LDAP Account Units** page of the SmartDashboard Mobile Access tab.

- **Local File Only**

  Retrieve the user details from the local file on the Security Gateway.

  The local phone directory on the Security Gateway is in the `$CPDIR/conf/dynamic_id_users_info.lst` file.

  Note - If this file does not exist yet, create it.

Configuring Resend Verification and Match Word

The DynamicID troubleshooting and match word features are configured in GuiDBedit Tool (see sk13009) or `dbedit` (see sk13301).

The GuiDBedit Tool table to edit depends on the Two Factor Authentication with SMS One Time Password (OTP) setting that you configured in SmartDashboard in the Mobile Access **Gateway Properties** > **Authentication**.

- If your DynamicID One Time Password settings are global across all of your Security Gateways (use the global settings configured in the Mobile Access tab is selected), in the GuiDBedit Tool select **Other > Mobile Access Global Properties**.
- If your DynamicID One Time Password settings are configured for a specific Security Gateway (this Security Gateway has its own two-factor authentication settings is selected), in the GuiDBedit Tool select **network_objects** and then select the specific Security Gateway you want to edit.

This table shows the DynamicID features that can be configured, and where in GuiDBedit Tool to configure them.

Feature	Attributes to Edit	Values and their Descriptions
Match Word	`use_message_matching_helper`	**true**: match word provided **false**: match word not provided (default)
Resend message	`enable_end_user_re_transmit_message`	**true**: enable resend SMS feature (default) **false**: disable resend SMS feature

Feature	Attributes to Edit	Values and their Descriptions
Display multiple phone numbers	`enable_end_user_select_phone_num`	**true**: enable option to choose from multiple phone numbers or email addresses when resending the verification code (default) **false**: one phone number or email address from the LDAP server or local file is used automatically without choice
Conceal displayed phone numbers	Edit these attributes: `reveal_partial_phone_num` and `number_of_digits_revealed`	For `reveal_partial_phone_num`: **true**: conceal part of the phone number or email address (default) **false**: display the full phone number or email address For `number_of_digits_revealed`: **1-20**: Choose the amount of digits to reveal (default is 4)

After editing the values in the GuiDBedit Tool:

1. Save all changes: **File** menu > **Save All**.
2. Close the GuiDBedit Tool.
3. Open SmartConsole.
4. Install the Access Control policy on the Security Gateway.

Configuring the Number of Times Messages are Resent

By default, users can request to resend the verification code message three times by clicking the **I didn't get the verification code** link before they are locked out of the Mobile Access Portal. The number of times the message can be resent is configured using the `cvpnd_settings` command from the Mobile Access CLI in expert mode.

The instructions below relate to actually resending the verification code message. The number of times users can try to input the verification code is configured in SmartDashboard in the **Two Factor Authentication Advanced** window.

To change the number of times the verification code message can be resent to 5, run this command in the Expert mode on the Security Gateway:

```
cvpnd_settings set smsMaxResendRetries 5
```

You can replace "5" with any other number to configure a different amount of retries.

After making the changes, run the "`cvpnrestart`" command to activate the settings.

If the Mobile Access Security Gateway is part of a cluster, be sure to make the same changes on each cluster member.

Two-Factor Authentication per Security Gateway

To configure two-factor authentication "Globally on, with custom settings per Security Gateway":

1. Set up basic two-factor authentication.
2. For each Security Gateway, in the Security Gateway Properties, go to **Gateway Properties > Mobile Access > Authentication**.
3. Configure one of these options:

- **To use the global settings** - Select **Global settings** and the global settings are used from the **Authentication to Gateway** page of the Mobile Access tab. This is the default.
- **To turn off two-factor authentication for the gateway** - Select **Custom Settings for this Gateway** and click **Configure**. In the window that opens, do not select the check box. This turns off two-factor authentication for this Security Gateway.
- **To activate two-factor authentication for the gateway with custom settings** -Select **Custom Settings for this Gateway** and click **Configure**. In the window that opens, select the check box. You must then configure custom SMS Provider Credentials for this Security Gateway. Optionally, configure **Advanced** options.

4. Repeat **step 2** and **step 3** for all other Security Gateways.
5. Install the Access Control policy.

Two-Factor Authentication per Application

To configure two-factor authentication per application:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. Configure basic two-factor authentication (see *"Basic DynamicID Configuration for SMS or Email" on page 168*).
   a. Configure the phone directory.
   b. Configure the application settings in **Mobile Access** tab **> Authentication**.
   c. Configure the Mobile Access Security Gateways to let the mobile devices use DynamicID.
3. Configure the *"Mobile Access Applications" on page 58*.
   a. In the **Protection Level** window, from the navigation tree click Authentication.
   b. Select **User must successfully authenticate via SMS**.
   c. Click **OK**.
4. Assign the protection level to Mobile Access applications that require *"Mobile Access Applications" on page 58*.
5. Click **Save** and then close SmartDashboard.
6. In SmartConsole, install the Access Control policy.

Changing the SMS Provider Certificates and Protocol

By default, it is recommended to use a secure (https) protocol for communication with the SMS provider. Mobile Access also validates the provider server certificate using a predefined bundle of trusted CAs.

If your SMS provider uses a non-trusted server certificate you can do one of the following:

- Add the server certificate issuer to the trusted CA bundle in the `$CVPNDIR/var/ssl/ca-bundle/` and run this command in the Expert mode:

  ```
  $CVPNDIR/bin/rehash_ca_bundle
  ```

- Ignore the server certificate validation by editing the `$CVPNDIR/conf/cvpnd.C` file and replacing the "`SmsWebClientProcArgs`" value with `("-k")`.

If your SMS provider is working with the non-secure HTTP protocol, edit the file `$CVPNDIR/conf/cvpnd.C` and replace the "`SmsWebClientProcArgs`" value with `("")`.

Multiple Log-in Options for Security Gateways R77.30 and lower

On Security Gateways R77.30 and lower, "Multiple Log-in" options is called "Multiple Realms" and is configured in the GuiDBedit Tool (see sk13009) or `dbedit` (see sk13301). It gives support for multiple authentication realms in the Mobile Access Portal. If you use this feature, we recommend that you upgrade your Security Gateways to this release and configure Multiple Login Options in SmartConsole.

If you upgrade your Management Server and Security Gateways to this release, see sk115856 for information about upgrading the multi-realms configuration.

If you upgrade only your Management Server and do not upgrade the Security Gateways, reconfigure Multiple Realms in GuiDBedit Tool after the upgrade.

How the Security Gateway Searches for Users

If you configure authentication for a blade from the main Security Gateway **Legacy Authentication** page, the Security Gateway searches for users in a standard way when they try to authenticate.

The Security Gateway searches in this order:

1. The internal users database.
2. If the specified user is not defined in this database, the Security Gateway queries the User Directory (LDAP) servers defined in the Account Unit one at a time, and according to their priority.

   If more than one Account Unit exists, the Security Gateway searches in all at the same time. .With multiple servers, the priority for servers can be set only in the scope of one account unit, but not between several account units.
3. If the information still cannot be found, the Security Gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

Session Settings

To open the Session window:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Additional Settings > Session**.

Simultaneous Logins to the Mobile Access Portal

Having a single user logged in to Mobile Access more than once, from two different locations for example, is a potential security issue.

Simultaneous login prevention enables a Security Gateway to automatically disconnect a remote user who is logged more than once.

When simultaneous login prevention is enabled, and a user's authentication information used to log in from two different computers, only the later login is considered legitimate, and the earlier session is logged out.

Note - The Simultaneous Login is not supported for the SNX client when the Office Mode Method is configured to allocate IP addresses from the `$FWDIR/conf/ipassignment.conf` file. See sk176343.

Configuring Simultaneous Login Prevention

Simultaneous login prevention is configured in SmartDashboard from the Mobile Access tab by selecting **Additional Settings > Session.**

The options are:

- **User is allowed several simultaneous logins to the Portal**

  Simultaneous login detection is disabled. This is the default option.

- **User is allowed only a single login to the portal**

  Inform user before disconnecting his previous session (option is not selected)

  The earlier user is disconnected and the later user is allowed. The earlier user is logged out. For Mobile Access Portal users, the following message appears:

  "**Your Mobile Access session has timed out. would you like to sign in again now?**". The later user is not informed that an earlier user is logged in.

- **User is allowed only a single login to the portal** (option selected)

  Inform user before disconnecting his previous session(option selected)

  The later user is informed that an earlier user is logged in, and is given the choice of canceling the login and retaining the existing session, or logging in and terminating the existing session. If the existing session is terminated, the user is logged out with the message:

  "**Your Mobile Access session has timed out. would you like to sign in again now?**".

Tracking of Simultaneous Logins

To track simultaneous login events, select **All Events** in the **Tracking** section of the **Additional Settings > Session** page.

When the Security Gateway disconnects a user, the Security Gateway records a log of the disconnection, containing the connection information of both logins.

All disconnect and connect events create a corresponding entry in the traffic log. The following values of the authentication status field relate to simultaneous logins:

- *Success* - User successfully logged in. Existing active sessions were terminated.
- *Inactive* - User successfully authenticated, but existing sessions need to be terminated prior to logging on.

- *Disconnected* - An existing user session has been terminated because the same user has logged on to another session.

Simultaneous Login Issues

These issues may arise in connection with simultaneous login:

Endpoint Connect - Simultaneous Login Issues

For Endpoint Connect users, Mobile Access does not prevent simultaneous login. This is equivalent to the **User can have several simultaneous logins to the portal** option. An Endpoint Connect user cannot log out another user with the same user name, and cannot be logged out by another user with the same user name.

SecureClient Mobile - Simultaneous Login Issues

With **User can have only a single simultaneous login to the portal** *selected* and **Inform user before disconnecting previous sessions** *not selected* SecureClient Mobile users can be logged off by another user, and can log off other users.

However, the **Inform user before disconnecting his previous session** option does not work, because no message can be sent to those users. User can be logged off, but cannot log off other users.

Other Simultaneous Login Issues

1. When a session is disconnected by another user and SSL Network Extender application mode client is being used, the SSL Network Extender window remains open, while the session is disconnected. Similarly, when a session is disconnected by another user and Secure Workspace is being used, Secure Workspace remains open, while the session is disconnected.
2. When a session is disconnected by another user and Citrix is being used, the Citrix window remains open, while the session is disconnected.
3. All current sessions are deleted when changing the section from **User can have only a single login to the Portal** to **User is allowed several simultaneous logins to the Portal**.

Session Timeouts

Once authenticated, remote users work in a Mobile Access session until they log out or the session terminates. Security best practices provide for limiting the length of active and inactive Mobile Access sessions to prevent abuse of secure remote resources.

Note - Mobile Access uses the system time to keep track of session timeouts. Changing the system time may disrupt existing session timeouts. Therefore, it is recommended to change the system time during low activity hours.

Mobile Access provides two types of session timeouts, both of which are configured in SmartDashboard from the Mobile Access tab by selecting **Additional Settings > Session**.

- **Re-authenticate users every** is the maximum session time. When this period is reached, the user must log in again.

  The default value is 60 minutes. Changing this timeout affects only future sessions, not current sessions.

- **Disconnect idle sessions after** is the disconnection time-out if the connection remains idle.

The default value is 15 minutes. When users connect via SSL Network Extender, this timeout does not apply.

For Capsule Clients:

1. Go to **SmartDashboard > Mobile Access** tab > **Capsule Workspace Settings** > **Mobile Profiles**.
2. Create or edit the applicable profile.
3. In the **Access Settings** section, configure the applicable value in the **Session timeout** field.

Roaming

The **Roaming** option allows users to change their IP addresses during an active session.

Note - SSL Network Extender users can always change IP address while connected, regardless of the Roaming setting.

Tracking

Configure Mobile Access to log session activity, including login attempts, logouts, timeouts, activity states and license expiration warnings.

Securing Authentication Credentials

Having multiple users on the same machine accessing the Mobile Access Portal can be a security hazard. A user logged in to the Mobile Access Portal can open a new browser window and get the access of the earlier session. Then the user can browse directly to the Mobile Access Portal without entering the login credentials again.

To make sure authentication credentials are not stolen by others, recommend to users that they log off or close all browser windows when done using a browser.

Mobile Access Authentication Use Cases

Use Case: Two-Factor Authentication with Certificates in Security Gateways R77.30 and lower

Select a main authentication method for Security Gateways R77.30 and lower. If you also select **Require client certificate when using Mobile applications** on the **Authentication** page, you require two-factor authentication for Capsule Workspace users: the main authentication method, and certificate.

With these settings, users authenticate to the Mobile Access Portal with only the main authentication method.

Capsule Workspace users receive the certificate information and register only one time. They provide the main authentication method credentials one time per session. Users might also need to enter a passcode, based on settings in the **Capsule Workspace Settings** in the **Mobile Access** tab.

To configure two-factor authentication with certificates for mobile devices on Security Gateways R77.30 and lower

1. Open the Security Gateway object.
2. Select **Mobile Access** > **Authentication**.
3. Select a main authentication method from these options:
   - Username and Password
   - RADIUS
   - SecurID
4. Select **Require client certificate when using Mobile applications** or **Require client certificate when using ActiveSync applications**.
5. Click **OK**.
6. Install the Access Control policy.

To configure two-factor authentication with the Mobile Access Portal in Security Gateways R77.30 and lower, see sk86240.

Use Case: Two Factor Authentication with Certificates on Security Gateways R80.10 and higher

You can configure two factor authentication with certificate on a Security Gateway R80.10 and higher in these ways:

- Create a new Login Option with Personal Certificate as the first factor and one or more additional methods that you choose as additional factors.
- Use the default Login Option, **Cert_Username_Password**, which includes a personal certificate as the first factor, and username and password as the second factor.

To create a new multi-factor login option that includes certificates:

1. Open the Security Gateway object.
2. Click **Mobile Access** > **Authentication**.
3. In the **Multiple Authentication Clients Settings** table, click **Add** to create a new option.
4. Click **New**.
5. In the **Multiple Login Options** window, enter the Login Option's **Name** and **Display Name**.

   The **Display Name** represents this Login Option to the user upon login and can be a descriptive name.
6. Under **Authentication Methods**, click **Add** to add the first factor.
   a. In the Authentication Factor window, select **Personal Certificate**. Note that Personal Certificate must be the first authentication factor.
   b. Configure the Authentication settings.
   c. Click **OK**.
7. Under **Authentication Methods**, click **Add** to add the second factor.

a. In the Authentication Factor window, select RADIUS, SecurID, DynamicID or Username and Password.

b. Configure the Authentication settings, if necessary.

c. Click **OK**.

8. To apply this Login Option only to the Mobile Access Portal or only to Capsule Workspace on mobile devices, under **Usage in Gateway**, select one or both client types.
9. Click **OK**.
10. Install the Access Control policy.

To use the built-in default Login Option Cert_Username_Password:

1. Open the Security Gateway object.
2. Click **Mobile Access** > **Authentication**.
3. In the **Multiple Authentication Clients Settings** table, click **Add**.
4. Select **Cert_Username_Password** from the list.
5. To apply this Login Option only to the Mobile Access Portal or only to Capsule Workspace on mobile devices:

   a. In the **Multiple Authentication Clients Settings** table, select **Cert_Username_Password** and click **Edit**.

   b. Under **Usage in Gateway**, select one or both client types.
6. Click **OK**.
7. Install the Access Control policy.

Note - The Login Options configured in the Multiple Authentication Clients Settings list are only available to clients that support multiple login options. To see which clients support the new multiple login options, see sk111583.

Use Case: Users Selecting a Login Option on Security Gateways R80.10 and higher

When more than one Login Option is configured, and users connect with clients that support Multiple Login Options, users select a Login Option to use when they log in.

In the Mobile Access Portal, in the login page, users see a drop-down list with all available login options, shown by their Display Name.

In the Capsule Workspace mobile application, users select the Login Option on the first connection to the Security Gateway. On subsequent connections, the same login option is shown automatically.

The Mobile Access Portal

Security Gateway Portals

The Security Gateway runs different web-based portals over HTTPS:

- Gaia Portal
- Identity Awareness (Captive Portal)
- DLP portal
- Mobile Access Portal
- SSL Network Extender portal
- Reverse Proxy SSL portal
- Reverse Proxy Clear portal
- UserCheck portal
- Endpoint Security portals (CCC)

All of these portals can resolve HTTPS hosts to IPv4 and IPv6 addresses over port 443.

These portals (and HTTPS inspection) support the latest versions of the TLS protocol. In addition to SSLv3 and TLS 1.0 (RFC 2246), the Security Gateway supports:

- TLS 1.1 (RFC 4346)
- TLS 1.2 (RFC 5246)

Support for TLS 1.1 and TLS 1.2 is enabled by default, but can be disabled in SmartDashboard (for web-based portals) or GuiDBedit Tool (see sk13009) (for HTTPS Inspection).

To configure TLS protocol support for portals:

1. In **SmartDashboard**, open **Global Properties > SmartDashboard Customization**.
2. In the **Advanced Configuration** section, click **Configure**.

   The **Advanced Configuration** window opens.
3. On the **Portal Properties** page, set minimum and maximum versions for SSL and TLS protocols.

To Configure TLS Protocol Support for HTTPS inspection:

1. In GuiDBedit Tool, on the **Tables** tab, select **Other > ssl_inspection**.
2. In the **Objects** column, select **general_confs_obj**.
3. In the **Fields** column, select the minimum and maximum TLS version values in these fields:
   - **ssl_max_ver** (default = TLS 1.2)
   - **ssl_min_ver** (default = SSLv3)

Portal Settings

Each Mobile Access-enabled Security Gateway leads to its own Mobile Access user portal. Remote users log in to the portal using an authentication scheme configured for that Security Gateway.

Portal URL

Remote users access the portal from a Web browser with https://<Gateway_IP>/sslvpn, where <Gateway_IP> is one of these:

- FQDN that resolves to the IP address of the Security Gateway
- IP address of the Security Gateway

Remote users that use HTTP are automatically redirected to the portal using HTTPS.

Note - If Hostname Translation is the method for link translation, **FQDN** is required.

Set up the URL for the first time in the Mobile Access First Time Wizard.

To change the Mobile Access Portal URL:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.
3. Change the **Main URL**.
4. Optional: Click the **Aliases** button to **Add** URL aliases that are redirected to the main portal URL. For example, portal.example.com can send users to the portal. To make the alias work, it must be resolved to the main URL on your DNS server.
5. Install policy.

Portal Certificate

If you do not import a certificate, the portal uses a Check Point auto-generated certificate. This might cause browser warnings if the browser does not recognize the Security Gateway's management. All portals on the same IP address use the same certificate.

To configure the accessibility settings for the portal:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.
3. Click **Import** to import a p12 certificate for the portal website to use.
4. Click **OK**.
5. Install policy.

Portal Accessibility Settings

Configure from where users access the Mobile Access Portal. The options are based on the topology configured for the Security Gateway.

To configure the accessibility settings for the portal:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.
3. In the **Accessibility** area, click **Edit**.
   - **Through all interfaces**
   - **Through internal interfaces**
   - **Including undefined internal interfaces**
   - **Including DMZ internal interfaces**
   - **Including VPN encrypted interfaces**
   - **According to the Firewall policy** - Select this if there is a rule that states who can access the portal.
4. Install policy.

Portal Customization

To customize the Mobile Access end user portal:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Customization**.

   The **Portal Customization** page opens.
3. Configure the following settings.
4. Install the policy.

Localization Features

Mobile Access localizes the user interface of the Mobile Access user portal and the Secure Workspace to multiple languages.

The Mobile Access user portal and the Secure Workspace can be configured by Security Gateway in the **Portal Settings > Portal Customization page** to use these languages:

- English (the default language)
- Bulgarian
- Chinese- Simplified
- Chinese- Traditional

- Finnish
- French
- German
- Italian
- Japanese
- Polish
- Romanian
- Russian
- Spanish

Auto Detection of User Language Preferences

Automatic language detection is an optional feature that gives priority to the language settings in the user's browser over the language chosen by the administrator.

Automatic language detection is activated by configuring the `CVPN_PORTAL_LANGUAGE_AUTO_DETECT` flag in the `Main.virtualhost.conf` file on Mobile Access.

By default, the language preference in the user's browser is not automatically detected. If automatic detection is configured, the language used in SmartDashboard is the first language supported by Mobile Access that is found in the Language Preference list defined in the user's browser settings. If no supported language is found in the Language Preference list in the user's browser, the language set by the administrator in SmartDashboard is used.

To activate automatic language detection, perform the following steps on each cluster member:

1. Open an SSH connection to Mobile Access, or connect to it via a console.
2. Log in to Mobile Access using your administrator user name and password.
3. Change to the Expert mode by typing expert and supplying the password.
4. Edit the `$CVPNDIR/conf/includes/Main.virtualhost.conf` file, and change the following line from:

   ```
   SetEnv CVPN_PORTAL_LANGUAGE_AUTO_DETECT 0
   ```

   to:

   ```
   SetEnv CVPN_PORTAL_LANGUAGE_AUTO_DETECT 1
   ```
5. Run the command: `cvpnrestart`.

Language Selection by End Users

Any explicit language selection by the user in any of the portal pages overrides both the administrator's default language setting, and the automatic language detection.

Users can select a language in the user portal sign-in page, in the **Change Language To** field.

Alternative Portal Configuration

Note - There should be a Mobile Access policy rule that includes the alternative portal as a Web application and allows its intended users to access it.

To specify an alternative user portal:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Portal Settings > Alternative Portal**.
3. Click **Add**.

   The **Mobile Access Sign-In Home Page** window opens.
4. In the **User Groups** tab, specify user groups that may access the alternative user portal.
5. In the **Install On** tab, specify the Mobile Access Security Gateways and Clusters that host the alternative portal.
6. In the **Sign-In Home Page** tab, choose an alternative portal for users, in place of the Mobile Access user portal that users reach by default. **URL** is the location of the alternative user portal for the user group(s) specified in the **User Groups** tab.

   When a user belongs to more than one group, the table in the **Alternative Portal** page acts as an ordered rule base. Users are directed to the alternative portal of the first group that they are part of.
7. Click **OK**.
8. Click **Save** and then close SmartDashboard.
9. In SmartConsole, install policy.

User Workflow for Mobile Access Portal

The user workflow includes these steps:

1. Sign in and select the portal language.
2. On first-time use, if you will use SSL Network Extender to access native applications, install ActiveX and Java Components.
3. Initial setup.
4. Access applications.

Signing In

In a browser, type in the URL assigned by the system administrator for the Mobile Access Security Gateway.

Best Practice - Some popup blockers can interfere with aspects of portal functionality. Tell users to configure popup blockers to allow pop-ups from Mobile Access.

If the Administrator configured Secure Workspace to be optional, users can choose to select it on the sign in page.

Users enter their authentication credentials and click **Sign In**. Before Mobile Access gives access to the applications on the LAN, the credentials of remote users are first validated. Mobile Access authenticates the users either through its own internal database, LDAP, RADIUS or RSA Authentication Manager. After the remote users are authenticated, and associated with Mobile Access groups, access is given to corporate applications.

Note - If the Endpoint Compliance Scanner is enabled, users computers might be scanned before they can access the Mobile Access **Sign In** page. This is to make sure that credentials are not compromised by 3rd party malicious software.

First Time Installation of ActiveX and Java Components

Some Mobile Access components such as the endpoint Compliance Scanner, Secure Workspace and SSL Network Extender require either an ActiveX component (for Windows with Internet Explorer machines) or a Java component to be installed on the endpoint machine.

When using one of these components for the first time on an endpoint machine using Windows and Internet Explorer, Mobile Access tries to install it using ActiveX. However, Internet Explorer may prevent the ActiveX installation because the user does not have Power User privileges, or display a yellow bar at the top of the page asking the user to explicitly allow the installation. The user is then instructed to click the yellow bar, or if having problems doing so, to follow a dedicated link. This link is used to install the required component using Java.

After the first of these components is installed, any other components are installed in the same way. For example, if the Endpoint compliance Scanner was installed using Java on Internet Explorer, Secure Workspace and SSL Network Extender are also installed using Java.

For general information about the Mobile Access Portal and Java compatibility see sk113410.

Note - To install using ActiveX after a component was installed using Java, delete the browser cookies.

Initial Setup

The user may be required to configure certain settings, such as application credentials. In addition, the user can define additional favorites for commonly used applications.

Accessing Applications

After the remote users have logged onto the Mobile Access Security Gateway, they are presented with a portal. The user portal enables access to the internal applications that the administrator has configured as available from within the organization, and that the user is authorized to use.

Endpoint Security on Demand

Endpoint Compliance Enforcement

The Check Point Endpoint Security on Demand scanner enforces endpoint compliance by scanning the endpoint to see if it complies with a pre-defined endpoint compliance policy. For example, an endpoint compliance policy can make sure that the endpoint client has updated Anti-Virus software and an active Firewall. If the endpoint is compliant with the endpoint compliance policy, the user is allowed to access the portal.

By ensuring that endpoints comply with a security policy, Endpoint Security on Demand protects enterprises from threats emanating from unsecured endpoint computers that can result in data loss and excessive bandwidth consumption.

The endpoint compliance policy is made up of rules. A policy can specify, for example, that the endpoint machine must have an approved Anti-Virus application, and that it must be free of spyware. A policy could also specify that a machine must be managed by the organization in order to gain full access to internal data and applications.

On Security Gateways, a combination of Endpoint Compliance Policy and Secure Workspace Policy can require the following Policy: Any client connecting to the Security Gateway from a machine that is not managed by the organization or that does not meet a specific enforcement policy, must use Check Point Secure Workspace. This ensures that no unauthorized information is accessed.

Endpoint Compliance Policy Granularity

The administrators can make compliance with a policy a requirement for accessing either the portal or specific applications. This makes it possible to assign varying levels of security clearance to the portal and to Mobile Access applications.

Endpoint Compliance policies can be assigned to Mobile Access Security Gateways. They can also be assigned to Protection Levels, which are in turn associated with Mobile Access applications.

- If an Endpoint Compliance policy is assigned to a Security Gateway, endpoint machines must comply with the policy before they are allowed to log in to the portal.
- If an endpoint machine does not comply with the Endpoint Compliance policy on a Security Gateway, users can be required to use Check Point Secure Workspace.
- To provide additional protection to an application, it is possible to "harden" the Endpoint Compliance protection that is enforced by the Security Gateway by assigning an Endpoint Compliance policy to a Protection Level, and then assigning that Protection Level to an application.

  To access that application, the endpoint machine must comply with the policy associated with the Protection Level, in addition to the policy associated with the Security Gateway.

In either case, the scan takes place *before* logging in to the portal. Only one scan is performed. Compliance to policies is determined according to the results of the scan.

Endpoint Compliance Policy Rule Types

There are different types of Endpoint Compliance policy rules, for different types of security applications. It is possible to have multiple rules of the same type, each with different settings.

Windows Security Rule

Windows security rules perform Windows-specific checks. For example:

- Check for the latest Windows Service Pack on endpoint.
- Check the enabled/disabled state of the built-in Microsoft Windows Automatic Updates system.
- Check for Microsoft Windows Hotfixes and patches on the endpoint.
- Enforce Windows patches by their ID.

Endpoint computers running Windows must pass these checks in order to gain access to the network.

At least one of the Hotfixes in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

Anti-Spyware Application Rule

Choose which Anti-Spyware applications endpoint computers (on the Windows platform) must have to gain access to the network.

Ensure that appropriate Anti-Spyware software is running on endpoint computers, and that the software version and virus signature files are up-to-date.

At least one of the Anti-Spyware applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Anti-Spyware enforcement rules are pre-configured with supported Anti-Spyware providers. To require a non-supported Anti-Spyware provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

Anti-Virus Application Rule

Choose which Anti-Virus applications the endpoint computer must have in order to gain access to the network.

Ensure that appropriate Anti-Virus software is running on endpoint computers, and that the software version and virus signature files are up-to-date.

At least one of the Anti-Virus applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Anti-Virus enforcement rules are pre-configured with supported Anti-Virus providers. To require a non-supported anti-virus provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

Firewall Application Rule

Choose which personal Firewall applications endpoint computers (on Windows, Linux or Macintosh platforms) must have to gain access to your network.

Ensure that appropriate Firewall software is installed, enabled and running on endpoint computers.

At least one of the Firewall applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Firewall enforcement rules are pre-configured with supported Firewall providers. To require a non-supported Firewall provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

Custom Check Rule

Perform custom checks on endpoint computers (on the Windows, Linux or Macintosh platforms) that are not covered by any of the other rule types. For example:

- Custom applications. These applications may include proprietary spyware scanners that supplement the predefined types and/or other special security solutions.
- Specific files.
- Registry keys or processes running on the endpoint computer.
- Non-English or localized names of processes and files.

Custom check rules can be configured to check for specific versions and modification dates.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule, and the error message that is presented to users in the event of non-compliance, such as remediation information.

OR Group of Rules

An "OR Group of Rules" rule includes a list of previously defined rules. An endpoint satisfies a rule of type "OR Group of Rules" if it satisfies one or more of the rules included in the "OR Group of Rules" rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

Spyware Scan Rule

Select the action that should take place for each type of spyware present on endpoint computers. You can change the protections for types of spyware threats.

Spyware Type	Description
Dialer	Software that change the user's dial-up connection settings so that instead of connecting to a local Internet Service Provider, the user connects to a different network, usually a toll number or international phone number.
Worm	Programs that replicate over a network for the purpose of disrupting communications or damaging software or data.
Keystroke Logger	Programs that record user input activity (keystrokes or mouse activity). Some keystroke loggers transmit the recorded information to third parties.
Hacker Tool	Tools that facilitate unauthorized access to a computer and/or extraction of data from a computer.

Spyware Type	Description
Remote Administration Tool	Commercially developed software that allows remote system access and control.
Trojan	Malicious programs that masquerade as harmless applications.
Adware	Programs that display advertisements or record information about Web use habits and forward it to marketers or advertisers without the user's authorization or knowledge.
Other	Any unsolicited software that secretly performs undesirable actions on a user's computer and does not fit any of the above descriptions.
Screen Logger	Software that record what a user's monitor displays.
Tracking Cookie	Cookies that are used to deliver information about the user's Internet activity to marketers.
Browser Plug-in	Software that modifies or adds browser functionality. Browser plug-ins change the default search page to a pay-per-search site, change the user's home page, or transmit the browser history to a third party.

Endpoint Security on Demand. For example, you can allow that a signature that is recognized as spyware by Mobile Access, but which you see as legitimate.

In the rule, set the action to take if an endpoint computer fails to comply. Set the error message that users see in the event of non-compliance, such as remediation information.

Endpoint Compliance Logs

If the end user machine is not compliant with one or more of the Endpoint Compliance policy rules, Mobile Access generates Endpoint Compliance-specific logs with the category "Endpoint Security on Demand". The log entries appear in SmartLog, and include the:

1. Rule ID and name that causes the authorization failure.
2. Policies that this rules belongs to.
3. A description in the "info" field of the log. Two logging levels are available to the administrator: (For configuration details, see the "Configuring Endpoint Compliance Logs" section.)

   Note - Mobile Access logs non-compliant rules from all policies, not only the Endpoint Compliance policy that is assigned to the Security Gateway or to an application. This means that there may be entries in SmartLog for rules that do not appear in the report presented to the end user.

   - **Summary**: Only one log entry per scan is written to SmartLog. The log entry shows endpoints that do not comply with the Endpoint Compliance policy. The date and time of the scan, the source IP, and the Endpoint Compliance scan ID are logged.

- **Details**: In addition to the Summary mode information, this adds a log entry for each non-compliant rule. For example, in the case of a Spyware Scan rule that screens for tracking cookies, a log entry is generated that contains the following fields:
  - Malware name: `unwantedexample`.
  - Malware type: `3rd party cookie`.
  - Description: `symptom type: URL. Symptom value: cookie:bob@unwantedexample.net.`

Configuring Endpoint Compliance

The workflow for configuring Endpoint Compliance enforcement is below. Each step is described in detail in the sections that follow:

1. **Plan the Endpoint Compliance Policy**

   Decide on security clearance levels for Mobile Access Portals and applications. For example, is it OK for users to gain access to all Mobile Access applications as long as they comply with a single policy? If some resources are more sensitive than others, you may wish to draw up a more stringent policy for some applications than for others.

2. **Use the ICSInfo Tool**

   Set up a stand-alone test computer with all the endpoint security applications you want to create enforcement rules for, and the run the `ICSinfo` tool to obtain the information needed to correctly define Endpoint Compliance policy rules.

3. **Create Endpoint Compliance Policies**

   Policies are made up of rules. In order to comply with the policy, endpoints must comply with all rules in the policy. Rules can be used in more than one policy. Rules that are not in a policy are not used.

   There are different types of rules for different security applications. The Endpoint Compliance policy configuration tool comes with a number of predefined rules which can be edited to match the needs of the organization.

4. **Configure Endpoint Compliance Settings for Applications and Gateways**

   Configure which Endpoint Compliance Policies should be assigned to which applications and Security Gateways.

   - To make access to the *portal* conditional on passing an Endpoint Compliance scan, assign a policy to a Security Gateway
   - To make access to *applications* conditional on passing an Endpoint Compliance scan:
     - Assign a policy to a *Protection Level*.
     - Assign Protection Levels to Mobile Access *applications*.

5. **Complete the Endpoint Compliance Configuration**

   Configure tracking options for the endpoint scan results, then save and install the security policy

Planning the Endpoint Compliance Policy

Defining the Endpoint Compliance policy for Mobile Access clients involves some planning, prior to performing the SmartDashboard configuration.

You need to define security clearance levels for the both the Mobile Access Portal (that is, the Security Gateway) and for portal applications. There are various approaches, and the best one to use depends on how granular you need to make the policy.

Basic Approach:

The simplest approach is to define a single Endpoint Compliance policy for the Security Gateway and all applications accessed via the Security Gateway. In this approach, all applications accessed via the Security Gateway are protected by the Endpoint Compliance policy of the Security Gateway. Users whose client machines comply with the policy have access to the portal and all applications.

For example:

Resource	Endpoint Compliance Policy
Security Gateway A	Low Security
Web App P	Rely on Security Gateway requirements
Web App Q	Rely on Security Gateway requirements
File Share R	Rely on Security Gateway requirements

Advanced Approach:

A more advanced approach is appropriate if there is one application (or a small number of applications) that has stricter security requirements than other applications. These additional requirements are specified in a separate Endpoint Compliance policy, which is enforced in addition to the Security Gateway policy. To access the Mobile Access Portal, all users must fulfill the threshold security requirements of the Security Gateway policy. Users clicking a link in the portal to an application with additional security requirements are only allowed access to the application if they fulfill those additional requirements.

For example:

Resource	Endpoint Compliance Policy
Security Gateway A	Low Security
Web App P	Rely on Security Gateway requirements
Web App Q	High Security
File Share R	Rely on Security Gateway requirements

Very Advanced Approach:

Where most or every application has its own endpoint security requirements, it is possible to define an individual Endpoint Compliance policy for each application. In this scenario, there are no Security Gateway security requirements: All users are able to access the portal. However, when clicking a link to an application, users are only allowed access if they fulfill the requirements for that application. If no requirements are configured for the application, users are allowed to access it.

For example:

Resource	Endpoint Compliance policy
Security Gateway A	None
Web App P	Low Security
Web App Q	High Security
File Share R	Medium Security

Example Rules for Endpoint Compliance Policies

The following table illustrates Endpoint Compliance policies with different rules, for different security requirements.

Rule	Description	High Security Endpoint Compliance Policy	Medium Security Endpoint Compliance Policy	Low Security Endpoint Compliance Policy
1	Default Windows Security rule	Yes	Yes	No
2	Anti-Virus applications check	Yes	Yes	Yes
3	Firewall applications check	Yes	Yes	Yes
4	Spyware Scan rule	Yes	No	No

Using the ICSInfo Tool

When defining Endpoint Compliance policy rules, you must use the correct format. This format varies from vendor to vendor. The `ICSinfo.exe` utility scans your computer, and generates an xml file that gives you the information in the correct format for all supported security programs it finds.

Run the ICSinfo tool before configuring the Endpoint Compliance policy rules.

To use the `ICSinfo.exe` utility:

1. Set up a stand-alone test computer with all the endpoint security applications you want to create enforcement rules for. Be sure to apply the latest updates to your security software.
2. Copy the `ICSinfo` tool from the Mobile Access Security Gateway to the test computer. The tool is located at `$CVPNDIR/htdocs/ICS/components/ICSinfo.exe`.
3. Run `ICSinfo.exe`.

   This utility lists all detected security software, along with the required information in the correct format.

   The XML format output file `ICSinfo.xml` can be viewed in a browser.

   The sections of the file can be collapsed or expanded by clicking the - or +.

4. Record the information for each security program and use this information to create your Endpoint Compliance policy rules.

Creating Endpoint Compliance Policies

To configure Endpoint Compliance policies:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
3. Click **Edit policies**.

   The Endpoint Compliance policy configuration tool opens at the **Policies** page.

4. Either create a new Endpoint Compliance policy or edit an existing policy.
   - To create an Endpoint Compliance policy click **New Policy**.

     The **Policies > New Policy** page opens.
   - To edit an existing policy, select the policy and click **Edit**.

     The **Policies > Edit Policy** page opens.
5. Give the policy a **Name**, and a **Description**.
6. For policies with Spyware Scan rules, if an endpoint computer has a valid Anti-Spyware of Anti-Virus application, make sure that the Endpoint Security on Demand Spyware Scan is necessary.

   If not, select **Bypass malware scan if endpoint meets Anti-Virus or Anti-Spyware requirements**.

   Note - This option is disabled if there is no Spyware Scan rule in the policy.
7. Within a Policy, either add previously defined Endpoint Compliance rules, or create new rules or edit previously defined rules.

   There are different types of rules for different security applications.

   It is possible to have multiple rules of the same type, each with different settings.
   - To add a previously defined rule, click **Add**.

     The **Add Enforcement Rules** page opens. Select a rule and click **OK**.
   - To create a rule, click **New Rule**, and select the rule type
   - To edit a previously defined rule, select the rule and click **Edit**.
8. Define the rules.

   Note - For explanations of fields in the Endpoint Compliance rules, see the online help.
9. Click **OK**.

   This takes you back to the Edit Policy or the New Policy page.
10. Click **OK**.

    This takes you back to the Policies page.
11. Click **OK**.

This completes the configuration of the Endpoint Compliance Policies, and takes you back to the Endpoint Security on Demand > Endpoint Compliance page.

After the Endpoint Compliance policies are configured, Endpoint Compliance settings can be configured to make use of the polices.

12. Close SmartDashboard.
13. In SmartConsole, install the policy.

Configuring Endpoint Compliance Settings for Applications and Security Gateways

To configure Endpoint Compliance:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
3. Click **Scan endpoint machine when user connects**.
4. Choose one of the available approaches:
   - Basic Approach - Configuring a Common Policy for the Portal and all Applications
   - Medium Approach - Configuring a Threshold Policy for the Portal, Hardened for Specific Applications
   - Advanced Approach - Configuring Individual Policies for Each Application

Basic Approach - Configuring a Common Policy for the Portal and all Applications

To assign a policy to the Security Gateway and require an Endpoint Compliance scan to connect to the Security Gateway:

1. Click **Threshold policy to access any application via this gateway, the endpoint must comply with the following policy**.
2. From the drop-down list, select the Endpoint Compliance policy that is used for all applications accessed with this Security Gateway.
3. Click **OK**.

To make sure that the applications use the Security Gateway settings for their Endpoint compliance:

1. From the Objects Bar, click **Custom Application/Sites > Mobile Applications > Web Applications**.
2. Double-click the application.

   The Web Application settings window opens.
3. From the navigation tree, click **Additional Settings > Protection Level**.
4. Make sure that **This application relies on the security requirements of the gateway** is selected.
5. Click **OK**.

6. Repeat these steps for each application.
7. Install policy.
8. Configure the Endpoint Compliance logs.

Medium Approach - Configuring a Threshold Policy for the Portal, Hardened for Specific Applications

To configure the Security Gateway settings:

1. Click **Threshold policy: to access any application via this gateway, the endpoint must comply with the following policy**.
2. From the drop-down list, select the default Endpoint Compliance policy to be used for applications accessed via this Security Gateway.
3. Click **OK**.

To make sure that the applications use the Security Gateway settings for their Endpoint compliance:

1. From the Objects Bar, click **Custom Application/Sites > Mobile Applications > Web Applications**.
2. Double-click the application that requires hardened endpoint security.

   The Web Application settings window opens.
3. From the navigation tree, click **Additional Settings > Protection Level**.
4. Click **This application has additional security requirements, specified by the following protection level**.
5. From the drop-down list, select a Protection Level for this application.

   To define a new Protection Level, click **Manage** and *"Mobile Access Applications" on page 58*.
6. Click **OK**.
7. Repeat these steps for each application.
8. Install policy.
9. Configure the Endpoint Compliance logs.

Advanced Approach - Configuring Individual Policies for Each Application

To configure the Security Gateway settings:

1. In the **Endpoint Compliance** page of the Security Gateway, click **No threshold: to protect applications, configure endpoint compliance requirements individually per application**.
2. Click **OK**.

To configure an individual policy for each application:

1. From the Objects Bar, click **Custom Application/Sites > Mobile Applications > Web Applications**.
2. Double-click the application that requires hardened endpoint security.

The Web Application settings window opens.

3. From the navigation tree, click **Additional Settings > Protection Level**.
4. Click **This application has additional security requirements, specified by the following protection level**.

   Note - If **This application relies on the security requirements of the gateway** is selected for the Mobile Access application, users are allowed to access the application without any Endpoint Compliance requirements.
5. From the drop-down list, select a Protection Level for this application.

   To define a new Protection Level, click **Manage** and *"Mobile Access Applications" on page 58*.
6. Click **OK**.
7. Repeat these steps for each application.
8. Install policy.
9. Configure the Endpoint Compliance logs.

Configuring Advanced Endpoint Compliance Settings

You can edit the Advanced Endpoint Compliance Settings to configure whether or not to allow access to the Security Gateway and applications if the Endpoint Compliance scanner is not supported on the endpoint operating system.

1. In SmartDashboard, from the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance** page.
2. Click **Edit**.

   The **Advanced Endpoint Compliance Settings** window opens.

   In this window you can decide whether or not to allow access to the Security Gateway and applications if the Endpoint Compliance scanner is not supported on the endpoint operating system.

The Endpoint Compliance scanner supports the following operating systems: Windows, Mac, and Linux.

Configuring Platform-Based Bypass Per OS

If you want to allow some endpoint operating systems to bypass Endpoint Compliance requirements, you must select the **Allow access** option in the **Advanced Endpoint Compliance Settings** window.

For details, see the operating system compatibility table in the Mobile Access Release Notes.

To configure different rules on endpoints with different operating systems, see SecureKnowledge solution sk34989.

Platform-Based Bypass Per Protection Level

Configuring Endpoint Compliance Settings per Protection Level lets you set Platform-Based Bypass per application.

By default all Advanced Endpoint Compliance Settings are taken from the SmartDashboard configuration, in the Advanced Endpoint Compliance Settings page.

Enabling Platform Based Bypass per Protection Level

To configure different access permissions for various Protection Levels for Endpoint Compliance scanning, run:

```
cvpnd_settings set useICSRelaxedModeInProtectionLevel true
```

To return to the default setting, change `true` to `false` in the above command.

Configuring the Protection Levels that are Bypassed

In the Mobile Access tab of SmartDashboard, under **Additional Settings > Protection Levels**, is a list of Protection Levels. From this page you can edit the Authentication and Endpoint Security settings that are required for applications assigned to each Protection Level. You can also create new Protection Levels.

In the Mobile Access application properties, assign a Protection Level to an application. For example, if you want to allow access to an application only if the user is compliant with Endpoint Compliance policy1, but you also need to accommodate the user connecting from an endpoint that does not support Endpoint Compliance scanning (such as an iPhone), then:

1. Create or use a Protection Level named ESOD_Relaxed_PL which enforces Endpoint Compliance Policy policy1.
2. Assign the Protection Level to the application.
3. Configure the Protection Level as "Bypassed".

   To configure different access permissions for various Protection Levels for Endpoint Compliance, from the Mobile Access CLI, in expert mode, run:

   ```
   cvpnd_settings listAdd ICSRelaxedModeProtectionLevelNames ESOD_Relaxed_
   PL
   ```

You can add other Protection Levels as well.

To restore a Protection Level from being "Bypassed", for Endpoint Compliance:

1. Run:

   ```
   cvpnd_settings listRemove ICSRelaxedModeProtectionLevelNames
   ```

2. Follow the on-screen instructions.

To finalize the configuration of granular platform-based bypass for Endpoint Security on Demand:

1. Restart the Mobile Access services by running `cvpnrestart`

   If the Mobile Access Security Gateway is part of a cluster, be sure to make the same change on each cluster member.

2. In SmartDashboard, assign the Protection Levels to the applications.
3. Install the policy.

Configuring Endpoint Compliance Logs

Mobile Access generates Endpoint Compliance-specific logs. The logs can be viewed in SmartLog, and have the category **Endpoint Security on Demand**. The Endpoint Security on Demand information is in the **info** field of the logs.

To configure tracking options for the Endpoint Compliance scanner:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
3. In the **Endpoint Compliance** page, in the **Tracking** section, enable **Log the endpoint scan results** to record the results of Endpoint Compliance scans to the log.
4. Select **Details** or **Summary** to determine the level of detail to record in the log file.
5. Click **Save** and then close SmartDashboard.
6. In SmartConsole, install the policy.

The Tracking options are:

- **Summary**: Only one log entry per scan is written to SmartLog. The log entry shows endpoints that do not comply with the Endpoint Compliance policy. The date and time of the scan, the source IP address, and the Endpoint Compliance scan ID are logged.
- **Details**: In addition to the Summary mode information, this adds a log entry for each non-compliant rule. For example, in the case of a Spyware Scan rule that screens for tracking cookies, a log entry is generated that contains the following fields:
  1. Malware name: `unwantedexample`.
  2. Malware type: `3rd party cookie`.
  3. Description: `symptom type: URL. Symptom value: cookie:bob@unwantedexample.net`.

Assign Policies to Security Gateways and Applications

To assign policies to Security Gateways:

1. On the **Endpoint Compliance** page, add all Mobile Access Security Gateways to the **Endpoint Security Settings on Mobile Access Security Gateways** section.
2. **Edit** each Security Gateway, whose access will be conditional on passing an Endpoint Compliance scan. Choose the **Threshold policy** and select **Scan the endpoint machine when a user connects**.

To assign policies to applications:

1. To make access to applications conditional on passing an Endpoint Compliance scan, assign a policy to a **Protection Level**.
2. Assign Protection Levels to **Mobile Access applications**.

Excluding a Spyware Signature from a Scan

To exclude a spyware signature from a scan:

1. Configure Mobile Access so that endpoint computers must undergo an Endpoint compliance scan before they connect. The Endpoint Compliance policy must include a Spyware Scan rule.
2. Set up a stand-alone test computer that has the spyware to be excluded from the scan.
3. Run an Endpoint compliance scan on the test computer by connecting from it to Mobile Access.

   When Endpoint Security on Demand detects the spyware (irrespective of the action configured in the Spyware Scan rule), the name of the spyware (something like `Win32.megaspy.passwordthief`) is included in the report.
4. Make a note of the name of the spyware.
5. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
6. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
7. Click **Edit Policies**.
8. Select the policy that is applicable to the clients, and click **Edit**.
9. Select the Spyware Scan rule from the list and click **Edit**.
10. In the **Software exception list** section, click **Add**.
11. Type the **Name** of the spyware, and a **Description**.
12. Click **OK** three times to close the Endpoint Compliance policy editor.
13. Click **Save** and then close SmartDashboard.
14. In SmartConsole, install policy.

Preventing an Endpoint Compliance Scan Upon Every Login

By default, the end user computer is scanned by the Endpoint Compliance scanner every time the user logs in. This is the default, and most secure configuration.

It is possible to configure Mobile Access so that after logging in, the user is not scanned, even after logging in again, until the end of a timeout period.

For configuration details, see sk34844.

Endpoint Compliance Scanner End-User Workflow

The Endpoint Compliance scanner on endpoint computers is supported on browsers that run ActiveX (for Windows with Internet Explorer), or Java.

When using the Endpoint Compliance scanner with Internet Explorer, the browser must be configured to download and run ActiveX controls and to allow Active Scripting. This section explains how to configure Internet Explorer to ensure that the Endpoint Compliance scanner will install and run properly on the endpoint computer.

To configure Internet Explorer for the Endpoint Compliance scanner:

1. Select **Tools > Internet Options** from the Internet Explorer menu.
2. Select the **Security** tab.
3. Select the Web content zone used by the endpoint computer for remote connections from the **Security Settings** window.
4. Click **Custom Level**.
5. Enable the following options in the **Security Settings** window and then click **OK**:
   - Download signed ActiveX controls
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked as safe for scripting
   - Active scripting
6. Select the **Privacy** tab > the**Medium** setting, and then click **Advanced**.
7. Enable **Override automatic cookie handling** and in the **1st party cookies** section, enable **Accept**.
8. Click **OK**.

Endpoint Compliance Scanner End-User Experience

When a user connects to a portal where the Endpoint Compliance is enabled, the end user computer is scanned before the user sees the login screen.

The Endpoint Compliance Scanner is installed on the endpoint machine, by using ActiveX (for Windows with Internet Explorer), or *"The Mobile Access Portal" on page 184*.

Note - The Endpoint Compliance scan starts if Endpoint compliance is configured for a Mobile Access application in a portal, even if portal access does not require compliance with a policy.

To login to the Mobile Access Portal with the Endpoint Compliance scanner enabled:

1. Enter the Mobile Access Portal URL in your browser.
2. If you are using the Endpoint Compliance scanner for the first time on a particular endpoint computer, you are prompted to download and install the Check Point Mobile Access Portal Agent.

   You may see these warnings:

   1. Do you trust the Mobile Access site you are connecting to?

   2. Do you trust the certificate of the server of the Mobile Access site?
3. During the scan, a progress bar is displayed.
4. If the endpoint computer successfully passes the Endpoint compliance scan, the Mobile Access Portal login screen appears.

If the endpoint computer fails to pass the scan, Endpoint Security on Demand displays a result screen showing the potentially harmful software and security rule violations detected during the scan.

- Click on a potentially harmful software item to display a short description of the detected malware, what it does and recommended removal method(s).
- If the **Continue Anyway** button appears, you can continue and log on to the Mobile Access Portal without removing the malware or correcting the security rule violation.
- If there is no **Continue Anyway** button, you must remove the detected malware or correct the security rule violation before you can log on to the Mobile Access Portal. When you have corrected the problem, click **Scan again** to repeat the scan.

5. When the Mobile Access Portal login page appears, you can log on normally.

Note - The user and administrator see the scan results as log entries in the Traffic Log. Each entry shows the user name, user group, source computer, malware name, malware type, and malware description.

Using Endpoint Security on Demand with Unsupported Browsers

Endpoint Security on Demand for Mobile Access requires browsers that support ActiveX or Java.

The following sections describe Endpoint Security on Demand behavior when users attempt to access the Mobile Access Portal using an unsupported browser.

- If the **Block access to all applications** option on the Endpoint compliance scan **Policy** page is enabled, and *either* of the following conditions exist, the endpoint computer cannot connect to the Mobile Access Portal.
  - The **Prevent Connectivity** option is enabled for at least one malware protection rule.
  - The **Restrict** action is selected for at least one enforcement rule (anti-virus or custom).

    In this case, Endpoint Security on Demand presents an error message and generates a log entry in the administrator's traffic log.
- In all other cases, users can log on to the Mobile Access Portal without passing an Endpoint compliance scan. In some cases, an incompatibility message appears with a **Continue** button that allows users to proceed with Mobile Access login. Endpoint Security on Demand generates a log entry in the administrator's traffic log.
- When an application's Protection Level is configured to require an Endpoint Compliance scan, users can still gain access to the Mobile Access Portal, but cannot run that application.

Preventing Portal Access with Unsupported Browsers

The following steps can prevent users using unsupported browsers from gaining access to the Mobile Access Portal and applications without passing an Endpoint Compliance scan:

- Enable the **Scan endpoint machine when user connects option**, and set a **threshold policy**. This setting is found on the **Endpoint Security on Demand > Endpoint compliance** page.
- Assign Protection Levels that require passing an Endpoint Compliance scan to all applications.
- Prevent users from using an unsupported browser to access the Mobile Access Portal by forcing Endpoint Security on Demand to reject all connections from unsupported browsers. See the "Configuring Advanced Endpoint Compliance Settings" section.

Completing the Endpoint Compliance Configuration

The Endpoint Compliance page shows:

- Number of Mobile Access Security Gateways configured to scan endpoint machines.
- Security policy required on the Security Gateway.
- Number of Mobile Access applications, with Level of Enforcement (full, partial, or none).

If this is correct for your organization:

1. Click **Save** and then close SmartDashboard.
2. In SmartConsole, install policy.

Secure Workspace

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the "real" workspace.

No data is allowed to leave this secure environment except through the Mobile Access Portal. Secure Workspace users cannot access any applications, files, system tools, or other resources from the virtual workspace unless they are explicitly permitted by the Secure Workspace policy.

Administrators can easily configure Secure Workspace policy to allow or prevent activity according to enterprise requirements.

Secure Workspace creates an encrypted folder called **My Secured Documents** on the virtual desktop that contains temporary user files. It deletes this folder and all other session data when the session terminates.

After Secure Workspace is enabled, configure a Security Gateway to either require all users to connect to the Mobile Access Portal through Secure Workspace, or to give users the option of connecting through Secure Workspace or from their endpoint computers.

Enabling Secure Workspace

To enable Secure Workspace for an Mobile Access Security Gateway:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Secure Workspace**.
3. To configure the Secure Workspace policy, click **Edit policy**.

   For details, see the "Configuring the Secure Workspace Policy" section.
4. Click **Save** and then close SmartDashboard.
5. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

The Security Gateway window opens and shows the **General Properties** page.

6. From the navigation tree, click **Mobile Access > Check Point Secure Workspace**.
7. To enable Secure Workspace on the Security Gateway, click **This gateway supports access to applications from within the Secure Workspace**.
8. Select the options to define the behavior of Secure Workspace when a user logs in to the Mobile Access Portal:
   - **Allow user to choose whether to use Check Point Secure Workspace**
   - **Users must use Check Point Secure Workspace**
   - **User must use Check Point Secure Workspace only if the following Endpoint Compliance policy is not satisfied** - This option lets you to set a rule that if a certain Endpoint Compliance policy is not satisfied by the client connecting to the Security Gateway, the client must use Secure Workspace. If the Endpoint Compliance policy is satisfied, using Secure Workspace is optional.
9. Select the Endpoint Compliance Policy that is enforced on the Security Gateway. If the criteria of the selected policy are not satisfied, the client connecting must use Secure Workspace.
10. Click **OK**.
11. In SmartConsole, install policy.

Configuring Advanced Secure Workspace Settings

In the **Endpoint Security on Demand > Secure Workspace** page, in the **Advanced Secure Workspace Settings** section, click **Edit**. The **Advanced Secure Workspace Settings** window opens.

In this window you can decide whether or not to allow access to the Security Gateway and applications if Secure Workspace is not supported on the endpoint operating system.

To configure advanced operating system-specific settings, see sk34989.

Configuring Platform-Based Bypass Per OS in Secure Workspace

If you want to let some endpoint operating systems to bypass Secure Workspace requirements, you must select the **Allow access** option in the **Advanced Secure Workspace Settings** window.

To configure different rules on endpoints with different operating systems, see sk34989.

Platform-Based Bypass Per Protection Level in Secure Workspace

Configuring Secure Workspace Settings per Protection Level allows you to configure "Platform-Based Bypass" per application.

By default all Advanced Secure Workspace Settings are taken from the SmartDashboard configuration, in the Advanced **Secure Workspace Settings** page.

Enabling Platform Based Bypass per Protection Level

To configure different access permissions for various Protection Levels for Secure Workspace, from the CLI run:

```
cvpnd_settings set useISWRelaxedModeInProtectionLevel true
```

To return to the default setting, change `true` to `false` in the above command.

Configuring the Protection Levels that are Bypassed

In the Mobile Access tab of SmartDashboard, under **Additional Settings > Protection Levels**, is a list of Protection Levels. From this page you can edit the Authentication and Endpoint Security settings that are required for applications assigned to each Protection Level. You can also create new Protection Levels. If you select, **Applications using this protections level can only be accessed from within Check Point Secure Workspace**, all applications assigned to that Protection level will only be accessed from within Secure Workspace.

However, if you want to allow access to an application only from Secure Workspace, but you also need to accommodate the user connecting from an endpoint that does not support Secure Workspace (such as an iPhone), then:

1. Create or use a Protection Level named ESOD_Relaxed_PL which enforces Endpoint Compliance Policy policy1.
2. Assign the Protection Level to the application.
3. Configure the Protection Level as "Bypassed".

   To configure different access permissions for various Protection Levels for Secure Workspace, from the Mobile Access CLI, in expert mode, run:

   ```
   cvpnd_settings listAdd ISWRelaxedModeProtectionLevelNames ESOD_Relaxed_
   PL
   ```

You can add other Protection Levels as well.

Restoring a Protection Level from being Bypassed for Secure Workspace

1. Run:

   ```
   cvpnd_settings listRemove ISWRelaxedModeProtectionLevelNames
   ```

2. Follow the on-screen instructions.

Finalize the Configuration for Secure Workspace

1. Restart the Mobile Access services by running `cvpnrestart`.

   If the Mobile Access Security Gateway is part of a cluster, make the same change on each cluster member.

2. In SmartDashboard, assign the Protection Levels to the applications.
3. Install the policy.

Applications Permitted by Secure Workspace

In its default configuration, Secure Workspace allows access to a limited group of applications. This is usually sufficient for most end-users working with the Mobile Access Portal and retrieving information from network hosts.

See sk114454 for the list of supported applications.

SSL Network Extender in Secure Workspace

When using SSL Network Extender inside Secure Workspace, Secure Workspace traffic and traffic from outside the Secure Workspace are encrypted.

Secure Workspace Policy Overview

Secure Workspace controls access to applications and directories on endpoint computers based on the Secure Workspace policy.

Each Mobile Access Security Gateway has its own Secure Workspace policy. The policy:

- Grants or denies permission for users to run applications.
- Allows applications to save files to specific files and directories.
- Defines general portal protection security settings and user experience behavior.

You can add to the list of *Approved Applications*, and can add, edit, or delete applications from the list.

You can define locations where the application is allowed to save files that remain after Secure Workspace shuts down. These locations are called *Allowed Save locations*. There is no need to define locations for files that are not needed after Secure Workspace shuts down. Temporary files are deleted when the Secure Workspace is closed.

Secure Workspace includes a built-in Firewall that lets you define *Outbound Firewall Rules*. These are the IP addresses and ports that approved applications are allowed to access. By default, desktop applications are allowed to access all addresses and ports.

Note that settings for the approved applications, save locations, and Outbound Firewall Rules are independent. For example, the save locations are not restricted to a particular application, and similarly, Outbound Firewall Rules apply to all applications.

Configuring the Secure Workspace Policy

The Secure Workspace policy determines the permitted activities and behavior that end users will experience when working in Secure Workspace.

To configure the Secure Workspace Policy:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand** > **Secure Workspace**.
3. Configure the Secure Workspace policy, click **Edit policy**.

   The **Secure Workspace Settings** window opens.
4. Fill in the fields in the tabs described in the next sections.

General Settings

Self Protection

- **Enable Secure Workspace Self Protection** - Best Practice is to select this to add driver-level protection for Secure Workspace and prevent attempts to tamper with the environment.

  This requires administrative privileges and the User Access Control (UAC) prompt might show during the Secure Workspace startup.

  - **Prevent Secure Workspace startup if the Self Protection driver fails to install** - When selected, Secure Workspace can only start if the Self Protection driver is successfully installed.

SSL Network Extender

- **Allow SSL Network Extender connections only from within Secure Workspace** - Select this option to use corporate resources from within Secure Workspace only. Use this if your organizational security policy requires access to corporate resources from within a clean, segregated environment, and with a strict set of allowed applications.

Data Protection

- **Prevent the host PC from printing secure documents** - Users cannot print documents from Secure Workspace.
- **Prevent copying clipboard content to the host PC** - Users cannot copy content from inside Secure Workspace to paste or save it outside of Secure Workspace.

Application Control Settings

- **Enable Reputation Services to validate the integrity of allowed applications in the Applications Table** - When a user starts an application that is not an Approved Application, Secure Workspace contacts Check Point Reputation Services to ask if the application is legitimate. Reputation Services returns one of three responses: The application is trusted, the application is untrusted, or the application is unknown. Configure the Secure Workspace policy to handle Reputation Services responses:
  - **Allow Trusted only**
  - **Allow Trusted and Unknown**

Application Table

Approved applications show on the Secure Workspace desktop, and are allowed to run on endpoint computers. You can add, edit, or remove applications from the list.

Configuring Applications in the Application Table

- To add an application: Click **Add Application**.
- To remove an application: Click **Remove**.
- To edit the information for the application: Click the application **Display Name** in the table.

When you add a new application or edit an application, you can include this information:

- **Display Name** (required)- The name of the approved application as it shows on the desktop.
- **Executable File** (required) - The path and filename for the application selected. .

  Enter the path in one of these formats:

  - Absolute path in this format: `<disk>:\<folder_path>\<binary_name>`. Secure Workspace allows the endpoint to run the binary from specified location only. The full path is necessary if the location of the program does not appear in the PATH.
  - File name, for example: `\<binary_name>`. Secure Workspace allows the endpoint to run the binary with the specified name from all locations on the disk. Use if the location appears in the PATH.
  - Path with environment variable, for example: `<path_with_env_variable>\<binary_name>`. Secure Workspace resolves the environment variable on the endpoint, and uses its value as part of the path to the executable.
- **Executable Original File Name** (optional) - Enter this if you also select an **Executable Vendor Name**, so Secure Workspace can make sure that the application certificate meets the requirement. The original filename shows in the details of the application's certificate.
- **Executable Vendor Name** (optional) - When a vendor is selected, Secure Workspace checks the application's certificate to make sure that it is signed by this vendor. The same application is blocked with a different vendor.
- **File hash** (optional) - Enter the MD5 or SHA256 signature of the application. You can add multiple hashes, for example, one for each version of the application.
- Select the hash type that you use: **MD5** or **SHA256**.
- **Comment** (optional) - Add a comment that describes the application.
- **Add shortcut to Start Menu** (optional) - Select to add a shortcut to the application to the Start Menu in the Secure Workspace. The shortcut is only added if the application exists on the client computer. You can also enter a command line argument to run as a shortcut.
- **Add shortcut to Desktop** (optional) - Select to add a shortcut to the application to the Desktop in Secure Workspace. The shortcut is only added if the application exists on the client computer. You can also enter a command line argument to run as a shortcut.

Vendor Control Settings

You can configure which applications users can access from Secure Workspace. If a vendor is trusted then all applications from this vendor are trusted. See sk114526 for the vendors trusted by default. You cannot add a vendor to the list.

- To block a vendor: Clear the checkbox for the vendor.
- To allow a vendor: Select the checkbox for the vendor.

Allowed Save Locations

Allowed Save locations are locations where applications are allowed to save files that remain after Secure Workspace shuts down. There is no need to define locations for temporary files that can be deleted after Secure Workspace shuts down.

To add an allowed save location:

1. In the **Allowed Save locations** tab, click **Add Location**.
2. In the window that opens enter:
   - **Name** - A descriptive name of the location.
   - **Path** - The complete path to the location.
   - **Description** (optional) - A longer description.
3. Click **Save Location**.

Outbound Firewall Rules

Outbound Firewall Rules define which IP addresses and ports approved applications are allowed to access when they make outbound connections.

These options are available:

- **Localhost Connection. Do not allow connection to application on host PC** - When selected Secure Workspace users can only use applications in Secure Workspace and cannot access the host PC. When cleared, users can access the host PC when Secure Workspace is active, but can only save things in the defined locations.
- **Accept Rules** - Select a rule in the table to enable it. Clear a rule in the table to disable it. Only connections that match enabled rules are allowed. The default rules are:
  - **Everywhere** - Allows desktop applications to access all addresses and ports.
  - **Localhost connection** - Required for Internet Explorer. Not recommended to delete.

Best practice is to use the default rules. You can delete the default rules and replace them with more restrictive rules, but do so carefully.

Virtual Registry Rules

You can add custom rules to the Secure Workspace virtual registry. Contact Check Point support for more information about this feature.

User Experience Settings

In the User Experience settings, configure what users see and how they interact with Secure Workspace.

General

- **Prevent Host PC/ Secure Workspace desktop switching** - Users cannot switch between the host PC and Secure Workspace environments. Access to the regular desktop is only allowed if Secure Workspace is closed.
- **Display welcome window** - When selected, "Welcome to Secure Workspace" is shown to users. Select if it always shows or if users can disable it.
- **Disable "Run" option in Start menu inside Secure Workspace** - Users cannot run programs with the **Run** command from the Start menu in Secure Workspace.
- **Hide all system drives** - Local drives are hidden when in Secure Workspace.

- **Prevent to start browser inside Secure Workspace** - Disable the automatic launch of an internet browser in Secure Workspace after Secure Desktop is started. As a result SSL Network Extender does not start and automatically establish a VPN tunnel.

Desktop Background - Change the Secure Workspace desktop background picture and its position.

Display Start dialog - Show a Start window that you customize.

Configuring a Secure Workspace Policy per Security Gateway

A Secure Workspace policy that is configured in SmartDashboard applies to all Mobile Access Security Gateways. To configure a Secure workspace policy for each Security Gateway, see sk34939.

Integration with Endpoint Security Reputation Service

Secure Workspace can work together with the Check Point Endpoint Security Reputation Services to check whether an application that is not an approved application is legitimate. Reputation Services identifies programs according to their filename and MD5 hash.

For details of the Endpoint Security Reputation Services, see your version of the *R80.40 Endpoint Security Server Administration Guide*. If you use Reputation Services, the sequence of Secure Workspace is:

1. The user selects a program to run in Secure Workspace.
2. Secure Workspace checks the policy. If the program is not allowed by the Secure Workspace policy, program execution is blocked.
3. If the program is allowed by the policy, Secure Workspace queries Reputation Services about the program.
4. Reputation Services returns one of three responses about the application: Trusted, Untrusted, or Unknown.
5. Secure Workspace allows or blocks the application according to the Reputation Services responses, as defined in the policy:
   - **Allow Trusted only**.
   - **Allow Trusted and Unknown**.

Secure Workspace End-User Experience

This section provides an overview of the Secure Workspace workflow.

Disabling Internet Explorer Protected Mode

If users use Internet Explorer to open the Mobile Access Portal on Windows Vista or higher, they must disable Internet Explorer Protected Mode. If Protected Mode is not disabled, SSL VPN might run, but they can have unexpected errors.

On Windows 7 and higher, protected mode is enabled by default. You can see that it is enabled:

- In the **Internet Options** > **Security** tab. See that **Enable Protected Mode** is selected.
- In the bottom right of the Internet Explorer browser window, it says **Protected Mode On**.

If Endpoint Security on Demand is configured on the Security Gateway, the scan detects that Protected mode is on and instruction to disable Protected Mode open.

If Endpoint Security on Demand is not configured on the Security Gateway, users are not alerted that they must disable Protected Mode. However they must do the same steps to disable Protected Mode so that they can access the SSL VPN portal without problems.

To disable Protected mode for the SSL VPN Portal:

In Internet Explorer, select **Tools** > **Internet Options**.

1. In the **Internet Options** window, select the **Security** tab.
2. In the **Security** tab, select **Trusted Sites** and clear the **Enable Protected Mode** checkbox.
3. Click **Sites**.
4. In the **Trusted sites** window:
    a. Click **Add**.
    b. In **Add this website to the zone**, enter the web address of the SSL VPN portal.

    The portal web address shows in the **Websites** area of the window.
5. Click **Close**.
6. Click **OK**.

All users must do these steps even if they do not get the instructions automatically. After these steps, close all Internet Explorer windows. The next time you open Internet Explorer, Protected Mode is off.

Logging on to the Mobile Access Portal Using Secure Workspace

Secure Workspace initializes when a user logs on to the Mobile Access Portal. If the administrator has configured the Mobile Access Security Gateway to require Secure Workspace, this occurs automatically. If the administrator has configured the Security Gateway to allow users to choose whether or not to use Endpoint Security on Demand, an option appears on the Login screen.

Working with the Secure Workspace Virtual Desktop

The Secure Workspace virtual desktop looks and feels like a normal Windows desktop.

The principal difference is that Secure Workspace only allows users to work with a limited number of pre-approved applications and files and, by default, does not allow users to print, customize the desktop or perform any system configuration activities. Since most users only use Secure Workspace to work with the Mobile Access Portal, these functions are rarely needed.

Start Menu and Taskbar

The virtual desktop Start menu and taskbar function in the same manner their "real" counterparts do. Configuration settings in the Secure Workspace policy determine which shortcuts and options are available to users.

Allowing Users to Save Files to the "Real" Desktop

Users occasionally need to download and save files from resources behind the Mobile Access Security Gateway to "real" desktop folders. Conversely remote users may need to upload files to the corporate network from the endpoint computer.

To allow this, the administrator must configure the Secure Workspace policy to allow endpoints to switch between the secure and regular desktops. This is accomplished in the **User Experience Settings** section of the Secure Workspace policy editor.

Accessing Files and Applications on the Endpoint Computer

Generally, users can access files and run applications in Secure Workspace in the same manner as on the "real" desktop. Since, by default, users have read-only (access) privileges to all folders and files, they can freely navigate the file system using Windows Explorer. When attempting to run a program or open a file for which a user does not have Secure Workspace permission, an error message appears.

Likewise, if a user attempts to save a file to a "real" desktop folder without Secure Workspace permissions, an error message appears.

Accessing Endpoint Applications in Secure Workspace

When SSL Network Extender *network mode* users initiate a Secure Workspace session, permitted Endpoint Applications are available in the virtual desktop as follows:

An Endpoint Application defined in the Native Application as...	... is available to Users as a
Path and executable name (already installed)	Shortcut in the Windows **Start** menu.
Runs via default browser	Shortcut on the desktop.
Downloaded-from-Mobile Access application	Link in the Mobile Access Portal.

Note - During a Secure Workspace session, SSL Network Extender cannot toggle between the Network Mode and the Application Mode. User can change the mode, but must start a new Secure Workspace session after doing so.

Switching Between Secure Workspace and the "Real" Desktop

You can switch back and forth between the Secure Workspace virtual workspace and the "real" desktop at any time. To do so, click the lock icon, located in the tray area of the taskbar.

Exiting Secure Workspace

To exit Secure Workspace:

1. From the Windows **Start** menu, select **Close Secure Workspace**.

   A confirmation and reminder to save open files appears.

2. Click **Yes, close it now** to continue closing Secure Workspace.

Troubleshooting Secure Workspace

Secure Workspace logs are automatically saved in `%temp%\IswTmp\Logs` when the environment variable `ISWLOG` is set to 0 (zero). If you have issues with Secure Workspace, you can examine these logs or send them to Check Point technical support.

If an application stops working, a Secure Workspace window opens to help you send technical information to Check Point. Users can manually open this window if a process hangs or they experience instability.

To collect technical information:

1. Press Ctrl+Alt+End.

   A Secure Workspace window opens to help you send technical information to Check Point.
2. Fill in the required information and click **Collect and Send**.
3. Send the file to Check Point support.

Endpoint Compliance Updates

Check Point provides Endpoint Compliance updates. You can download Endpoint Security on Demand updates from the **Mobile Access** tab in SmartDashboard.

You can configure Endpoint Security on Demand to retrieve updates automatically according to a defined schedule or you can manually download and install the updates.

Working with Automatic Updates

You can periodically check for and automatically download Endpoint Compliance updates. You can choose to download updates from the Check Point Download Center or you can install updates previously downloaded to your Security Management Server.

Note - Before performing an Endpoint Security on Demand update, install a policy at least once.

To configure automatic updates:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance Updates**.
3. In the **Update Configuration** section, click **Configure**.

   The **Automatic Updates** window opens.
4. On the **Activation** tab, click **Enter User Center credentials**.
5. Enter your User Center email address and password.
6. Click the **Endpoint Security on Demand** tab.
7. Configure these update settings:
   a. To install updates from the Download Center, select the **Check Point website** option.
   b. To install updates from your Security Management Server, select the **My local Security Management Server** option. If you want to install updates from the Download Center when the Security Management Server is unavailable, enable the indicated option.
   c. Select the interval, in minutes, after which Endpoint Security on Demand checks for available downloads.
8. In the **Tracking Configuration** tab, select the various tracking options from the lists. You can select logging events or a variety of alert types.

9. If there is a proxy server between the Security Management Server and the User Center, select the **Proxy** tab, and enter the proxy host name or IP address, and the proxy port number (for example: 8080).
10. Click **OK** to complete the definition.
11. Click **Save** and then close SmartDashboard.
12. In SmartConsole, install policy.

Performing Manual Updates

To perform a manual Endpoint Security on Demand update:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance Updates**.
3. Click **Update Databases Now**.
4. Enter your Check Point User Center credentials and click **Next**.
5. Choose the **All supporting gateways** option to download to all available Mobile Access Security Gateways. Alternatively, choose the **Select** option to select specific Mobile Access Security Gateways for update, and then select the applicable Mobile Access Security Gateways in the left-hand list and then click **Add**.
6. Click **Finish**. A progress bar appears during the download.
7. Click **Save** and then close SmartDashboard.
8. In SmartConsole, install policy.

Advanced Password Management Settings

If your organization uses Microsoft Active Directory (AD) to manage users, you can use these password settings allow continuous remote access for your users.

Note - Mobile Access does not support Microsoft Active Directory 2000.

Password Expiration Warning

Administrators can configure SmartDashboard to tell users to change their passwords before they expire. This is an efficient way to ensure that users have continuous access to resources. See sk33404.

Managing Expired Passwords

Passwords expire in these cases:

- The password exceeds the maximum number of days set in the Active Directory Group Policy.
- The **User must change password at next logon** option in the Active Directory configuration is enabled.

When the password expires, a message tells the user that the login failed. The administrator can configure a setting in SmartDashboard to give users the option to enter a new password after the old one expired. Users whose passwords expired then receive a message: **Your password has expired. Enter a new password**. They must then enter and confirm a new password to enter the Mobile Access or VPN client portal.

Configuring Password Change After Expiration

You can configure password change after expiration on Security Gateways R71 or higher. Make sure that the LDAP server is configured to work with LDAP over SSL.

To enable password change after expiration:

1. In SmartDashboard, select **Global Properties > User Directory (LDAP)**.
2. Under **User Directory (LDAP) Properties**, select **Enable Password change when a user's Active Directory password expires**.
3. In the **LDAP Account Unit Properties** window, make sure the assigned **Profile** is **Microsoft_AD**.
4. Make sure that the Login DN for the LDAP server, as configured in SmartDashboard, has sufficient permissions to modify the passwords of Active Directory users.
5. In the LDAP Server Properties window in the **Encryption** tab, select **Use Encryption (SSL)**.
6. If the LDAP schema of the Active Directory is not extended with Check Point's LDAP schema, use GuiDBedit Tool (see sk13009) to make these changes:

- Select **Managed Objects > LDAP > Microsoft_AD > Common**
- Find `SupportOldSchema` and change its value to `1`

For more about LDAP and user management, see the *R80.40 Security Management Administration Guide*.

Session Visibility and Management Utility

Introduction to Session Visibility and Management

When the Session Visibility and Management Utility is enabled, each time a user connects remotely to an R77.30 or higher Security Gateway, the data is recorded in an SQL database.

You can run queries on this database with the Session Visibility and Management Utility.

You can use the Utility to:

- Show session information based on constraints
- Terminate user sessions based on constraints

The main commands are described below. You can also edit the configuration XML file to create custom commands. See sk104644 for advanced configuration.

These Check Point clients are fully supported with the Session Visibility and Management Utility:

- Capsule Workspace for iOS and Android
- Mobile Access Portal with SSL Network Extender (Application and Network modes)
- Remote Access VPN as part of the Endpoint Security Suite
- Remote Access clients: Endpoint Security VPN, Check Point Mobile for Windows, SecuRemote

These clients are supported but sessions on them cannot be terminated:

- Capsule Connect
- Capsule VPN
- Windows 8.1 Check Point VPN Plugin

Enabling the Utility

By default the Session Visibility and Management Utility is disabled.

To enable or disable the Session Visibility and Management Utility:

1. For SecurePlatform only, run on the Security Gateway this long command:

   ```
   $CVPNDIR/bin/cvpnd_settings $FWDIR/conf/sessionIS.C set "database_
   conf:dataDir" "/var${FWDIR}/datadir/postgres/sessions" nobackup ; chown
   cp_postgres /var$FWDIR/datadir/postgres/sessions/postgresql.conf
   ```

2. To enable: On the Security Gateway, run: `RAsession_util on`

   To disable:On the Security Gateway, run: `RAsession_util off`

3. Run: `cpstop`

4. Run: `cpstart`
5. In a cluster environment, make the change on all cluster members.

Seeing the Number of Open Sessions

To see the number of sessions open at a given time:

```
RAsession_util show sessions_num
```

Disconnecting Remote Access Users

To disconnect a user:

```
RAsession_util terminate {all | byuser <user> | bysession_id <id> | custom
<SQL constraint>}
```

Parameter	Description
`all`	Disconnect all Remote Access users
`byuser`	Disconnect a user by user name
`bysession_id`	Disconnect the session with the given session ID
`custom`	Disconnect users that match an SQL constraint

Examples:

```
# RAsession_util terminate all
# RAsession_util terminate byuser james_wilson
# RAsession_util terminate bysession_id 521bd4788
# RAsession_util terminate custom "src_ip='1.1.1.1'"
```

Seeing User Data

To see data of connected users:

```
RAsession_util show users {all | byname <user_name> | where <where_clause>}
```

Parameter	Description
`all`	Show all users
`byuser`	Show data of the given user name
`where`	Show users by constraint
`certs`	Show user certificates by constraints

Examples:

```
# RAsession_util show users all
# RAsession_util show users byuser "james_wilson"
# RAsession_util show users where "client_name='Mobile Access Portal'"
```

(This command shows all the users connected from the Mobile Access Portal.)

Using Constraints

To disconnect or see data of users that match a non-default definition, use constraints. First, become familiar with the Check Point scheme for Remote Access sessions. Then, use the field names or types to run a `terminate` or `show users` command on matching users.

To see valid constraint fields:

```
RAsession_util show scheme
```

Examples:

This command shows the given fields where the client is the **Mobile Access Portal**, and the results are ordered according to the **creation time**:

```
RAsession_util show custom -FIELDS "session_id,user_name,client_name,browser_
name,machine_name,os_name" -WHERE "client_name='Mobile Access Portal'" -
ORDERBY "creation_time"
```

This command shows the given fields where the client type is **Capsule Workspace**:

```
RAsession_util show custom -FIELDS "user_name,sessionid,client_ver,client_
build_number,os_name,os_ver,device_type" -WHERE "client_name='Capsule
Workspace'"
```

Session Visibility and Management Commands

SCHEME

Description: Shows the table scheme of the database.

Usage: SCHEME

Parameters: None

SESSION_OP

Description: Performs an operation on a session or session based on the defined constraints.

Usage: SESSION_OP <Operation_type> <Sql_constraint [list_of_parameters]>

Parameters:

Parameter	Description
Operation_ type	Type of operation to perform on sessions. Only `terminate` is supported in this release.

Parameter	Description
Sql_constraint	Criteria to select the sessions on which to perform the operation. For example, "username='aa'". It can also be a parametric SQL "WHERE" clause that includes $ signs instead of values, for example, "username=$1 and srcip=$2". The "WHERE" clause means that the first parameter in the List_of_parameters will be placed instead of $1, and the second will be as $2.
List_of_ parameters	Can be empty or list of parameters to be placed instead of the $ signs in the "WHERE" clause.

Examples:

```
SESSION_OP terminate "username='James Wilson'"
```

```
SESSION_OP terminate "username=$1 and srcip=$2" "James Wilson,192.0.2.10"
```

SELECT

Description: Run a query on the sessions table.

Usage: `SELECT <-FIELDS <fields>> [-WHERE <where_clause> [list_of_parameters]] [-GROUPBY <group_by_fields>] [-ORDERBY <order_by_fields>] [-LIMIT <limit_size> [-OFFSET <offset_number>]]`

Parameters:

Parameter	Description
FIELDS <fields>	FIELDS flag with list of fields to select delimited by ",".
WHERE <where_ clause>	WHERE flag with the SQL WHERE clause. <where_clause> can also include $ signs instead of values, for example, "username=$1 and srcip=$2". This where_clause means that the first parameter in the "List_of_parameters" will be placed instead of $1, and the second will be as $2 .
List_of_ parameters	Can be empty or list of parameters to be placed instead of the $ signs in the WHERE clause.
GROUPBY <group_by_ fields>	GROUPBY flag with list of fields to group by delimited by ",".
ORDERBY <order_by_ fields>	ORDERBY flag with list of fields to order the result by delimited by ",".
LIMIT <limit_ size>	LIMIT flag with the limit size.
OFFSET <offset_ number>	OFFSET flag with the result offset.

Example:

```
SELECT -FIELDS "login name,clientname,sessionid" -WHERE "loginname='aa'" -
ORDERBY "clientname"
```

Reverse Proxy

You can configure a Mobile Access Security Gateway to be a reverse proxy for Web Applications on your servers. Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Then the Security Gateway passes the request to an internal server, based on the Reverse Proxy rules. This lets external clients access resources on internal servers, while the internal addresses of the servers are hidden.

Configure the reverse proxy with rules that:

- Map the external addresses of the internal servers to their real network addresses.
- Give permission to external clients to access specified resources on the servers.
- Define if the connections between users and resources use HTTP or HTTPS.

By default, reverse proxy is disabled. Enable and configure it in the CLI.

Configuring Reverse Proxy

In CLI, you can:

- Enable or disable reverse proxy.
- Show the reverse proxy rules and applications.
- Add a new rule or an application.
- Edit an existing rule.
- Delete a rule.
- Apply reverse proxy rule configuration changes.

Note - After each change in the Reverse Proxy rules that you make in the CLI, you MUST run this to apply the changes: `ReverseProxyCLI apply config`

Syntax

```
ReverseProxyCLI {on | off | show {rules|applications} | add {rule <rule_name>
| application <app_name> {capsule_docs | outlook_anywhere} <ext_hostname>
<int_hostname>} | edit rule <rule_name> | remove rule <rule_name> | apply
config}
```

Parameters

Parameter	Description
`on`	Enable the reverse proxy.
`off`	Disable the reverse proxy.
`show {rules|applications}`	Show the reverse proxy rules and applications.

Parameter	Description
`add {rule <rule_name> | application {capsule_docs | lync | outlook_anywhere} <ext_hostname> <int_hostname>}`	Add a reverse proxy rule or application. The **Add** rule command runs in interactive mode. Select actions as prompted. Note that for external hostname and internal hostname, when you enter the URL, you can specify: ■ The protocol: http or https ■ The internal port The **Add** application command adds a set of one or more reverse proxy rules that allows access to supported internal applications. The supported applications are: Outlook Anywhere and Capsule Docs.
`edit rule <rule_name>`	Edit a reverse proxy rule. This command option runs in interactive mode. Select actions as prompted.
`remove rule <rule_name>`	Delete a reverse proxy rule.
`apply config`	Apply the reverse proxy configuration changes. **Note** - To apply reverse proxy rule configuration changes, you must run the apply command at the end of each configuration session.

Important Notes:

- The external ports allowed through the reverse proxy are 80 and 443. All internal ports are allowed.
- If the Gaia Portal of the Mobile Access Security Gateway is:

  `https://<IP Address of Security Gateway>/` with a "/" at the end, you MUST change either the URL or the port.

  For example, change the URL one of these:

  - `https://<IP Address of Security Gateway>/gaia`
  - `https://<IP Address of Security Gateway>:4434`

  To change the Gaia Portal URL:

  1. In the Security Gateway object, click **Platform Portal**.
  2. Change the **Main URL**.
  3. Click **OK**.
  4. Install policy.

  If you do not change either the URL or the port, the Gaia Portal is not accessible.

For complete examples and advanced CLI and XML configuration, see sk110348.

Troubleshooting Reverse Proxy

You can troubleshoot the reverse proxy through standard Check Point monitoring tools, such as SmartLog.

Note - The destination is not shown in logs.

For advanced troubleshooting instructions, contact Check Point Technical Support.

To configure reverse proxy to send traffic logs:

1. In SmartDashboard > **Mobile Access** tab, go to **Additional Settings** > **Logging**.
2. In the **Tracking** area, select **Log Access for Web Applications**, and select one of the events to log:
   - **Unsuccessful access events** (Denied and Failed logs)
   - **All access events** (Allowed, Denied and Failed logs)
3. Install Policy.

The logs are available in SmartLog > **Mobile Access logs**.

Identify Reverse Proxy logs by these criteria:

- **Category**: Mobile Access
- **Application**: Reverse Proxy

The **Access** section of the log can show:

- **Allowed** - **Authorized URL** - The Reverse Proxy allowed the URL request (only shows if the **All access events** logging option is configured).
- **Denied** - **Unauthorized URL** -The Reverse Proxy blocked the URL request. If this is a mistake, you can allow the URL.

  To allow a blocked URL:

  - In the command line, run: `ReverseProxyCLI show rules`
  - Look in the relevant rule in the **Paths** column, find the path that is unauthorized in the log, and add the path that was blocked to the rule.
- **Failed** - The Reverse Proxy failed to forward the request for the Endpoint Security Management Server with one of these messages:
  - **Internal Server Error** - The internal server aborted the connection with the Security Gateway. Make sure the server is up and running.
  - **Proxy not found** -The given proxy host could not be resolved.
  - **Can't resolve host name** - The *<internal_host>* configured in your application or rule cannot be resolved.

    You can see it in the **Internal Server** column with one of these commands:

    - `ReverseProxyCLI show applications`
    - `ReverseProxyCLI show rules`

    Make sure that this hostname can be resolved from the Security Gateway.

    To do this, run `nslookup` on the host to see that the Security Gateway can resolve it.
  - **Internal host connection failed** -Failed to connect to the internal server, make sure the server is up and running.

- **Invalid URL** -The URL from the Security Gateway to the internal server was not formatted correctly.
- **SSL handshake failed** -A problem occurred somewhere in the SSL/TLS handshake between the Security Gateway and the internal server.
- **Server response was too slow** - Operation timeout
- **Page not found**

To turn on debugging for reverse proxy:

1. In the `/opt/CPcvpn-R80.40/conf/ReverseProxy_conf/httpd_common.conf` file, find the parameter `ReverseProxyHandlerTraceLog`, and change its value from **Off** to **On**.

   See the reverse proxy trace logs in:

   `/opt/CPcvpn-R80.40/log/trace_log/`

2. For HTTPS:

   In the `/opt/CPcvpn-R80.40/conf/ReverseProxy_conf/httpd_ssl.conf` file, find the parameter `LogLevel`, and change its value from **emerg** to **debug**.

   See the log files for HTTPS:

   `$CVPNDIR/log/reverseproxy_ssl_debug_log`

3. For HTTP:

   In the `/opt/CPcvpn-R80.40/conf/ReverseProxy_conf/httpd_clear.conf` file, find the parameter`LogLevel`, and change its value from **emerg** to **debug**.

   See the log files for HTTP:

   `$CVPNDIR/log/reverseproxy_debug_log`

To enable cvpnd logs:

1. Run: `cvpnd_admin debug set TDERROR_ALL_ALL=5`
2. See the logs in: `$CVPNDIR/log/cvpnd.elg`

To disable, run: `cvpnd_admin debug off`

To make sure that reverse proxy processes are running:

1. Run: `ps -ef | grep httpd`
2. In the output, find:
   - For HTTPS:

     `ReverseProxySSL/httpd.conf`
   - For HTTP:

     `ReverseProxyClear/httpd.conf`

Reverse Proxy Known Limitations

- Not supported at this time:
  - No GUI (SmartDashboard).
  - No Access control on user level.
  - No granularity of networks or interfaces.
  - No link translation on sites returned with Reverse Proxy.
- If the Mobile Access policy contains applications configured with the Host Translation link translation method, the host names in these applications must be different from the names of the hosts in the communication through the Reverse Proxy.
- Reverse proxy has one certificate for SSL termination. To support multiple web servers over HTTPS, the certificate must be a wild card certificate, or it must use Subject Alternate Names (SAN).
- Lync (Skype for Business) is not supported.
- When you configure reverse proxy on cluster, the rules are not synchronized automatically between members.

Best Practice - Use `ReverseProxyCLI` to add all rules to one member, and then synchronize the rules with the other members.

To synchronize reverse proxy rules between Cluster Members:

1. In the `$CVPNDIR/conf/ReverseProxy_conf/` directory, copy this file from the configured Cluster Member to other Cluster Members:

   `$CVPNDIR/conf/ReverseProxy_conf/ReverseProxyConf.xml`

2. Apply the configuration on each member.

   Run:

   `ReverseProxyCLI apply config`

Mobile Access Blade Configuration and Settings

Interoperability with Other Software Blades

The Mobile Access Software Blade is fully integrated with the other Software Blades. Any Security Gateway running on SecurePlatform or Gaia with the Firewall blade enabled can also have the Mobile Access blade enabled.

Most Network objects, Resources, and Users created in SmartDashboard also apply to Mobile Access and can be used when configuring Access to Applications. Similarly, any Network objects, Users and User Groups that you create or modify in Mobile Access appear in the SmartDashboard navigation tree and are usable in all of the SmartDashboard applications.

IPS Blade

When you enable Mobile Access on a Security Gateway certain IPS Web Intelligence protections are activated. The settings of these protections are taken from a local file and are not connected to the IPS profile. These IPS protections always apply to Mobile Access traffic only, even if the Security Gateway does not have the IPS blade enabled.

Disabling Protections for Advanced Troubleshooting

You should only disable the Mobile Access Web Intelligence protections for advanced troubleshooting.

Important - We do not recommend that you deactivate these protections because of potential security risks to the Security Gateway while the protections are off.

To disable the local Web Intelligence protections:

1. Backup the `$CVPNDIR/conf/httpd.conf` configuration file.
2. Edit `$CVPNDIR/conf/httpd.conf` by deleting or commenting out this line:

   `LoadModule wi_module /opt/CPcvpn-<`*`current version`*`>/lib/libModWI.so`

   Where <*current version*> is the Check Point version installed. For example, R77.20.

Changing to an IPS Profile Configuration for Mobile Access

We recommend using the local IPS Web Intelligence protections that are automatically configured and activated when you enable the Mobile Access blade. If you want to use the IPS profile that you assign to the Security Gateway instead of the local file, make sure that certain crucial protections are active so that your Security Gateway stays secure.

To change to a Security Gateway IPS profile configuration for Mobile Access instead of the local configuration:

1. Edit the IPS profile assigned to the Security Gateway to include all of the protections listed in the "IPS Protections Crucial for Mobile Access" section.
2. From the CLI, run:

   ```
   cvpnd_settings set use_ws_local_configuration false
   ```
3. When prompted, backup the `$CVPNDIR/conf/cvpnd.C` file.
4. Restart the Check Point processes. Run: `cvpnstop ; cvpnstart`

Note - If IPS is disabled, Mobile Access will use the local IPS configuration to ensure that the Security Gateway is protected. This is true regardless of the use_ws_local_configuration flag settings.

To switch back to the local, automatic IPS settings for Mobile Access:

1. From the CLI, run:

   ```
   cvpnd_settings set use_ws_local_configuration true
   ```
2. Restart the Check Point processes. Run: `cvpnstop ; cvpnstart`

IPS Protections Crucial for Mobile Access

The protections listed below should always be active on Mobile Access traffic. They are included in the local IPS settings that are automatically activated when Mobile Access is enabled on a Security Gateway. See that most but not all are included in the **Recommended_Protection** IPS Profile.

Protection Name	In Recommended_Protection Profile?
HTTP Format Sizes	yes
HTTP Methods	yes
ASCII Only Request	yes
General HTTP Worm Catcher	yes
Directory Traversal	yes
Cross-Site Scripting	no
Command Injection	yes
Header Rejection	yes
Malicious Code Protector	no
Non Compliant HTTP	yes

Anti-Virus and Anti-Malware Blade

Certain Anti-Virus settings configured for a Security Gateway in the **Traditional Anti-Virus > Security Gateway > HTTP** page of the **Threat Prevention** tab also apply to Mobile Access traffic. To activate traditional Anti-Virus protection, enable the **Traditional Anti-Virus** on the Security Gateway.

These settings apply to Mobile Access traffic when **Traditional Anti-Virus** is configured to scan traffic **By File Direction**:

- **Incoming files arriving to** - Inspects traffic that Mobile Access users upload to Mobile Access. (The drop-down menu is not relevant.)
- **Outgoing files leaving** - Inspects the traffic that Mobile Access users download from Mobile Access. (The drop-down menu is not relevant.)
- The **Internal Files** field is not relevant since Mobile Access uses an external interface.
- **Exceptions** are not supported.

If **Traditional Anti-Virus** is configured to scan traffic **By IPs**, all portal traffic is scanned according to the settings defined for the Mail, FTP and HTTP protocols in SmartDashboard.

Mobile Access Anti-Virus protections always work in **proactive mode** regardless of which option you select.

Note - After SSL Network Extender traffic is rerouted to the Security Gateway, Anti-Virus inspects the traffic as it does to any other unencrypted traffic.

Enabling Traditional Anti-Virus

The Anti-Virus blade and Traditional Anti-Virus can be activated on Security Gateways in your system.

Note - You cannot activate the Anti-Virus blade and Traditional Anti-Virus on the same Security Gateway.

To configure Traditional Anti-Virus:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Other > More Settings > Enable Traditional Anti-Virus**.
3. Click **OK**.
4. Define rules in the Access Control Policy to allow the specified services. Anti-Virus scans only accepted traffic.
5. From **Anti-Bot and Anti-Virus** tab > **Traditional Anti-Virus**, select the services to scan using these options:
   a. From the **Database Update** page, configure when to perform automatic signature updates or initiate a manual signature update.
   b. From the **Security Gateway** > **Mail Protocol** page, configure Anti-Virus scanning options for **Mail Anti-Virus**, **Zero Hour Malware**, **SMTP**, and **POP3** services.
   c. From the **Security Gateway** > **FTP** page, configure FTP traffic scanning options.
   d. From the **Security Gateway** > **HTTP** page, configure HTTP traffic scanning options.

e. From the **Security Gateway** > **File Types** page, configure the options to scan, block or pass traffic according to the file type and configure continuous download options.

f. From the **Security Gateway** > **Settings** page, configure options for file handling and scan failures.

IPsec VPN Blade

The IPsec VPN blade and Mobile Access blade can be enabled on the same Security Gateways. They can be used in parallel to enable optimal site to site and remote access VPN connectivity for your environment.

Certain VPN Clients that worked with Mobile Access in previous versions do not work with the Mobile Access blade on Security Gateways R71 and higher. They only work with the IPsec VPN blade.

These are:

- Endpoint Connect
- SecureClient Mobile

SSL Network Extender works either with Mobile Access or with IPsec VPN. However, if the Mobile Access blade is enabled on a Security Gateway, SSL Network Extender must be configured through Mobile Access. If you had SSL Network Extender configured through IPsec VPN and now you enabled the Mobile Access blade on the Security Gateway, you must reconfigure SSL Network Extender policy in the Mobile Access tab of SmartDashboard. Rules regarding SSL Network Extender in the main security rule base are not active if the Mobile Access tab is enabled.

Office Mode can be configured either with Mobile Access or with IPsec VPN.

Concurrent Connections to the Security Gateway

In the **Gateway Properties** > **Optimization > Capacity Optimization** section you can configure the maximum limit for concurrent connections.

When users connect to corporate resources through the Mobile Access blade, it creates multiple connections. For example, from the user to the Security Gateway, and from the Security Gateway to the internal server. Therefore, in an environment with over 1000 remote users, we recommend that you increase the maximum concurrent connections.

For example: The default maximum is 25,000. If you have 2000 mobile access users, increase the maximum to 29,000 (2 times 2000).

Server Certificates

For secure SSL communication, Security Gateways must establish trust with endpoint computers by showing a *Server Certificate*. This section discusses the procedures necessary to generate and install server certificates.

Check Point Security Gateways, by default, use a certificate created by the Internal Certificate Authority on the Security Management Server as their server certificate. Browsers do not trust this certificate. When an endpoint computer tries to connect to the Security Gateway with the default certificate, certificate warning messages open in the browser. To prevent these warnings, the administrator must install a server certificate signed by a trusted certificate authority.

All portals on the same Security Gateway IP address use the same certificate.

Obtaining and Installing a Trusted Server Certificate

To be accepted by an endpoint computer without a warning, Security Gateways must have a server certificate signed by a known certificate authority (such as Entrust, VeriSign or Thawte). This certificate canbe issued directly to the Security Gateway, or be a chained certificate that has a certification path to a trusted root certificate authority (CA).

The next sections describe how to get a certificate for a Security Gateway that is signed by a known Certificate Authority (CA).

Generating the Certificate Signing Request

First, generate a *Certificate Signing Request* (CSR). The CSR is for a *server* certificate, because the Security Gateway acts as a server to the clients.

Note - This procedure creates private key files. If private key files with the same names already exist on the computer, they are overwritten without warning.

1. From the Security Gateway command line, log in to the Expert mode.
2. Run:

   ```
   cpopenssl req -new -out <CSR file> -keyout <private key file> -config
   $CPDIR/conf/openssl.cnf
   ```

   This command generates a private key. You see this output:

   ```
   Generating a 2048 bit RSA private key
   .+++
   ...+++
   writing new private key to 'server1.key'
   Enter PEM pass phrase:
   ```

3. Enter a password and confirm.

   Fill in the data.

   - The **Common Name** field is mandatory. This field must have the Fully Qualified Domain Name (FQDN). This is the site that users access. For example: `portal.example.com`.
   - All other fields are optional.

4. Send the CSR file to a trusted certificate authority. Make sure to request a *Signed Certificate* in PEM format. Keep the `.key` private key file.

Generating the P12 File

After you get the Signed Certificate for the Security Gateway from the CA, generate a P12 file that has the Signed Certificate and the private key.

1. Get the Signed Certificate for the Security Gateway from the CA.

   If the signed certificate is in P12 or P7B format, convert these files to a PEM (Base64 encoded) formatted file with a CRT extension.

2. Make sure that the CRT file has the full certificate chain up to a trusted root CA.

Usually you get the certificate chain from the signing CA. Sometimes it split into separate files. If the signed certificate and the trust chain are in separate files, use a text editor to combine them into one file. Make sure the server certificate is at the top of the CRT file.

3. From the Security Gateway command line, log in to the Expert mode.
4. Use the `*.crt` file to install the certificate with the `*.key` file that you generated.
   a. Run:

      ```
      cpopenssl pkcs12 -export -out <output file> -in <signed cert chain file> -inkey <private key file>
      ```

      For example:

      ```
      cpopenssl pkcs12 -export -out server1.p12 -in server1.crt -inkey server1.key
      ```

   b. Enter the certificate password when prompted.

Generating Wildcard Certificates for Hostname Translation

If you use Hostname Translation, you need a wildcard certificate. This lets clients access Web applications on sub-domains behind the Security Gateway. If Mobile Access uses a fixed domain certificate, client browsers issue certificate warnings when users try to access Web applications in a sub-domain behind the Mobile Access Security Gateway. This is because each Web application URL is translated to a different Mobile Access hostname.

Before you begin, make sure the Hostname Translation support is configured in the *"Mobile Access Applications" on page 58* and in the *"Mobile Access Applications" on page 58*.

To prepare a request a 3rd-Party wildcard server certificate:

1. In **Subject DN**, start with `CN=`*`FQDN`*.

   For example: `CN=sslvpn.example.com`
2. In **Alternate Name**, enter two DNS names: the FQDN and the wildcard.

   For example:

   ```
   sslvpn.example.com, *.sslvpn.example.com
   ```

To configure wildcard certificate generation:

1. Backup and edit the configuration file of the **csr_gen** script:
   - R75.20 and higher - **$CPDIR/conf/openssl.cnf**
   - R66.x, R71.x, R75, R75.10 - **$CVPNDIR/conf/openssl.cnf**
2. In the `[ req ]` section, uncomment the line:

   ```
   req_extensions = v3_req
   ```
3. In the `[ v3_req ]` section, add this line:

   `subjectAltName=DNS:`*`FQDN`*`,DNS:*.`*`ParentDomain`*

   For example: `subjectAltName=DNS:sslvpn.example.com,DNS:*.sslvpn.example.com`
4. Save **openssl.cnf**.

5. Run **csr_gen** and create the CSR.

   To make sure the CSR was generated properly, run:

   - R75.x - `cpopenssl req -in requestFile.csr -text`
   - earlier versions - `openssl req -in requestFile.csr -text`

6. When asked for the CommonName (CN), enter the FQDN. For example: `sslvpn.example.com`
7. Restore the **openssl.cnf** file from the backup.

Installing the Signed Certificate

To install the certificate:

1. Log in to SmartConsole.
2. From the left Navigation Toolbar, click **Gateways & Servers**.
3. Open the Identity Awareness Security Gateway object.
4. In the navigation tree, click the appropriate Software Blade page:
   - **Mobile Access** > **Portal Settings**
   - **Platform Portal**
   - **Data Loss Prevention**
   - **Identity Awareness** > **Captive Portal** > **Settings** > **Access Settings**

   In the **Certificate** section, click **Import** or **Replace**.
5. Install the Access Control Policy on the Security Gateway.

   Note - The **Repository of Certificates** on the IPsec VPN page of the Security Gateway object is only for self-signed certificates. It does not affect the certificate installed manually using this procedure.

Viewing the Certificate

To see the new certificate from a Web browser:

The Security Gateway uses the certificate when you connect with a browser to the portal. To see the certificate when you connect to the portal, click the lock icon that is next to the address bar in most browsers.

The certificate that users see depends on the actual IP address that they use to access the portal - not only the IP address configured for the portal in SmartDashboard.

To see the new certificate from SmartConsole:

From a page that contains the portal settings for that blade/feature, click **View** in the **Certificate** section.

Web Data Compression

Mobile Access can be configured to compress Web content. This can produce a much faster website for users. It also reduces bandwidth needs, and therefore, costs.

Most compression algorithms, when applied to a plain-text file, can reduce its size by 70% or more, depending on the content in the file.

Be aware that compression does increase the CPU usage of Mobile Access, which in itself does have some performance implications.

Most browsers can accept compressed data, uncompress it and display it.

If configured to compress data, Mobile Access compresses the data received from Web servers (the http or https response). If the Web browser at the endpoint compresses the http or https request, Mobile Access uncompresses it and sends it on to the server. This is illustrated in the figure below.

Mobile Access supports the gzip, deflate, and compress compression methods.

It is possible to specify the mime types that will be compressed.

Item	Description
1	Web Browser
2	Compressed Request
3	Mobile Access enabled Security Gateway
4	Uncompressed request (e.g., gunzip)
5	Web Server
6	Response
7	Compressed Response (e.g., gzip)

Configuring Data Compression

Web data compression is configured per Security Gateway in GuiDBedit Tool (see sk13009).

To configure data compression by Mobile Access:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with GuiDBedit Tool to the Management Server.
3. In the top left pane, go to **Network Objects** > **network_objects**.
4. In the top right pane click Security Gateway / Cluster object.
5. In the bottom pane, search for **web_compression** under **connectra_settings** and fill in the following parameters:

- **enable_web_compression** - Enter **true** to enable data compression and **false** to disable it.
- **compression_level** - Enter a value between 1 and 9. The higher the number, the more CPU is used. The default is 5.
- **compress_specific_mime** - Enter **true** if you want to compress specific mime types and **false** if you do not.
- **mime_types** - If you typed true for **compress_specific_mime**, enter the mime type, for example, **text/html**.

6. Save the changes in GuiDBedit Tool (**File** menu > **Save All**) and close it.
7. Connect with SmartConsole to the Management Server.
8. Install policy on the Security Gateway / Cluster object.

Using Mobile Access Clusters

A remote access enabled Security Gateway is a business critical device for an organization. A failure of a Security Gateway results in immediate loss of remote access traffic in and out of the organization. Many of these sessions may be mission critical, and losing them will result in loss of critical data.

Using ClusterXL, you can set up a Load Sharing or High Availability clustering solution that distributes network traffic among Mobile Access cluster members.

A cluster of Mobile Access Security Gateways provides:

- Transparent failover in case of cluster member failure.
- Zero downtime for mission-critical environments.
- Enhanced throughput (in Load Sharing modes).

All cluster members are aware of the sessions tracked through each of the other cluster members. The cluster members synchronize their sessions and status information across a secure synchronization network.

The Sticky Decision Function

If you are using SSL Network Extender, you must enable the Sticky Decision Function.

A connection is *sticky* when all of its packets are handled, in either direction, by a single cluster member.

The Sticky Decision Function distributes sessions from client IP addresses between the cluster members, and ensures that connections from a given IP always pass through the same member.

How Mobile Access Applications Behave on Failover

The table below summarizes the end-user experience upon failover for each Mobile Access application.

Application	Survives failover?	User experience upon failover
Web browsing through the user portal Domino Web Access Outlook Web Access File Shares	Yes	User is unaware of failover. If the failover happens while a user is clicking a link or waiting for a server response, user may be disconnected and may need to refresh the page.
Web Mail	No	If failover occurs while a user is clicking a link or waiting for a server response, user sees an error page. By clicking the link "Go to the login page" the user returns to the Inbox, and the original session is lost.
Citrix	No	User is disconnected, and the Citrix session is lost. User must actively re-establish a connection.
Endpoint Compliance Scan	Yes	Re-scan may be required if user logs out of the portal, or needs to log in again.
Secure Workspace	Yes	User is unaware of failover. However, if the failover happens while a user is clicking a link or waiting for a server response, user may be disconnected and may need to refresh the page.
Multi challenge login	No	If user is in the middle of a multi-challenge login he/she is redirected to the initial login page.
SSL Network Extender Network Mode	Yes	The user may notice the connection stalling for a few seconds, as if there was a temporary network disconnection.
SSL Network Extender Application Mode	No	SSL Network Extender remains open and in a connected state. However, connections of applications using the VPN tunnel are lost. Some applications (such as Outlook) try to reopen lost connections, while others (Telnet for example) are closed (or exit).
SSL Network Extender - Downloaded-to-Mobile Access applications	Mode dependent	Network Mode - Survives failover. Application Mode - Does not survive failover.

Troubleshooting Mobile Access

Troubleshooting Web Connectivity

Web connectivity issues can occur in Mobile Access Web Applications, while working with applications that use/require HTTP cookies. This is because some cookies usually forwarded by Microsoft Internet Explorer to a Web server are not forwarded by Mobile Access in the same scenario. To solve this, see sk31636.

Troubleshooting Outlook Web Access

Note - This section applies to Outlook Web Access-related issues occurring when working through Mobile Access without SSL Network Extender.

If you have problems with Outlook Web Access (OWA) after deploying Mobile Access:

1. Read the relevant sections in this Administration Guide. See *"Mobile Access Applications" on page 58*.
2. Go over the Troubleshooting OWA Checklist.
3. Look for a description that matches your issues in the "Common OWA problems" section.

Troubleshooting OWA Checklist

The following sections describe steps to take if you are experiencing problems using Outlook Web Access with Mobile Access.

1. Check your traffic logs for errors. The logs may help you to pinpoint the problem.
2. Reproduce the scenario without Mobile Access and ensure that the problem does not occur.
3. Verify connectivity. Make sure that:
   - The Mobile Access machine has a network route to all relevant Microsoft Exchange servers and relevant server ports are accessible, usually port 80 or 443.

     HTTP and/or HTTPS packets must be able to reach Microsoft Exchange servers.
   - Mobile Access users have a network route to the Mobile Access machine.
4. Verify that your configuration is valid. Make sure that:
   - The Outlook Web Access version is supported by Mobile Access.
   - Client-side browsers are supported by OWA and by Mobile Access.
   - OWA Services are configured to use protocols acceptable by the servers in question. For example, if an Exchange server is configured to accept HTTPS traffic only, the corresponding OWA Web application on Mobile Access must utilize HTTPS.
   - Security restrictions are disabled (see the "Troubleshooting Security Restrictions in OWA" section).
   - Users are authorized to access all necessary resources.

- OWA services are configured with correct paths, according to the specific version of the Microsoft Exchange server.

Unsupported Feature List

The following OWA features, platforms and product versions are not supported by Mobile Access:

- Outlook Web Access (OWA) 5.5.
- OWA 2000 on Microsoft Exchange 2003. (*)
- Outlook Mobile Access.

(*) These products and platforms have not been tested with Mobile Access. However, Mobile Access has been successfully integrated in such environments.

Note - According to Microsoft, only the following OWA configuration supports non-IE browsers: OWA 2000 / 2003 running on Microsoft Exchange 2003 using "Outlook Web Access Basic" scheme.

If you must use one of these features, use SSL Network Extender.

Common OWA problems

These sections describe issues related to browsing to OWA through Mobile Access.

Note - Examine your traffic logs for errors, to pinpoint the problem.

Troubleshooting Authentication with OWA

After users log in to Mobile Access, and attempt to access an OWA application, they are required by OWA to provide authentication credentials.

Outlook Web Access has two authentication schemes: the regular HTTP-based authentication (HBA), which is the default, and Form-Based authentication (FBA). In addition, Mobile Access supports single sign-on (SSO) through HBA and FBA.

HBA Problems

If an internal Web Server requests Integrated Windows Authentication (NTLM) or any other HTTP-based authentication, Mobile Access either displays a dialog box requesting login credentials, or tries to use the user's portal credentials, depending on the configuration of the Mobile Access Web application. HBA-related problems may result from the use of IIS web-based password management services.

IIS Web applications (such as Outlook Web Access) can be configured to use IIS Web-based password management services. These services make it possible for users to change their Windows NT passwords via a web server. These services use IIS HTR technology which is known to be vulnerable to attack, and can allow an attacker to run malicious code on the user system. Microsoft has long advocated that customers disable HTR on their Web servers, unless there is a business-critical need for the technology (Microsoft Security Bulletin MS02-028).

In keeping with the Microsoft recommendation, IPS protects against HTR exploits by default. If you wish to allow the use of the HTR mechanism, deactivate the "htr" worm pattern in the IPS **General HTTP Worm Catcher** protection. Install the Security policy from SmartDashboard after making these changes.

Single Sign On Problems

When troubleshooting, eliminate the possibility of Single Sign On problems by removing the OWA user credentials from the credentials list in the Mobile Access user portal.

Troubleshooting Authorization with OWA

The authorization mechanisms of Mobile Access allow administrators to grant access to various resources on a per-path, per-host and per-port basis. Mobile Access views Outlook Web Access as a Web application with special properties, connecting to a special Web server.

Authorization-related problems may result from:

- **Discrepancies in the OWA Web Application Configuration versus the setup in Microsoft Exchange server.**

  Possible discrepancies may occur in the configuration of the OWA port, protocol or paths versus the setup of the corresponding Microsoft Exchange server.

  OWA Service must be configured in accordance with the Microsoft Exchange server configuration. Otherwise, Mobile Access will not be able to authorize access to the application.

  Authorization Example Scenario

  A user launches an OWA application, gets to the Form-Based Authentication (FBA) page and authenticates using his/her credentials. Subsequently, the user gets the "Access denied" page.

  Cause: The Microsoft Exchange server side component (IIS or other) is configured to accept both HTTP and HTTPS traffic, whereas the Mobile Access OWA Web application is configured to authorize HTTP traffic only.

  Explanation: The Form Based Authentication setting on the Microsoft Exchange server requires clients to use SSL, which means that some server-side component (be it IIS or other) must also accept SSL traffic. The following message is displayed to the Microsoft Exchange administrator upon FBA configuration:

  Forms Based Authentication requires clients to use a SSL connection. If SSL encryption is not off-loaded to another source, complete the following steps:

  - Configure SSL
  - Restart the IIS service

  This means that IIS is likely to be configured to work over SSL. However, in complex cases, such as SSL encryption being off-loaded to another source, and the IIS server itself allowing HTTP traffic, the Mobile Accessadministrator may not be aware of the need to authorize HTTPS traffic. As a result, discrepancies may occur.

  Note - When FBA is in use, always set the OWA Web application to allow HTTPS traffic.

  Solution - Make sure that the OWA application configuration on the Mobile Access blade matches the configuration requirements of the Microsoft Exchange server.

- **Alternative References to OWA.**

Some companies access their OWA applications via intermediary websites. These intermediary websites may reference the OWA server by its IP(s) or host name(s). If, when defining access to the OWA server, the intermediary website is ignored, it can cause an authorization failure in Mobile Access.

User experiences may vary. In some cases the problem may result in a run-time JavaScript error or OWA becomes unresponsive (see Insufficient User Permissions for more information).

To troubleshoot such problems, test OWA operations without using any mediator (such as proxies, Security Gateways, or websites).

User experiences may vary widely. However, most authorization failures will result in the following error message: Error: Access denied. The destination of your request has not been configured , or you do not have authorization access to it. (401).

Troubleshooting Security Restrictions in OWA

Mobile Access utilizes many built-in security features that screen inner networks from external threats. In addition, the Mobile Access endpoint security features protect the endpoint devices.

Occasionally, protection mechanisms may interfere with legitimate user activities. To eliminate this possibility, switch off all Web Intelligence protections during troubleshooting and the install the security policy.

User experiences may vary widely so they are not detailed here. Use the following steps to troubleshoot issues with security restrictions.

1. Check the traffic log to see if any relevant URL was blocked due to security restrictions.
2. To reduce the number of false-positives:
   - In SmartDashboard, in the IPS tab, go to **Protections > By Protocol > Integrated > Web Intelligence** and turn all settings of Application Layer Protection Level to *Low*.
   - In the **ASCII Only Request** protection, clear **Block non ASCII characters in form fields**.
   - Install the Security policy from SmartDashboard.
3. If Step 2 did not solve the problem, try the following:
   - Modify the **Endpoint Compliance** page of the Mobile Access Web Application to **Allow caching of all content**.
   - In SmartDashboard, in the IPS tab, go to **Web Intelligence** and
     - In the **HTTP Protocol Inspection > HTTP Methods** protection, clear **Block standard Unsafe HTTP methods**.
     - In the **Malicious Code > General HTTP Worm Catcher** protection, disable the "htr" worm pattern.
   - Install the Security Policy from the administration portal.
4. If Step 3 did not solve the problem, try the following steps in order:
   a. Turn off all Web Intelligence protections.
   b. Turn off all IPS protections.
   c. Install the Security policy from SmartDashboard.

Troubleshooting Performance Issues in OWA

Performance issues may occur with OWA for the following reasons:

- **Logging Issues**

  Generations of Debug and Trace logs (that are accessed via the console), and the storage of these log records when they grow too big, may considerably degrade the performance of the machine.

  Note - Traffic and event logs (that are accessible using the SmartConsole clients) do not degrade the performance of Mobile Access.

  Note - To get rid of these logs, turn off Debug logs, Trace logs, and purge the existing Debug logs and Trace logs.

  To turn off Debug logs and Trace logs:

  1. Modify `$CVPNDIR/conf/httpd.conf as follows:`
     a. Set the `LogLevel` parameter to `emerg`.
     b. Make sure the following lines are commented. Commented lines are preceded by `#`:

     ```
     #CvpnTraceLogMaxByte 10000000
     #CvpnWsDebugSubjects ...
     ```

  2. Run the `cvpnrestart` command
  3. If you have a Mobile Access cluster, repeat on all cluster members.

  To purge existing Debug logs and Trace logs:

  1. Empty or delete all `httpd.log*` files located in `$CVPNDIR/log` directory
  2. Empty or delete the `mod_ws.log` file located in `$CVPNDIR/log` directory
  3. Empty or delete the `mod_ws_boa.log` file located in `$CVPNDIR/log` directory
  4. Delete all files located under `$CVPNDIR/log/trace_log` directory
  5. If you have a Mobile Access cluster, repeat on all cluster members.

- **OWA over SSL or OWA with Form Based Authentication Enabled**

  The Outlook Web Access service can be configured to work over SSL inside secure networks. This option is normally used if the Microsoft Exchange server is configured to accept SSL-encrypted traffic (HTTPS).

  This is the case if OWA is configured to use Form Based Authentication (FBA). Upon enabling FBA, the Exchange administrator is prompted by the IIS to change the Web application to work over SSL.

  Configuring OWA to use SSL inside secure networks may cause degradation in performance and browsing experience. This is because, in such a topology, the amount of SSL negotiations grows considerably. SSL negotiations are very CPU-intensive, and therefore may cause performance degradation.

To solve this problem:

- Change the topology to use HTTP instead of HTTPS inside secure networks.
- Use a stronger machine.

Slow Network Problems

Introducing Mobile Access into an OWA topology allows users to connect to enterprise resources from remote locations.

Users connecting from remote locations may be subject to temporary or permanent network problems. The rate of packet loss in those networks can vary widely, as can the throughput.

Latency Overhead Problems

Mobile Access inspects and modifies all HTTP traffic passing through the Security Gateway. It takes time to process each particular packet of information.

There is therefore a difference in latency between connections passing through Mobile Access and those that do not. The overhead in absolute elapsed time is proportional to the amount of data passed through the network.

Latency and therefore performance problems when working through Mobile Access may be felt in particular by users with large numbers of emails, calendar events, task items and the like.

To solve this problem:

Minimize the latency overhead by increasing the performance of Mobile Access. You can do this by using a stronger machine.

SSL Time-out Problems

SSL time-out problems can occur with Internet Explorer while working through Mobile Access. They can cause slowness and even temporary or permanent unresponsiveness of the browser.

To solve this problem:

- If feasible, upgrade Internet Explorer by following the instructions in the relevant Microsoft articles below.
- Alternatively, configure Mobile Access, so that it does not use keep-alive packets when communicating with those hosts or paths.

To configure Mobile Access to work without keep-alive packets to specific locations:

1. Supply additional `LocationMatch` directives for each host used by the Web Application in question. All directives go in the `$CVPNDIR/conf/includes/Main.virtualhost.conf` file, in the `VirtualHost` section.

   For more information, see: http://httpd.apache.org/docs/2.0/mod/core.html#locationmatch

   ```
   <LocationMatch "CVPNHost=<IP or DNS namedelimited by dots>">
     SetEnv nokeepalive
   </LocationMatch>
   ```

   For example:

   ```
    <LocationMatch "CVPNHost=208\.77\.188\.166">
     SetEnv nokeepalive
   </LocationMatch>
   ........
   <LocationMatch "CVPNHost=myhost\.example\.com|CVPNHost=myhost">
     SetEnv nokeepalive
   </LocationMatch>
   ```

2. Run `cpstop` and then `cpstart`.
3. Repeat for each Mobile Access cluster member.

- Authorization Problems

Saving File Attachments with OWA

When trying to save a file attachment with Outlook Web Access (OWA), Mobile Access adds the full path to the file name. For example, the file name appears something like:

```
Bulletin1H.PDF,CVPNHost=192.168.201.6,CVPNProtocol=http,CVPNOrg=full,CVPNExtension=.PDF
```

To solve this, configure the Web Application to use Path Translation or Hostname Translation (see *"Mobile Access Applications" on page 58*).

Troubleshooting Citrix

Note - This section refers to Citrix-related issues occurring when working through Mobile Access without the use of SSL Network Extender.

If you have issues with Citrix after the deployment of Mobile Access, see *"Mobile Access Applications" on page 58* > section about Citrix Services. Then try the troubleshooting checklist.

Troubleshooting Citrix Checklist

Follow the steps below to pinpoint the issue that may be causing trouble with Citrix.

Connectivity Issues

1. Make sure that Mobile Access has a network route to all Web Interface servers intended to be used and relevant server ports are accessible. Usually ports 80 or 443.

   HTTP and/or HTTPS protocols must be traversible towards Web Interface servers.

2. Make sure that Mobile Access has a network route to all Presentation servers intended to be used and relevant server ports are accessible. Usually ports 1494 or 2598.

   ICA protocol must be traversible towards Presentation servers.

3. Make sure that Mobile Access machine has a network route to all STA servers intended to be used, if any, and port 80 on STA servers is accessible, and HTTP protocol is traversible.

4. Make sure that Mobile Access users have a network route to the Mobile Access machine.

Configuration Issues

1. Make sure that Citrix servers and clients are of those versions supported by Mobile Access.

2. Make sure that all necessary STA servers are configured with corresponding Citrix Services on Mobile Access.

3. Make sure that the Mobile Access server certificate:

   - is issued to the Fully Qualified Domain Name (such as www.example.com) of the Security Gateway
   - is properly configured
   - is trusted by the client-side

Troubleshooting File Shares

- Mobile Access gives an informative error message when an attempt to access a file share fails. However, if a user tries to access a share that does not exist on the file server, Mobile Access cannot always distinguish this error from an Access Denied error. In this case the user may be presented with the credentials input form again, or get an Access Denied error.
- The Windows Explorer viewer can normally be used for browsing website. However, the Mobile Access SSL Network Extender window may not load properly when using it, and the user may be presented with the Mobile Access login page. It is recommended to use the Web-based viewer instead.
- When browsing file shares through the Mobile Access user portal, users can open most files by clicking them. However, some files, for example .wmv extension files, cannot be opened that way, and must be downloaded to the local desktop and opened from there. When using the Mobile Access Web-based file viewer, download the file by right-clicking on the file and choosing "Save Target As...". When using the Windows File Explorer viewer, download the file by copying or drag-and-dropping it to the local desktop.

- When accessing files via Mobile Access, the client application used to view a file depends on the file type. Some file types (such as jpg files) can be configured to be opened by a Web browser. In some client configurations, the result of opening such a file may show the Mobile Access login page instead of the requested file. If this happens, verify that the client uses the latest recommended browser version including all patches and fixes. Specifically, install Internet Explorer patch Q823353 on the endpoint.
- When using Mobile Access file shares with VSX, the DNS resolving of the hostname might not work correctly with file shares. Make sure that the `/etc/resolve.conf` file is configured correctly or change the value of `vsxMountWithIPAddress` in the `$CVPNDIR/conf/cvpnd.C` from `false` to `true`. The file share will use the host ip for the mount instead of the hostname.
- If you have functionality or UI issues with File Sharing, or when using File Sharing with an unsupported browser, you can switch to the R77 File Sharing UI to resolve issues.

  To switch between the R77 and R80.x File Sharing UI:

  1. Backup the file: `$CVPNDIR/htdocs/HFS/.include/conf/properties.ini`
  2. Edit the file. Change the value of this line: `use.old.design=`

     Use these values:

     - true - to enable R77 File Sharing UI
     - false - to enable R80.x File Sharing UI
  3. Save the changes.

Troubleshooting Push Notifications

Scenario: Push notifications are configured but users do not see push notification in Capsule Workspace.

Use the **Push Notification Status Utility** and **Monitoring Push Notification Usage** to troubleshoot Push Notifications with Mobile Access (see *"Mobile Access for Smartphones and Tablets" on page 131*) .

Also see sk109039.

Mobile Access FAQ

Question	See:
Which browsers and operating systems does Mobile Access support?	*R80.40 Release Notes*
Can you store credentials?	*"Single Sign On" on page 84*
How to configure Multi-factor authentication?	*"User Authentication in Mobile Access" on page 158*
How to configure different authentication for different Security Gateways?	*"User Authentication in Mobile Access" on page 158*
How to configure a proxy for Mobile Access?	■ For an Exchange Server - *"Exchange Mail Applications for Smartphones and Tablets" on page 126* ■ For DynamicID with SMS - *"User Authentication in Mobile Access" on page 158* ■ For a web application - sk34810
How to allow access to internal resources without the Mobile Access Portal?	*"Reverse Proxy" on page 224*
Is WebSocket supported for Web applications?	*"Mobile Access Applications" on page 58*
What is SNX?	*"Native Applications for Client-Based Access" on page 101*

Command Line Reference

See the *R80.40 CLI Reference Guide*.

Below is a limited list of applicable commands.

Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description
TAB	Shows the available nested subcommands: `main command` `→ nested subcommand 1` `→ → nested subsubcommand 1-1` `→ → nested subsubcommand 1-2` `→ nested subcommand 2` Example: `cpwd_admin` `config` `-a <options>` `-d <options>` `-p` `-r` `del <options>` Meaning, you can run only **one** of these commands: ■ This command: `cpwd_admin config -a <options>` ■ Or this command: `cpwd_admin config -d <options>` ■ Or this command: `cpwd_admin config -p` ■ Or this command: `cpwd_admin config -r` ■ Or this command: `cpwd_admin del <options>`
Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

admin_wizard

Description

Runs the administration client wizard to test connectivity to websites, Exchange server services, or LDAP server.

Note - This wizard saves its log messages in these files:

- `$CVPNDIR/log/AdminWizardLog.elg`
- `$CVPNDIR/log/wizard.elg`
- `$CVPNDIR/log/wizardDns`
- `$CVPNDIR/log/wizardEstimation`
- `$CVPNDIR/log/wizardLdap`
- `$CVPNDIR/log/wizardProxy`

Syntax

```
admin_wizard
      cancel
      estimation
      exchange_wizard <Exchange Server Address> <User Name> <Password>
[<Options>]
      ldap <LDAP server>
      wizard <Web Site Address>
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help.
`cancel`	Kills the administration client wizard that already runs.
`estimation`	Estimates how many seconds the wizard will run.
`exchange_wizard <Exchange Server Address> <User Name> <Password> [<Options>]`	Tests the response from an Exchange server: ■ Finds the address protocol (HTTP or HTTPS) and authentication method (Basic or NTLM) of the Exchange server services. ■ Checks accessibility of Mobile Access ActiveSync and EWS services for users. ■ For Web command, checks access to the URL. ■ For OWA command, returns the URL to the outlook web access.

Parameter	Description
	The parameters are: ■ *<Exchange Server Address>* - Specifies the Exchange server by its IP address or hostname. ■ *<User Name>* - Specifies the user name on the Exchange Server. ■ *<Password>* - Specifies the password on the Exchange Server. ■ *<Options>* - Specifies the test options.

Parameter	Description
	The available test options are: ■ `-t {as | ews | owa | all}` - Specifies the services to test on the Exchange server: **Note** - To specify more than one service, separate them with a comma. For example: `as,ews` • `all` - Tests all of the services (default) • `as` - Tests ActiveSync • `ews` -Tests Exchange Web Services • `owa` - Searches for the Outlook Web Application (OWA) address of the Exchange server ■ `-d <DNS Servers>` - Specifies the DNS servers. ■ `-x <Proxy Servers>` - Specifies the Proxy servers. ■ `-c <Username>:<Password>` - Specifies the user name and password for Proxy server authentication. ■ `-n` - Allows only NTLM authentication instead of Basic and NTLM. ■ `-m <Domain Name>` - Specifies the user domain name. ■ `-s <ActiveSync Path>` - Tests a specified ActiveSync service path (Default: `/Microsoft-Server-ActiveSync`). ■ `-e <EWS Path>` - Tests a specified Exchange Web Services service path (Default: `/EWS/Exchange.asmx`). ■ `-f <File Name>` - Writes the test results to the specified file ■ `-r` - Sends a request with the configured Proxy, DNS, HTTP protocol, and authentication method. • If you also specify the "`-n`" option, then the NTLM authentication method is used. • If you do not specify the "`-n`" option, then only the Basic authentication method is used. ■ `-v` - Makes the HTTP requests verbose. The verbose result files are saved in the `$CVPNDIR/log/trace_log/` directory. ■ `-p` - Validates the SSL certificate of the web server.
`ldap <LDAP server>`	Tests connectivity to the specified LDAP server. You can specify the LDAP server by its IP address or hostname.
`wizard <Web Site Address>`	Tests connectivity to the specified URL.

Example 1 - Check URL accessibility of 'www.checkpoint.com'

```
admin_wizard wizard www.checkpoint.com
```

Example 2 - Check accessibility to the LDAP server 192.168.0.55

```
admin_wizard ldap 192.168.0.55
```

Example 3 - Check accessibility for username 'user1' to ActiveSync and EWS on the Exchange server 'exchange.example.com'

```
admin_wizard exchange_wizard exchange.example.com username user1 -t as,ews
```

cvpnd_admin

Description

Changes the behavior of the Mobile Access **cvpnd** process.

Syntax

```
cvpnd_admin
      appMonitor status
      clear_kernel_tables
      clear_portal_cache
      debug <options>
      ics_update
      isEnabled
      license <options>
      policy [{graceful | hard}]
      revoke <Certificate Serial Number>
```

Parameters

Parameter	Description
`appMonitor <options>`	Controls the Application Monitor. The Application Monitor is a software component that monitors internal servers to track their up time. If problems are found, a system alert log is created. The available <*options*> are: ■ `restart` - Restarts the Application Monitor. ■ `start` - Start the Application Monitor. ■ `status` - Shows the status of the Application Monitor feature, the applications monitored by the Application Monitor and their status. ■ `stop` - Stops the Application Monitor.
`clear_kernel_tables`	Clears all Mobile Access kernel tables.
`clear_portal_cache`	Clears the cache for the applications presented in the Mobile Access Portal for all open sessions.
`debug set TDERROR_ALL_ALL=5`	Enables all `cvpnd debug` output for the running **cvpnd** process. The output is in the `$CVPNDIR/log/cvpnd.elg` file.  **Note** - When you enable all debug topics, it might impact the performance. Debug topics are provided by *Check Point Support*.
`debug off`	Disables all `cvpnd debug` output.

Parameter	Description
`debug trace on` `debug trace users=<Username>`	The `TraceLogger` feature generates full captures of incoming and outgoing authenticated Mobile Access traffic. The output is saved in the `$CVPNDIR/log/trace_log/` directory. ■ `debug trace on` - Enables the `TraceLogger` feature for all users. ■ `debug trace users=<Username>` - Enables the `TraceLogger` feature for a specified username **Important:** ■ The `TraceLogger` feature has a major effect on performance, because all traffic is saved as files. ■ The `TraceLogger` feature uses a lot of disk space, because all traffic is saved as files. After a maximum number of files is saved, the oldest files are removed from the disk, which also has a performance cost. ■ The `TraceLogger` feature creates a security concern: end-user passwords that are sent to internal resources might appear in the capture files.
`ics_update`	Updates the Mobile Access services after you published a new ICS update.
`isEnabled`	Checks if Mobile Access is enabled by policy.
`license <options>`	Shows Mobile Access license count and status: ■ `all` - Shows information about the MOB and MOBMAIL licenses. ■ `mob` - Shows information about the MOB license. ■ `mobmail` - Shows information about the MOBMAIL license.
`policy [{graceful | hard}]`	Updates the Mobile Access services according to the current policy: ■ `policy` - For Apache services, each `httpd` process waits until its current request is finished, then exits. ■ `policy graceful` - For Apache services, each `httpd` process waits until its current request is finished, then exits. ■ `policy hard` - For Apache services, all `httpd` processes exit immediately, terminating all current `http` requests.
`revoke <Certificate Serial Number>`	Notifies about revocation of a certificate with a given serial number.

cvpnd_settings

Description

Changes a Mobile Access Gateway local configuration file `$CVPNDIR/conf/cvpnd.C`.

The `cvpnd_settings` commands allow to get attribute values or set them in order to configure the **cvpnd** process.

Important - Changes made by with the `cvpnd_settings` command are **not** saved during the Mobile Access Gateway upgrade. Keep a backup of your `$CVPNDIR/conf/cvpnd.C` file after you make manual changes.

Warning - The **cvpnd** process may not start, if you make a mistake in the syntax - attribute names or their values.

General Syntax

```
cvpnd_settings [<Configuration File>] {get | set | add | listAdd |
listRemove | internal} <Attribute-Name> [<Attribute-Value>]
```

Syntax for DynamicID Resend

```
cvpnd_settings [<Configuration File>] {set | get} smsMaxResendRetries
[<Number>]
```

Syntax for Kerberos Authentication

```
cvpnd_settings [<Configuration File>] {set | get} useKerberos {true |
false}
```

```
cvpnd_settings [<Configuration File>] {listAdd | listRemove} kerberosRealms
[<Your AD Name>]
```

Parameters

Run this command to see the full explanation of the parameters: `cvpnd_settings -h`

Parameter	Description
`-h`	Shows built-in help with full explanation of the parameters.
<Configuration File>	Specifies the path and the name of configuration file to change.
`get`	Gets the value of an existing attribute, or values of a list.

Parameter	Description
`set`	Sets the value of an attribute. If the specified attribute does not exist in the configuration file, then the command adds it.
`add`	Adds a new attribute. If the specified attribute already exists in the configuration file, then the command does not change it.
`listAdd`	Adds the specified attribute to a list.
`listRemove`	Removes the specified attribute from a list.
`internal`	Specifies that the command must change the `$CVPNDIR/conf/cvpnd_internal_settings.C` file instead of the `$CVPNDIR/conf/cvpnd.C` file.
<Attribute-Name>	Specifies the attribute name.
<Attribute-Value>	Specifies the attribute value.
<Number>	Specifies the number of SMS resend attempts.
<Your AD Name>	Specifies the Active Directory name.

Examples 1 - Set the value of the attribute 'myFlag' to 1

```
cvpnd_settings set myFlag 1
```

Examples 2 - See the current value of the attribute 'myFlag'

```
cvpnd_settings get myFlag
```

Examples 3 - Empty the value of the attribute 'myFlag', or create a new attribute/list 'myFlag'

```
cvpnd_settings set myFlag
```

Examples 4 - Add the attribute 'myFlag' with the value 'a.example.com' to a list

```
cvpnd_settings listAdd myFlag a.example.com
```

cvpn_ver

Description

Shows the version of the Mobile Access Software Blade.

Best Practice - Run the "`fw ver -k`" command to get all version details.

Syntax

```
cvpn_ver
```

Example

```
[Expert@MyGW:0]# cvpn_ver
This is Check Point Mobile Access R80.40 - Build 123
[Expert@MyGW:0]#
```

cvpnrestart

Description

Restarts all Mobile Access blade services.

Warning - While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

Syntax

```
cvpnrestart [--with-pinger]
```

Parameters

Parameter	Description
`--with-pinger`	Restarts the **Pinger** service, responsible for ActiveSync and Outlook Web Access push mail notifications.

cvpnstart

Description

Starts all Mobile Access blade services, after you stopped them with the *"cvpnstop" on page 262* command.

Syntax

```
cvpnstart
```

cvpnstop

Description

Stops all Mobile Access blade services.

Warning - While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

Syntax

```
cvpnstop
```

deleteUserSettings

Description

Deletes all persistent settings (favorites, cookies, credentials) of one or more end-users.

Syntax

```
deleteUserSettings [-s] <Username1> [<Username2> ...]
```

Parameters

Parameter	Description
`-s`	Runs in silent mode with no output to the end-user's screen.
<Username>	Specifies the user name, whose settings to delete.  **Notes:** ■ When you refer to an internal user, use its username. ■ When you refer to an LDAP user, use the full DN according to your LDAP settings.

Example 1 - Delete an internal user named 'user1

```
deleteUserSettings [-s] user1
```

Example 2 - Delete an LDAP user named 'user1', whose DN is 'CN=user1,OU=users,DC=example,DC=com':

```
deleteUserSettings [-s] CN=user1,OU=users,DC=example,DC=com
```

fwpush

Description

Sends command interrupts to the **fwpushd** process on the Mobile Access Gateway.

Note - Users get the push notifications only while they are logged in.

Syntax

```
fwpush
      debug <options>
      del <options>
      info
      print
      send <options>
      unsub <options>
```

Parameters

Parameter	Description
`debug {off | on | reset | set all all | stat}`	Controls the debug of the Mobile Access Push Notifications daemon. For more information, see sk109039.
`del {-token <Token> | -uid <User-UID>}`	Deletes a specified token, or all tokens for a specified user. The available options are: ■ Delete the specified token for all users: `fwpush del -token <Token>` ■ Delete all tokens for a specified user: `fwpush del -uid <User-UID>`

Parameter	Description
`info`	Gets data on notifications in the push queue: ■ Number of items in queues ■ Number of seconds the oldest item is in the queue ■ Number of seconds the newest item is in the queue ■ Number of seconds a batch waits in the queue ■ Number of seconds to the sending of the next batch ■ Number of batch errors and authentication request timeouts
`print`	Shows the push notifications queue and the pending batches.
`send -token <Token> -os {iPhone | Android} -msg "<Notification Message>"` `send {-user <Username> | -uid <User-UID>} -msg "<Notification Message>"`	Sends an on-demand push notification message from a command line.  **Important** - Before you use the "`fwpush send`" command, make sure the user is: (A) registered on the Exchange Server, (B) connected.
`unsub {<Token> | -user <Username> | -uid <User-UID> | -all}`	Unsubscribes a user from push notifications. The available options are: ■ Unsubscribe all users from the specified token: `fwpush unsub <Token>` ■ Unsubscribe the specified user from all tokens: `fwpush unsub -user <Username>` or `fwpush unsub -uid <User-UID>` ■ Unsubscribe all users from all tokens: `fwpush unsub -all`

Viewing the details of connected users

```
UserSettingsUtil show_exchange_registered_users
```

Example output:

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=USA,DC=AD,DC=CHECKPOINT,DC=COM User Settings id:
c4b6c6fbb0c4xxxxxxxx265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023ebxxxxxxxxxca22ea788cfb3cxxxxxxxxxx Device id:
46c5XXXXcc1d10b4e18cf5a1xxxxxxxx
[Expert@MyGW:0]#
```

Notes:

- To use the "*<Token>*" parameter in the "`fwpush`" commands, use the value of the **Push Token** attribute.
  In the above example:
  `xxxxxxxxxxxxx65b48e424023ebxxxxxxxxxca22ea788cfb3cxxxxxxxxxx`
- To use the "*<Username>*" parameter in the "`fwpush`" commands, use the value of the **CN** attribute.
  In the above example: `JohnD`
- To use the "*<User-UID>*" parameter in the "`fwpush`" commands, use the value of the **User Settings id** attribute.
  In the above example: `c4b6c6fbb0c4xxxxxxxx265e93e0e372`

Example

```
[Expert@MyGW:0]# fwpush send -uid JohnD -msg "Hello - push"
```

ics_updates_script

Description

Manually starts an Endpoint Security on Demand (ESOD) update on the Mobile Access Gateway.

For more information, see the contents of the `$CVPNDIR/bin/ics_updates_script` file.

Syntax

```
$CVPNDIR/bin/ics_updates_script <Path to Local ICS Updates Package>
```

Parameters

Parameter	Description
<Path to Local ICS Updates Package>	Specifies the full path to the local ICS Updates package. Do **not** specify the name of the ICS Updates package.

Notes

- Usually, it is not necessary to run this command, and you start the ESOD updates from SmartConsole:
  1. Connect with SmartConsole to the Management Server.
  2. From the left navigation panel, click **Manage & Settings**.
  3. In the Mobile Access section, click **Configure in SmartDashboard**.

     The SmartDashboard opens on the Mobile Access tab.
  4. From the left tree, click Endpoint Security on Demand > **Endpoint Compliance Updates**.
  5. Click **Update Database Now**.
  6. Enter the applicable User Center credentials.
  7. Click **Next**.
  8. Select the applicable Mobile Access Gateways.
  9. Click **Finish**.
  10. Close the SmartDashboard.
- Make sure to run only one instance of this command at a time.

listusers

Description

Shows a list of end-users connected to the Mobile Access Gateway, along with their source IP addresses.

Syntax

```
listusers
```

Example

```
[Expert@MyGW:0]# listusers
------------------------------
UserName    | IP
------------------------------
Tom , 192.168.0.51
John , 192.168.0.130
Jane , 192.168.0.7
[Expert@MyGW:0]#
```

rehash_ca_bundle

Description

Imports all of the Certificate Authority (CA) files from the `$CVPNDIR/var/ssl/ca-bundle/` directory into the Mobile Access trusted CA bundle.

The trusted CA bundle is used when the Mobile Access Gateway accesses an internal server (such as OWA) through HTTPS.

If the SSL server certificate of the internal server is not trusted by the Mobile Access Gateway, the Mobile Access Gateway responds based on the settings for the Internal Web Server Verification feature. The default setting is **Monitor**.

To accept certificates from a specified server, add its server certificate CA to the CA bundle.

Syntax

```
rehash_ca_bundle
```

Example

```
[Expert@MyGW:0]# rehash_ca_bundle
Doing /opt/CPcvpn-R80.40/var/ssl/ca-bundle/
AC_Ra__z_Certic__mara_S.A..pem => 6f2c1157.0
AOL_Time_Warner_Root_Certification_Authority_1.pem => ed9bb25c.0
... ... ...
beTRUSTed_Root_CA_-_RSA_Implementation.pem => 16b3fe3c.0
thawte_Primary_Root_CA.pem => 2e4eed3c.0
[Expert@MyGW:0]#
```

UserSettingsUtil

Description

Shows details of users connected to the Mobile Access Gateway.

Syntax

```
UserSettingsUtil show_exchange_registered_users [<Username>]
```

Parameters

Parameter	Description
<Username>	Specifies the user name. **Notes:** ■ When you refer to an internal user, use its username. ■ When you refer to an LDAP user, use the full DN according to your LDAP settings.

Example 1 - To show all users

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=USA,DC=AD,DC=CHECKPOINT,DC=COM User Settings id:
c4b6c6fbb0c4xxxxxxxx265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxxx Device id:
46c5XXXXcc1d10b4e18cf5a1xxxxxxxx
[Expert@MyGW:0]#
```

Example 2 - To show an internal user named 'user1'

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users user1
```

Example 3 - To show an LDAP user named 'user1', whose DN is 'CN=user1,OU=users,DC=example,DC=com'

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users CN=user1,OU=users,DC=example,DC=com
```

Check Point
SOFTWARE TECHNOLOGIES LTD.

28 December 2021

QUANTUM SECURITY MANAGEMENT

R81

Administration Guide

STEP UP TO
5TH GENERATION
CYBER SECURITY

Check Point Copyright Notice

Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R81
For more about this release, see the R81 home page.

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
28 December 2021	Updated *"High Availability Troubleshooting" on page 347*.
22 December 2021	Updated: ■ *"The Columns of the Access Control Rule Base" on page 184* ■ *"Object Categories" on page 159* ■ Updated values of IKE Certificate Validity Period in *"CA Procedures" on page 359* ■ Updated *"Network Security for IoT Devices" on page 337*
27 November 2021	Updated: ■ *"Configuring a Security Gateway to Access the Management Server or Log Server at its NATed IP Address" on page 139*
01 November 2021	Updated: ■ *"Creating a New Security Gateway" on page 126*
28 October 2021	Added notes in: ■ *"Central Deployment of Hotfixes and Version Upgrades" on page 140* ■ *"Network Security for IoT Devices" on page 337*
06 October 2021	Updated: ■ *"Working with Policy Packages" on page 176* ■ *"Database Revisions" on page 327* ■ *"SmartTasks" on page 332*
05 September 2021	Updated: ■ *"Viewing Licenses in SmartConsole" on page 135*
13 August 2021	Updated: ■ *"Secure Internal Communication (SIC)" on page 129* ■ *"Creating Application Control and URL Filtering Rules" on page 202* ■ *"Best Practices for Access Control Rules" on page 228* ■ *"Database Revisions" on page 327*
08 July 2021	Updated: ■ *"Central Deployment of Hotfixes and Version Upgrades" on page 140*
09 May 2021	Added: ■ *"Configuring Implied Rules or Kernel Tables for Security Gateways" on page 147*

Date	Description
27 April 2021	Updated: ■ *"Managing Server and Gateway Licenses" on page 134* ■ *"Network Security for IoT Devices" on page 337*
17 April 2021	Updated: ■ *"migrate" on page 623* ■ *"migrate_server" on page 627*
28 January 2021	Added: ■ *"Configuring a Security Gateway to Access the Management Server or Log Server at its NATed IP Address" on page 139*
16 November 2021	Updated: ■ *"Account Units" on page 92*
03 November 2020	First release of this document

Table of Contents

Glossary

A

Administrator
A user with permissions to manage Check Point security products and the network environment.

API
In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components.

Appliance
A physical computer manufactured and distributed by Check Point.

B

Bond
A virtual interface that contains (enslaves) two or more physical interfaces for redundancy and load sharing. The physical interfaces share one IP address and one MAC address. See "Link Aggregation".

Bonding
See "Link Aggregation".

Bridge Mode
A Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

CA
Certificate Authority. Issues certificates to gateways, users, or computers, to identify itself to connecting entities with Distinguished Name, public key, and sometimes IP address. After certificate validation, entities can send encrypted data using the public keys in the certificates.

Certificate
An electronic document that uses a digital signature to bind a cryptographic public key to a specific identity. The identity can be an individual, organization, or software entity. The certificate is used to authenticate one identity to another.

CGNAT
Carrier Grade NAT. Extending the traditional Hide NAT solution, CGNAT uses improved port allocation techniques and a more efficient method for logging. A CGNAT rule defines a range of original source IP addresses and a range of translated IP addresses. Each IP address in the original range is automatically allocated a range of translated source ports, based on the number of original IP addresses and the size of the translated range. CGNAT port allocation is Stateless and is performed during policy installation. See sk120296.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
A Security Gateway that is part of a cluster.

CoreXL
A performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
Also CoreXL FW Instance. On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

D

DAIP Gateway
A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the IP address of the external interface is assigned dynamically by the ISP.

Data Type
A classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

Database
The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

Distributed Deployment
The Check Point Security Gateway and Security Management Server products are deployed on different computers.

Domain
A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

Domain Log Server
A Log Server for a specified Domain, as part of a Multi-Domain Log Server. It stores and processes logs from Security Gateways that are managed by the corresponding Domain Management Server. Acronym: DLS.

E

Expert Mode
The name of the full command line shell that gives full system root permissions in the Check Point Gaia operating system.

External Network
Computers and networks that are outside of the protected network.

External Users
Users defined on external servers. External users are not defined in the Security Management Server database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

F

Firewall
The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restrictive shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for Check Point Gaia operating system.

H

Hotfix
A piece of software installed on top of the current software in order to fix some wrong or undesired behavior.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Inline Layer
Set of rules used in another rule in Security Policy.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPv4
Internet Protocol Version 4 (see RFC 791). A 32-bit number - 4 sets of numbers, each set can be from 0 - 255. For example, 192.168.2.1.

IPv6
Internet Protocol Version 6 (see RFC 2460 and RFC 3513). 128-bit number - 8 sets of hexadecimal numbers, each set can be from 0 - ffff. For example, FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF.

L

Link Aggregation
Technology that joins (aggregates) multiple physical interfaces together into one virtual interface, known as a bond interface. Also known as Interface Bonding, or Interface Teaming. This increases throughput beyond what a single connection could sustain, and to provides redundancy in case one of the links should fail.

Log
A record of an action that is done by a Software Blade.

Log Server
A dedicated Check Point computer that runs Check Point software to store and process logs in Security Management Server or Multi-Domain Security Management environment.

M

Management High Availability
Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

Management Interface
Interface on Gaia computer, through which users connect to Portal or CLI. Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member.

Management Server
A Check Point Security Management Server or a Multi-Domain Server.

Multi-Domain Log Server
A computer that runs Check Point software to store and process logs in Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Security Management
A centralized management solution for large-scale, distributed environments with many different Domain networks.

Multi-Domain Server
A computer that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Acronym: MDS.

N

Network Object
Logical representation of every part of corporate topology (physical machine, software component, IP Address range, service, and so on).

O

Open Server
A physical computer manufactured and distributed by a company, other than Check Point.

P

Permission Profile
A predefined group of SmartConsole access permissions assigned to Domains and administrators. With this feature you can configure complex permissions for many administrators with one definition.

Policy Layer
A layer (set of rules) in a Security Policy.

Policy Package
A collection of different types of Security Policies, such as Access Control, Threat Prevention, QoS, and Desktop Security. After installation, Security Gateways enforce all Policies in the Policy Package.

R

Rule
A set of traffic parameters and other conditions in a Rule Base that cause specified actions to be taken for a communication session.

Rule Base
Also Rulebase. All rules configured in a given Security Policy.

S

SecureXL
Check Point product that accelerates IPv4 and IPv6 traffic. Installed on Security Gateways for significant performance improvements.

Security Gateway
A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

Security Management Server
A computer that runs Check Point software to manage the objects and policies in Check Point environment.

Security Policy
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Single Sign-On
A property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. Acronym: SSO.

SmartConsole
A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

SmartDashboard
A legacy Check Point GUI client used to create and manage the security settings in R77.30 and lower versions.

SmartUpdate
A legacy Check Point GUI client used to manage licenses and contracts.

Software Blade
A software blade is a security solution based on specific business needs. Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

SSO
See "Single Sign-On".

Standalone
A Check Point computer, on which both the Security Gateway and Security Management Server products are installed and configured.

T

Traffic
Flow of data between network devices.

U

User Database
Check Point internal database that contains all users defined and managed in SmartConsole.

User Groups
Named groups of users with related responsibilities.

User Template
Property set that defines a type of user on which a security policy will be enforced.

Users
Personnel authorized to use network resources and applications.

V

VLAN
Virtual Local Area Network. Open servers or appliances connected to a virtual network, which are not physically connected to the same network.

VLAN Trunk
A connection between two switches that contains multiple VLANs.

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

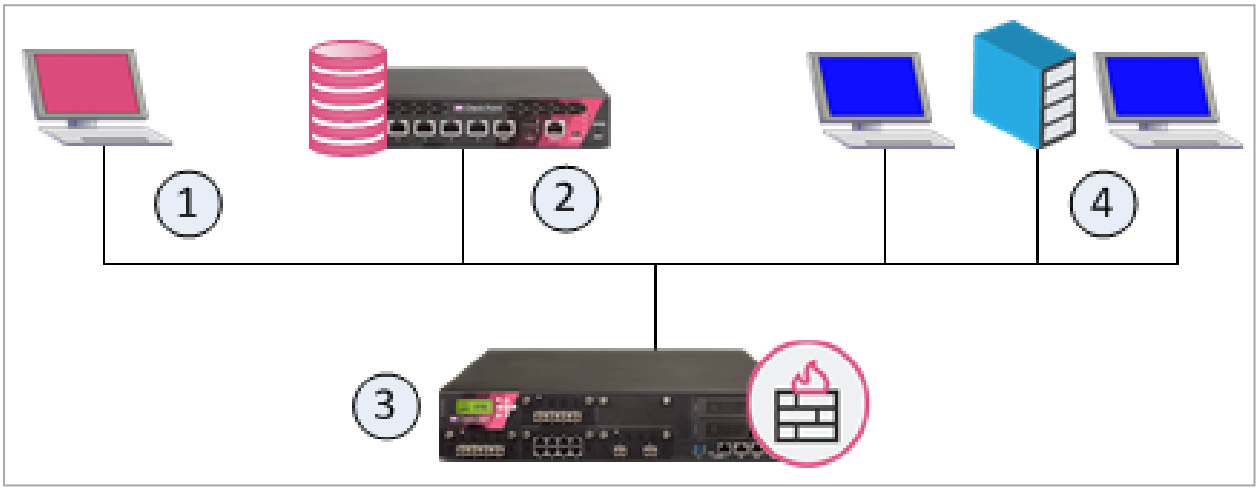
VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Welcome

Check Point offers effective Security Management solutions to help you keep up with constantly growing needs and challenges of your organizational network. This Administration Guide focuses on the basic Security Management Server deployment.

If you are interested in deployments for organizations with multiple sites, refer to the *R81 Multi-Domain Security Management Administration Guide*.

These are the basic components of Check Point security architecture.



Item	Description
1	SmartConsole - Check Point Graphical User Interface for connection to and management of Security Management Servers.
2	Security Management Server - Manages Security Gateways with defined security policies and monitors security events on the network.
3	Security Gateway - Placed at the perimeter of the network topology, to protect your environment through enforcement of the security policies.
4	Your environment to protect.

Getting Started

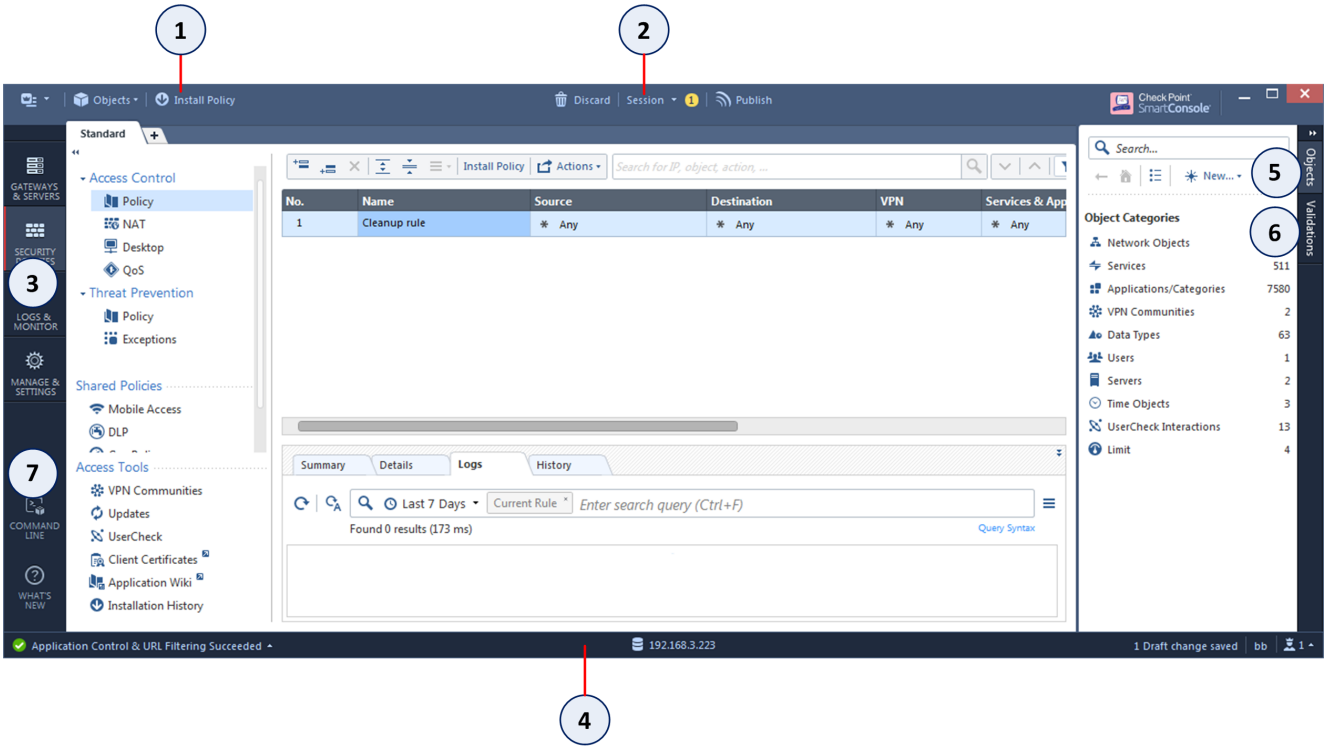
Before you deploy a Check Point security solution, familiarize yourself with:

- Check Point SmartConsole
- Basic setup of a Check Point Security Management Server
- Basic setup of Check Point Security Gateways
- Administrative task delegation
- Security management in a non-GUI environment

Understanding SmartConsole

Check Point SmartConsole makes it easy to manage security for complex networks. Before you configure your cyber security environment and policies, become familiar with Check Point SmartConsole.

SmartConsole Window



Item	Description	Item	Description
1	Global Toolbar	5	Objects Bar (F11)
2	Session Management Toolbar	6	Validations pane
3	Navigation Toolbar	7	Command line interface button
4	System Information Area		

SmartConsole Toolbars

Global Toolbar (top of SmartConsole)

	Description
	The main SmartConsole Menu. When SmartConsole is connected to a Security Management Server, this includes: ■ Manage policies and layers ■ Open Object Explorer ■ New object (opens menu to create a new object) ■ Publish session ■ Discard session ■ Session details ■ Install policy ■ Verify Access Control Policy ■ Install Database ■ Uninstall Threat Prevention policy ■ Management High Availability ■ Manage Licenses and Packages ■ Global Properties ■ View (opens menu to select a View to open)
	Create new objects or open the Object Explorer
	Install policy on managed Security Gateways

Session Management Toolbar (top of SmartConsole)

	Description
	Discard changes made during the session
	Enter session details to view the number of changes made in the session.
	Publish the SmartConsole session, to make the changes visible to other administrators, and ready to install on Security Gateways. **Note** - When the policy is installed, published changes are installed on the Security Gateways and enforced.

Navigation Toolbar (left side of SmartConsole)

	Keyboard Shortcut	Description
	Ctrl+1	**Gateways & Servers** configuration view: ■ Manage Security Gateways ■ Activate Software Blades ■ Add, edit, or delete Security Gateways and clusters (including virtual clusters) ■ Run scripts ■ Backup and restore Security Gateways ■ Open a command line interface on the Security Gateway ■ View Security Gateway status
	Ctrl+2	Security Policies Access Control view: ■ Manage Access Control: Content Awareness, VPN, Application & URL Filtering, and Mobile Access ■ Edit multiple policies at the same time ■ Add, edit, or delete NAT rules ■ Use the Access Tools Security Policies Threat Prevention view: ■ Manage Threat Prevention: IPS, Anti-Bot, Anti-Virus, Threat Emulation ■ Edit the unified threat Rule Base ■ Configure threat profiles ■ Add, edit, or delete exceptions and exception groups ■ Use the Threat Tools Shared Policies Views: ■ Manage Mobile Access, DLP, Geo Policy and inspection Settings
	Ctrl+3	Logs & Monitor view: ■ View high level graphs and plots ■ Search through logs ■ Schedule customized reports ■ Monitor Security Gateways ■ View compliance information
	Ctrl+4	Manage & Settings view - review and configure the Security Management Server settings: ■ Administrators ■ Permissions profiles ■ Trusted clients ■ Administrator sessions, and session settings ■ Blades ■ Revisions ■ Preferences ■ Sync with User Center

Command Line Interface Button (left bottom corner of SmartConsole)

	Keyboard Shortcut	Description
	F9	Open a command line interface for management scripting and API

For more SmartConsole shortcuts, see *"Keyboard Shortcuts for SmartConsole" on page 42*.

Objects Bar (right side of SmartConsole)

	Description
Objects	Manage security and network objects

Validations Pane (right side of SmartConsole)

	Description
Validations	View validation errors

System Information Area (bottom of SmartConsole)

	Description
Task List	Management tasks in progress. Expand to view recent tasks
Server Details	The IP address of the server to which SmartConsole is connected. If Management High Availability is configured, click to view the details.
Session Status	The number of changes made in the session and the session status.
Connected administrators	Connected administrators: Yourself and others.

Search Engine

In each view you can search the Security Management Server database for information relevant to the view. For example:

- Gateway, by name or IP address
- Access Control rule
- NAT rule
- Threat Prevention profile
- Specific threat or a threat category
- Object tags

You can search for an object in the Security Management Server database in two ways:

- Enter the prefix of the object's name. For example, to find *USGlobalHost*, you can enter *USG* in the search box.
- Enter any sequence of characters in the object's name and add an asterisk (*) before such sequence.

  For example, to find *USGlobalHost*, you can enter **oba*, **host*, **SG* and so on in the search box.

IP Search

You can run an advanced search for an IP address, network, or port. It returns direct and indirect matches for your search criteria.

- IP address: xxx.xxx.xxx.xxx
- Network: xxx.xxx.0.0/16 or xxx.xxx
- Port: svc:<xxx>

These are the different IP search modes:

- **General** - (Default). Returns direct matched results and indirect results in IP ranges, networks, groups, groups with exclusion, and rules that contain these objects.
- **Packet** - Matches rules as if a packet with your IP address arrives at the Security Gateway.

General IP Search

This is the default search mode. Use it to search in Rule Bases and in objects. If you enter a string that is not a valid IP or network, the search engine treats it as text.

When you enter a valid IP address or network, an advanced search is done and on these objects and rules:

- Objects that have the IP address as a text value for example, in a comment
- Objects that have an IP address property (direct results)
- Groups, networks, and address ranges that contain objects with the text value or address value
- Rules that contain those objects

Packet Search

A Packet Search matches rules as if a packet with your IP address arrives at the Security Gateway.

It matches rules that have:

- The IP address in a column of the rule
- "Any"
- A Group-with-exclusion or negated field with the IP address in its declaration

To run a Packet Search:

1. Click the search box.

   The search window opens.
2. Click **Packet** or enter: "mode:Packet"
3. To search a specific rule column, enter: *ColumnName:Criteria*

Rule Base Results

When you enter search criteria and view the matched results, the value that matched the criteria in a rule is highlighted.

If there is...	This is highlighted
A direct match on an object name or on textual columns	Only the specific matched characters
A direct match on object properties	The entire object name
A negated column	The negated label
A match on "Any"	"Any"

Known Limitation:

- Packet search does not support IPv6.

Access and Threat Tools

The **Access Tools** section in the **Security Policies Access Control** view and the **Threat Tools** section in the **Security Policies Threat Prevention** view give you more management and data collection tools.

Access Tools in the Security Policies Access Control view

Tool	Description
VPN Communities	Create, edit, or delete VPN Communities.
Updates	Update the Application & URL Filtering database, schedule updates, and configure updates.
UserCheck	Configure UserCheck interaction objects for Access Control policy actions.
Client Certificates	Create and distribute client certificates that allow users to authenticate to the Security Gateway from handheld devices.
Application Wiki	Browse to the Check Point AppWiki. Search and filter the Web 2.0 Applications Database, to use Check Point security research in your policy rules for actions on applications, apps, and widgets.
Installation History	See the Policy installation history for each Security Gateway, and who made the changes. See the revisions that were made during each installation, and who made them. Install a specific version of the Policy.

Threat Tools in the Security Policies Threat Prevention view

Tool	Description
Profiles	Create, edit, or delete profiles.
IPS Protections	Edit IPS protections per profile.
Protections	See statistics on different protections.
Whitelist Files	Configure Whitelist Files list.
Indicators	Configure indicators of malicious activity and how to handle it.
Updates	Configure updates to the Malware database, Threat Emulation engine and images, and the IPS database.
UserCheck	Configure UserCheck interaction objects for Threat Prevention policy actions.
Threat Wiki	Browse to the Check Point ThreatWiki. Search and filter Check Point's Malware Database, to use Check Point security research to block malware before it enters your environment, and to best respond if it does get in.
Installation History	See the Policy installation history for each Security Gateway, and who made the changes. See the revisions that were made during each installation, and who made them. Install a specific version of the Policy.

Shared Policies

The **Shared Policies** section in the **Security Policies** shows the policies that are not in a Policy package. They are shared between all Policy packages.

Shared policies are installed with the Access Control Policy.

Software Blade	Description
Mobile Access	Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP	Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
HTTPS Inspection	The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. The HTTPS Policy shows if HTTPS Inspection is enabled on one or more Security Gateways.

Software Blade	Description
Inspection Settings	You can configure Inspection Settings for the Security Gateway (see *"Preferences and Management Settings" on page 327*): ■ Deep packet inspection settings ■ Protocol parsing inspection settings ■ VoIP packet inspection settings

API Command Line Interface

You can also configure objects and rules through the API command line interface, which you can access from SmartConsole.

	ick to open the command line interface.
	Click to open the API reference (in the command line interface). Use the Command Line Reference to learn about **Session management** commands, **Host** commands, **Network** commands, and **Rule** commands.

In addition to the command line interface, you can create and run API scripts to manage configuration and operations on the Security Management Server (see *"Managing Security through API" on page 48*).

Keyboard Shortcuts for SmartConsole

From R80.20, there are additional keyboard shortcuts that you can use to navigate between the different SmartConsole fields:

Keyboard shortcut	Description
Ctrl+S	Publish the SmartConsole session.
Ctrl+Alt+S	Discard the SmartConsole session.
Shift+Alt+Enter	Install policy.
F10	Show/hide task details.
F11	Show/hide Object Explorer.
Ctrl+O	Manage policies and layers
Ctrl+E	Open Object Explorer
Ctrl+F3	Switch to high-contrast theme
Alt+Space	System menu
F1	Open the relevant online help

Keyboard shortcut	Description
Alt+F4	Close SmartConsole

Shortcuts for the specific views that support them:

Keyboard shortcut	Description
Ctrl+T	Open new tab
Ctrl+W or Ctrl+F4	Close current tab
Ctrl+Tab	Move to the next tab
Ctrl+Shift+Tab	Move to the previous tab
Delete	Delete the currently selected item
Ctrl+A	Select all elements
Esc	Cancel operation to close window
Enter or mouse double-click	Edit item

Shortcuts for views that contain a Rule Base:

Keyboard shortcut	Description
Ctrl+G	Go to rule (in the Access Control Rule Base)
Ctrl+X	Cut rule
Ctrl+C	Copy rule
Ctrl+V	Paste rule below the selected rule
Delete	Remove a used item from a rule cell
Ctrl+F	Open Rule Base search
F3	Navigate to the next Rule Base search result
Ctrl+arrow up	Go to the first rule in the Rule Base
Ctrl+arrow down	Go to the last rule in the Rule Base
Space or +	Open drop-down menu for the current cell in the Rule Base
Shift+arrow up/down	Move between objects in the Rule Base

Shortcuts for the Logs & Monitor view:

Keyboard shortcut	Description
Ctrl+G	Switch to grid view (in the Logs and Audit Logs views)
Ctrl+L	Switch to table view (in the Logs and Audit Logs views)
Ctrl+R	Resolve objects
F5	Refresh query
F6	Enable auto-refresh
Ctrl+D	Add to favorites
Ctrl+S	Organize favorites

Connecting to the Security Management Server through SmartConsole

To log in to a Security Management Server through Check Point SmartConsole, you must have an administrator account configured on the Security Management Server. When installing the Security Management Server, you create one administrator in the First Time Configuration Wizard. After that, you can create additional administrators accounts with SmartConsole, or using the Gaia Portal.

To log in to the Security Management Server through SmartConsole

1. Launch the SmartConsole application.
2. Enter your administrator authentication credentials. These can be a *username*, or a *certificate file*, or a *CAPI certificate*.

   Logging in with a username:

   - Enter the **Username** and **Password**.

   Logging in with a certificate file:

   - From the drop-down list, select **Certificate File**.
   - Browse to the file.
   - Enter the password of the certificate file.

   Logging in with a certificate in the CAPI repository:

   - From the drop-down list, select **CAPI Certificate**.
   - Select the certificate from drop-down list.
3. Enter the name or the IP address of the Security Management Server.
4. Click **Login**.

   The SmartConsole authenticates the Security Management Server. The first time you connect, SmartConsole shows the fingerprint.
5. Confirm the fingerprint.

The fingerprint and the IP address of the Security Management Server are saved to the user settings in Windows.

Planning Security Management

After installing the Security Management Server and Security Gateway, you can continue with cyber security configuration for your environment.

Define your Organization's Topology

Network topology consists of network components, both physical and logical, such as physical and virtual Security Gateways, hosts, hand-held devices, CA servers, third-party servers, services, resources, networks, address ranges, and groups. Each of these components corresponds to an object in your Check Point security management configuration. Configure those objects in SmartConsole. See *"Network Object Types" on page 161*.

Define users and user groups that your security environment protects

You can add users and groups to the database manually, through LDAP and User Directory, or with the help of Active Directory.

To add users: see *"User Database" on page 56*.

To add groups: see *"Managing User Groups" on page 65*.

To use LDAP and User Directory, see *"LDAP and User Directory" on page 66*.

To use Active Directory, see *"Microsoft Active Directory" on page 87*.

Define Access Rules for Protection of your Organization's Resources

Configure access rules and group them in policies that are enforced on the Security Gateways. You can define access policies based on traffic, applications, Web sites, and data (see *"Managing Policies" on page 176*). Set up preventative actions against known threats with Check Point Anti-Virus and Anti-Malware. Educate users about the validity and security of the operations they attempt with the help of UserCheck. Track network traffic and events through logging and monitoring.

Enforce Access Policies

Configure the Security Gateways. Make sure to activate the appropriate Software Blades. Then, install your policies on the Security Gateways.

Configuring the Security Management Server and Security Gateways

To start setting up your security environment, configure the Security Management Server and the Security Gateways. The Security Gateways enforce the security policy that you define on the Security Management Server.

To configure the Security Management Server in SmartConsole

1. In the Gateways & Servers view, find the Security Management Server object.

   You can search for it by name or IP address in the **Search** box at the top of the view.

   When you select the Security Management Server object, the **Summary** tab at the bottom of the pane shows the Software Blades that are enabled on it.

2. Open the object properties window, and enable the Management Software Blades, as necessary:
   - **Network Policy Management** - Manage a comprehensive security policy, unified for all security functionalities. This is automatically enabled.
   - **Endpoint Policy Management** - Manage security and data on end-user computers and hand-held devices. Enable this Software Blade if you have or will install an Endpoint Security Management Server.
   - **Logging & Status** - Monitor security events and status of Security Gateways, VPNs, users, and more, with advanced visuals and data management features.
   - **Identity Logging** - Add user identities, and data of their computers and devices, from Active Directory domains, to log entries.

- **User Directory** - Populate your security scope with user accounts from the LDAP servers in your environment.
- **Compliance** - Optimize your security settings and comply with regulatory requirements
- **SmartEvent** - Manage and correlate security events in real-time.

To configure the Security Gateways in SmartConsole

1. From the navigation toolbar, select Gateways & Servers.
2. Click **New**, and select Gateway.
3. In the **Check Point Security Gateway Creation** window that opens, select a configuration mode:
   - **Wizard Mode** - run the configuration wizard
   - **Classic Mode** - configure the Security Gateway in classic mode (see *"Managing Gateways" on page 126*)

Setting up for Team Work

As an administrator, you can delegate tasks, such as defining objects and users, to other administrators. Make sure to create administrator accounts (see *"Managing Administrator Accounts" on page 103*) with the privileges that are required to accomplish those tasks.

If you are the only administrator, we recommend that you create a second administrator account with Read Only permissions, which is useful for troubleshooting, consultation, or auditing.

Managing Security through API

This section describes the API Server on a Management Server and the applicable API Tools.

API

You can configure and control the Management Server through API Requests you send to the API Server that runs on the Management Server.

The API Server runs scripts that automate daily tasks and integrate the Check Point solutions with third party systems, such as virtualization servers, ticketing systems, and change management systems.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see:

- The API Documentation:
  - Online - *Check Point Management API Reference*
  - Local - `https://<Server IP Address>/api_docs`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.
- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

  These APIs also let other Check Point processes communicate with the Management Server over the HTTPS protocol.

  `https://<IP Address of Management Server>/web_api/<command>`

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

   The **Management API Settings** window opens.
5. Configure the **Startup Settings** and the **Access Settings**.

   ### Configuring Startup Settings

   Select **Automatic start** to automatically start the API server when you start or reboot the Management Server.

   Notes:
   - If the Management Server has more than 4GB of RAM installed, the **Automatic start** option is activated by default during Management Server installation.
   - If the Management Server has less than 4GB of RAM, the **Automatic Start** option is deactivated.

   ### Configuring Access Settings

   Select one of these options to configure which clients can connect to the API Server:

   - **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
   - **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
   - **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
6. Publish the SmartConsole session.
7. Restart the API Server on the Management Server with this command:

   ```
   api restart
   ```

   Note - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server.

API Key Authentication

An API key is a token that a client provides when making API calls.

API key authentication provides an administrator the ability to use a token for authenticating to the API interface instead of using a the usual username / password.

Configuring API key authentication for administrators

You can use SmartConsole to configure an API key for authenticating to the management API.

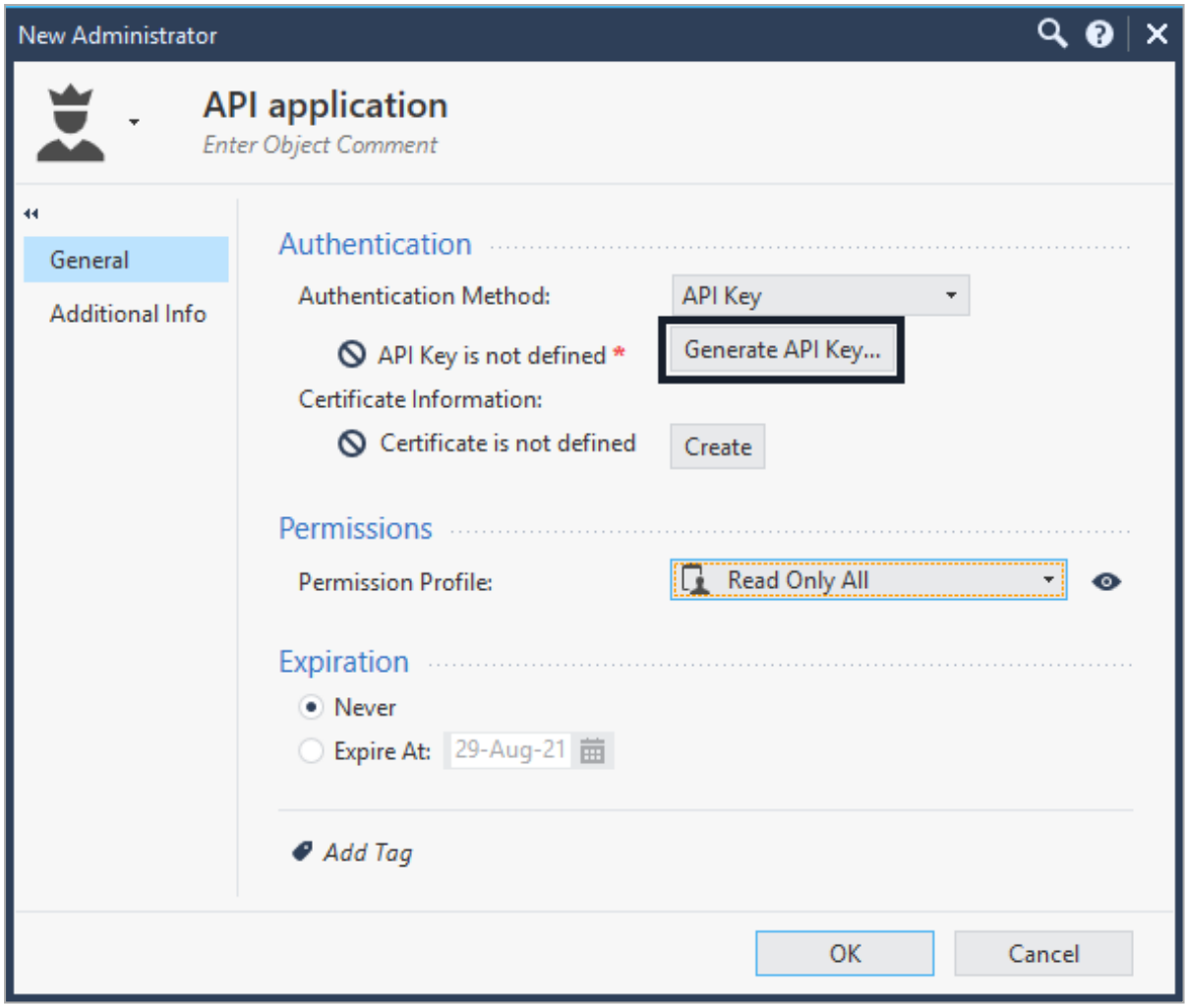
Note - The administrator can only use the API key for executing API commands and cannot use it for SmartConsole authentication.

To configure API authentication for an administrator in SmartConsole

1. In SmartConsole click **Manage & Settings** > **Permissions & Administrators** > **Administrators**

   Click the **New** icon ✳ at the top menu.

   The **New Administrator** window opens.
2. Give the administrator a name
3. In the **Authentication Method** field select **API Key**.
4. Click **Generate API key**.



5. A new API key window opens.
   a. Click **Copy key to Clipboard**
   b. Save the key for a later use (provide it to the relevant administrator).
6. Click **OK**.
7. Publish the SmartConsole session.

Example

This example demonstrates how to use the API-key for *login* and creating a *simple-gateway* using the API.

1. Log in to the Expert mode.
2. Use the previously generated key for the login, and save the standard output to a file (redirect it to a file using the ">" sign):

   Syntax:

   ```
   mgmt_cli login api-key <api-key> > /<Path_To>/<Filename>
   ```

   Example:

```
mgmt_cli login api-key mvYSiHVmlJM+J0tu2FqGag12 > /var/tmp/token.txt
```

3. Run a mgmt_cli command, use the **-s** /<*path_to*>/<*filename*>flag

   Syntax:

   ```
   mgmt_cli -s /<Path_To>/<Filename> add simple-gateway name "<Name of
   Security Gateway Object>" ip-address <IP address> one-time-password
   <Password> <Name of Software Blade> true <Name of Software Blade>
   true ... <Name of Software Blade> true
   ```

   Example:

   ```
   mgmt_cli -s /var/tmp/token.txt add simple-gateway name "gw1" ip-
   address 192.168.3.181 one-time-password "aaaa" firewall true vpn
   true
   ```

   For more details, see the *Check Point Management API Reference*.

Managing User and Administrator Accounts

Check Point supports different Authentication Methods for end users and administrators.

Security Gateways authenticate individual users. The Security Management Server authenticates administrators.

Users and Administrators authenticate using credentials. All the methods required a username and password.

Users and administrators can be stored in the Check Point User Database or on an LDAP server. See *"User Database" on page 56*.

Authentication Methods for Users and Administrators

This section describes the supported authentication methods for users and administrators.

Check Point Password

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

Operating System Password

OS Password is stored on the operating system of the computer on which the Security Gateway(for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

TACACS

Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

SecurID

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway or the Security Management Server act as an AM agent and direct all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API.

There are no specific parameters required for the SecurID authentication method.

Managing User Accounts

The following sections describe the supported authentication methods for users.

User Database

Users defined in SmartConsole are saved to the *User Database* on the Security Management Server, together with the user authentication schemes and encryption keys. Then, the user database is installed on Security Gateways and Check Point hosts:

- On Security Gateways - When the policy is installed (when you click **Install Policy**)
- On Check Point hosts with an active **Management** blade (such as Log Server) - When the database is installed (when you click Menu > **Install Database**)

The user database does **not** contain information about users defined elsewhere than on the Security Management Server (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the management server.

Creating, Modifying, and Removing User Accounts

To create a new user

1. In the **Object Bar** (F11)tree, click **New** > **More** > **User** > **User**.

   The **New User** window opens.
2. Choose a template.
3. Click **OK**.
4. Configure required and optional settings in **General Properties**. (see *"User > General Properties" on the next page*).
5. Select and configure **Authentication** (see *"Configuring Authentication" on the next page*).

   Important - If you do not select an authentication method, the user cannot log in or use network resources.
6. In **Location**, select objects from which this user can access or send data and traffic. See *"User > Location" on the next page*.
7. If the user has specified working days or hours, configure *when* the user can be authenticated for access. See *"User > Time" on the next page*.
8. Click **OK**.

To change an existing user

1. In the object tree, click **Users** > **Users**.
2. Double-click a user.

   The **User Properties** window opens.

3. Change the properties as necessary.
4. Click **OK**.

User > General Properties

Required settings:

- **User Name** - A unique, case sensitive character string.

  If you generate a user certificate with a non-Check Point Certificate Authority, enter the Common Name (CN) component of the Distinguished Name (DN). For example, if the DN is: [CN = James, O = My Organization, C = My Country],
  enter `James` as the user name. If you use Common Names as user names, they must contain exactly one string with no spaces.

- **Expiration Date** - The date, after which the user is no longer authorized to access network resources and applications. By default, the date defined in the Default Expiration Settings shows as the expiration date. See *"Configuring Default Expiration Settings for Users" on page 59*.

Optional settings:

- **Comment**
- **Email Address**
- **Mobile Phone Number**

Configuring Authentication

Select an **Authentication Scheme**:

- **SecurID**
- **Check Point Password** - Enter the password string (between 4 and 8 characters) and confirm it
- **OS Password**
- **RADIUS** - Select a RADIUS server or a group of servers
- **TACACS** - Select a TACACS server

User > Location

In the **Allowed locations** section:

Source - Click **Add**, to add selected objects to this user's permitted resources. The user can get data and traffic from these objects.

Destination - Click **Add**, to add selected objects to this user's permitted destinations. The user can send data and traffic to these objects.

User > Time

From and **To** - Enter start time and end time of an expected workday. This user will not be authenticated if a login attempt is made on a time outside the given range.

Days in week or **Daily** - Select the days that the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

User > Certificates

Generate and register SIC certificates for user accounts. This authenticates the user in the Check Point system. Use certificates with required authentication for added access control.

To create a new certificate

1. Open the **User Properties** window > **Certificates** page.
2. Click **New**.
3. Select key or `p12` file:
   - **Registration key for certificate enrollment** - Select to send a registration key that activates the certificate. When prompted, select the number of days the user has to activate the certificate, before the registration key expires.
   - **Certificate file (p12)** - Select to create a `.p12` certificate file with a private password for the user. When prompted, enter and confirm the certificate password.
4. Click **OK**.

If a user will not be in the system for some time (for example, going on an extended leave), you can revoke the certificate. This leaves the user account in the system, but it cannot be accessed until you renew the certificate.

To revoke a certificate, select the certificate and click **Revoke**.

User > Encryption

If the user will access resources from a remote location, traffic between the remote user and internal resources will be encrypted. Configure encryption settings for remote access users.

To configure encryption

1. Open the **User Properties** window > **Encryption** page.
2. Select an encryption method for the user.
3. Click **Edit**.

   The encryption **Properties** window opens.

   The next steps are for **IKE Phase 2**. The options can be different for different methods.
4. Open the **Authentication** tab.
5. Select the authentication schemes:
   a. **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.
   b. **Public Key** - The user authenticates with a public key contained in a certificate file.
6. Click **OK**.
7. Click **OK**.

Configuring Default Expiration Settings for Users

If a user account is about to expire, notifications show when you open the properties of the user in SmartConsole.

To configure the default expiration settings

1. From the **Menu**, select **Global Properties**.

   The **Global Properties** window opens.
2. Click **User Accounts**.
3. Select **Expire at** or **Expire after**.
   - **Expire at** - Select the expiration date from the calendar control.
   - **Expire after** - Enter the number of days (from the day the account is made) before user accounts expire.
4. Select **Show accounts expiration indication**, and enter the number of days.

   Expiration warnings in the SmartConsole User object show this number of days before an account expires. During this time, if the user account is to be active for longer, you can edit the user account expiration configuration. This will avoid loss of working time.

Delete a User

To delete a user:

1. In the object tree, click **Users** > **Users**.
2. Right-click the account and select **Delete**.

   The confirmation window opens.
3. Click **Yes**.

Granting User Access using RADIUS Server Groups

The Security Gateway lets you control access privileges for authenticated RADIUS users, based on the administrator's assignment of users to RADIUS groups. These groups are used in the Security Rule Base to restrict or give users access to specified resources. Users are unaware of the groups to which they belong.

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the Security Gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

To use RADIUS groups, you must define a return attribute in the RADIUS user profile of the RADIUS server. This attribute is returned to the Security Gateway and contains the group name (for example, **RAD_<group to which the RADIUS users belong>**) to which the users belong.

Use these RADIUS attributes (refer to RFC 2865):

- For SecurePlatform - attribute "Class" (25)
- For other operating systems, including Gaia, Windows, and IPSO-attribute "Vendor-Specific" (26)

SecurID Authentication for Security Gateway

Sample workflow for SecurID authentication configuration:

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway or the Security Management Server act as an AM agent and direct all access requests to the AM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation. There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API.

There are no specific parameters required for the SecurID authentication method.

To configure a Security Gateway to use SecurID Authentication:

1. **Configure Security Gateway to use SecurID authentication**

    a. In SmartConsole, from the left navigation panel, click **Gateways & Servers** view.

    b. Right-click a Security Gateway object and select **Edit**.

    c. From the left tree, click **Other** > **Legacy Authentication**.

    d. In the **Enabled Authentication Schemes** section, make sure **SecurID** is selected.

    e. Click **OK**.

2. **Configure the API to send authentication requests**

    You can select to enable one of two API types:

- **SDK-supported API**

  A proprietary API that uses a proprietary communication protocol on UDP port 5500 through SDKs available for selected platforms.

  To enable SecurID authentication over SDK-supported API

  a. Generate the `sdconf.rec` file on an ACE/Server and copy it to your computer.

     For details, refer to RSA documentation.

     Important - Use the IP address of a Security Gateway interface that connects to the ACE/Server:
     - **For a single Security Gateway** – Configure the single IP address as the Authentication Agent.
     - **For a Cluster** – Configure these IP addresses as Authentication Agents: Physical IP address of each Cluster Member and Cluster Virtual IP address.
     - **For a VSX Virtual System on single VSX Gateway** – Configure these IP addresses as Authentication Agents: IP address of the VSX Gateway and IP address of the Virtual System.
     - **For a VSX Virtual System on VSX Cluster** – Configure these IP addresses as Authentication Agents: Cluster Virtual IP address of the VSX Cluster and Cluster Virtual IP address of the Virtual System.

  b. Open the SecurID object in SmartConsole, click **Browse** and import the `sdconf.rec` file into the SecurID object.

  c. Install policy.

     Note - During the policy installation, the `sdconf.rec` file is transferred the Security Gateway to `/var/ace/sdconf.rec`.

- **REST API**

  To enable SecurID authentication over REST API

  a. Connect to the command line on the Security Gateway.

  b. Log in to the Expert mode.

  c. On a VSX Gateway or VSX Cluster Member, go to the context of VSID 0:

  ```
  vsenv 0
  ```

  d. Back up the current `$CPDIR/conf/RSARestServer.conf` file:

  ```
  cp -v $CPDIR/conf/RSARestServer.conf{,_BKP}
  ```

  e. Edit the `$CPDIR/conf/RSARestServer.conf` file.

  Fill in these fields:

  - `host` - The configured host name of the RSA server.
  - `port`, `client key`, and `accessid` - From the RSA SecurID Authentication API window.
  - `certificate` - The name of the certificate file.

  f. Save the changes in the file and exit the editor.

Note - If you do not complete the REST API configuration, the authentication is performed through the SDK-supported API.

3. **Define user groups**

   a. In SmartConsole, open the **Objects Bar (F11)**.

   b. Click **New** > **More** > **User** > **User Group**.

   The **New User Group** window opens.

   c. Enter the name of the group, for example *SecurID_Users*.

   Make sure the group is empty.

   d. Click **OK**.

   e. Publish the SmartConsole session.

   f. Install the policy.

4. **Configure SecurID authentication settings for users**

   The procedure for doing this is different for Internal Users (that are defined in the internal User Database on the Security Management Server) and for External Users.

   To configure SecurID authentication settings for Internal Users

   Internal users are users that are defined in the internal User Database on the Security Management Server.

a. Create a new user. In SmartConsole, open the **Objects Bar (F11)**.

b. Click **New** > **More** > **User** > **User**.

The **New User** window opens.

c. Choose a template.

d. Click **OK**.

e. In the **General** page:

- Enter a default **Name**. This name will be used to authenticate users on by the Authentication Manager.
- Set the **Expiration** date.

f. In the **Authentication** page, from the **Authentication Method** drop-down list, select **SecurID**.

g. Click **OK**.

To configure SecurID authentication settings for External Users

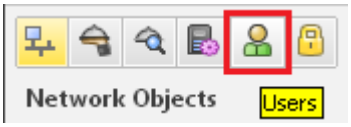
External users are users that are not defined in the internal Users Database on the Security Management Server.

a. In SmartConsole, click **Manage & Settings** > **Blades**.

b. In the **Mobile Access** section, click **Configure in SmartDashboard**.

Legacy SmartDashboard opens.

c. In the bottom left Network Objects pane, and click **Users**.



d. Right-click on an empty space and select the applicable option:

- If you support only one external authentication scheme, select **New** > **External User Profile > Match all users**.
- If you support more than one external authentication scheme, select **New** > **External User Profile > Match by domain**.

e. Configure the **External User Profile** properties:

i. **General Properties** page:

- If selected **Match all users**, then configure:
  - In the **External User Profile name** field, leave the default name `generic*`.
  - In the **Expiration Date** field, set the applicable date.
- If selected **Match by domain**, then configure:
  - In the **External User Profile name** field, enter the applicable name. This name will be used to authenticate users on the Authentication Manager.
  - In the **Expiration Date** field, set the applicable date.
  - In the **Domain Name matching definitions** section, configure the applicable settings.

ii. **Authentication** page:

From the **Authentication Scheme** drop-down list, select **SecurID**.

iii. Click **OK**.

f. From the top toolbar, click **Update** (or press the **CTRL S** keys).

g. Close the Legacy SmartDashboard.

5. **Complete the SecurID authentication configuration**

a. Make sure that connections between the Security Gateway and the Authentication Manager are not NATed in the Address Translation Rule Base.

On a Virtual System, follow the instructions in sk107281.

b. Save, verify, and install the policy in SmartConsole.

When a Security Gateway has multiple interfaces, the SecurID agent on the Security Gateway sometimes uses the wrong interface IP to decrypt the reply from the Authentication Manager, and authentication fails.

To overcome this problem, place a new text file, named `sdopts.rec` in the same directory as `sdconf.rec`.

The file should contain this line:

```
CLIENT_IP=<IP Address>
```

Where `<IP Address>` is the primary IP address of the Security Gateway, as defined on the Authentication Manager. This is the IP address of the interface, to which the server is routed.

Example:

```
CLIENT_IP=192.168.20.30
```

Note - On a VSX Gateway and VSX Cluster Members, you must create the same `sdopts.rec` file in the context VSID 0 and in the context of each applicable Virtual System.

Configuring TACACS+ Authentication

To configure a Security Gateway to use TACACS+ authentication, you must set up the server and enable its use on the Security Gateway.

To define a TACACS+ server

1. Define a TACACS Host object: **Object Explorer** > **New** > **Host**
2. Enter a name and IP address.
3. Define a TACACS server: **Object Explorer** > **New** > **Server** > **More** > **TACACS**.
4. Enter a name.
5. In **Host**, select the TACACS host.
6. Select the **Type**.

   Best Practice: The default is **TACACS**, but **TACACS+** is recommended.
7. In **Service**, select the **TACACS+** service (or **TACACS** UDP service if you selected **TACACS** type).
8. Enter a **Secret key**. (If you selected **TACACS** type, this is not available. If you selected **TACACS+**, it is required.)
9. Click **OK**.

To enable TACACS on the Security Gateway

1. Right-click the Security Gateway object and select **Edit**.
2. Click **Other** > **Legacy Authentication**.
3. In the **Enabled Authentication Schemes** section, click **TACACS**.
4. Click **OK**.

To enable TACACS authentication for users

1. In the Object Explorer, click **Users** > **User Templates**.
2. Edit the **Default** user template.
3. In the **Authentication** page, **Authentication method** list, select **TACACS**.
4. When **TACACS server** shows, select the TACACS server you defined.
5. Click **OK**.

   When you create a new user account, TACACS is the default selected authentication.

Managing User Groups

User groups are collections of user accounts. Add the user group to the *Source* or *Destination* of a rule. You cannot add individual users to a rule.

You can also edit user groups, and delete user groups that are not used in the Rule Base.

Adding User Groups

To create a new user group

1. In the **Object Bar** (F11), click **New > More > User > User Group**.

   The **New User Group** window opens.
2. Enter a name for the new group.
3. For each user or a group of users, click the [**+**] sign and select the object from the list.
4. Configure the optional settings:
   - **Mailing List Address**
   - **Comment**
   - **Tag**
   - **Color**
5. Click **OK**.

To add new users or other user groups to a group

1. In the **Object Bar** (F11), select **Object Categories** > **User** > **User Groups**
2. Right-click the User group and click **Edit**.

   The **User Group** window opens.
3. Click **+**
4. Select users or user groups.
5. Click **OK**.

LDAP and User Directory

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution.

If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

- Users can be managed externally by an LDAP server.
- The Security Gateways can retrieve CRLs.
- The Security Management Server can use the LDAP data to authenticate users.
- User data from other applications gathered in the LDAP user database can be shared by different applications.

You can choose to manage Domains on the Check Point users' database, or to implement an external LDAP server.

Note - User Directory requires a special license. If you have the Mobile Access Software Blade, you have the User Directory license.

User Directory lets you configure:

- *High Availability*, to duplicate user data across multiple servers for backup. See *"Account Units and High Availability" on page 97*.
- *Multiple Account Units*, for distributed databases.
- *Define LDAP Account Units*, for encrypted User Directory connections. See *"Modifying the LDAP Server" on page 96*.
- *Profiles*, to support multiple LDAP vendors. See *"User Directory Profiles" on page 76*.

User Directory and Identity Awareness

Identity Awareness uses User Directory.

Identity Awareness lets you enforce network access and audit data, based on network location, the identity of the user, and the identity of the computer.

You can use Identity Awareness in the Access Control, Threat Prevention, and DLP Rule Bases.

User Directory Considerations

Before you begin, plan your use of User Directory.

- Decide whether you will use the User Directory servers for user management, CRL retrieval, user authentication, or all of those.

  See *"Working with LDAP Account Units" on page 92*.

- Decide how many Account Units you will need.

  You can have one for each User Directory server, or you can divide branches of one User Directory server among different Account Units.

  See *"Account Units" on page 92*.

- Decide whether you will use High Availability setup.

  See *"Account Units and High Availability" on page 97*.

- Determine the order of priority among the User Directory servers for High Availability and querying purposes.

  See *"Setting High Availability Priority" on page 98*.

- Assign users to different Account Units, branches, and sub-branches, so that users with common attributes (such as their role in the organization, permissions, an so on) are grouped together.

  See *"Managing Users on a User Directory Server" on page 99*.

The User Directory Schema

The User Directory default schema is a description of the structure of the data in a user directory.

It has user definitions defined for an LDAP server.

This schema does not have Security Management Server or Security Gateway specific data, such as IKE-related attributes, authentication methods, or values for remote users.

You can use the default User Directory schema, if all users have the same authentication method and are defined according to a default template.

But if users in the database have different definitions, it is better to apply a Check Point schema to the LDAP server.

See *"Check Point Schema for LDAP" below*.

Check Point Schema for LDAP

The Check Point Schema adds Security Management Server and Security Gateway specific data to the structure in the LDAP server.

Use the Check Point Schema to extend the definition of objects with user authentication functionality.

For example, an Object Class entitled **fw1Person** is part of the Check Point schema.

This Object Class has mandatory and optional attributes to add to the definition of the Person attribute.

Another example is **fw1Template**.This is a standalone attribute that defines a template of user information.

Schema Checking

When schema checking is enabled, User Directory requires that every Check Point object class and its associated attributes is defined in the directory schema.

Before you work with User Directory, make sure that schema checking is disabled. Otherwise the integration will fail.

After the Check Point object classes and attributes are applied to the User Directory server's schema, you must enable schema checking again.

OID Proprietary Attributes

Each of the proprietary object classes and attributes (all of which begin with "`fw1`") has a proprietary Object Identifier (OID), listed below.

Object Class OIDs

object class	OID
fw1template	1.3.114.7.4.2.0.1
fw1person	1.3.114.7.4.2.0.2

The OIDs for the proprietary attributes begin with the same prefix ("1.3.114.7.4.2.0.X").

Only the value of "X" is different for each attribute.

See *"User Directory Schema Attributes" below*.

User Directory Schema Attributes

cn

The entry's name.

This is also referred to as "Common Name".

For users this can be different from the uid attribute, the name used to login to the Security Gateway.

This attribute is also used to build the User Directory entry's distinguished name, that is, it is the RDN of the DN.

uid

The user's login name, that is, the name used to login to the Security Gateway.

This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication methods.

The login name is used by the Security Management Server to search the User Directory server(s).

For this reason, each user entry should have its own unique UID value.

It is also possible to login to the Security Gateway using the full DN.

The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing.

The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different User Directory servers.

description

Descriptive text about the user.

The default is "`no value`".

mail

User's email address.

The default is "`no value`".

member

An entry can have zero or more values for this attribute.

- **In a template:** The DN of user entries using this template. DNs that are not users (object classes that are not one of: "`person`", "`organizationalPerson`", "`inetOrgPerson`", or "`fw1person`") are ignored.
- **In a group:** The DN of user.

userPassword

Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is:

"`{crypt}xxyyyyyyyyyyy`"

where:

- "`xx`" is the "salt"
- "`yyyyyyyyyyy`" is the hashed password

It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the User Directory server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password.

The Security Gateway never reads this attribute, though it does write it. Instead, the User Directory bind operation is used to verify a password.

fw1authmethod

One of these:

- RADIUS
- TACACS
- SecurID
- OS Password
- Defender

This default value for this attribute is overridden by **Default authentication scheme** in the **Authentication** tab of the **Account Unit** window in SmartConsole.

For example: a User Directory server can contain User Directory entries that are all of the object-class "`person`" even though the proprietary object-class "`fw1person`" was not added to the server's schema.

If **Default authentication scheme** in SmartConsole is "Internal Password", all the users will be authenticated using the password stored in the "`userPassword`" attribute.

fw1authserver

"X" in OID	fw1person	fw1template	default
1	y	y	"undefined"

The name of the server that will do the authentication.

This field must be given if fw1auth-method is "`RADIUS`" or "`TACACS`".

For all other values of fw1auth-method, it is ignored. Its meaning is given below:

method	meaning
RADIUS	name of a RADIUS server, a group of RADIUS servers, or "Any"
TACACS	name of a TACACS server

"X" in OID	fw1template
2	y

fw1pwdLastMod

The date on which the password was last modified.

The format is `yyyymmdd` (for example, 20 August 1998 is 19980820).

A password can be modified through the Security Gateway as a part of the authentication process.

"X" in OID	fw1person	fw1template	default
3	y	y	If no value is given, then the password has never been modified.

fw1expiration-date

The last date on which the user can login to a Security Gateway, or "no value" if there is no expiration date.

The format is `yyyymmdd` (for example, 20 August 1998 is 19980820).

The default is "`no value`".

"X" in OID	fw1person	fw1template	default
8	y	y	"no value"

fw1hour-range-from

The time from which the user can login to a Security Gateway.

The format is `hh:mm` (for example, 8:15 AM is 08:15).

"X" in OID	fw1person	fw1template	default
9	y	y	"00:00"

fw1hour-range-to

The time until which the user can login to a Security Gateway.

The format is `hh:mm` (for example, 8:15 AM is 08:15).

"X" in OID	fw1person	fw1template	default
10	y	y	"23:59"

fw1day

The days (of week) on which the user can login to a Security Gateway.

Can have the values "`SUN`","`MON`", and so on.

"X" in OID	fw1person	fw1template	default
11	y	y	all days of the week

fw1allowed-src

The names of one or more network objects from which the user can run a client, or "`Any`" to remove this limitation, or "`no value`" if there is no such client.

The names should match the name of network objects defined in Security Management Server.

"X" in OID	fw1person	fw1template	default
12	y	y	"no value"

fw1allowed-dst

The names of one or more network objects which the user can access, or "`Any`" to remove this limitation, or "`no value`" if there is no such network object.

The names should match the name of network objects defined on the Security Management Server.

"X" in OID	fw1person	fw1template	default
13	y	y	"no value"

fw1allowed-vlan

Not currently used.

"X" in OID	fw1person	fw1template	default
14	y	y	"no value"

fw1SR-keym

The algorithm used to encrypt the session key in SecuRemote.

Can be "`CLEAR`", "`FWZ1`", "`DES`", or "`Any`".

"X" in OID	fw1person	fw1template	default
15	y	y	"Any"

fw1SR-datam

The algorithm used to encrypt the data in SecuRemote.

Can be "`CLEAR`", "`FWZ1`", "`DES`", or "`Any`".

"X" in OID	fw1person	fw1template	default
16	y	y	"Any"

fw1SR-mdm

The algorithm used to sign the data in SecuRemote.

Can be "`none`" or "`MD5`".

"X" in OID	fw1person	fw1template	default
17	y	y	"none"

fw1enc-fwz-expiration

The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the Security Gateway.

"X" in OID	fw1person	fw1template
18	y	y

fw1sr-auth-track

The exception to generate on successful authentication via SecuRemote.

Can be "`none`", "`cryptlog`", or "`cryptalert`".

"X" in OID	fw1person	fw1template	default
19	y	y	"none"

fw1groupTemplate

This flag is used to resolve a problem related to group membership.

The group membership of a user is stored in the group entries to which it belongs, in the user entry itself, or in both entries.

Therefore there is no clear indication in the user entry if information from the template about group relationship should be used.

If this flag is "`TRUE`", then the user is taken to be a member of all the groups to which the template is a member.

This is in addition to all the groups in which the user is directly a member.

"X" in OID	fw1person	fw1template	default
20	y	y	"False"

fw1ISAKMP-EncMethod

The key encryption methods for SecuRemote users using IKE.

This can be one or more of: "`DES`", "`3DES`".

A user using IKE (formerly known as ISAMP) may have both methods defined.

"X" in OID	fw1person	fw1template	default
21	y	y	"DES", "3DES"

fw1ISAKMP-AuthMethods

The allowed authentication methods for SecuRemote users using IKE, (formerly known as ISAMP).

This can be one or more of: "`preshared`", "`signatures`".

"X" in OID	fw1person	fw1template	default
22	y	y	"signatures"

fw1ISAKMP-HashMethods

The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP).

This can be one or more of: "`MD5`", "`SHA1`".

A user using IKE must have both methods defined.

"X" in OID	fw1person	fw1template	default
23	y	y	"MD5", "SHA1"

fw1ISAKMP-Transform

The IPSec Transform method for SecuRemote users using IKE, (formerly known as ISAMP).

This can be one of: "`AH`", "`ESP`".

"X" in OID	fw1person	fw1template	default
24	y	y	"ESP"

fw1ISAKMP-DataIntegrityMethod

The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP).

This can be one of: "`MD5`", "`SHA1`".

"X" in OID	fw1person	fw1template	default
25	y	y	"SHA1"

fw1ISAKMP-SharedSecret

The pre-shared secret for SecuRemote users using IKE, (formerly known as ISAMP).

The value can be calculated using the `fw ikecrypt` command line.

"X" in OID	fw1person	fw1template
26	y	y

fw1ISAKMP-DataEncMethod

fw1ISAKMP-DataEncMethod

The data encryption method for SecuRemote users using IKE, (formerly known as ISAMP).

"X" in OID	fw1person	fw1template	default
27	y	y	"DES"

fw1enc-Methods

The encryption method allowed for SecuRemote users.

This can be one or more of: "`FWZ`", "`ISAKMP`" (meaning IKE).

"X" in OID	fw1person	fw1template	default
28	y	y	"FWZ"

fw1userPwdPolicy

Defines when and by whom the password should and can be changed.

"X" in OID	fw1person
29	y

fw1badPwdCount

Number of allowed wrong passwords entered sequentially.

"X" in OID	fw1person
30	y

fw1lastLoginFailure

Time of the last login failure.

"X" in OID	fw1person
31	4

memberof template

DN of the template that the user is a member of.

"X" in OID	fw1person
33	4

Netscape LDAP Schema

To add the propriety schema to your Netscape directory server, use the `$FWDIR/lib/ldap/schema.ldif` file.

Important - This deletes the object class definition from the schema and adds the updated one in its place.

We recommend that you back up the User Directory server before you run the command.

The `ldif` file:

- Adds the new attributes to the schema
- Deletes old definitions of `fw1person` and `fw1template`
- Adds new definitions of `fw1person` and `fw1template`

To change the Netscape LDAP schema, run the **ldapmodify** command with the **schema.ldif** file.

Note - On some server versions, the `delete objectclass` operation can return an error, even if it was successful. Use `ldapmodify` with the `-c` (continuous) option.

User Directory Profiles

The User Directory profile is a configurable LDAP policy that lets you define more exact User Directory requests and enhances communication with the server.

Profiles control most of the LDAP server-specific knowledge. You can manage diverse technical solutions, to integrate LDAP servers from different vendors.

Use User Directory profiles to make sure that the user management attributes of a Security Management Server are correct for its associated LDAP server.

For example, if you have a certified OPSEC User Directory server, apply the OPSEC_DS profile to get enhanced OPSEC-specific attributes.

LDAP servers have difference object repositories, schemas, and object relations.

- The organization's user database may have unconventional object types and relations because of a specific application.
- Some applications use the `cn` attribute in the User object's Relatively Distinguished Name (RDN) while others use `uid`.
- In Microsoft Active Directory, the user attribute `memberOf` describes which group the user belongs to, while standard LDAP methods define the `member` attribute in the group object itself.
- Different servers implement different storage formats for passwords.
- Some servers are considered v3 but do not implement all v3 specifications. These servers cannot extend the schema.
- Some LDAP servers already have built in support for certain user data, while others require a Check Point schema extended attribute.

  For example, Microsoft Active Directory has the `accountExpires` user attribute, but other servers require the Check Point attribute `fw1expirationdate`, which is part of the Check Point defined `fw1person` objectclass.
- Some servers allow queries with non-defined types, while others do not.

Default User Directory Profiles

These profiles are defined by default:

- **OPSEC_DS** - the default profile for a standard OPSEC certified User Directory.
- **Netscape_DS** - the profile for a Netscape Directory Server.
- **Novell_DS** - the profile for a Novell Directory Server.
- **Microsoft_AD** - the profile for Microsoft Active Directory.

Modifying User Directory Profiles

Profiles have these major categories:

- **Common** - Profile settings for reading and writing to the User Directory.
- **Read** - Profile settings only for reading from the User Directory.
- **Write** - Profile settings only for writing to the User Directory.

Some of these categories list the same entry with different values, to let the server behave according to type of operation. You can change certain parameters of the default profiles for finer granularity and performance tuning.

To apply a profile:

1. Open the Account Unit.
2. Select the profile.

To change a profile:

1. Create a new profile.
2. Copy the settings of a User Directory profile into the new profile.
3. Change the values.

Fetch User Information Effectively

User Directory servers organize groups and members through different means and relations. User Directory operations are performed by Check Point on users, groups of users, and user templates where the template is defined as a group entry and users are its members. The mode in which groups/templates and users are defined has a profound effect on the performance of some of the Check Point functionality when fetching user information. There are three different modes:

- Defining a "Member" attribute per member, or "*Member*" user-to-group membership mode. In this case, each member of a specific group gets the 'Member" attribute, where the value of this attribute is the DN of that member.
- Defining a "Memberof" attribute per group, or "*MemberOf*" user-to-group membership mode. In this case, each group gets the "Memberof" attribute per group, where the value of this attribute is the DN of a group entry. This is referred to as "*MemberOf*" user-to-group membership mode.
- Defining a "Memberof" attribute per member and group, or "*Both*" user-to-group membership mode. In this case both members and groups are given the "Memberof" attribute.

The most effective mode is the "MemberOf" and "Both" modes where users' group membership information is available on the user itself and no additional User Directory queries are necessary.

Setting User-to-Group Membership Mode

Set the user-to-group membership mode in the profile objects for each User Directory server in the `objects_5_0.C` file.

- To specify the user-to-group and template-to-group membership mode set the `GroupMembership` attribute to one of the following values: "`Member`", "`MemberOf`", "`Both`" accordingly.
- To specify the user-to-template membership mode set the `TemplateMembership` attribute to one of the following values: "`Member`", "`MemberOf`" accordingly.

After successfully converting the database, set the User Directory server profile in the `objects_5_0.C` file to the proper membership setting and start the Security Management Server.

Make sure to install policy/user database on all Security Gateways to enable the new configuration.

Profile Attributes

UserLoginAttr

The unique username User Directory attribute (uid).

In addition, when fetching users by the username, this attribute is used for query.

Default	Other
■ uid (most servers) ■ SamAccountName (in Microsoft_AD)	One value allowed

UserPasswordAttr

This user password is User Directory attribute.

Default	Other
■ userPassword (most servers) ■ unicodePwd (in Microsoft_AD)	One value allowed

TemplateObjectClass

The object class for Check Point User Directory templates.

If you change the default value with another object-class, make sure to extend that objectclass schema definition with relevant attributes from `fw1template`.

default	Other
fw1template	Multiple values allowed

ExpirationDateAttr

The account expiration date is User Directory attribute.

This could be a Check Point extended attribute or an existing attribute.

Default	Other
■ fw1expiration-date (most servers) ■ accountExpires (in Microsoft_AD)	One value allowed

ExpirationDateFormat

Expiration date format.

This format will be applied to the value defined at `ExpirationDateAttr`.

Default	Other
CP format is yyyymmdd	One value allowed

PsswdDateFormat

The format of the password modified date is User Directory attribute.

This formation will be applied to the value defined at `PsswdDateAttr`.

Default	Other
■ CP (most servers) format is yyyymmdd ■ MS (in Microsoft_AD)	One value allowed

PsswdDateAttr

The password last modified date is User Directory attribute.

Default	Other
■ fw1pwdLastMod (most servers) ■ pwdLastSet (in Microsoft_AD)	One value allowed

BadPwdCountAttr

User Directory attribute to store and read bad password authentication count.

Default	Other
fw1BadPwdCount	One value allowed

ClientSideCrypt

If 0, the sent password will not be encrypted.

If 1, the sent password will be encrypted with the algorithm specified in the DefaultCryptAlgorithm.

Default	Other
■ 0 for most servers ■ 1 for Netscape_DS if not using encrypted password, SSL is recommended	One value allowed

DefaultCryptAlgorith

The algorithm used to encrypt a password before updating the User Directory server with a new password.

Default	Other
■ Plain (for most servers) ■ Crypt (for Netscape_DS) ■ SHAI1	One value allowed

CryptedPasswordPrefix

The text to prefix to the encrypted password when updating the User Directory server with a modified password.

Default	Other
{Crypt} (for Netscape_DS)	One value allowed

PhoneNumberAttr

User Directory attribute to store and read the user phone number.

Default	Other
internationalisednumber	One value allowed

AttributesTranslationMap

General purpose attribute translation map, to resolve problems related to peculiarities of different server types.

For example, an X.500 server does not allow the "-" character in an attribute name.

To enable the Check Point attributes containing "-", specify a translation entry: (e.g., "`fw1-expiration=fw1expiration`").

Default	Other
none	Multiple values allowed

ListOfAttrsToAvoid

All attribute names listed here will be removed from the default list of attributes included in read/write operations.

This is most useful in cases where these attributes are not supported by the User Directory server schema, which might fail the entire operation.

This is especially relevant when the User Directory server schema is not extended with the Check Point schema extension.

Default	Other
There are no values by default. In case the User Directory server was not extended by the Check Point schema, the best thing to do is to list here all the new Check Point schema attributes.	Multiple values allowed

BranchObjectClass

Use this attribute to define which type of objects (objectclass) is queried when the object tree branches are displayed after the Account Unit is opened in SmartConsole.

Default	Other
■ Organization OrganizationalUnit Domain (most servers) ■ Container (extra for Microsoft_AD)	Multiple values allowed

BranchOCOperator

If "One" is set, an "OR"ed query will be sent and every object that matches the criteria will be displayed as a branch.

If "All" is set, an "AND"ed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

OrganizationObjectClass

This attribute defines what objects should be displayed with an organization object icon.

A new object type specified here should also be in BranchObjectClass.

Default	Other
organization	Multiple values allowed

OrgUnitObjectClass

This attribute defines what objects should be displayed with an organization object icon.

A new object type specified here should also be in BranchObjectClass.

Default	Other
■ organizationalUnit (most servers) ■ Contained (added to Microsoft_AD)	Multiple values allowed

DomainObjectClass

This attribute defines what objects should be displayed with a Domain object icon.

A new object type specified here should also be in BranchObjectClass.

Default	Other
Domain	Multiple values allowed

UserObjectClass

This attribute defines what objects should be read as user objects.

The user icon will be displayed on the tree for object types specified here.

Default	Other
■ User (in Microsoft_AD) ■ Person OrganizationalPerson InertOrgPerson FW1 Person (most servers)	Multiple values allowed

UserOCOperator

If "One" is set, an "OR"ed query will be sent and every object that matches one of the types will be displayed as a user.

If "All" is set, an "AND"ed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

GroupObjectClass

This attribute defines what objects should be read as groups.

The group icon will be displayed on the tree for objects of types specified here.

Default	Other
Groupofnames Groupofuniquenames (most servers) Group Groupofnames (in Microsoft_AD)	Multiple values allowed

GroupOCOperator

If "One" is set, an "OR"ed query will be sent and every object that matches one of the types will be displayed as a user.

If "All" is set, an "AND"ed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

GroupMembership

Defines the relationship Mode between the group and its members (user or template objects) when reading group membership.

Default	Other
■ Member mode defines the member DN in the Group object (most servers) ■ MemberOf mode defines the group DN in the member object (in Microsoft_AD) ■ Modes define member DN in Group object and group DN in Member object.	One value allowed

UserMembershipAttr

Defines what User Directory attribute to use when reading group membership from the user or template object if GroupMembership mode is 'MemberOf' or 'Both' you may be required to extend the user/template object schema in order to use this attribute.

Default	Other
MemberOf	One value allowed

TemplateMembership

Defines the user to template membership mode when reading user template membership information.

Default	Other
■ Member mode defines the member DN in the Group object (most servers) ■ MemberOf mode defines the group DN in the member object (in Microsoft_AD)	One value allowed

TemplateMembershipAttr

Defines which attribute to use when reading the User members from the template object, as User DNs, if the TemplateMembership mode is Member.

Default	Other
member	Multiple values allowed

UserTemplateMembershipAttr

Defines which attribute to use when reading from the User object the template DN associated with the user, if the TemplateMembership mode is MemberOf.

Default	Other
member	Multiple values allowed

OrganizationRDN

This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when you create a new organizational unit in SmartConsole.

Default	Other
o	One value allowed

OrgUnitRDN

This value is used as the attribute name in the Relatively Distinguished Name (RDN) when you create a new organizational Unit in SmartConsole.

Default	Other
ou	One value allowed

UserRDN

This value is used as the attribute name in the Relatively Distinguished Name (RDN), when you create a new User object in SmartConsole.

Default	Other
cn	One value allowed

GroupRDN

This value is used as the attribute name for the RDN, when you create a new Group object in SmartConsole.

Default	Other
cn	One value allowed

DomainRDN

This value is used as the attribute name for the RDN, when you create a new Domain object in SmartConsole.

Default	Other
dc	One value allowed

AutomaticAttrs

This field is relevant when you create objects in SmartConsole.

The format of this field is `Objectclass:name:value` meaning that if the object created is of type `ObjectClass` then additional attributes will be included in the created object with name '`name`' and value '`value`'.

Default	Other
user:userAccountControl:66048 For Microsoft_AD This means that when a user object is created an extra attribute is included automatically: userAccountControl with the value 66048	Multiple values allowed

GroupObjectClass

This field is used when you modify a group in SmartConsole.

The format of this field is **ObjectClass:memberattr** meaning that for each group objectclass there is a group membership attribute mapping.

List here all the possible mappings for this User Directory server profile.

When a group is modified, based on the group's objectclass the right group membership mapping is used.

Default	Other
groupOfNames:member groupOfUniqueNames:uniqueMember (All other servers)	Multiple values allowed

OrgUnitObjectClass

This determines which ObjectClass to use when creating/modifying an OrganizationalUnit object.

These values can be different from the read counterpart.

Default	Other
OrganizationalUnit	Multiple values allowed

OrganizationObjectClass

This determines which ObjectClass to use when creating and/or modifying an Organization object.

These values can be different from the read counterpart.

Default	Other
Organization	Multiple values allowed

UserObjectClass

This determines which ObjectClass to use when creating and/or modifying a user object.

These values can be different from the read counterpart.

Default	Other
User (in Microsoft_AD) person organizationalPerson inetOrgPerson fw1Person (All other servers)	Multiple values allowed

DomainObjectClass

Determines which ObjectClass to use when creating and/or modifying a domain context object.

These values can be different from the read counterpart.

Default	Other
Domain	Multiple values allowed

Microsoft Active Directory

The Microsoft Windows 2000 advanced server (or later) includes a sophisticated User Directory server that can be adjusted to work as a user database for the Security Management Server.

By default, the Active Directory services are disabled. In order to enable the directory services:

- run the `dcpromo` command from the **Start > Run** menu, *or*
- run the Active Directory setup wizard using the **System Configuration** window.

The Active Directory has the following structure:

```
DC=qa, DC=checkpoint,DC=com
CN=Configuration,DCROOT
CN=Schema,CN=Configuration,DCROOT
CN=System,DCROOT
CN=Users,DCROOT
CN=Builtin,DCROOT
CN=Computers,DCOOT
OU=Domain Controllers,DCROOT
...
```

Most of the user objects and group objects created by Windows 2000 tools are stored under the `CN=Users, DCROOT` branch, others under `CN=Builtin, DCROOT` branch, but these objects can be created under other branches as well.

The branch `CN=Schema, CN=Configuration, DCROOT` contains all schema definitions.

Check Point can take advantage of an existing Active Directory object as well as add new types. For users, the existing user can be used "as is" or be extended with `fw1person` as an auxiliary of "User" for full feature granularity. The existing Active Directory "Group" type is supported "as is". A User Directory template can be created by adding the `fw1template` object-class. This information is downloaded to the directory using the `schema_microsoft_ad.ldif` file (see *"Adding New Attributes to the Active Directory" on page 89*).

Performance

The number of queries performed on the directory server is significantly low with Active Directory. This is achieved by having a different object relations model. The Active Directory group-related information is stored inside the user object. Therefore, when fetching the user object no additional query is necessary to assign the user with the group. The same is true for users and templates.

Manageability

SmartConsole allows the creation and management of existing and new objects. However, some specific Active Directory fields are not enabled in SmartConsole.

Enforcement

It is possible to work with the existing Active Directory objects without extending the schema. This is made possible by defining an Internal Template object and assigning it with the User Directory Account Unit defined on the Active Directory server.

For example, if you wish to enable all users with IKE+Hybrid based on the Active Directory passwords, create a new template with the IKE properties enabled and "Check Point password" as the authentication method.

Updating the Registry Settings

To modify the Active Directory schema, add a new registry DWORD key named `Schema Update Allowed` with the value different from zero under `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`.

Delegating Control

Delegating control over the directory to a specific user or group is important since by default the Administrator is not allowed to modify the schema or even manage directory objects through User Directory protocol.

To delegate control over the directory

1. Display the **Users and Computers Control** console.
2. Right-click on the domain name displayed in the left pane and choose **Delegate control** from the right-click menu.

   The Delegation of Control wizard window is displayed.
3. Add an Administrator or another user from the System Administrators group to the list of users who can control the directory.
4. Reboot the machine.

Extending the Active Directory Schema

Modify the file with the Active Directory schema, to use SmartConsole to configure the Active Directory users.

To extend the Active Directory schema

1. From the Security Gateway, go to the directory of the schema file: `$FWDIR/lib/ldap`.
2. Copy `schmea_microsoft_ad.ldif` to the **C:** drive in the Active Directory server.
3. From Active Directory server, with a text editor open the schema file.
4. Find the value `DOMAINNAME`, and replace it with the name of your domain in LDIF format.

   For example, the domain `sample.checkpoint.com` in LDIF format is: `DC=sample,DC=checkpoint,DC=com`
5. Make sure that there is a dash character - at the end of the `modify` section.

   This is an example of the `modify` section.

   ```
   dn: CN=User,CN-
   Schema,CN=Configuration,DC=sample,DC=checkpoint,DC=com
   changetype: modify
   add: auxiliaryClass
   auxiliaryClass: 1.3.114.7.3.2.0.2
   -
   ```
6. Run:

   ```
   ldifde -i -f c:/schema_microsoft_ad.ldif
   ```

Adding New Attributes to the Active Directory

Below is the example in LDAP Data Interchange (LDIF) format that adds one attribute to the Microsoft Active Directory:

```
dn:CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
changetype: add
adminDisplayName: fw1auth-method
attributeID: 1.3.114.7.4.2.0.1
attributeSyntax: 2.5.5.4
cn: fw1auth-method
distinguishedName:
CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
instanceType: 4
isSingleValued: FALSE
LDAPDisplayName: fw1auth-method
name: fw1auth-method
objectCategory:
CN=Attribute-Schema,CN=ConfigurationCN=Schema,CN=Configuration,DCROOT
ObjectClass: attributeSchema
oMSyntax: 20
rangeLower: 1
rangeUpper: 256
showInAdvancedViewOnly: TRUE
```

All Check Point attributes can be added in the same way.

The definitions of all attributes in LDIF format are contained in the `schema_microsoft_ad.ldif` file located in the `$FWDIR/lib/ldap` directory.

Before attempting to run the `ldapmodify` command, edit `schema_microsoft_ad.ldif` and replace all instances of `DCROOT` with the domain root of your organization. For example if your domain is `support.checkpoint.com`, replace `DCROOT` with `dc=support,dc=checkpoint,dc=com`.

After modifying the file, run the `ldapmodify` command to load the file into the directory. For example if you use the Administrator account of the `dc=support,dc=checkpoint,dc=com domain` the command syntax will be as follows:

Note - A shell script is available for UNIX gateways. The script is at:
`$FWDIR/lib/ldap/update_schema_microsoft_ad`

```
ldapmodify -c -h support.checkpoint.com -D
cn=administrator,cn=users,dc=support,dc=checkpoint,dc=com" -w SeCrEt -f
$FWDIR/lib/ldap/schema_microsoft_ad.ldif
```

Retrieving Information from a User Directory Server

When a Security Gateway requires user information for authentication, it goes through this process:

1. The Security Gateway searches for the user in the *internal users database*.
2. If the specified user is not defined in the *internal users database*, the Security Gateway queries the *LDAP server* defined in the Account Unit with the highest priority.

3. If the query against an LDAP server with the highest priority fails (for example, the connection is lost), the Security Gateway queries the server with the next highest priority.

   If there is more than one Account Unit, the Account Units are queried concurrently. The results of the query are taken from the first Account Unit to meet the conditions, or from all the Account Units which meet the conditions.

4. If the query against all LDAP servers fails, the Security Gateway matches the user against the generic external user profile..

Running User Directory Queries

Use queries to get User Directory user or group data. For best performance, query Account Units when there are open connections. Some connections are kept open by the Security Gateways, to make sure the user belongs to a group that is permitted to do a specified operation.

To query User Directory

1. In SmartConsole, go to **Manage & Settings** > **Blades**.
2. Click **Configure in SmartDashboard**.

   SmartDashboard opens.
3. In the **Objects Tree**, click **Users**.
4. Double-click the **Account Unit** to open a connection to the LDAP server.
5. Right-click the **Account Unit** and select **Query Users/Group**.

   The **LDAP Query Search** window opens.

   Click **Advanced** to select specified objects types, such as Users, groups, or templates.
6. Define the query.
7. To add more conditions, select or enter the values and click **Add**.

Query conditions:

- **Attributes** - Select a user attribute from the drop-down list, or enter an attribute.
- **Operators** - Select an operator from the drop-down list.
- **Value** - Enter a value to compare to the entry's attribute. Use the same type and format as the actual user attribute. For example, if **Attribute** is fw1expiration-date, then **Value** must be in the **yyyymmdd** syntax.
- **Free Form** - Enter your own query expression. See RFC 1558 for information about the syntax of User Directory (LDAP) query expressions.
- **Add** - Appends the condition to the query (in the text box to the right of **Search Method**).

Example of a Query

If you create a query where:

- **Attributes=mail**
- **Contains**
- **Value=Andy**

The server queries the User Directory with this filter:

```
filter:(&(|(objectclass=fw1person)(objectclass=person)
(objectclass=organizationalPerson)(objectclass=inetOrgPerson))
(|(cn=Brad)(mail=*Andy*)))
```

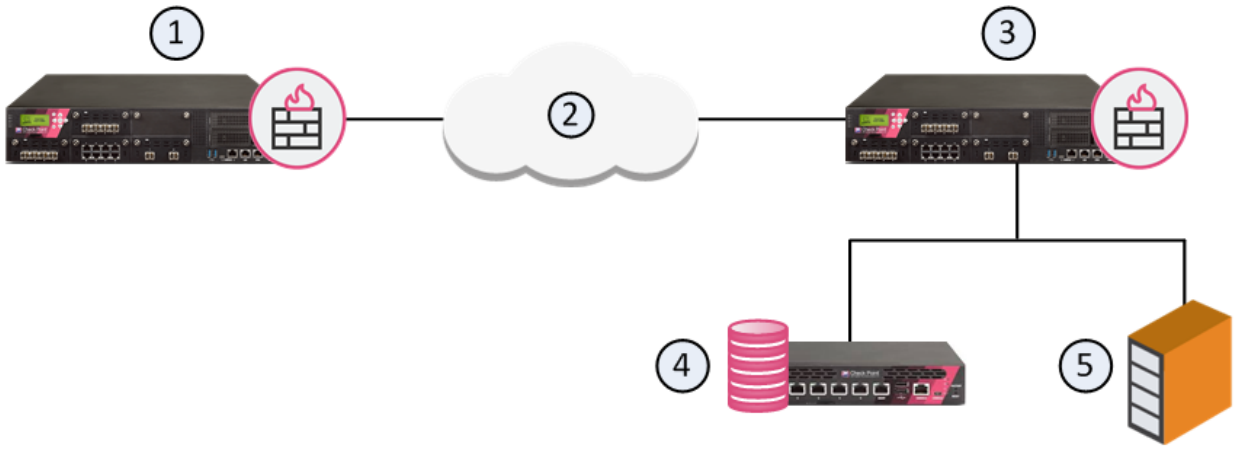
Querying Multiple LDAP Servers

The Security Management Server and the Security Gateways can work with multiple LDAP servers concurrently. For example, if a Security Gateway needs to find user information, and it does not know where the specified user is defined, it queries all the LDAP servers in the system. (Sometimes a Security Gateway can find the location of a user by looking at the user DN, when working with certificates.)

User Directory

Deploying User Directory

User Directory integrates the Security Management Server and an LDAP server and lets the Security Gateways use the LDAP information.



Item	Description
1	Security Gateway - Retrieves LDAP user information and CRLs
2	Internet
3	Security Gateway - Queries LDAP user information, retrieves CRLs, and does bind operations for authentication
4	Security Management Server - Uses User Directory to manage user information
5	LDAP server - Server that holds one or more Account Units

Enabling User Directory

In SmartConsole, enable the Security Management Server to manage users in the Account Unit. See *"Working with LDAP Account Units" on the next page*.

Note - You cannot use the SmartConsole User Database when the User Directory LDAP server is enabled.

To enable User Directory on the Security Management Server

1. From the Menu, select **Global Properties** > **User Directory**.

   The **User Directory** page opens.
2. Select **Use User Directory for Security Gateways**.
3. Configure login and password settings.
4. Click **OK**.
5. In the Gateways & Servers view (Ctrl+1), open the Security Management Server object for editing
6. On **General Properties** page, **Management** tab, select **Network Policy Management** and **User Directory**.
7. Click **OK**.
8. Install the policy.

Account Units

An *Account Unit* represents branches of user information on one or more LDAP servers. The Account Unit is the interface between the LDAP servers and the Security Management Server and Security Gateways.

You can have a number of Account Units representing one or more LDAP servers. Users are divided among the branches of one Account Unit, or between different Account Units.

Note - When you enable the Identity Awareness and Mobile Access Software Blade , SmartConsole opens a First Time Configuration Wizard. The **Active Directory Integration** window of this wizard lets you create a new AD Account Unit. After you complete the wizard, SmartConsole creates the AD object and Account Unit.

Working with LDAP Account Units

Use the **LDAP Account Unit Properties** window in SmartConsole to create a new or to edit an existing Account Unit or to create a new one manually.

To create or edit an existing LDAP Account Unit:

1. - **Create**: In the **Objects** tab, click **New > More > User/Identity > LDAP Account unit**.
   - **Edit**: In SmartConsole, open the **Object Explorer** (press the **CTRL+E** keys) > **Users/Identities** > **LDAP Account Units** > Right-click the LDAP Account Unit and select **Edit**.

   The **LDAP Account Unit Properties** window opens.
2. Edit the settings in these tabs:

- **General**

  Configure how the Security Management Server uses the Account Unit

  These are the configuration fields in the **General** tab:

  - **Name** - Name for the Account Unit
  - **Comment** - Optional comment
  - **Color** - Optional color associated with the Account Unit
  - **Profile** - LDAP vendor
  - **Domain** - Domain of the Active Directory servers, when the same user name is used in multiple Account Units (this value is also necessary for AD Query and SSO)
  - **Prefix** - Prefix for non-Active Directory servers, when the same user name is used in multiple Account Units
  - **Account Unit usage** - Select applicable options:
    - **CRL retrieval** - The Security Management Server manages how the CA sends information about revoked licenses to the Security Gateways
    - **User Management** - The Security Management Server uses the user information from this LDAP server (User Directory must be enabled on the Security Management Server).

      Note - LDAP SSO (Single Sign On) is only supported for Account Unit objects that use **User Management**.

    - **Active Directory Query** - This Active Directory server is used as an Identity Awareness source.

      Note - This option is only available if the **Profile** is set to **Microsoft_AD**.

  - **Enable Unicode support** - Encoding for LDAP user information in non-English languages
  - **Active Directory SSO configuration** - Click to configure Kerberos SSO for Active Directory - **Domain Name**, **Account Name**, **Password**, and **Ticket encryption method**

- **Servers**

  Manage LDAP servers that are used by this Account Unit. You can add, edit, or delete LDAP server objects.

  To configure an LDAP server for the Account Unit

  a. To add a new server, click **Add**. To edit an existing one, select it from the table and click **Edit**.

     The **LDAP Server Properties** window opens.

  b. From the **Host** drop-down menu, select the server object.

     If necessary, create a new SmartConsole server object:

     i. Click **New**.

     ii. In the **New Host** window opens, enter the settings for the LDAP server.

     iii. Click **OK**.

  c. Enter the login credentials and the **Default priority**.

  d. Select access permissions for the Check Point Gateways:

     - **Read data from this server**
     - **Write data to this server**

  e. In the **Encryption** tab, configure the optional SSL encryption settings. To learn about these settings, see the Help. Click **?** or press F1 in the **Encryption** tab.

  f. Click **OK**.

  To remove an LDAP server from the Account Unit:

  a. Select a server from the table.

  b. Click **Remove**.

  If all the configured servers use the same login credentials, you can modify those simultaneously.

  To configure the login credentials for all the servers simultaneously:

  a. Click **Update Account Credentials**.

     The **Update Account to All Servers** window opens.

  b. Enter the login credentials.

  c. Click **OK**.

- **Objects Management**

  Configure the LDAP server for the Security Management Server to query and the branches to use

  Note - Make sure there is LDAP connectivity between the Security Management Server and the LDAP Server that holds the management directory.

  To configure LDAP query parameters:

  a. From the **Manage objects on** drop-down menu, select the LDAP server object.

  b. Click **Fetch branches**.

  The Security Management Server queries and shows the LDAP branches.

  c. Configure **Branches in use**:

  - To add a branch, click **Add** and in the LDAP Branch Definition window that opens, enter a new **Branch Path**
  - To edit a branch, click **Edit** and in the LDAP Branch Definition window that opens, modify the **Branch Path**
  - To delete a branch, select it and click **Delete**

  d. Select **Prompt for password when opening this Account Unit**, if necessary (optional).

  e. Configure the number of **Return entries** that are stored in the LDAP database (the default is 500).

- **Authentication**

  Configure the authentication scheme for the Account Unit. These are the configuration fields in the Authentication tab:

  - **Use common group path for queries** - Select to use one path for all the LDAP group objects (only one query is necessary for the group objects)
  - **Allowed authentication schemes** - Select one or more authentication schemes allowed to authenticate users in this Account Unit - **Check Point Password**, **SecurID**, **RADIUS**, **OS Password**, or **TACACS**
  - Users' default values - The default settings for new LDAP users:
    - **User template** - Template that you created
    - **Default authentication scheme** - one of the authentication schemes selected in the **Allowed authentication schemes** section
  - **Limit login failures** (optional):
    - **Lock user's account after** - Number of **login failures**, after which the account gets locked
    - **Unlock user's account after** - Number of **seconds**, after which the locked account becomes unlocked
  - **IKE pre-shared secret encryption key** - Pre-shared secret key for IKE users in this Account Unit

3. Click **OK**.
4. Install the Access Control Policy.

Configuring LDAP query parameters

1. From the **Manage objects on** drop-down menu, select the LDAP server object.
2. Click **Fetch branches**.

   The Security Management Server queries and shows the LDAP branches.
3. Configure **Branches in use**:
   - To add a branch, click **Add** and in the LDAP Branch Definition window that opens, enter a new **Branch Path**
   - To edit a branch, click **Edit** and in the LDAP Branch Definition window that opens, modify the **Branch Path**
   - To delete a branch, select it and click **Delete**
4. Select **Prompt for password when opening this Account Unit**, if necessary (optional).
5. Configure the number of **Return entries** that are stored in the LDAP database (the default is 500).

Modifying the LDAP Server

1. On the **LDAP Account Unit Properties > Servers** tab, double-click a server.

   The **LDAP Server Properties** window opens.
2. On the **General** tab, you can change:

- Port of the LDAP server
- Login DN
- Password
- Priority of the LDAP server, if there are multiple servers
- Security Gateway permissions on the LDAP server

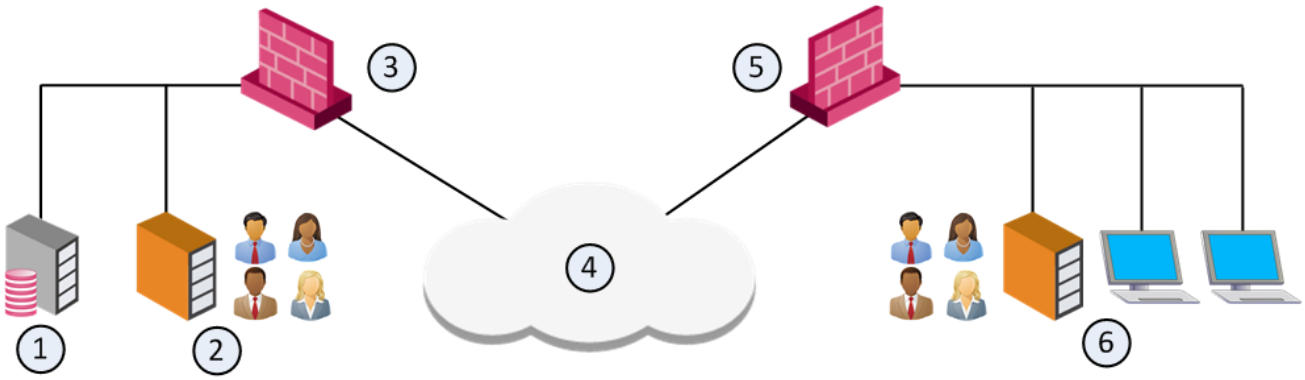
3. On the **Encryption** tab, you can change the encryption settings between Security Management Server / Security Gateways and LDAP server.

   If the connections are encrypted, enter the encryption port and strength settings.

   Note - User Directory connections can be authenticated by client certificates from a Certificate Authority (CA). To use certificates, the LDAP server must be configured with SSL strong authentication. See *"Authenticating with Certificates" on the next page*.

Account Units and High Availability

With User Directory replications for High Availability, one Account Unit represents all the replicated User Directory servers. For example, two User Directory server replications can be defined on one Account Unit, and two Security Gateways can use the same Account unit.



Item	Description
1	Security Management Server. Manages user data in User Directory. It has an Account Unit object, where the two servers are defined.
2	**User Directory server** replication.
3	Security Gateway. Queries user data and retrieves CRLs from nearest User Directory server replication (2).
4	Internet
5	Security Gateway. Queries user data and retrieves CRLs from nearest User Directory server replication (6).
6	**User Directory server** replication.

Setting High Availability Priority

With multiple replications, define the priority of each LDAP server in the Account Unit. Then you can define a server list on the Security Gateways.

Select one LDAP server for the Security Management Server to connect to. The Security Management Server can work with one LDAP server replication. All other replications must be synchronized for standby.

To set priority on the Account Unit

1. Open the **LDAP Account Unit Properties** window.
2. Open the **Servers** tab.
3. Add the LDAP servers of this Account Unit in the order of the priority that you want.

Authenticating with Certificates

The Security Management Server and Security Gateways can use certificates to secure communication with LDAP servers. If you do not configure certificates, the management server, Security Gateways, and LDAP servers communicate without authentication.

To configure User Directory to use certificates

1. Close all SmartConsole windows connected to the Management Server.
2. On each Account Unit, to which you want to authenticate with a certificate, set the `ldap_use_cert_auth` attribute to `true`:
   a. Connect with GuiDBedit Tool (see sk13009) to the Management Server.
   b. In the left pane, browse to **Table > Managed Objects > servers**.
   c. In the right pane, select the Account Unit object.
   d. In the bottom pane, search for the `ldap_use_cert_auth` attribute, and set it to **true**.
   e. Save the changes and close GuiDBedit Tool.
3. Connect with SmartConsole to the Management Server.
4. Add a CA object:
   a. From the **Objects Bar** (F11), click **New** > **More** > **Server** > **More** > **Trusted CA**.

      The Certificate Authority Properties window opens.
   b. In Certificate Authority Type, select **External Check Point CA**.
   c. Set the other options of the CA.
5. For all necessary network objects (such as Security Management Server, Security Gateway, Policy Server) that require certificate-based User Directory connections:

a. On the **IPSec VPN** page of the network object properties, click **Add** in the **Repository of Certificates Available** list.

Note - A management-only server does not have an IPSec VPN page. The User Directory on a management-only server cannot be configured to authenticate to an LDAP server using certificates.

b. In the **Certificate Properties** window, select the defined CA.

6. Test connectivity between the Security Management Server and the LDAP Server. See *"Managing LDAP Information" below*.

Managing Users on a User Directory Server

Managing Users on a User Directory Server

In SmartConsole, users and user groups in the Account Unit show in the same tree structure as on the LDAP server.

- To see User Directory users, open **Users and Administrators**. The **LDAP Groups** folder holds the structure and accounts of the server.
- You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.

Distributing Users in Multiple Servers

The users of an organization can be distributed across several LDAP servers. Each LDAP server must be represented by a separate Account Unit.

Managing LDAP Information

User Directory lets you use SmartDashboard to manage information about users and OUs (Organizational Units) that are stored on the LDAP server.

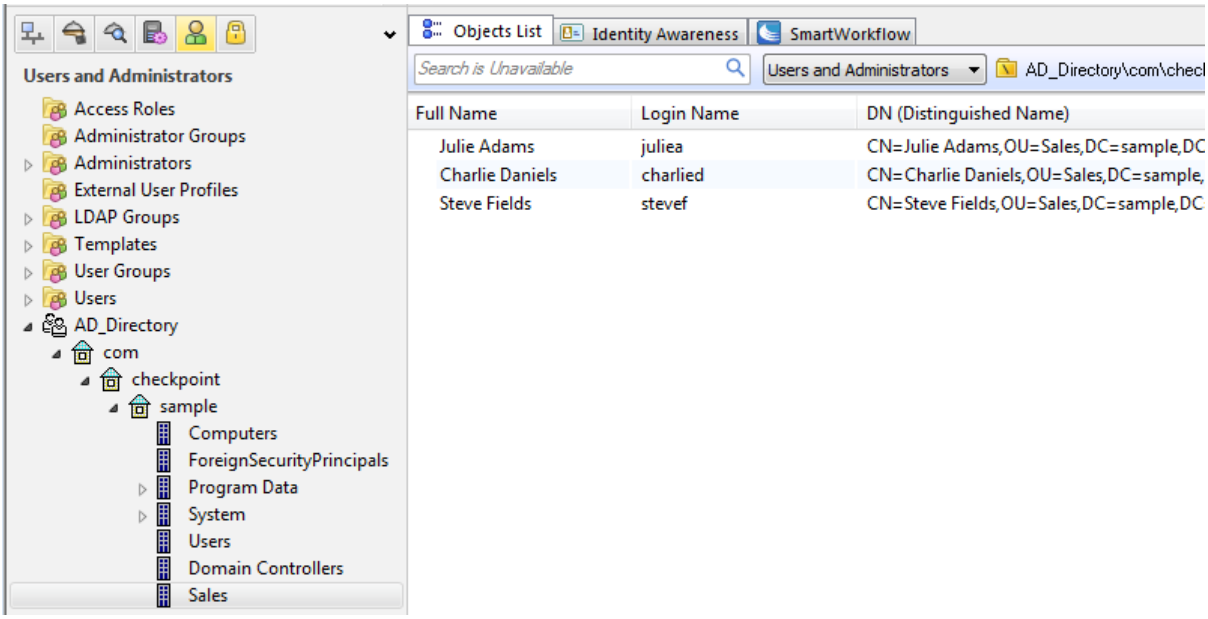
To manage LDAP information from SmartDashboard

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. Click **Configure in SmartDashboard**.

   SmartDashboard opens.
3. From the object tree, select **Servers and OPSEC**.
4. Double-click the Account Unit.

   The LDAP domain is shown.
5. Double-click the LDAP branch.

   The Security Management Server queries the LDAP server and SmartDashboard shows the LDAP objects.
6. Expand the **Objects List** pane.



7. Double-click the LDAP object.

   The **Objects List** pane shows the user information.

8. Right-click a user and select **Edit**.

   The **LDAP User Properties** window opens.

9. Edit the user information and settings. Click **OK**.

LDAP Groups for the User Directory

Create LDAP groups for the User Directory. These groups classify users according to type and can be used in Policy rules. You can add users to groups, or you can create dynamic filters.

To create LDAP groups for User Directory

1. In SmartConsole, open **Object Categories > New > More > Users > LDAP group**.
2. In the **New LDAP Group** window that opens, select the **Account Unit** for the User Directory group.
3. Define **Group's Scope** - select one of these:
   - **All Account-Unit's Users** - All users in the group
   - **Only Sub Tree** - Users in the specified branch
   - **Only Group in branch** - Users in the branch with the specified DN prefix
4. Apply an advanced **LDAP filter:**
   a. Click **Apply filter for dynamic group**.
   b. Enter the filter criteria.
5. Click **OK**.

Examples

- If the User objects for managers in your organization have the object class "myOrgManager", define the Managers group with the filter: **objectclass=myOrgManagers**
- If users in your organization have an e-mail address ending with us.org.com, you can define the US group with the filter: **mail=*us.org.com**

Access Roles

Access role objects let you configure network access according to:

- Networks
- Users and user groups
- Computers and computer groups
- Remote access clients (supported for Security Gateways R80.10 and higher)

After you activate the Identity Awareness Software Blade, you can create access role objects and use them in the **Source** and **Destination** columns of Access Control Policy rules.

Adding Access Roles

Important - Before you add Active Directory users, machines, or groups to an access role, make sure there is LDAP connectivity between the Security Management Server and the AD Server that holds the management directory. The management directory is defined on the **Objects Management** tab in the **Properties** window of the **LDAP Account Unit**.

To create an access role

1. In the object tree, click **New> More > Users > Access Role**.

   The **New Access Role** window opens.
2. Enter a **Name** for the access role.
3. Enter a **Comment** (optional).
4. Select a **Color** for the object (optional).
5. In the **Networks** pane, select one of these:
   - **Any network**
   - **Specific networks** - For each network, click + and select the network from the list
6. In the **Users** pane, select one of these:
   - **Any user**
   - **All identified users** - includes any user identified by a supported authentication method (internal users, Active Directory users, or LDAP users).
   - **Specific users/groups** - For each user or user group, click + and select the user or the group from the list
7. In the **Machines** pane, select one of these:

- **Any machine**
- **All identified machines** - includes machines identified by a supported authentication method (Active Directory).
- **Specific machines** - For each machine, click + and select the machine from the list

8. In the **Remote Access Clients** pane, select the clients for remote access.
9. Click **OK**.

Identity Awareness engine automatically recognizes changes to LDAP group membership and updates identity information, including access roles. For more, see the *R81 Identity Awareness Administration Guide*.

Authentication Rules

To make an authentication rule

1. Add users to user groups.
2. Define an access role for networks, users and user groups, and computers and computer groups. See *"Access Roles" on the previous page*.
3. Make the authentication rules with the access roles in the Source.

Managing Administrator Accounts

This section describes how to create and manage Administrator Accounts.

Configuring Authentication Methods for Administrators

These instructions show how to configure authentication methods for administrators. For information on user authentication, see *"Managing User Accounts" on page 56*.

For background information about the authentication methods, see *"Authentication Methods for Users and Administrators" on page 54*.

Configuring Check Point Password Authentication for Administrators

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

To configure a Check Point password for a SmartConsole administrator

1. Go to Manage & Settings > **Permissions & Administrators** > Administrators.
2. Click **New**.
3. The **New Administrator** window opens.
4. Give the administrator a name.
5. In **Authentication method**, select *Check Point Password*.
6. Click **Set New Password**, type the **Password**, and **Confirm** it.
7. Assign a **Permission Profile**.
8. Click **OK**.
9. Publish the SmartConsole session.

Configuring OS Password Authentication for Administrators

These instructions show how to configure OS Password Authentication for administrators.

OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

To configure an OS password for a SmartConsole administrator

1. Go to Manage & Settings > **Permissions & Administrators** > Administrators.
2. Click **New**.
3. The **New Administrator** window opens.
4. Give the administrator a name.
5. In **Authentication method**, select *OS Password*.
6. Assign a **Permission Profile**.
7. Click **OK**.
8. Publish the SmartConsole session.

Configuring RADIUS Server Authentication for Administrators

You can perform RADIUS authentication for SmartConsole administrators through a RADIUS server or a RADIUS server group. A RADIUS server group is a high availability group of identical RADIUS servers which includes any or all the RADIUS servers in the system. When you create the group, you define a priority for each server in the group. If the server with the highest priority fails, the one with the next highest priority in the group takes over, and so on. Note - When defining a group of RADIUS servers, all members of the group must use the same protocol.

To learn how to configure a RADIUS server, refer to the vendor documentation.

To configure a RADIUS Server for SmartConsole administrator authentication

1. **In SmartConsole, add a new RADIUS Server object**

   Go to the Object Explorer and select **New** > **More Object Types** > **Server** > **More** > **New RADIUS**.

2. **Configure the RADIUS Server properties**

   a. Give the server a **Name**. It can be any name.

   b. Click **New** and create a **New Host** with the **IP address** of the RADIUS server.

   c. Click **OK**.

   d. Make sure that this host shows in the **Host** field of the **Radius Server Properties** window.

   e. In the **Shared Secret** field, type the secret key that you defined previously on the RADIUS server.

   f. Click **OK**.

   g. Publish the SmartConsole session.

3. **Add a new administrator**

    a. Go to Manage & Settings > **Permissions & Administrators** > Administrators.

    b. Click **New**.

    The **New Administrator** window opens.

    c. Give the administrator the name that is defined on the RADIUS server.

    d. Assign a **Permission Profile**.

    e. In **Authentication method**, select **RADIUS**.

    f. Select the **RADIUS Server** defined earlier.

    g. Click **OK**.

    h. Publish the SmartConsole session.

To configure a RADIUS server group for SmartConsole administrator authentication

1. In SmartConsole, configure all the servers that you want to include in the server group, as explained in *"To configure a RADIUS Server for SmartConsole administrator authentication" on the previous page*. For each server, enter its priority in the group. The lower the number is, the higher the priority. For example, if you create a group with 3 servers, with priorities 1,2 and 3, the server with number 1 is approached first, the server with number 2 second, and the server with number 3, third.
2. Create the server group: In SmartConsole, go to **Object Explorer** and click **New** > **Server** > **More** > **RADIUS Group**.
3. Configure the group properties and add servers to the group:

    a. Give the group a **Name**. It can be any name.

    b. Click the plus (+) for each server you want to add, and select each server from the drop-down list.

    c. Click **OK**.

    d. Publish the SmartConsole session.
4. Add a new administrator as explained in *"To configure a RADIUS Server for SmartConsole administrator authentication" on the previous page*.
5. Publish the SmartConsole session.

Configuring SecurID Server Authentication for Administrators

These instructions show how to configure a SecurID server for SmartConsole administrators. To learn how to configure a SecurID server, refer to the vendor documentation.

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway or the Security Management Server act as an AM agent and direct all access requests to the RSA RM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API.

To configure the Security Management Server for SecurID (this procedure is only relevant if you are using an SDK-supported API)

1. Connect to the Security Management Server.
2. Copy the `sdconf.rec` file to the `/var/ace/` directory.

   If the `/var/ace/` directory does not exist, create it with this command:

   ```
   mkdir -v /var/ace/
   ```
3. Assign all permissions to the `sdconf.rec` file:

   ```
   chmod -v 777 /var/ace/sdconf.rec
   ```

To configure a SecurID Server for a SmartConsole administrator

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New SecurID**.
2. Configure the **SecurID Properties**:
   a. Give the server a **Name**. It can be any name.
   b. This step is relevant for SDK-supported API only: Click **Browse** and select the `sdconf.rec` file. This must be a copy of the file that is on the Security Management Server.
   c. Click **OK**.
3. Add a new administrator:
   a. Go to Manage & Settings > **Permissions & Administrators** > Administrators.
   b. Click **New**.

      The **New Administrator** window opens.
   c. Give the administrator a name.
   d. Assign a **Permission Profile**.
   e. In **Authentication method**, select *SecurID*.
4. In the SmartConsole Menu, click **Install Database**.

Configuring TACACS Server Authentication for Administrators

You can perform TACACS authentication for SmartConsole administrators through a TACACS server or a TACACS server group. A TACACS server group is a High Availability group of identical TACACS servers in the system. When you create the group, you define a priority for each server. If the server with the highest priority fails, the one with the next highest priority in the group takes over, and so on.

Note - All TACACS servers in the group must use the same protocol.

To learn how to configure a TACACS server, refer to the vendor documentation.

To configure a TACACS server for SmartConsole administrator authentication

1. **In SmartConsole, add a new TACACS server object**

   Go to **Object Explorer** and click **New** > **Server** > **More** > **TACACS**.

2. **Configure the TACACS server properties**

   a. Enter the server **Name**.

   b. In the **Host** field, click the drop-down arrow, click **New**, and create a **New Host** with the **IP address** of the TACACS server.

   c. Click **OK**.

   This host now appears in the **Host** field of the **New TACACS** window.

   d. Select a **Server type**.

   e. If your server type is TACACS+, type the **Secret key** that you defined previously on the TACACS+ server.

   f. Click **OK**.

   g. Publish the SmartConsole session.

3. **Add a new administrator**

   a. Go to Manage & Settings > **Permissions & Administrators** > Administrators.

   b. Click **New**.

   The **New Administrator** window opens.

   c. Enter the administrator name that is defined on the TACACS server.

   d. In **Authentication Method**, select **TACACS**.

   e. Select the **TACACS Server** defined earlier from the drop-down list.

   f. Assign a **Permission Profile**.

   g. Click **OK**.

   h. Publish the SmartConsole session.

To configure a TACACS Server group for SmartConsole administrator authentication

1. In SmartConsole, configure all the servers that you want to include in the server group, as explained in *"To configure a TACACS server for SmartConsole administrator authentication" above*. For each server, enter its priority in the group. The lower the number is, the higher the priority. For example, if you create a group with 3 servers, with priorities 1,2 and 3, the server with number 1 is approached first, the server with number 2 second, and the server with number 3, third.
2. Create the server group: In SmartConsole, go to **Object Explorer** and click **New** > **Server** > **More** > **TACACS Group**.
3. Configure the group properties and add servers to the group:

a. Enter the group **Name**.

b. Click the **+** icon for each server you want to add, and select the server from the drop-down list.

c. Click **OK**.

d. Publish the SmartConsole session.

4. Add a new administrator, according to the instructions in *"To configure a TACACS server for SmartConsole administrator authentication" on the previous page*
5. Publish the SmartConsole session.

Configuring API key authentication for administrators

You can use SmartConsole to configure an API key for administrators to use the management API.

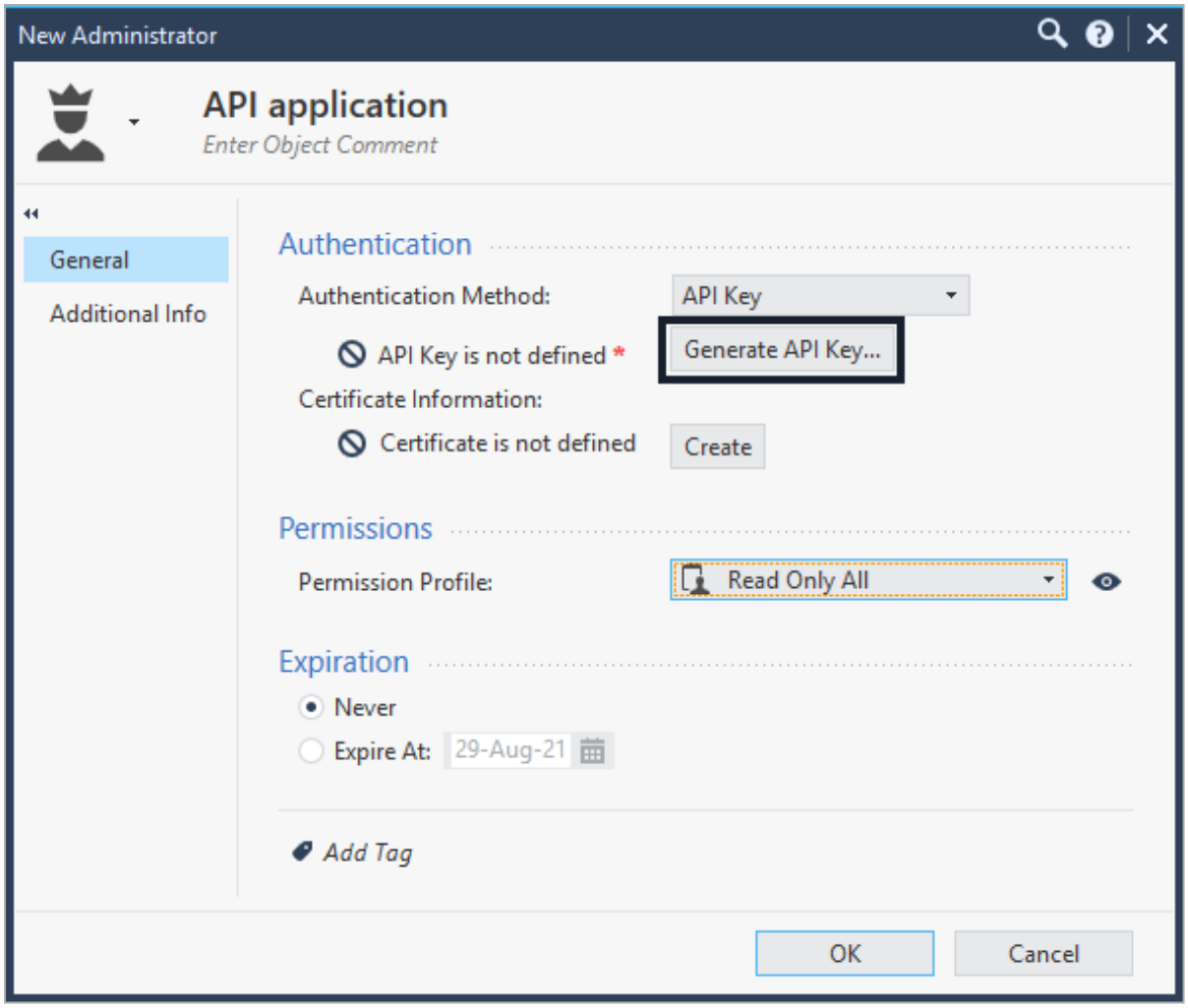
Note - This administrator can only use the API for executing API commands and cannot be used for SmartConsole authentication.

To configure API authentication for an Administrator using SmartConsole

1. In SmartConsole click **Manage & Settings** > **Permissions & Administrators** > **Administrators**

   Click the **New** icon ✳ at the top menu.

   The **New Administrator** window opens.
2. Give the administrator a name
3. In the **Authentication Method** field select **API Key**.
4. Click **Generate API key**.



5. A new API key window opens.
   a. Click **Copy key to Clipboard**
   b. Save the key for a later use (provide it to the relevant administrator).
6. Click **OK**
7. Publish the SmartConsole session.

Example

This example demonstrates how to use the API-key for *login* and creating a *simple-gateway* using the API.

1. Log in to the Expert mode.
2. Use the previously generated key for the login, and save the standard output to a file (redirect it to a file using the ">" sign):

   Syntax:

   ```
   mgmt_cli login api-key <api-key> > /<path_to>/<filename>
   ```

   Example:

```
mgmt_cli login api-key mvYSiHVmlJM+J0tu2FqGag12 > /var/tmp/token.txt
```

3. Run a `mgmt_cli` command with the "**-s**" flag.

   Syntax:

   ```
   mgmt_cli -s /<path_to>/<filename> add simple-gateway name <gateway
   name> ip-address <ip address> one-time-password <password> blade
   <true>
   ```

   Example:

   ```
   mgmt_cli -s /var/tmp/token.txt add simple-gateway name "gw1" ip-
   address 192.168.3.181 one-time-password "aaaa" firewall true vpn
   true
   ```

   For more details, see the *Check Point Management API Reference*.

Creating, Changing, and Deleting an Administrator Account

To successfully manage security for a large network, we recommend that you first set up your administrative team, and delegate tasks.

We recommend that you create administrator accounts in SmartConsole, with the procedure below or with the First Time Configuration Wizard.

If you create it through the SmartConsole, you can choose one of these authentication methods:

Authentication Method	Description
Check Point Password	Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.
OS Password	OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server. Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication. The RADIUS protocol uses UDP to communicate with the Security Gateway or the Security Management Server. RADIUS servers and RADIUS server group objects are defined in SmartConsole.

Authentication Method	Description
SecurID	SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM. Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of the RSA users and their assigned hard or soft tokens. The Security Gateway or the Security Management Server act as an AM Agent and direct all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to the RSA Authentication Manager documentation. There are no specific parameters required for the SecurID authentication method.
TACACS	Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers. TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

Creating an Administrator Account

To create an Administrator Account Using SmartConsole

1. Click **Manage & Settings > Permissions & Administrators**.

   The Administrators pane shows by default.

2. Click **New Administrator**.

   The **New Administrators** window opens.

3. Enter a unique name for the administrator account.

   Note - This parameter is case-sensitive.

4. Set the Authentication Method, or create a certificate, or the two of them.

   Note - If you do not do this, the administrator will not be able to log in to SmartConsole.

To define an Authentication Method:

In the **Authentication Method** section, select a method and follow the instructions in *"Managing Administrator Accounts" on page 103*.

To create a Certificate - If you want to use a certificate to log in:

In the **Certificate Information** section, click **Create**, and follow the instructions in *"Creating an Administrator Account" on the previous page*.

5. Select a **Permissions** profile for this administrator, or create a new one (see *"Changing and Creating Permission Profiles" on page 115*)
6. Set the account **Expiration** date:
   - For a permanent administrator - select **Never**
   - For a temporary administrator - select an **Expire At** date from the calendar

   The default expiration date shows (see *"Configuring Default Expiration Settings for Users" on page 59*).

   After the expiration date, the account is no longer authorized to access network resources and applications.
7. **Optional**: Configure **Additional Info - Contact Details**, **Email** and **Phone Number** of the administrator.
8. Click **OK**.

To create an Administrator Account with cpconfig

We do not recommend creating an administrator with `cpconfig`, the Check Point Configuration Tool. Use it only if there is no access to SmartConsole or the Gaia Portal. If you use `cpconfig` to create an administrator:

- You must restart Check Point Services to activate the administrator.
- It does not show the other administrators
- Check Point Password is automatically configured as the authentication method.

Changing an Existing Administrator Account

1. Click Manage & Settings > **Permissions & Administrators**.
2. Double-click an administrator account.

   The Administrators properties window opens.

Deleting an Administrator Account

To make sure your environment is secure, the best practice is to delete administrator accounts when personnel leave or transfer.

To remove an administrator account

1. Click Manage & Settings > **Permissions & Administrators**.

   The Administrators pane shows by default.

2. Select an administrator account and click **Delete**.
3. Click **Yes** in the confirmation window that opens.

Creating a Certificate for Logging in to SmartConsole

When you define an administrator, you must configure the authentication credentials for the administrator.

The authentication credentials for the administrator can be one of the supported authentication methods, or a certificate, or the two of them.

You can create a certificate file in SmartConsole. The administrator can use this file to log in to SmartConsole using the *Certificate File* option. The administrator must provide the password for the certificate file.

You can import the certificate file to the CryptoAPI (CAPI) certificate repository on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole using the *CAPI Certificate* option. The SmartConsole administrator does not need to provide a password.

To create a certificate file

1. In the **New Administrator** window, in the **Certificate Information** section, click **Create**.
2. Enter a password.
3. Click **OK**.
4. Save the certificate file to a secure location on the SmartConsole computer.

The certificate file is in the PKCS #12 format, and has a `.p12` extension.

Note - Give the certificate file and the password to the SmartConsole administrators. The administrator must provide this password when logging in to SmartConsole with the **Certificate File** option.

To Import the certificate file to the CAPI repository:

1. On the Microsoft Windows SmartConsole computer, double-click the certificate file.
2. Follow the instructions.

Configuring Default Expiration for Administrators

If you want to use the same expiration settings for multiple accounts, you can set the default expiration for administrator accounts. You can also choose to show notifications about the approaching expiration date at the time when an administrator logs into SmartConsole or one of the SmartConsole clients. The remaining number of days, during which the account will be alive, shows in the status bar.

To configure the default expiration settings

1. Click **Manage & Settings > Permissions & Administrators > Advanced**.
2. Click **Advanced**.
3. In the **Default Expiration Date** section, select a setting:

- **Never expires**
- **Expire at** - Select the expiration date from the calendar control
- **Expire after** - Enter the number of days, months, or years (from the day the account is made) before administrator accounts expire

4. In the **Expiration notifications** section, select **Show 'about to expire' indication in administrators view** and select the number of **days in advance** to show the message about the approaching expiration date.
5. Publish the SmartConsole session.

Setting SmartConsole Timeout

Use the SmartConsole in a secure manner, and enforce secure usage for all administrators. Setting a SmartConsole timeout is a basic requirement for secure usage. When an administrator is not using the SmartConsole, it logs out.

To set the SmartConsole timeout

1. Click Manage & Settings.
2. Select **Permissions & Administrators** > **Advanced**.
3. In the **Idle Timeout area**, select **Perform logout after being idle**.
4. Enter a number of minutes.

   When a SmartConsole is idle after this number of minutes, the SmartConsole automatically logs out the connected administrator, but all changes are preserved.

Revoking Administrator Certificate

If an administrator that authenticates through a certificate is temporarily unable to fulfill administrator duties, you can revoke the certificate for the account. The administrator account remains, but no one can authenticate to the Security Management Server with the certificate. However, if the account has an additional authentication method (a password, for example), that method can be used to authenticate to the account.

To revoke an administrator certificate

1. Click Manage & Settings > **Permissions & Administrators**.
2. Select an administrator account and click **Edit**.
3. In **General** > **Authentication**, click **Revoke**.

Assigning Permission Profiles to Administrators

A permission profile is a predefined set of Security Management Server and SmartConsole administrative permissions that you can assign to administrators. You can assign a permission profile to more than one administrator. Only Security Management Server administrators with the *Manage Administrators* permission in the profile can create and manage permission profiles.

To learn about permission profiles for Multi-Domain Security Management administrators, see the *R81 Multi-Domain Security Management Administration Guide*.

Changing and Creating Permission Profiles

Administrators with Super User permissions can edit, create, or delete permission profiles.

These are the predefined, default permission profiles. You cannot change or delete the default permission profiles. You can clone them, and change the clones:

- **Read Only All** - Full Read Permissions. No Write permissions.
- **Read Write All** - Full Read and Write Permissions.
- **Super User** - Full Read and Write Permissions, including managing administrators and sessions.

To change the permission profile of an administrator

1. Click Manage & Settings > **Permissions & Administrators**.
2. Double-click the administrator account.

   The Administrators properties window opens.
3. In the **Permissions** section, select another **Permission Profile** from the list.
4. Click **OK**.

To change a permission profile

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Permission Profiles**.
2. Double-click the profile to change.
3. In the **Profile** configuration window that opens change the settings as needed.
4. Click **Close**.

To create a new permission profile

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Permission Profiles**.
2. Click **New Profile**.

   The **New Profile** window opens.
3. Enter a unique name for the profile.
4. Select a profile type:
   - **Read/Write All** - Administrators can make changes to all features
   - **Auditor (Read Only All)** - Administrators can see all information but cannot make changes
   - **Customized** - Configure custom settings (see *"Configuring Customized Permissions" on the next page*).
5. Click **OK**.

To delete a permission profile

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Permission Profiles**.
2. Select a profile and click **Delete**.

   You cannot delete a profile that is assigned to an administrator. To see which administrators use a profile, in the error message, click **Where Used**.

   If the profile is not assigned to administrators, a confirmation window opens.
3. Click **Yes** to confirm.

Configuring Customized Permissions

Configure administrator permissions for Gateways, **Access Control**, **Threat Prevention**, **Others**, **Monitoring and Logging**, **Events and Reports**, **Management**. For each resource, define if administrators that are configured with this profile can configure the feature or only see it.

Permissions:

- **Selected** - The administrator has this feature.
- **Not selected** - The administrator does not have this feature.

Note - If you cannot clear a feature selection, the administrator access to it is mandatory.

Some features have **Read** and **Write** options. If the feature is selected:

- **Read** - The administrator has the feature but cannot make changes.
- **Write** - The administrator has the feature and can make changes.

To configure customized permissions

1. In the **Profile** object, in the **Overview > Permissions** section, select **Customized**.
2. Configure permissions in these pages of the **Profile** object:
   - **Gateways** -configure the **Provisioning** and the **Scripts** permissions.
   - **Access Control** - configure Access Control Policy permissions. (see *"Configuring Permissions for Access Control and Threat Prevention" on page 118*).
   - **Threat Prevention** - configure Threat Prevention Policy permissions (see *"Configuring Permissions for Access Control and Threat Prevention" on page 118*).
   - **Others** - configure permissions for **Common Objects**, user databases, **HTTPS Inspection** features, and **Client Certificates**.
   - **Monitoring and Logging** - configure permissions to generate and see logs and to use monitoring features (see *"Configuring Permissions for Monitoring, Logging, Events, and Reports" on page 118*).

- **Events and Reports** - configure permissions for SmartEvent features see *"Configuring Permissions for Monitoring, Logging, Events, and Reports" on the next page*).

3. In the **Management** section, configure this profile with permissions to:
   - **Manage Administrators** -Manage other administrator accounts.
   - **Manage Sessions** -Lets the administrator configure the session management settings (single or multiple sessions)
   - the session mode for single or multiple sessions
   - **High Availability Operations** -Configure and work with High Availability.
   - **Management API Login** -Log in with the management API.
4. Click **OK**.

Configuring Permissions for Access Control Layers

You can simplify the management of the Access Control Policy by delegating ownership of different Layers to different administrators.

To do this, assign a permission profile to the Layer. The permission Profile must have this permission: **Edit Layer by the selected profiles in a layer editor**.

An administrator that has a permission profile with this permission can manage the Layer.

Workflow

1. Give Layer permissions to an administrator profile.
2. Assign the permission profile to the Layer.

To give Layer permissions to an administrator profile

1. In the **Profile** object, in the **Access Control > Policy** section, select **Edit Layer by the selected profiles in a layer editor**.
2. Click **OK**.

To assign a permission profile to a Layer

1. In SmartConsole, click **Menu** > **Manage policies and layers**.
2. In the left pane, click **Layers**.
3. Select a Layer.
4. Click **Edit**.
5. In the left pane, select **Permissions**.
6. Click **+**
7. Select a profile with Layer permissions.
8. Click **OK**.
9. Click **Close**.
10. Publish the SmartConsole session.

Configuring Permissions for Access Control and Threat Prevention

In the **Profile** object, select the features and the Read or Write administrator permissions for them.

- **Access Control**

  To edit a Layer, a user must have permissions for all Software Blades in the Layer.

  - **Actions**
    - **Install Policy** - Install the Access Control Policy on Security Gateways.
    - **Application & URL Filtering Update** - Download and install new packages of applications and websites, to use in access rules.
- **Threat Prevention**
  - **Actions**
    - **Install Policy** - Install the Threat Prevention Policy on Security Gateways.
    - **IPS Update** -Download and install new packages for IPS protections.

Configuring Permissions for Monitoring, Logging, Events, and Reports

In the **Profile** object, select the features and the Read or Write administrator permissions for them.

- **Monitoring and Logging Features**

  These are *some* of the available features:

  - **Monitoring**
  - **Management Logs**
  - **Track Logs**
  - **Application and URL Filtering Logs**
- **Events and Reports Features**

  These are the permissions for SmartEvent:

  - **SmartEvent**
    - **Events** - views in SmartConsole > **Logs & Monitor**
    - **Policy** -**SmartEvent Policy and Settings** on SmartEvent GUI.
    - **Reports** - in SmartConsole > **Logs & Monitor**
  - **SmartEvent Application & URL Filtering reports only**

Defining Trusted Clients

To limit the access to the Security Management Server from a specified list of hosts, you must configure **Trusted Clients**.

You can configure **Trusted Clients** in these ways:

Trusted Client Definition	Description
Any	All hosts
IPv4 Address	A single host with the specified IPv4 address
IPv4 Address Range	Hosts with IPv4 addresses in the specified range
IPv4 Netmask	Hosts with IPv4 addresses in the subnet defined by the specified IPv4 address and netmask
IPv6 Address	A single host with the specified IPv6 address
IPv6 Address Range	Hosts with IPv6 addresses in the specified range
IPv6 Netmask	Hosts with IPv6 addresses in the subnet defined by the specified IPv6 address and netmask
Name	A host with the specified hostname
Wild cards (IP only)	Hosts with IP addresses described by the specified regular expression

Administrators with Super User permissions can add, edit, or delete trusted clients in SmartConsole.

Adding a new trusted client

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Trusted Clients**.
2. Click **New**.

   The **New Trusted Client** window opens.
3. Enter a unique name for the client.
4. Select a client type and configure corresponding values:
   - **Any** - No values to configure
   - **IPv4 Address** - Enter an IPv4 address of a host
   - **IPv4 Address Range** - Enter the first and the last address of an IPv4 address range
   - **IPv4 Netmask** - Enter the IPv4 address and the netmask
   - **IPv6 Address** - Enter an IPv6 address of a host
   - **IPv6 Address Range** - Enter the first and the last address of an IPv6 address range
   - **IPv6 Netmask** - Enter the IPv6 address and the netmask
   - **Name** - Enter a host name
   - **Wild cards (IP only)** - Enter a regular expression that describes a set of IP addresses
5. Click **OK**.

Modifying a trusted client settings

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Trusted Clients**.
2. Double-click the client you want to edit.
3. In the **Trusted Client** configuration window that opens, change the settings as needed.
4. Click **OK**.

Deleting a trusted client

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Trusted Clients**.
2. Select a trusted client and click **Delete**.

   The confirmation window opens.
3. Click **Yes** to confirm.

Note - Administrators can also configure the **GUI Clients** in the Check Point Configuration Tool on the Security Management Server (see *"cpconfig" on page 425*).

Restricting Administrator Login Attempts

For administrators that login to the Security Management Server using a Check Point password, you can configure these login restrictions:

- The number of login attempts before SmartConsole automatically locks an administrator.
- The number of minutes before SmartConsole unlocks the administrator's account after it was locked.

To configure login restrictions

1. Go to the Manage & Settings view or to the **Multi-Domain** view.
2. Go to **Permissions & Administrators** > **Advanced** > **Login Restrictions**.

Note - these restrictions apply *only* to administrators that authenticate to the Security Management Server using a Check Point password.

Unlocking Administrators

An administrator who has the **Manage Administrators** permission can unlock another administrator *if the locked administrator authenticates to the Security Management Server using a Check Point password*.

To unlock an administrator:

1. Go to the Manage & Settings view or to the **Multi-Domain** view.
2. Right-click the locked administrator and select **Unlock Administrator**.

Or:

Use the unlock administrator API command.

Note - The **Unlock Administrator** feature does **not** apply to administrators using other authentication methods.

Session Flow for Administrators

In SmartConsole, administrators work with sessions. A session is created each time an administrator logs into SmartConsole. Changes made in the session are saved automatically. You can generate a changes report to show you all the changes made in a session. These changes are private and available only to the administrator. To avoid configuration conflicts, other administrators see a lock icon on objects and rules that are being edited in other sessions.

Administrators can publish or discard their private changes. To include private changes in the policy installation, you must publish your changes in the session. This is also true if you want to make your private changes available to other administrators. Unpublished changes from other sessions are not included in the policy installation.

Before you publish a session, we recommend that you give the session a name and add a brief description that documents the work process.

Publishing a Session

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, or the use of objects that are not valid in the Rule Base. Make sure you correct these errors before publishing.

To publish a SmartConsole session

On the SmartConsole toolbar, click **Publish**. When a session is published, a new database version is created and shows in the list of database revisions.

To add a name or description to a session

1. In the SmartConsole toolbar, click **Session**.

   The **Session Details** window opens.
2. Enter a name for the database version.
3. Enter a description.
4. Click **OK**.

To discard a session

In the SmartConsole toolbar, click **Discard**.

Working in SmartConsole Session View

The Session view shows all unpublished sessions in the system. The view shows the sessions of the current administrator, sessions of other administrators and sessions from other applications. The columns in the view can be customized and show the session owner, name, description, connection mode, number of private changes, number of locks, application and other values.

To see session information, click Manage & Settings > **Sessions** > **View Sessions**.

Actions available to administrators on private sessions are determined by the **Manage Sessions** permission on their profile.

Administrators without the Manage Session permission can:	Administrators with the Manage Session Permission can:
■ Publish and discard their own sessions ■ See sessions opened by other administrators, the number the locks they have and number of changes they have made ■ Take over sessions created by applications, for example sessions created by the API command line tool	■ Publish and discard their own sessions ■ See sessions opened by other administrators, the number the locks they have and number changes they have made ■ **Publish & Disconnect** the private sessions of other administrators ■ **Disconnect & Discard** the private sessions of other administrators ■ **Disconnect** another administrator's private session ■ **Take over** sessions created by applications, for example sessions created by the API command line tool ■ **Take over** the private sessions of other administrators.  **Note** - If you want to keep changes made in your own private session, publish these changes *before* you take over the session of another administrator. If you do not publish your changes, you will lose them. When you take over, you disconnect the other administrator's SmartConsole session. ■ **Publish & Disconnect** the private sessions of other administrators. The action applies to both SmartConsole sessions and command line API sessions. ■ **Disconnect** the private session of other administrators ■ **Discard & Disconnect** the private session of other administrators

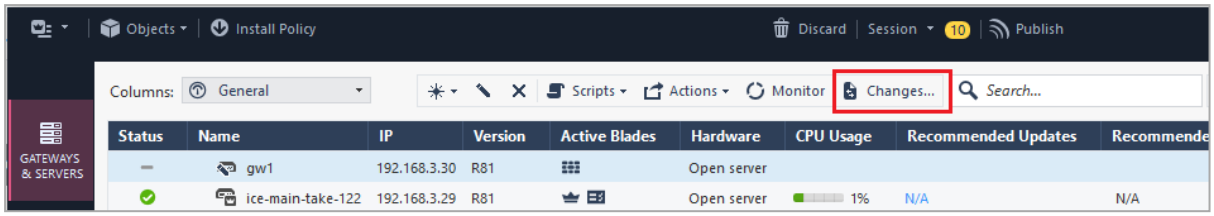
Viewing Changes Made in Private Sessions

You can generate a report to show you the changes made in a specific session, it can be your current session or a different one. Tracking the changes made in sessions lets you track and monitor the changes made, and troubleshoot bugs.

To view the changes made in your current session:

Click the **Changes** button in the toolbar of one of these views:

- The **Security Policies** view > Threat Prevention policy and Access Control policy
- The **Gateways & Servers** view



A report is generated which shows the changes made in the current private session.

To view the changes made in any session of your choice:

1. In SmartConsole, go to the **Manage & Settings** view > **Sessions** > **View Sessions.**

   The list of sessions appears.
2. Click on the required session,
3. Click the **Changes** button in the toolbar.

   A changes report is generated. The report shows a comparison between the selected private sessions.

Note - There is inconsistency between the number of changes which appears in the session toolbar and the Revisions view.

Administrators Working with Multiple Sessions

Administrators working with multiple sessions can open multiple additional private sessions without publishing changes made in the current private session.

Use Case

Suppose you are making changes in a private session and are asked to solve some immediate problem. The task involves making a change and publishing it. You do not wish to publish or discard your current private session.

You open a new private session, make the change required to resolve the issue, publish the change, then return to your previous private session.

To do this, you need to work with multiple sessions. To switch on multiple sessions, you need the **Manage Sessions** permission selected on your administrator profile.

To enable working in multiple sessions

1. Open the relevant permission profile.
2. Make sure the **Manage Sessions** permission is selected on the **Management** page.
3. Open SmartConsole > **Manage & Settings** View > **Sessions** > **Advanced**.
4. Select **Each administrator can manage multiple SmartConsole sessions at the same time**.
5. **Publish** the change.

When working with multiple sessions, you can:

- Open and manage multiple sessions to the Security Management Server using the same administrator account
- Switch between the active session and previously saved sessions
- Publish, discard and disconnect other sessions
- Take over other sessions

The SmartConsole Session menu

After multiple sessions are enabled, the SmartConsole Session menu has these new options:

Option	Description
Edit sessions details	Lets you change the session name and description.
Create new session	**In the current window** Opens a new session in the current SmartConsole **In a new window** Opens a new session in a new SmartConsole
Recent	Shows a list of recent sessions. Selecting a session opens the session in the current SmartConsole
More	Opens the **Open Session** window that shows sessions that you previously created and saved. ■ Sessions shown in this window are owned by the current user in the current domain. ■ The **Open Session > Actions** menu has options to open a saved session in the current SmartConsole or open the session in a new SmartConsole.

The SmartConsole Session View

When multiple sessions are enabled, you can perform these additional actions:

Action	You can:
For sessions that you own	■ Discard and Disconnect ■ Publish and Disconnect ■ Disconnect ■ Open an older session
For sessions owned by other administrators that have made private changes	■ Publish and Disconnect their changes ■ Discard and Disconnect ■ Disconnect ■ Take over their changes
For sessions owned by other administrators that have not made private sessions	■ Disconnect ■ Take over

Notes:

- When working in single session, you need to publish or discard your changes before taking over another session. In multiple sessions, you do not have to publish or discard your session before taking over the session of another administrator.
- In multiple sessions, an administrator connecting from another desktop to an already connected session can still take over the connected session by default.

Switching between Multiple and Single Session

If the session management settings switch from multiple SmartConsole sessions to allow only a single SmartConsole session at a time:

- Administrators can still publish, discard and open sessions that they own.
- Cannot create new sessions until they have published or discarded all their unpublished sessions with private sessions
- Cannot take over the sessions of other administrators or applications (for example sessions created with API commands in the *mgmt_cli* utility) until they have published or discarded all their previously saved private sessions.

Managing Gateways

This section describes how to create, update, and manage Security Gateways, and to use Secure Internal Communication (SIC) methods for Check Point platforms and products to authenticate each other.

Creating a New Security Gateway

A Security Gateway enforces security policies configured on the Security Management Server.

To install security policies on the Security Gateway, configure the Security Gateway object in SmartConsole.

To define a new Security Gateway object

1. From the navigation toolbar, select Gateways & Servers.
2. Click **New**, and select Gateway.

   The **Check Point Security Gateway Creation** window opens.
3. Click **Classic Mode**.

   The Check Point Gateway properties window opens and shows the **General Properties** screen.
4. Enter the host **Name** and the **IPv4 Address** or **IPv6 Address**.
5. Click **Communication**.

   The **Trusted Communication** window opens.
6. Select a **Platform**.

   Important - Make sure to select the correct Appliance model. Otherwise, policy installation may fail.
7. In the **Authentication** section, enter and confirm the **One-time password**.

   If you selected **Small Office Appliance** platform, make sure **Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time** is selected.
8. Click **Initialize** to establish trusted communication with the Security Gateway (see *"Secure Internal Communication (SIC)" on page 129*).

   If trust fails to establish, click **OK** to continue configuring the Security Gateway.
9. Click **OK**.
10. The **Get Topology Results** window that opens, shows interfaces successfully configured on the Security Gateway.
11. Click **Close**.
12. In the **Platform** section, select the **Hardware**, the **Version**, and the **OS**.

If trust is established between the server and the Security Gateway, click **Get** to automatically retrieve the information from the Security Gateway.

13. Select the Software Blades to enable on the Security Gateway.

    For some of the Software Blades a first-time setup wizard will open. You can run the wizard now or later. For more on the setup wizards, see the relevant Administration Guide.

Manually Updating the Gateway Topology

As the network changes, you must update the Security Gateway topology.

To update the Security Gateway topology

1. In SmartConsole, click **Gateways & Servers**.
2. Double-click the Security Gateway object.

   The Security Gateway property window opens.
3. Click **Network Management**.
4. Click **Get Interfaces** and select the applicable option:
   - **Get Interfaces With Topology**

     A warning window asks if you want to overwrite the existing Topology and Anti-Spoofing settings.

     Click **Yes**.
   - **Get Interfaces Without Topology**
5. The **Get Topology Results** window opens.
6. Click **Accept**.
7. Configure the applicable Topology and Anti-Spoofing settings for the interfaces.
8. Click **OK**.
9. Install the Access Control Policy.

Get Interfaces API

From R81 Jumbo Hotfix Accumulator Take 5, you can use the Check Point API to execute the Get Interfaces command.

The Get Interfaces API:

- Supports a larger number of interfaces compared with SmartConsole.
- Supports these interfaces which are not supported by SmartConsole: Bridge and Bond interfaces without IP addresses.
- Configures the default topology for internal networks for Security Gateway and ClusterXLR80.20 and higher to **Network defined by routes**, where applicable (the default in SmartConsole is **This network (Internal)**).
- Does not get unnecessary Bridge and Bond satellite interfaces.

The Get Interfaces API command only supports Security Gateways and ClusterXL that run on Gaiaoperating system.

For explanations on how to use the API Get Interfaces command, see the *Check Point Management API Reference*.

Dynamically Updating the Security Gateway Topology

This feature is supported only for Security Gateways R77.20 and above. Once selected, the range of IP addresses behind the internal interface is automatically calculated every second (default value) without the need for the administrator to click **Get Interfaces** and install a policy.

To configure dynamic topology updates

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Edit**.
3. In the **Topology** section, click **Modify**.
4. In the **Leads To** section, select **Network defined by routes**.
5. Click **OK**.

This default update value is configured in **SmartConsole > Preferences** and set to one second. The value set here applies to all internal interfaces for all gateways in the Domain.

To set the update value for a specific interface

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Actions > Settings**.
3. Select **Use custom update time (seconds)** and set the applicable update time.
4. Click **OK**.

Dynamic Anti-Spoofing

When Anti-Spoofing is selected and you click **Get interfaces**, the Security Gateway generates a list of valid IP addresses based on the IP address and netmask of the interface and the routes assigned to the interface.

Anti-Spoofing drops packets with a source IP address that does not belong to the network behind the packet's interface. For example, packets with an internal IP address that comes from an external interface.

When the **Network defined by routes** option is selected along with **Perform Anti-Spoofing based on interface topology**, you get *Dynamic Anti-Spoofing*. The valid IP addresses range is automatically calculated without the administrator having to do click **Get Interfaces** or install a policy.

Secure Internal Communication (SIC)

Check Point platforms and products authenticate each other through one of these Secure Internal Communication (SIC) methods:

- Certificates.
- Standards-based TLS for the creation of secure channels.
- 3DES or AES128 for encryption.

  Security Gateways R71 and higher use AES128 for SIC. If one of the Security Gateways is below R71, the Security Gateways use 3DES.

SIC creates trusted connections between Security Gateways, management servers and other Check Point components. Trust is required to install polices on Security Gateways and to send logs between Security Gateways and management servers.

Note - From R81 Jumbo Hotfix Accumulator take 34 and higher, to see SIC errors, examine the `$CPDIR/log/sic_info.elg` file on the Security Management Server and on the Security Gateway.

Initializing Trust

To establish the initial trust, a Security Gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

Note - Make sure the clocks of the Security Gateway and Security Management Server are synchronized, before you initialize trust between them. This is necessary for SIC to succeed. To set the time settings of the Security Gateway and Security Management Server, go to the **Gaia Portal** > **System Management** > **Time**.

To initialize Trust

1. In SmartConsole, open the Security Gateway network object.
2. In the **General Properties** page of the Security Gateway, click **Communication**.
3. In the **Communication** window, enter the **Activation Key** that you created during installation of the Security Gateway.
4. Click **Initialize**.

   The ICA signs and issues a certificate to the Security Gateway.

Trust state is **Initialized but not trusted**. The Internal Certificate Authority (ICA) issues a certificate for the Security Gateway, but does not yet deliver it.

The two communicating peers authenticate over SSL with the shared Activation Key. The certificate is downloaded securely and stored on the Security Gateway. The Activation Key is deleted.

The Security Gateway can communicate with Check Point hosts that have a security certificate signed by the same ICA.

SIC Status

After the Security Gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this Security Gateway:

- **Communicating** - The secure communication is established.
- **Unknown** - There is no connection between the Security Gateway and Security Management Server.
- **Not Communicating** - The Security Management Server can contact the Security Gateway, but cannot establish SIC. A message shows more information.

Trust State

If the Trust State is compromised (keys were leaked, certificates were lost) or objects changed (user leaves, open server upgraded to appliance), reset the Trust State. When you reset Trust, the SIC certificate is revoked.

The Certificate Revocation List (CRL) is updated for the serial number of the revoked certificate. The ICA signs the updated CRL and issues it to all Security Gateways during the next SIC connection. If two Security Gateways have different CRLs, they cannot authenticate.

1. In SmartConsole, from the Gateways & Servers view, double-click the Security Gateway object.
2. Click **Communication**.
3. In the **Trusted Communication** window that opens, click **Reset**.
4. Install Policy on the Security Gateways.

   This deploys the updated CRL to all Security Gateways. If you do not have a Rule Base (and therefore cannot install a policy), you can reset Trust on the Security Gateways.

Important - Before a new trust can be established in SmartConsole, make sure the same one-time activation password is configured on the Security Gateway.

Troubleshooting SIC

If SIC fails to Initialize:

1. Make sure there is connectivity between the Security Gateway and Security Management Server.
2. Make sure that the Security Management Server and the Security Gateway use the same SIC activation key (one-time password).

3. If the Security Management Server is behind a gateway, make sure there are rules that allow connections between the Security Management Server and the remote Security Gateway. Make sure Anti-spoofing settings are correct.
4. Make sure the name and the IP address of the Security Management Server are in the `/etc/hosts` file on the Security Gateway.

   If the IP address of the Security Management Server mapped through static NAT by its local Security Gateway, add the public IP address of the Security Management Server to the `/etc/hosts` file on the remote Security Gateway. Make sure the IP address resolves to the server's hostname.
5. Make sure the date and the time settings of the operating systems are correct. If the Security Management Server and remote the Security Gateway reside in different time zones, the remote Security Gateway may have to wait for the certificate to become valid.
6. Remove the Security Policy on the Security Gateway to let all the traffic through:
   a. Connect to the command line on the Security Gateway
   b. Log in to the Expert mode.
   c. Run:

      ```
      fw unloadlocal
      ```

      Important - See the *R81 CLI Reference Guide* > Chapter *Security Gateway Commands* > Section *fw* > Section *fw unloadlocal*.
7. Try to establish SIC again.

Remote User access to resources and Mobile Access

If you install a certificate on a Security Gateway that has the Mobile Access Software Blade already enabled, you must install the policy again. Otherwise, remote users will not be able to reach network resources.

To establish a new trust state for a Security Gateway

1. Open the command line interface on the Security Gateway.
2. Run:

   cpconfig
3. Enter the number for **Secure Internal Communication** and press Enter.
4. Enter **y** to confirm.
5. Enter and confirm the activation key.
6. When done, enter the number for **Exit**.
7. Wait for Check Point processes to stop and automatically restart.

In SmartConsole:

1. In the **General Properties** window of the Security Gateway, click **Communication**.
2. In the **Trusted Communication** window, enter the one-time password (activation key) that you entered on the Security Gateway.
3. Click **Initialize**.
4. Wait for the **Certificate State** field to show **Trust established**.
5. Click **OK**.

Understanding the Check Point Internal Certificate Authority (ICA)

The ICA (Internal Certificate Authority) is created on the Security Management Server when you configure it for the first time. The ICA issues certificates for authentication:

- **Secure Internal Communication (SIC)** - Authenticates communication between Security Management Servers, and between Security Gateways and Security Management Servers.
- **VPN certificates for gateways** - Authentication between members of the VPN community, to create the VPN tunnel.
- **Users** - For strong methods to authenticate user access according to authorization and permissions.

ICA Clients

In most cases, certificates are handled as part of the object configuration. To control the ICA and certificates in a more granular manner, you can use one of these ICA clients:

- The Check Point Configuration Tool - This is the `cpconfig` CLI utility. One of the options creates the ICA, which issues a SIC certificate for the Security Management Server.
- SmartConsole - SIC certificates for Security Gateways and administrators, VPN certificates, and user certificates.
- *"The ICA Management Tool" on page 350* - VPN certificates for users and advanced ICA operations.

See audit logs of the ICA in SmartConsole **Logs & Monitor** > **New Tab** > **Open Audit Logs View**.

SIC Certificate Management

Manage SIC certificates in the

- **Communication** tab of the Security Gateway properties window.
- *"The ICA Management Tool" on page 350*.

Certificates have these configurable attributes:

Attributes	Default	Comments
validity	5 years	
key size	2048 bits	

Attributes	Default	Comments
KeyUsage	5	Digital Signature and Key encipherment
ExtendedKeyUsage	0 (no KeyUsage)	VPN certificates only

To learn more about key size values, see RSA key lengths.

To view license information for each Software Blade

Step	Instructions
1	Select a Security Gateway or a Security Management Server.
2	In the **Summary** tab below, click the object's **License Status** (for example: **OK**). The **Device & License Information** window opens. It shows basic object information and **License Status**, license **Expiration Date**, and important quota information (in the **Additional Info** column) for each Software Blade. **Notes:** ■ Quota information, quota-dependent license statuses, and blade information messages are only supported for R80 and higher. ■ The tooltip of the SKU is the product name.

The possible values for the Software Blade **License Status** are:

Status	Description
Active	The Software Blade is active and the license is valid.
Available	The Software Blade is not active, but the license is valid.
No License	The Software Blade is active but the license is not valid.
Expired	The Software Blade is active, but the license expired.
About to Expire	The Software Blade is active, but the license will expire in thirty days (default) or less (7 days or less for an evaluation license).
Quota Exceeded	The Software Blade is active, and the license is valid, but the quota of related objects (Security Gateways, Virtual Systems, files, and so on, depending on the blade) is exceeded.
Quota Warning	The Software Blade is active, and the license is valid, but the number of objects of this blade is 90% (default) or more of the licensed quota.
N/A	The license information is not available.

Managing Licenses

After you run the First Time Configuration Wizard on a Security Management Server, and the Security Management Server connects to the User Center, it automatically activates its license . If the Security Management Server loses Internet connectivity before the license is activated, it tries again, on an interval.

If you make changes to Management Software Blade licenses of a Security Management Server in the Check Point User Center, these changes are automatically synchronized with that Security Management Server.

Notes:

- Automatic activation is supported on Check Point appliances only.
- Automatic synchronization is supported on all R80.30 servers and higher.

To make sure that your environment is synchronized with the User Center, even when the Security Management Server is not connected to the Internet, we recommend that you configure a Check Point server with Internet connectivity as a proxy.

Managing Server and Gateway Licenses

Starting from R81, you can add or remove licenses manually in SmartConsole.

Adding and removing a license

Step	Instructions
1	In SmartConsole, from the left navigation panel, click Gateways & Servers.
2	In the top pane, select the object of the applicable Management Server or Security Gateway.
3	In the bottom pane, click the **Licenses** tab.
4	Add or remove a license: ■ To add a license from a license file: a. Click **Add** and select **License File**. b. Browse for the license file. c. Select the license file. d. Click **Open**. ■ To add a license from a license string: a. Click **Add** and select **License String**. b. Paste the license string. c. Click **OK**. ■ To remove a license: a. Select the license in the leftmost column. b. Click **Remove**.

Note - To add or remove licenses on the **Licenses** tab, an administrator must have the **Run One Time Script** permission selected in their profile. To assign this permission, in SmartConsole, go to **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles**. Open the relevant permission profile, go to **Gateways** > **Scripts**, and select **Run One-Time Scripts**.
See also *"Assigning Permission Profiles to Administrators" on page 114*

You can see these columns with license information:

Column	Description
IP Address	The IP address, for which this license was generated.
Expiration Date	Date when the Check Point support contract expires.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.

Important - To distribute licenses to CloudGuard IaaS Security Gateways, see the *R81 CloudGuard Controller Administration Guide*.

Configuring a Proxy Gateway

To configure a proxy on a Check Point server

1. On the Security Management Server, add these lines to `$CPDIR/tmp/.CPprofile.sh`:
   - `_cpprof_add HTTP_CLIENT_PROXY_SICNAME "<proxy server sic name>" 0 0`
   - `_cpprof_add HTTP_CLIENT_PROXY_IP "<proxy server IP>" 0 0`
2. Reboot the Security Management Server.

Viewing Licenses in SmartConsole

To view license information

Step	Instructions
1	From the left navigation panel, click **Gateways & Servers**.
2	From the **Columns** drop-down list, select **Licenses**.

You can see these columns:

Column	Description
License Status	The general state of the Software Blade licenses: ■ **OK** - All the blade licenses are valid. ■ **Not Activated** - Blade licenses are not installed. This is only possible in the first 15 days after the establishment of the SIC with the Security Management Server. After the initial 15 days, the absence of licenses will result in the blade error message. ■ **Error with <number> blade(s)** - The specified number of blade licenses are not installed or not valid. ■ **Warning with <number> blade(s)** - The specified number of blade licenses have warnings. ■ **N/A** - No available information.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.
Account ID	User's account ID.
Support Level	Check Point level of support.
Support Expiration	Date when the Check Point support contract expires.

To view license information for each Software Blade

Step	Instructions
1	Select a Security Gateway or a Security Management Server.
2	In the **Summary** tab below, click the object's **License Status** (for example: **OK**). The **Device & License Information** window opens. It shows basic object information and **License Status**, license **Expiration Date**, and important quota information (in the **Additional Info** column) for each Software Blade. **Notes:** ■ Quota information, quota-dependent license statuses, and blade information messages are only supported for R80 and higher. ■ The tooltip of the SKU is the product name.

The possible values for the Software Blade **License Status** are:

Status	Description
Active	The Software Blade is active and the license is valid.
Available	The Software Blade is not active, but the license is valid.
No License	The Software Blade is active but the license is not valid.

Status	Description
Expired	The Software Blade is active, but the license expired.
About to Expire	The Software Blade is active, but the license will expire in thirty days (default) or less (7 days or less for an evaluation license).
Quota Exceeded	The Software Blade is active, and the license is valid, but the quota of related objects (Security Gateways, files, virtual systems, and so on, depending on the blade) is exceeded.
Quota Warning	The Software Blade is active, and the license is valid, but the number of objects of this blade is 90% (default) or more of the licensed quota.
N/A	The license information is not available.

Viewing license information for VSX:

SmartConsole reports an error when viewing VS Licenses.

To see the VSX license information:

Select the VSG Gateway or VSX Cluster object (and not objects of Virtual Systems or Virtual Routers).

Monitoring Licenses in SmartConsole

To keep track of license issues, you can use these options:

Option	Description
License Status view	To see and export license information for Software Blades on each specific Security Management Server, Security Gateway, or Log Server object.
License Status report	To see filter and export license status information for all configured Security Management Server, Security Gateway, or Log Server objects.
License Inventory report	To see filter and export license information for Software Blades on all configured Security Management Server, Security Gateway, or Log Server objects.

The SmartEvent Software Blade lets you customize the **License Status** and **License Inventory** information from the **Logs & Monitor** view of SmartConsole.

It is also possible to view license information from the **Gateways & Servers** view of SmartConsole without enabling the SmartEvent blade on Security Management Server..

The Gateways & Servers view in SmartConsole lets you see and export the *License Inventory* report.

Step	Instructions
1	View the License Inventory report from the Gateways & Servers view: 1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**. 2. From the top toolbar, click **Actions** > **License Report**. 3. Wait for the **SmartView** to load and show this report. By default, this report contains: ■ *Inventory* page: Blade Names, Devices Names, License Statuses ■ *License by Device* page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date
2	Export the License Inventory report from the Gateways & Servers view: 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

The Logs & Monitor view in SmartConsole lets you see, filter and export the *License Status* report.

Step	Instructions
1	View License Status report from the Logs & Monitor view: 1. In SmartConsole, from the left navigation panel, click **Logs & Monitor** 2. At the top, open a new tab by clicking **New Tab**, or **[+]**. 3. In the left section, click **Views**. 4. In the list of reports, double-click **License Status**. 5. Wait for the **SmartView** to load and show this report. By default, this report contains: ■ Names of the configured objects, License status for each object, CK, SKU, Account ID, Support Level, Next Expiration Date
2	Filter the License Status report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button **> View Filter**. The **Edit View Filter** window opens. 2. Select a **Field** to filter results. For example, **Device Name**, **License Status**, **Account ID**. 3. Select the logical operator - **Equals**, **Not Equals**, or **Contains**. 4. Select or enter a filter value. Note - Click the **X** icon to delete a filter. 5. Optional: Click the **+** icon to configure additional filters. 6. Click **OK** to apply the configured filters. The report is filtered based on the configured filters.
3	Export the License Status report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

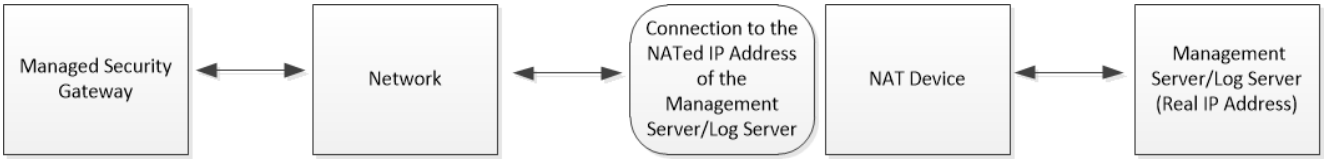
The Logs & Monitor view in SmartConsole lets you see, filter and export the *License Inventory* report.

Step	Instructions
1	View the License Inventory report from the Logs & Monitor view: 1. In SmartConsole, from the left navigation panel, click **Logs & Monitor** 2. At the top, open a new tab by clicking **New Tab**, or **[+]**. 3. In the left section, click **Reports**. 4. In the list of reports, double-click **License Inventory**. 5. Wait for the **SmartView** to load and show this report. By default, this report contains: ■ *Inventory* page: Blade Names, Devices Names, License Statuses ■ *License by Device* page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date
2	Filter the License Inventory report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button **> Report Filter**. The **Edit Report Filter** window opens. 2. Select a **Field** to filter results. For example, **Blade Name**, **Device Name**, **License Overall Status**, **Account ID**. 3. Select the logical operator - **Equals**, **Not Equals**, or **Contains**. 4. Select or enter a filter value. Note - Click the **X** icon to delete a filter. 5. Optional: Click the **+** icon to configure additional filters. 6. Click **OK** to apply the configured filters. The report is filtered based on the configured filters.
3	Export the License Inventory report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

Configuring a Security Gateway to Access the Management Server or Log Server at its NATed IP Address

Starting from R81 Jumbo Hotfix Accumulator Take 13, you can configure a Security Gateway to access the Security Management Server or Log Server at the server's NATed IP address for fetching policy or sending logs.

This diagram describes the flow of this process:



Procedure:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. On a VSX Gateway / each VSX Cluster Member, go to the context of the applicable Virtual System:

   ```
   vsenv <VSID>
   ```

4. Run the applicable command (this change survives reboot):
   a. To force the Security Gateway / Cluster Member to connect only to the **public (NATed)** IP address (this is the default behavior) of the Management Server or Log Server, run:

      ```
      ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 FORCE_NATTED_IP -n 1
      ```

   b. To force the Security Gateway / Cluster Member to connect only to the **real** IP address of the Management Server or Log Server, run:

      ```
      ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 FORCE_NATTED_IP -n 0
      ```

   Notes:
   - This change survives reboot.
   - In a Cluster, you must configure all the Cluster Members in the same way.

5. Restart the FWD process:

   See the instructions in sk97638 > section *Infrastructure Processes*.

Central Deployment of Hotfixes and Version Upgrades

Introduction

Use Central Deployment in SmartConsole to perform batch deployment of:

- Jumbo Hotfix Accumulators and Hotfixes on Security Gateways and Cluster Members.
- Upgrade Packages on Security Gateways and Cluster Members.

You can Deploy a Hotfix or Upgrade Package from:

- The Check Point Cloud.
- The Package Repository on the Management Server.

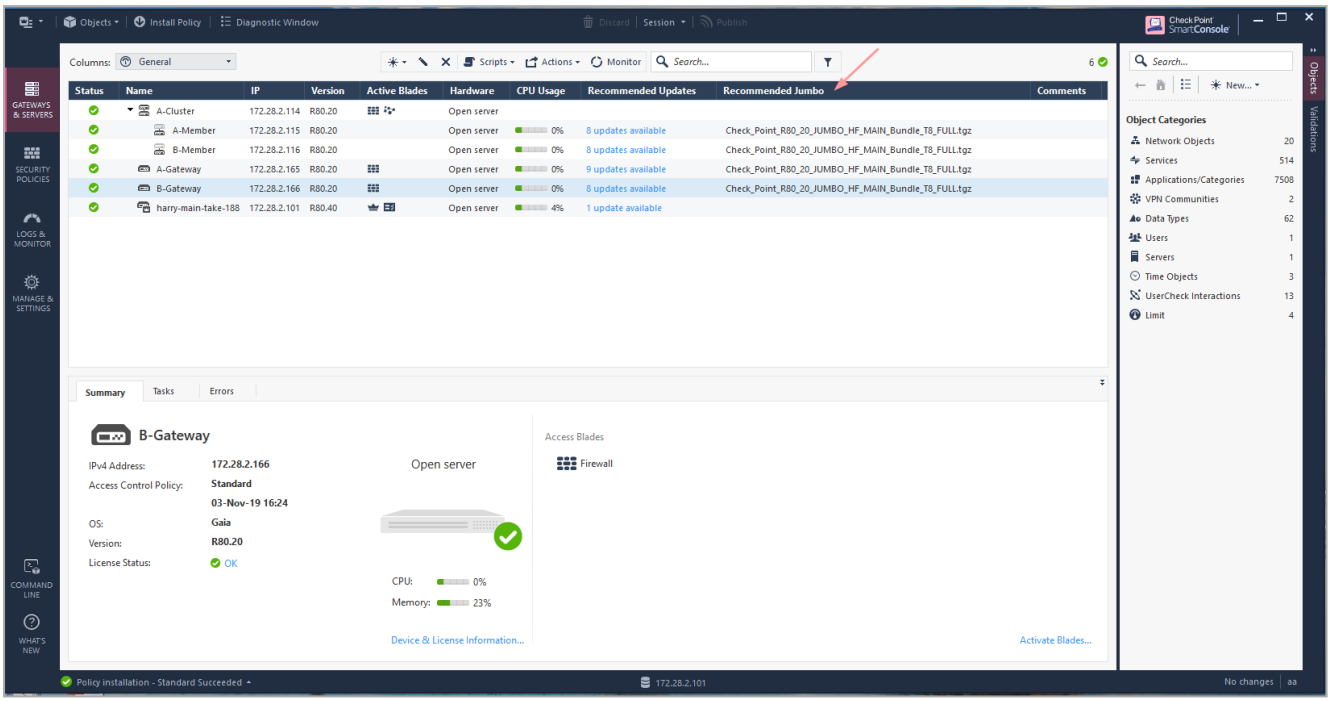
  First, you must upload the applicable package to the Package Repository. See *"Adding a package to the Package Repository" on page 142*.

To use Central Deployment through the API, see the *Check Point Management API Reference*.

> **Best Practice** - Use the Package Repository on the Management Server if the target's connectivity to the Management Server is better than the target's connectivity to the cloud, or if the target is overloaded with traffic.

Note - You can select up to 30 Security Gateways and Cluster Members, but installation can take place only on 10 targets at the same time. The Management Server places each target above the 10th in a queue. Each time an installation completes on one of the targets, the Management Server installs it on the next target in the queue.

Some Security Gateways have Recommended Hotfixes. See the **Recommended Jumbo** column in the **Gateways & Servers** view:



You can deploy a Recommended Jumbo Hotfix Accumulator or a specific Jumbo Hotfix Accumulator take.

Prerequisites

To use Central Deployment:

- The administrator must have the **Manage Licenses and Packages** permissions on the Management Server.
- The latest build of the CPUSE Deployment Agent must be installed on the target Security Gateways and Cluster Members.
- SIC must already be established between the Management Server and the target Security Gateways and Cluster Members.
- A policy must be installed on the target Security Gateways and Cluster Members.
- Only full clusters can be deployed (you cannot select and deploy one cluster member).

To use Central Deployment directly from the Check Point Cloud:

1. The Management Server must be able to connect to the Check Point Cloud.
2. The target Security Gateways and Cluster Members must be able to connect to the Check Point Cloud.

To install the *Recommended* Jumbo Hotfix Accumulator on the target Security Gateways and Cluster Members, at least these Jumbo Hotfix Accumulator takes must be installed:

Target Version	Minimal Jumbo Hotfix Accumulator Take
R80.40 and higher	Any take.
R80.30	Take 76 or higher.
R80.20	A Take higher than Take 118.
R80.10	A Take higher than Take 245.

Important - Central Deployment does not support:

- Connecting from SmartConsole to the Management Server through a proxy server. In this case, use the applicable API command.
- ClusterXL in Load Sharing mode.
- VRRP Cluster.
- Standalone server.
- Scalable Chassis 40000 / 60000.
- Centrally Managed Quantum Spark Appliances running Gaia Embedded operating system.
- Standby Security Management Server.
- On Multi-Domain Servers, SmartConsole connected to the Global Domain, or the Multi-Domain Server context.

Installation

Adding a package to the Package Repository

1. From the left navigation panel, click **Manage & Settings**.
2. From the left tree, click **Package Repository**.
3. Click **New** and select one of these options:
   - **Download from cloud** - To download the package to the Package Repository from the Check Point Cloud, enter the package name and click **Download**.
   - **Upload from local** - To upload the package to the Package Repository from your device, browse to the applicable package and click **Open**.

   After the download or upload is complete, the package appears in the **Package Repository** window in SmartConsole > **Manage & Settings** view.

Note - Add packages to the repository one at a time

Installing a Hotfix or Upgrade Package on multiple Security Gateways or Cluster Members

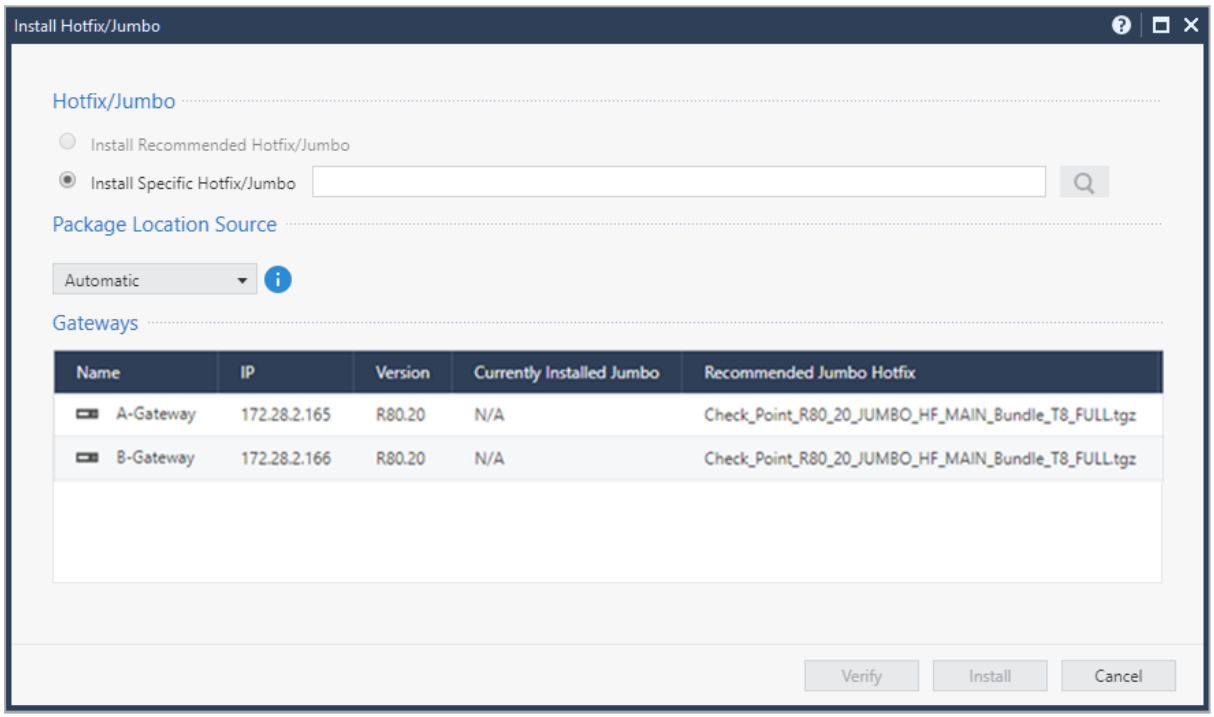
1. From the left navigation panel, click **Gateways & Servers**.
2. Select the target Security Gateways or Cluster Members for deployment.

   To select multiple targets, press and hold the **CTRL** key.

   To upgrade Cluster Members, select the cluster object.
3. From the toolbar menu, click **Actions** (⮌) and select one of these options:
   - **Install Hotfix/Jumbo**
   - **Version Upgrade**

   The **Install Hotfix** or **Version Upgrade** window opens, and shows Information about the selected targets and their corresponding recommended Hotfix or Upgrade Package.

   Example:



4. Select one of these options:
   - **Install Recommended Hotfix/Jumbo** or

     Upgrade to Recommended Major Version

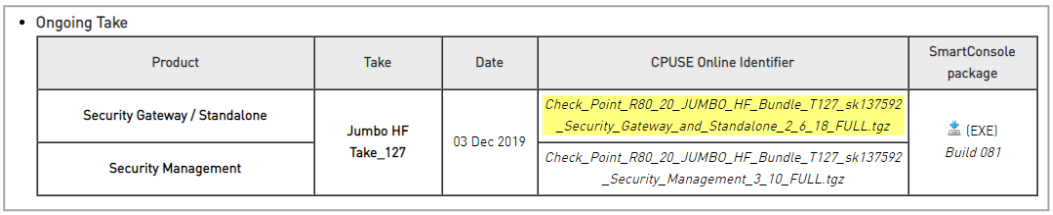
     Note - If there is no recommended Jumbo Hotfix Accumulator for the selected targets, this option is grayed out.
     If a recommended Jumbo Hotfix Accumulator applies only to some of the selected targets, the deployment takes place only for those targets.

- **Install Specific Hotfix/Jumbo** or

  Upgrade to Specific Major Version

  a. Enter the version number / Hotfix file name. You can copy the Hotfix file name from the applicable SK article to the **Install Specific Hotfix** text box.

  Example:



- Ongoing Take

Product	Take	Date	CPUSE Online Identifier	SmartConsole package
Security Gateway / Standalone	Jumbo HF Take_127	03 Dec 2019	Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592_Security_Gateway_and_Standalone_2_6_18_FULL.tgz	(EXE) Build 081
Security Management			Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592_Security_Management_3_10_FULL.tgz	

  b. Click the search icon next to the text box:

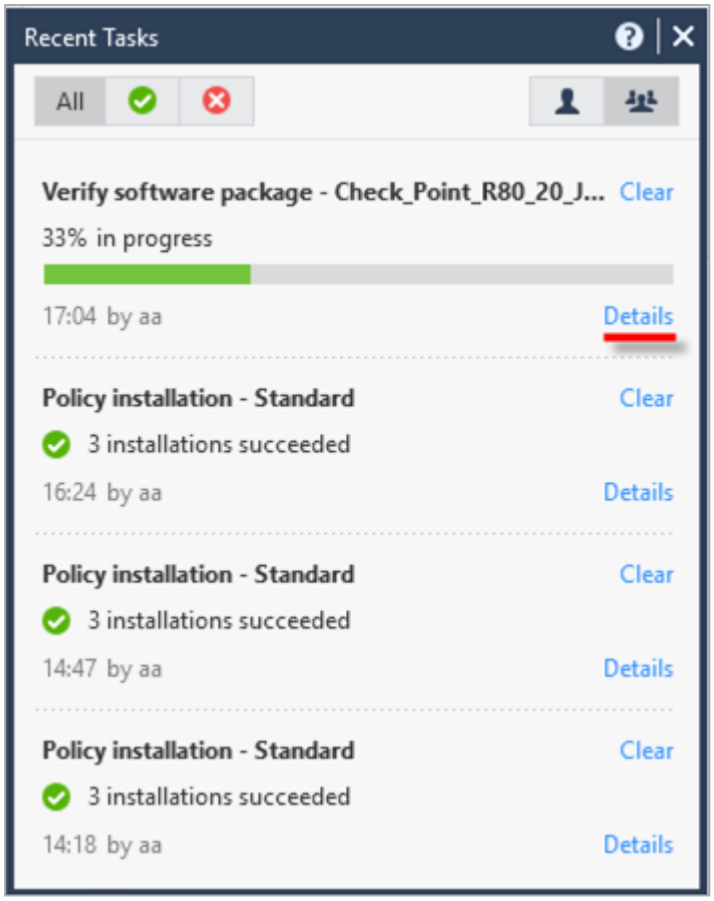
  This process makes sure that the package is available for download from the Check Point servers.

5. Select the **Package Location Source**:
   - **Gateway** - The package is downloaded from the Check Point Cloud.
   - **Management** - The package is uploaded from the Package Repository.
   - **Automatic** - If the package is in the Package Repository, it is downloaded from the Package Repository. If the package is not in the Package Repository, the package is downloaded from the Check Point Cloud.
6. Click **Verify**.

   The **Install Hotfix** or **Upgrade Version** window is minimized, and the verification process starts. The verification process makes sure that the selected Hotfix Take or Upgrade Package can be installed on the targets. The verification process checks other installed Hotfixes are not overridden and that enough free disk space is available for the process to complete.

   To see the progress of the verification process open the **Tasks** view in the bottom left corner of SmartConsole and click **Details**.

   Example:



7. Repeat steps 1-6.
8. Click **Install**.
9. Central Deployment verifies that Access Control Policy is installed.
10. After the installation is complete, you must install the applicable Threat Prevention policy on the target Security Gateways and Clusters

Note - If different targets have different recommended Hotfixes or Upgrade Packages, each target gets its applicable recommended Hotfix or Upgrade Package.

How the Central Deployment Upgrades a Cluster

When you use the Central Deployment to install a software package on a ClusterXL in High Availability mode or VSX Cluster (non-VSLS), the Central Deployment follows these steps:

1. Verifies that the states of the Cluster Members are valid (Active and Standby).
2. Prepares the Access Control Policy for the Cluster:
   a. Changes the version in the Cluster object.
   b. Changes the applicable configuration settings and Access Control Policy.
3. Upgrades the Standby Cluster Member to the new version.
4. Runs a Full Connectivity Upgrade:

   a. Makes sure the upgraded Cluster Member is in the Standby or Ready state.
   b. Performs cluster failover to one of the upgraded Cluster Members.
5. Upgrades the former Active Cluster Member.
6. Verifies that the states of the Cluster Members are valid (Active and Standby).

Configuring Implied Rules or Kernel Tables for Security Gateways

Introduction

An administrator configures Security Policy and other inspection settings in SmartConsole.

During a policy installation, the Management Server creates the applicable files and transfers them to the target Security Gateways.

The Management Server creates these files based on:

- Security Policy in SmartConsole
- Global properties in SmartConsole
- Security Gateway properties
- Multiple configuration files on the Management Server that control the inspection of various network protocols

It is possible to modify these configuration files on the Management Server to fine-tune the inspection in your network (in Check Point INSPECT language).

There are two main categories of these configuration files:

- Files for Security Gateways that have the same software version as the Management Server.
- Files for Security Gateways that have the a lower software version than the Management Server. This category is called "Backward Compatibility".

Configuration files

File Name	Controls	Location
`user.def`	User-defined implied rules.	See *"Location of 'user.def' Files on the Management Server" on page 150*
`implied_rules.def`	Default implied rules.	See *"Location of 'implied_rules.def' Files on the Management Server" on page 151*
`table.def`	Definitions of various kernel tables.	See *"Location of 'table.def' Files on the Management Server" on page 152*
`crypt.def`	VPN encryption macros.	See *"Location of 'crypt.def' Files on the Management Server" on page 153*

File Name	Controls	Location
`vpn_table.def`	Definitions for various kernel tables that hold VPN data. For example, VPN timeouts, number of VPN tunnels, whether a specific kernel table should be synchronized between cluster members, and others.	See *"Location of 'vpn_ table.def' Files on the Management Server" on page 154*
`communities.def`	VPN encryption macros for X11 server (X Window System) traffic.	See *"Location of 'communities.def' Files on the Management Server" on page 155*
`base.def`	Definitions of packet inspection for various network protocols.	See *"Location of 'base.def' Files on the Management Server" on page 156*
`dhcp.def`	Definitions of packet inspection for DHCP traffic - DHCP Request, DHCP Reply, and DHCP Relay.	See *"Location of 'dhcp.def' Files on the Management Server" on page 157*
`gtp.def`	Definitions of packet inspection for GTP (GPRS Tunnelling Protocol) traffic.	See *"Location of 'gtp.def' Files on the Management Server" on page 158*

Configuration Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Back up the current file:

   ```
   cp -v /<Full Path to File>/<File Name>{,_BKP}
   ```

   Example:

   ```
   cp -v $FWDIR/conf/user.def.FW1{,_BKP}
   ```

4. Edit the current file:

   ```
   vi /<Full Path to File>/<File Name>
   ```

   Example:

   ```
   vi $FWDIR/conf/user.def.FW1
   ```

5. Make the applicable changes as described in the applicable SK article, or as instructed by Check Point Support.
6. Save the changes in the file and exit the editor.
7. Connect with SmartConsole to the Security Management Server.
8. In SmartConsole, install the Access Control Policy on the applicable Security Gateway or Cluster object.

Location of 'user.def' Files on the Management Server

The '`user.def`' files contain the user-defined implied rules.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/conf/user.def.FW1`
R80.40	`$FWDIR/conf/user.def.R8040CMP`
R80.30SP on Maestro	`$FWDIR/conf/user.def.R8040CMP`
R80.30	`$FWDIR/conf/user.def.R8040CMP`
R80.20SP on Maestro, or Chassis	`$FWDIR/conf/user.def.R8040CMP`
R80.20	`$FWDIR/conf/user.def.R8040CMP`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`$FWDIR/conf/user.def.SFWCMP`
R80.10	`$FWDIR/conf/user.def.R8040CMP`
R77.30	`$FWDIR/conf/user.def.R77CMP`
R77.20.x on 1100, 1200R, 1400 Appliances	`$FWDIR/conf/user.def.SFWR77CMP`

Location of 'implied_rules.def' Files on the Management Server

The '`implied_rules.def`' files contain the default implied rules.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/implied_rules.def`
R80.40	`/opt/CPR8040CMP-R81/lib/implied_rules.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/implied_rules.def`
R80.30	`/opt/CPR8040CMP-R81/lib/implied_rules.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/implied_rules.def`
R80.20	`/opt/CPR8040CMP-R81/lib/implied_rules.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/implied_rules.def`
R80.10	`/opt/CPR8040CMP-R81/lib/implied_rules.def`
R77.30	`/opt/CPR77CMP-R81/lib/implied_rules.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/implied_rules.def`

Location of 'table.def' Files on the Management Server

The '`table.def`' files contain definitions of various kernel tables for Security Gateways.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/table.def`
R80.40	`/opt/CPR8040CMP-R81/lib/table.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/table.def`
R80.30	`/opt/CPR8040CMP-R81/lib/table.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/table.def`
R80.20	`/opt/CPR8040CMP-R81/lib/table.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/table.def`
R80.10	`/opt/CPR8040CMP-R81/lib/table.def`
R77.30	`/opt/CPR77CMP-R81/lib/table.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/table.def`

Location of 'crypt.def' Files on the Management Server

The '`crypt.def`' files contain VPN encryption macros.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/crypt.def`
R80.40	`/opt/CPR8040CMP-R81/lib/crypt.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/crypt.def`
R80.30	`/opt/CPR8040CMP-R81/lib/crypt.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/crypt.def`
R80.20	`/opt/CPR8040CMP-R81/lib/crypt.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/crypt.def`
R80.10	`/opt/CPR8040CMP-R81/lib/crypt.def`
R77.30	`/opt/CPR77CMP-R81/lib/crypt.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/crypt.def`

Location of 'vpn_table.def' Files on the Management Server

The '`vpn_table.def`' files contain definitions for various kernel tables that hold VPN data.

For example, VPN timeouts, number of VPN tunnels, whether a specific kernel table should be synchronized between cluster members, and others.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/vpn_table.def`
R80.40	`/opt/CPR8040CMP-R81/lib/vpn_table.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/vpn_table.def`
R80.30	`/opt/CPR8040CMP-R81/lib/vpn_table.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/vpn_table.def`
R80.20	`/opt/CPR8040CMP-R81/lib/vpn_table.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/vpn_table.def`
R80.10	`/opt/CPR8040CMP-R81/lib/vpn_table.def`
R77.30	`/opt/CPR77CMP-R81/lib/vpn_table.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/vpn_table.def`

Location of 'communities.def' Files on the Management Server

The '`communities.def`' files contain VPN encryption macros for X11 server (X Window System) traffic.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/communities.def`
R80.40	`/opt/CPR8040CMP-R81/lib/communities.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/communities.def`
R80.30	`/opt/CPR8040CMP-R81/lib/communities.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/communities.def`
R80.20	`/opt/CPR8040CMP-R81/lib/communities.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/communities.def`
R80.10	`/opt/CPR8040CMP-R81/lib/communities.def`
R77.30	`/opt/CPR77CMP-R81/lib/communities.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/communities.def`

Location of 'base.def' Files on the Management Server

The '`base.def`' files contain definitions of packet inspection for various network protocols.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/base.def`
R80.40	`/opt/CPR8040CMP-R81/lib/base.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/base.def`
R80.30	`/opt/CPR8040CMP-R81/lib/base.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/base.def`
R80.20	`/opt/CPR8040CMP-R81/lib/base.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/base.def`
R80.10	`/opt/CPR8040CMP-R81/lib/base.def`
R77.30	`/opt/CPR77CMP-R81/lib/base.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/base.def`

Location of 'dhcp.def' Files on the Management Server

The '`dhcp.def`' files contain definitions of packet inspection for DHCP traffic - DHCP Request, DHCP Reply, and DHCP Relay.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/dhcp.def`
R80.40	`/opt/CPR8040CMP-R81/lib/dhcp.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/dhcp.def`
R80.30	`/opt/CPR8040CMP-R81/lib/dhcp.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/dhcp.def`
R80.20	`/opt/CPR8040CMP-R81/lib/dhcp.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/dhcp.def`
R80.10	`/opt/CPR8040CMP-R81/lib/dhcp.def`
R77.30	`/opt/CPR77CMP-R81/lib/dhcp.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/dhcp.def`

Location of 'gtp.def' Files on the Management Server

The '`gtp.def`' files contain definitions of packet inspection for GTP (GPRS Tunnelling Protocol) traffic.

Location of files on an R81 Security Management Server:

Version of the Target Security Gateway	Location of the File
R81	`$FWDIR/lib/gtp.def`
R80.40	`/opt/CPR8040CMP-R81/lib/gtp.def`
R80.30SP on Maestro	`/opt/CPR8040CMP-R81/lib/gtp.def`
R80.30	`/opt/CPR8040CMP-R81/lib/gtp.def`
R80.20SP on Maestro, or Chassis	`/opt/CPR8040CMP-R81/lib/gtp.def`
R80.20	`/opt/CPR8040CMP-R81/lib/gtp.def`
R80.20.x on 1530, 1550, 1570, 1590 Appliances	`/opt/CPSFWR80CMP-R81/lib/gtp.def`
R80.10	`/opt/CPR8040CMP-R81/lib/gtp.def`
R77.30	`/opt/CPR77CMP-R81/lib/gtp.def`
R77.20.x on 1100, 1200R, 1400 Appliances	`/opt/CPSFWR77CMP-R81/lib/gtp.def`

Managing Objects

Network Objects, defined in SmartConsole and stored in the proprietary Check Point object database, represent physical and virtual network components (such as Security Gateways, servers, and users), and logical components (such as IP address ranges and Dynamic Objects). Before you create Network Objects, analyze the needs of your organization:

- What are the physical components of your network: devices, hosts, Security Gateways and their active Software Blades?
- What are the logical components: services, resources, applications, ranges?
- Who are the users? How should you group them, and with what permissions?

Object Categories

Objects in SmartConsole represent networks, devices, protocols and resources. SmartConsole divides objects into these categories:

Icon	Object Type	Examples
	Network Objects	Security Gateways, hosts, networks, address ranges, dynamic objects, security zones
	Services	Services, Service groups
	Custom Applications/Sites	Applications, Categories, Mobile applications
	VPN Communities	Site to Site or Remote Access communities
	Users	Users, user groups, and user templates
	Data Types	International Bank Account Number - IBAN, HIPAA - Medical Record Number - MRN, Source Code.
	Servers	Trusted Certificate Authorities, RADIUS, TACACS
	Time Objects	Time, Time groups
	UserCheck Interactions	Message windows: Ask, Cancel, Certificate Template, Inform, and Drop

Icon	Object Type	Examples
	Limit	Download and upload bandwidth  **Important** : After policy installation, a bandwidth limit is not enforced on a connection that is matched to an Access Control rule with the Action "**Limit**" in one of these scenarios: ■ The '**Keep all connections**' option is selected in the security object ■ The '**Keep connections open after the policy has been installed**' option is selected in the Service object used in this rule

Actions with Objects

You can add, edit, delete, and clone objects. A clone is a copy of the original object, with a different name. You can also replace one object in the Policy with another object.

Note - Do not create two objects with the same name. A validation error shows when you try to publish the SmartConsole session. To resolve, change one of the object names.

To work with objects, right-click the object in the object tree or in the Object Explorer, and select the action.

You can delete objects that are not used, and you can find out where an object is used.

To clone an object

1. In the object tree or in the Object Explorer, right-click the object and select **Clone**.

   The **Clone Object** window opens.
2. Enter a name for the cloned object.
3. Click **OK**.

To find out where an object is used

In the object tree or in the Object Explorer, right-click the object and select **Where Used**.

To replace an object with a different object

1. In the object tree or in the Object Explorer, right-click the object and select **Where Used**.
2. Click the **Replace** icon.
3. From the **Replace with** list, select an item.
4. Click **Replace**.

To delete all instances of an object

1. In the object tree or in the Object Explorer, right-click the object and select **Where Used**.
2. Click the **Replace** icon.
3. From the **Replace with** list, select **None (remove item)**.
4. Click **Replace**.

Object Tags

Object tags are keywords or labels that you can assign to the network objects or groups of objects for search purposes. These are the types of tags you can assign:

- User tags - Assigned manually to individual objects or groups of objects
- System tags - Predefined keywords, such as "application"

Each tag has a name and a value. The value can be static, or dynamically filled by detection engines.

Adding a Tag to an Object

To add a tag to an object

1. Open the network object for editing.
2. In the **Add Tag** field, enter the label to associate with this object.
3. Press **Enter**.

   The new tag shows to the right of the **Add Tag** field.
4. Click **OK**.

Network Object Types

Networks

A Network is a group of IP addresses defined by a network address and a net mask. The net mask indicates the size of the network.

A Broadcast IP address is an IP address which is destined for all hosts on the specified network. If this address is included, the Broadcast IP address will be considered as part of the network.

Network Groups

A network group is a collection of hosts, gateways, networks, or other groups. Groups can be used to facilitate and simplify network management. When you have the same set of objects which you want to use in different places in the Rule Base, you can create a group to include such set of objects and reuse it. Modifications are applied to the group instead of to each member of the group.

Groups are also used where SmartConsole lets you select only one object, but you need to work with more than one. For example, in the Security Gateway object > **Network Management** > **VPN Domain** > **Manually defined**, you can only select on object from the drop-down menu. If you want to select more than one object for your VPN Domain, you can create a group, add the required objects to the group, and select the group from the drop-down menu.

Grouping Network Objects

To create a group of network objects

1. In the **Objects** tree, click **New** > **Network Group**.

   The **New Network Group** window opens.
2. Enter a name for the group
3. Set optional parameters:
   - Object comment
   - Color
   - Tag (as custom search criteria)
4. For each network object you want to add, click the [**+**] sign and select it from the list that shows.
5. Click **OK**.

From version R80.20.M2, you can also associate groups to a network object directly from the object editor.

To associate groups to a network object

1. Open the object editor, and go to **Groups** in the navigation tree.
2. For each group you want to add, click the [**+**] sign and select it from the list that shows.

Check Point Hosts

A Check Point Host can have multiple interfaces but no routing takes place. It is an endpoint that receives traffic for itself through its interfaces. (In comparison, a Security Gateway routes traffic between its multiple interfaces.) For example, if you have two unconnected networks that share a common Security Management Server and Log Server, configure the common server as a Check Point Host object.

A Check Point Host has one or more Software Blades installed. But if the Firewall blade is enabled on the Check Point Host, it cannot function as a Security Gateway. The Host requires SIC and other features provided by the actual Security Gateway.

A Check Point Host has no routing mechanism, is not capable of IP forwarding, and cannot be used to implement Anti-Spoofing. If the host must do any of these, convert it to be a Security Gateway.

The Security Management Server object is a Check Point Host.

Note - When you upgrade a Management Server from R77.30 or earlier versions, Node objects are converted to Host objects.

Gateway Cluster

A cluster is a group of Security Gateways defined as one logical object. Clustered gateways add redundancy through High Availability or Load Sharing.

Address Ranges

An address range is a range of IP addresses on the network, defined by the lowest and the highest IP addresses. Use an Address Range object when you cannot define a range of IP addresses by a network IP and a net mask. The Address Range objects are also necessary for the implementation of NAT and VPN.

Wildcard Objects

Wildcard objects let you define IP address objects that share a common pattern that can be permitted or denied access in a security policy.

Note - This feature is only supported for R80.20 and above gateways.

To create a new wildcard object

1. Open **Object Explorer** > **New** > **More** > **Network Object** > **Wildcard object**.
2. Enter the Wildcard IP address and Wildcard Netmask in IPv4 or IPv6 Format.
3. Click **OK**.

Understanding Wildcard Objects

The wildcard object contains a wildcard IP address and a wildcard netmask.

The *wildcard netmask* is the mask of bits that indicate which parts of the IP address must match and which do not have to match. For example:

Wildcard IP:	194.	29.	0.	1
Wildcard Netmask:	0.	0.	3.	0

The third octet represents the mask of bits. If we convert the 3 to binary, we get 00000011.

The 0 parts of the mask must match the equivalent bits of the IP address.

The 1 parts of the mask do not have to match, and can be any value.

0 0 0 0 0 0	1 1
Must match the equivalent bits in the IP address	Do not have to match

The binary netmask produces these possible decimal values:

128	64	32	16	8	4	2	1	
						Binary		**Decimal**
0	0	0	0	0	0	0	0	**0**

0	0	0	0	0	0	0	1		1
0	0	0	0	0	0	1	0		2
0	0	0	0	0	0	1	1		3

The netmask permits only these IP addresses:

- 194.29.0.1
- 194.29.1.1
- 192.29.2.1
- 194.29.3.1

Examples of Use Cases

Scenario One

A supermarket chain has all of its cash registers on subnet 194.29.x.1, where x defines the region. In this use case, all the cash registers in this region must have access to the database server at 194.30.1.1.

Instead of defining 256 hosts (194.29.0.1, 194.29.1.1, 194.29.2.1....194.29.255.1), the administrator creates a wildcard object that represents all the cash registers in the region:

Wildcard IP:	194.	29.	0.	1
Wildcard Mask:	0.	0.	255.	0

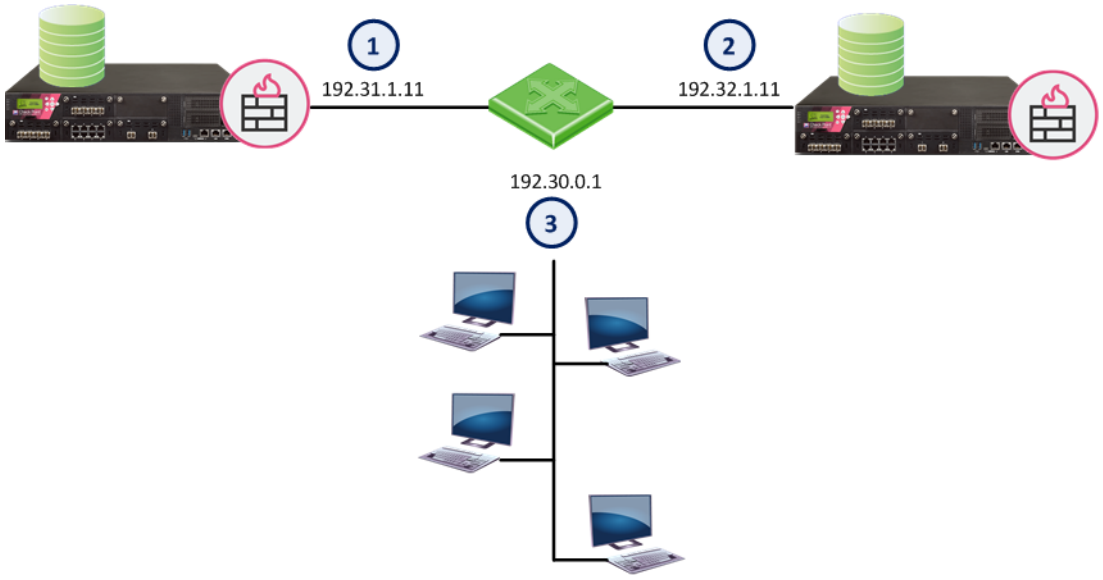
The wildcard object can now be added to the Access Control Policy.

Source	Destination	Action	Track
Wildcard Object	Database server object	Accept	Log

Scenario Two

In this use case, a supermarket chain has stores in Europe and Asia.

The 192.30.0-255.1 network contains both the Asian and European regions, and the stores within those regions.



Item	Description
1	Database Server for Europe
2	Database Server for Asia
3	European and Asia network

The administrator wants stores in the European and Asia regions to access different database servers. In this topology, the third octet of the European and Asia network's IP address will be subject to a wildcard. The first four bits of the wildcard will represent the region and the last four bits will represent the store number.

Bits that represent the region	Bits that represent the store number
0000	0000

In the Wildcard IP:

- The Asia region is represented by **0001xxxx** (Region **1** in decimal)
- The European region is represented by **0010xxxx** (Region **2** in decimal)

In binary:

Binary		Decimal
Region	**Store**	
0001	0000	16 - Asia Region
0010	0000	32 - European Region

To include all the stores of a particular region, the last four bits of the wildcard mask must be set to 1 (15 in Decimal):

Binary		Decimal

Region	Store	
xxxx	1111	15 - all Asian stores
xxxx	1111	15 - all European stores

A wildcard object that represents all the Asian stores will look like this:

Wildcard IP address	192.30.16.1	(The region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30.**16-31**.1

A wildcard object that represents all the European stores will look like this:

Wildcard IP address	192.30.32.1	(the region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30.**32-47**.1

The administrator can now use these wildcard objects in the Access Control Policy:

Source	Destination	Action	Track
Asian Stores Wildcard	Database Server for Asia	Accept	Log
European Stores Wildcard	Database Server for Europe	Accept	Log

Scenario Three

In this scenario, the netmask bits are not consecutive.

Wildcard IP	1	1	0	1
Wildcard mask	0	0	5	0

Wildcard IP	00000001.00000001.00000000.00000001
Wildcard Mask	00000000.00000000.00000101.00000000

Mask:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0

Which will match only these IP addresses:

IP Address	Binary	Comment
1.1.0.1	00000001.00000001.00000000.00000001	The IP address itself

IP Address	Binary	Comment
1.1.1.1	00000001.00000001.00000001.00000001	The equivalent bit at position 23 does not matter
1.1.4.1	00000001.00000001.00000100.00000001	The equivalent bit at position 21 does not matter
1.1.5.1	00000001.00000001.00000101.00000001	The equivalent bits at positions 21 and 23 do not matter

IPv6

The same principles apply to IPv6 addresses. For example, if the wildcard object has these values:

IPv6 Address	2001::1:10:0:1:41
Wildcard netmask	0::ff:0:0

The wildcard will match: 2001::1:10:0-255:1:41

Domains

A Domain object lets you define a host or DNS domain by its name only. It is not necessary to have the IP address of the site.

You can use the Domain object in the source and destination columns of an Access Control Policy.

You can configure a Domain object in two ways:

- Select **FQDN**

  In the object name, use the Fully Qualified Domain Name (FQDN). Use the format `.x.y.z` (with a dot "." before the FQDN). For example, if you use `.www.example.com` then the Gateway matches `www.example.com`

  This option is supported for R80.10 and higher, and is the default. It is more accurate and faster than the non-FQDN option.

The Security Gateway looks up the FQDN with a direct DNS query, and uses the result in the Rule Base.

This option supports SecureXL Accept templates. Using domain objects with this option in a rule has no effect on the performance of the rule, or of the rules that come after it.

- Clear **FQDN**

This option enforces the domain and its sub-domains. In the object name, use the format `.x.y` for the name. For example, use `.example.com` or `.example.co.uk` for the name. If you use `.example.com`, then the Gateway matches `www.example.com` and `support.example.com`

The Gateway does the name resolution using DNS reverse lookups, which can be inaccurate. The Gateway uses the result in the Rule Base, and caches the result to use again.

When upgrading from R77, this option is enforced.

Updatable Objects

An updatable object is a network object which represents an external service, such as Office 365, AWS, GEO locations and more. External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically on the Security Gateway each time the provider changes a list. There is no need to install policy for the updates to take effect. You can use updatable objects in all three types of policies: Access Control, Threat Prevention and HTTPS Inspection. You can use an updatable object in the Access Control, Threat Prevention or the HTTPS Inspection policy as a source or a destination. In the Threat Prevention policy, you can also use an updatable object as the protected scope.

These are the currently supported external services for updatable objects:

- Online services - Office 365, Azure, and AWS
- GEO locations - The GEO database provides mapping of location data to IP addresses. For each location, there is a network object you can import to SmartConsole. You can block or allow access to and from specific locations based on their IP addresses.

Note - For Access Control, this feature is supported for R80.20 and above gateways. For Threat Prevention and HTTPS Inspection, this feature is supported for R80.40 and above gateways.

Adding an Updatable Object to the Security Policy

A customer uses Office365 and wants to allow access to Microsoft Exchange services.

To add the Microsoft Exchange Updatable Object to the Security Gateway

1. Make sure the Security Management Server and the Security Gateway have access to the Check Point cloud.
2. Go to SmartConsole > Security Policies > **Access Control** > **Policy**.
3. Create a new rule.
4. In the Destination column, click the + sign and select **Import** > **Updatable Objects**.

   The **Updatable Objects** window opens.
5. Select the objects to add. For this use case, select the **Exchange Services** object.

   Note - You can also add objects to the **Source** column.
6. Click **OK**.
7. Install policy.

The Exchange Services object is added to the Rule Base.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Accept Exchange	WirelessZone	Exchange Services	Any	Any	Accept	Log

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
2	Accept Exchange	Exchange Services	WirelessZone	Any	Any	Accept	Log

You can monitor the updates in the **Logs & Monitor > Logs** view.

To monitor the updates

1. Go to SmartConsole > **Logs & Monitor**.
2. From the search bar, enter Updatable Objects.
3. Double-click the relevant log.

   The **Log Details** window shows.
4. `Succeeded` shows in the **Status** field when the update is successful.

Dynamic Objects

A dynamic object is a "logical" object where the IP address is resolved differently for each Security Gateway, using the `dynamic_objects` command.

For Security GatewaysR80.10 and higher, dynamic objects support SecureXL Accept templates. Therefore, there is no performance impact on a rule that uses a dynamic object, or on rules that come after it.

Dynamic Objects are predefined for **LocalMachine-all-interfaces**. The DAIP computer interfaces (static and dynamic) are resolved into this object.

Generic Data Center Objects

From R81, you can enforce access to and from IP addresses defined in files located in external web servers.

To do that, use the Generic Data Center object in SmartConsole. The Generic Data Center object points to a JSON file in an external server which contains the IP addresses which you want to access. This way, when the Generic Data Center object is used in a policy, SmartConsole can retrieve the IP information from the JSON file as necessary.

You can host the JSON file also locally on the Security Management Server.

This feature is useful in cases where one administrator creates the Rule Base and defines the objects, and another administrator manages the content of these objects.

This feature is supported in the Access Control, Threat Prevention, HTTPS Inspection, and NAT Rule Bases.

The feature is supported only on a Security Management Server R81 and higher and Security Gateway (Cluster) R81 and higher.

After you create the Generic Data Center object, any change made in the file is automatically enforced on the Security Gateway with no need to install policy.

To create the JSON file, follow the guidelines described in sk167210.

Using the Generic Data Center object in a Security Policy

1. In SmartConsole, go to the Object Explorer and click **New** > **More** > **Cloud** > **Data Center** > **Generic Data Center**.

   The **New Generic Data Center** object window opens.

2. Configure these fields:

   a. **URL** - Enter the URL of the JSON file.

   b. **Interval** - Enter the internal at which the file is sampled.

      The default interval is 60 seconds.

   c. **Add Custom Header** - If you need to add a custom header to the request to the server, select this checkbox and enter the **Key** and **Value**.

   d. Click **Test Connection** to make sure you can access the file.

3. Add the applicable Generic Data Center object to your Rule Base:

   In the **Source** or **Destination** column, click **Import** > **Data Center** > **Generic Data Center**, and select the applicable data center object from the list.

   Note - The list contains all the data center objects included in you JSON file.

4. **Install Policy**.

Limitations

- You can make up to 15,000 changes in a JSON file between two time intervals at which the JSON file is sampled.
- The number of generic data center objects + dynamic objects + updatable objects in all policy packages cannot exceed 2,000.

Security Zones

Security Zones let you to create a strong Access Control Policy that controls the traffic between parts of the network.

A Security Zone object represents a part of the network (for example, the internal network or the external network). You assign a network interface of a Security Gateway to a Security Zone. You can then use the Security Zone objects in the Source and Destination columns of the Rule Base.

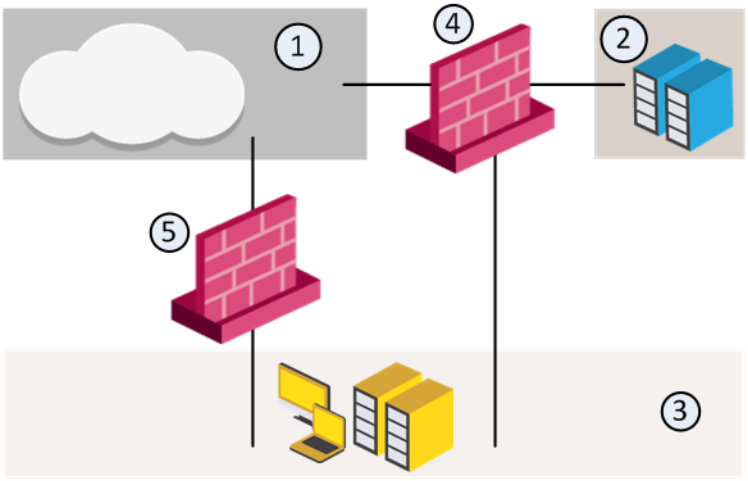
Use Security Zones to:

- Simplify the Policy. Apply the same rule to many Gateways.
- Add networks to Gateways interfaces without changing the Rule Base.

For example, in the diagram, we have three Security Zones for a typical network: *ExternalZone* (1), *DMZZone* (2) and *InternalZone* (3).

- Gateway (4) has three interfaces. One interface is assigned to *ExternalZone* (1), one interface is assigned to *DMZZone* (2), and one interface is assigned to *InternalZone* (3).

- Gateway (5) has two interfaces. One interface is assigned to *ExternalZone* (1) and one interface is assigned to *InternalZone* (3).



A Security Gateway interface can belong to only one Security Zone. Interfaces to different networks can be in the same Security Zone.

Workflow

1. Define Security Zone objects. Or, use the predefined Security Zones (see *"Predefined Security Zones" on the next page*).
2. Assign Gateway interfaces to Security Zones (see *"Creating and Assigning Security Zones" below*).
3. Use the Security Zone objects in the Source and Destination of a rule. For example:

Source	Destination	VPN	Service	Action
InternalZone	ExternalZone	Any Traffic	Any	Accept

4. Install the Access Control Policy (see *"Installing the Access Control Policy" on page 230*).

Creating and Assigning Security Zones

Before you can use Security Zones in the Rule Base, you must assign Gateway interfaces to Security Zones.

To create a Security Zone

1. In the **Objects bar** (F11), click **New** > **More** > **Network Object** > Security Zone.

   The **Security Zone** window opens.
2. Enter a name for the Security Zone.
3. Enter an optional comment or tag.
4. Click **OK**.

To assign an interface to a Security Zone

1. In the Gateways & Servers view, right-click a Security Gateway object and select **Edit**.

   The **Gateway Properties** window opens.

2. In the **Network Management** pane, right-click an interface and select **Edit**.

   The **Interface** window opens. The **Topology** area of the **General** pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface **Leads To**.

3. Click **Modify**.

   The **Topology Settings** window opens.

4. In the Security Zone area, click **User Defined** and select **Specify Security Zone**.

5. From the drop-down box, select a Security Zone.

   Or click **New** to create a new one.

6. Click **OK**.

Predefined Security Zones

These are the predefined Security Zones, and their intended purposes:

- **WirelessZone** - Networks that can be accessed by users and applications with a wireless connection.
- **ExternalZone** - Networks that are not secure, such as the Internet and other external networks.
- **DMZZone** - A DMZ (demilitarized zone) is sometimes referred to as a *perimeter* network. It contains company servers that can be accessed from external sources.

  A DMZ lets external users and applications access specific internal servers, but prevents the external users accessing secure company networks. Add rules to the Security Gateway Rule Base that allow traffic to the company DMZ. For example, a rule that allows HTTP and HTTPs traffic to your web server in the DMZ.
- **InternalZone** - Company networks with sensitive data that must be protected and used only by authenticated users.

Externally Managed Gateways and Hosts

An Externally Managed Security Gateway or a Host is a gateway or a Host which has Check Point software installed on it. This Externally Managed gateway is managed by an external Security Management Server. While it does not receive the Check Point Security Policy Security Policy, it can participate in Check Point VPN communities and solutions.

Interoperable Devices

An Interoperable Device is a device that has no Check Point Software Blades installed.

The Interoperable Device:

- Cannot have a policy installed on it
- Can participate in Check Point VPN communities and solutions.

VoIP Domains

There are five types of VoIP Domain objects:

- VoIP Domain SIP Proxy
- VoIP Domain H.323 Gatekeeper

- VoIP Domain H.323 Gateway
- VoIP Domain MGCP Call Agent
- VoIP Domain SCCP Call Manager

In many VoIP networks, the control signals follow a different route through the network than the media. This is the case when the call is managed by a *signal routing* device. Signal routing is done in SIP by the *Redirect Server*, *Registrar*, and/or *Proxy*. In SIP, signal routing is done by the *Gatekeeper* and/or *Gateway*.

Enforcing signal routing locations is an important aspect of VoIP security. It is possible to specify the endpoints that the signal routing device is allowed to manage. This set of locations is called a *VoIP Domain*. For more information, see the *R81 VoIP Administration Guide*.

Logical Servers

A Logical Server is a group of machines that provides the same services. The workload of this group is distributed between all its members.

When a Server group is stipulated in the **Servers group** field, the client is bound to this physical server. In Persistent server mode the client and the physical server are bound for the duration of the session.

- Persistency by Service - once a client is connected to a physical server for a specified service, subsequent connection to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.
- Persistency by Server - once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

Balance Method

The load balancing algorithm stipulates how the traffic is balanced between the servers. There are several types of balancing methods:

- **Server Load** - The Security Gateway determines which Security Management Server is best equipped to handle the new connection.
- **Round Trip Time** - On the basis of the shortest round trip time between Security Gateway and the servers, executed by a simple ping, the Security Gateway determines which Security Management Server is best equipped to handle the new connection.
- **Round Robin** - the new connection is assigned to the first available server.
- **Random** - the new connection is assigned to a server at random.
- Domain - the new connection is assigned to a server based on domain names.

Open Security Extension (OSE) Devices

The Open Security Extension features let you manage third-party devices with the Check Point SmartConsole. The number of managed devices, both hardware and software packets, depends on your license. OSE devices commonly include hardware security devices for routing or dedicated Network Address Translation and Authentication appliances. Security devices are managed in the Security Policy as Embedded Devices.

The Security Management Server generates Access Lists from the Security Policy and downloads them to selected routers and open security device. Check Point supports these devices:

OSE Device	Supported Versions
Cisco Systems	9.x, 10.x, 11.x, 12.x

The Check Point Rule Base must not have these objects. If it does, the Security Management Server does not generate Access Lists.

- Drop (in the Action column)
- Encrypt (Action)
- Alert (Action)
- RPC (Service)
- ACE (Service)
- Authentication Rules
- Negate Cell

Defining OSE Device Interfaces

OSE devices report their network interfaces and setup at boot time. Each OSE device has a different command to list its configuration. You must define at least one interface for each device, or **Install Policy** will fail.

To define an OSE Device

1. From the Object Explorer, click **New** > **More**.
2. Click Network **Object** > **More** > **OSE Device**.
3. Enter the general properties (see *"OSE Device Properties Window - General Tab" below*).

   We recommend that you also add the OSE device to the host lists on other servers: `hosts` (Linus) and `lmhosts` (Windows).
4. Open the **Topology** tab and add the interfaces of the device.

   You can enable Anti-Spoofing on the external interfaces of the device. Double-click the interface. In the **Interface Properties** window > **Topology** tab, select **External** and **Perform Anti-Spoofing**.
5. Open the **Setup** tab and define the OSE device and its administrator credentials (see *"Anti-Spoofing Parameters and OSE Devices Setup (Cisco)" on the next page*).

OSE Device Properties Window - General Tab

- **Name** - The name of the OSE device, as it appears in the system database on the server.
- **IP Address** -The device's IP address.
- **Get Address** - Click this button to resolve the name to an address.
- **Comment** - Text to show on the bottom of the **Network Object** window when this object is selected.
- **Color** - Select a color from the drop-down list. The OSE device will be represented in the selected color in SmartConsole, for easier tracking and management.
- **Type** - Select from the list of supported vendors.

Anti-Spoofing Parameters and OSE Devices Setup (Cisco)

For Cisco (Version 10.x and higher) devices, you must specify the direction of the filter rules generated from anti-spoofing parameters. The direction of enforcement is specified in the **Setup** tab of each router.

For Cisco routers, the direction of enforcement is defined by the **Spoof Rules Interface Direction** property.

Access List No - The number of Cisco access lists enforced. Cisco routers Version 12x and below support an ACL number range from 101-200. Cisco routers Version 12x and above support an ACL range number from 101-200 and also an ACL number range from 2000-2699. Inputting this ACL number range enables the support of more interfaces.

For each credential, select an option:

- **None** - Credential is not needed.
- **Known** - The administrator must enter the credentials.
- **Prompt** - The administrator will be prompted for the credentials.

Username - The name required to logon to the OSE device.

Password - The Administrator password (Read only) as defined on the router.

Enable Username - The user name required to install Access Lists.

Enable Password - The password required to install Access Lists.

Version - The Cisco OSE device version (9.x, 10.x, 11.x, 12.x).

OSE Device Interface Direction - Installed rules are enforced on data packets traveling in this direction on all interfaces.

Spoof Rules Interface Direction - The spoof tracking rules are enforced on data packets traveling in this direction on all interfaces.

Managing Policies

SmartConsole offers a number of tools that address policy management tasks, both at the definition stage and for maintenance.

At the definition stage:

- *Policy Packages* let you group different types of policies, to be installed together on the same installation targets.
- *Predefined Installation Targets* let you associate each package with a set of gateways. You do not have to repeat the gateway selection process each time you install a Policy Package.

At the maintenance level:

- *Search* gives versatile search capabilities for network objects and the rules in the Rule Base.
- *Database version control* lets you track past changes to the database.

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules:
  - Firewall
  - NAT
  - Application & URL Filtering
  - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
  - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
  - Threat Emulation - Detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox
  - Threat Extraction- Extracts potentially malicious content from e-mail attachments before they enter the corporate network
- **HTTPS Inspection** - Consists of rules to inspect traffic encrypted by the Transport Layer Security (TLS) protocol between internal browser clients and web servers.

Important - Legacy SmartDashboard does not show the QoS and Desktop policies when an administrator with read-only permissions is logged in, and the "Desktop Security" policy is enabled in the policy package.

The installation process:

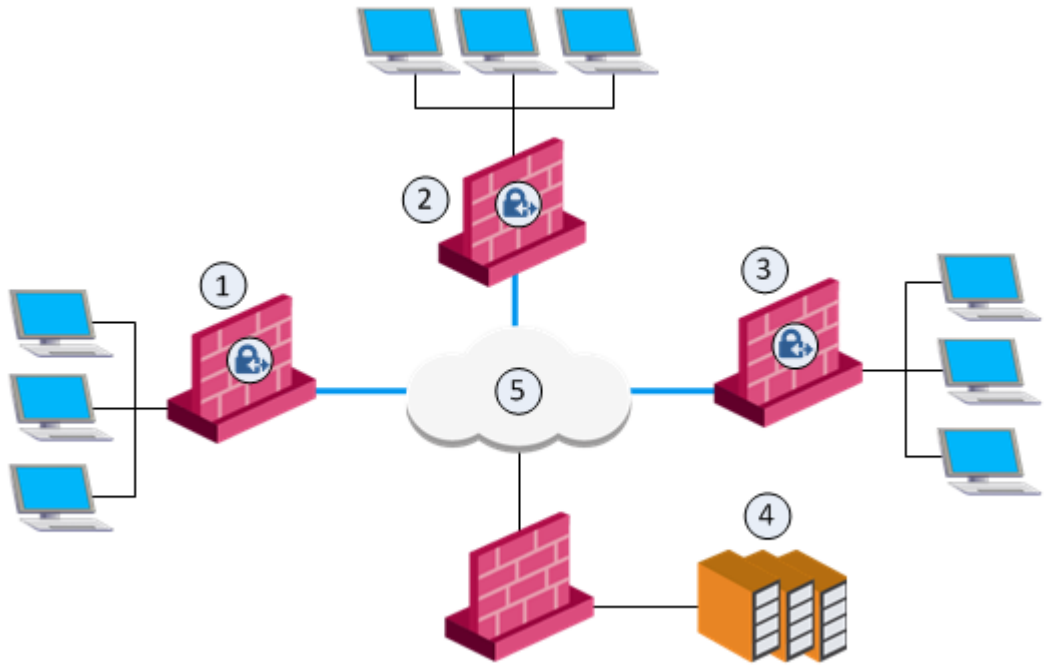
- Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

  If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.
- Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced.
- Distributes the user database and object database to the selected installation targets.

You can create different policy packages for different types of sites in an organization.

Example

An organization has four sites, each with its own requirements. Each site has a different set of Software Blades installed on the Security Gateways:



Item	Security Gateway	Installed Software Blades
1	Sales California	Firewall, VPN
2	Sales Alaska	Firewall, VPN, IPS, DLP
3	Executive management	Firewall, VPN, QoS, and Mobile Access
4	Server farm	Firewall

Item	Security Gateway	Installed Software Blades
5	Internet	

To manage these different types of sites efficiently, you need to create three different Policy Packages . Each Package includes a combination of policy types that correspond to the Software Blades installed on the site's Security Gateway. For example:

- A policy package that includes the Access Control policy type. The Access Control policy type controls the firewall, NAT, Application & URL Filtering, and Content Awareness Software Blades. This package also determines the VPN configuration.

  Install the Access Control policy package on *all* Security Gateways.

- A policy package that includes the QoS policy type for the QoS blade on Security Gateway that manages bandwidth.

  Install this policy package on the *executive management* Security Gateway.

- A policy package that includes the Desktop Security Policy type for the Security Gateway that handles Mobile Access.

  Install this policy package on the *executive management* Security Gateway.

Creating a New Policy Package

1. From the Menu, select **Manage policies and layers**.

   The **Manage policies and layers** window opens.

2. Click **New**.

   The **New Policy** window opens.

3. Enter a name for the policy package.

4. In the **General** page > **Policy types** section, select one or more of these policy types:

   - **Access Control & HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**

   To see the **QoS**, and **Desktop Security** policy types, enable them on one or more Gateways:

   Go to gateway editor > **General Properties** > **Network Security** tab:

   - For QoS, select **QoS**
   - For Desktop Security, select **IPSec VPN** and **Policy Server Pol**

5. On the **Installation targets** page, select the gateways the policy will be installed on:

   - **All gateways**
   - **Specific gateways** - For each gateway, click the [**+**] sign and select it from the list.

   To install Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets.

6. Click **OK**.

7. Click **Close**.

   The new policy shows on the **Security Policies** page.

Adding a Policy Type to an Existing Policy Package

1. From the Menu, select **Manage policies and layers**.

   The **Manage policies and layers** window opens.
2. Select a policy package and click the **Edit** button.
3. The **New Policy** package window opens.
4. On the **General** > **Policy types** page, select the policy type to add:
   - **Access Control & HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**
5. Click **OK**.

Installing a Policy Package

1. On the Global Toolbar, click **Install Policy**.

   The **Install Policy** window opens and shows the installation targets (Security Gateways).
2. From the **Select a policy** menu, select a policy package.
3. Select one or more policy types that are available in the package.
4. Select the **Install Mode**:
   - **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target gateways.

     Note - If you select **For Gateway clusters install on all the members, if fails do not install at all**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.
5. Click **Install**.

Installing the User Database

When you make changes to user definitions through SmartConsole, they are saved to the user database on the Security Management Server. User authentication methods and encryption keys are also saved in this database. The user database does **not** contain information about users defined externally to the Security Gateway (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the Security Management Server.

You must choose to install the policy or the user database, based on the changes you made:

- Install the policy, if you modified additional components of the Policy Package (for example, added new Security Policy rules) that are used by the installation targets
- Install the user database, if you only changed the user definitions or the administrator definitions - from the Menu, select **Install Database**

The user database is installed on:

- Security Gateways - during policy installation
- Check Point hosts with one or more Management Software Blades enabled - during database installation

You can also install the user database on Security Gateways and on a remote server, such as a Log Server, from the command line interface on the Security Management Server.

To install user database from the command line interface:

On the Security Management Server, run in the Expert mode:

```
fwm dbload <Main IP address of Name of Security Gateway Object>
```

For more information, see the *R81 CLI Reference Guide* - Chapter *Security Management Server Commands* - Section *fwm* - Sub-section *fwm dbload*.

Note - Check Point hosts that do not have active Management Software Blades do not get the user database installed on them.

Uninstalling a Policy Package

You can uninstall a policy package through a command line interface on the gateway.

To uninstall a policy package

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Run:

   ```
   fw unloadlocal
   ```

Warning

- The "`fw unloadlocal`" command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the Security Gateway (Cluster Member).
- The "`fw unloadlocal`" command removes all policies from the Security Gateway (Cluster Member). This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

For more information, see the *R81 CLI Reference Guide* - Chapter *Security Gateway Commands* - Section *fw* - Sub-section *fw unloadlocal*.

Viewing Rule Logs

You can search for the logs that are generated by a specific rule, from the Security Policy or from the Logs & Monitor > **Logs** tab.

To see logs generated by a rule (from the Security Policy)

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Logs** - By default, shows the logs for the *Current Rule*. You can filter them by **Source**, **Destination**, **Blade**, **Action**, **Service**, **Port**, **Source Port**, **Rule** (**Current rule** is the default), **Origin**, **User**, or **Other Fields**.
   - **History** (Access Control Policy only) - List of rule operations (Audit logs) related to the rule in chronological order, with the information about the rule type and the administrator that made the change.

To see logs generated by a rule (by Searching the Logs)

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. Right-click the rule number and select **Copy Rule UID**.
4. In the Logs & Monitor > **Logs** tab, search for the logs in one of these ways:
   - Paste the Rule UID into the query search bar and press Enter.
   - For faster results, use this syntax in the query search bar:

     ```
     layer_uuid_rule_uuid:*_<UID>
     ```

     For example, paste this into the query search bar and press Enter:

     ```
     layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10
     ```

Policy Installation History

How to work with the policy installation history

In the Installation History you can choose a Security Gateway, a date and time when the Policy was installed, and:

- See the revisions that were installed on the Security Gateway and who installed the Policy.
- See the changes that were installed and who made the changes.
- Revert to a specific version, and install the last "good" Policy.

To work with the Policy installation history:

1. In SmartConsole, go to **Security Policies**.
2. From the **Access Tools** or the **Threat Prevention Tools**, select **Installation History**.
3. In the **Gateways** section, select a Security Gateway.
4. In the **Policy Installation History** section, select an installation date.
5. Perform the applicable action:
   - **To see the revisions that were installed and who made them**:

     Click **View installed changes**.
   - **To see the changes that were installed and who made them :**

     Click **View**.
   - **To revert to a specific version of the policy:**

     Click **Install specific version**.

Concurrent Install Policy

Starting from R81, one administrator or more can run *different* policy installation tasks on multiple gateways at the same time. In earlier versions, you can only run the *same* policy installation task on multiple gateways at the same time.

Concurrent Install Policy only supports the Access Control and Threat Prevention policies. It does not support the Desktop and QoS policies.

The maximum number of policy installation tasks (of different policies) that can run at the same time is 5. If more than 5 policy installation requests are sent, any request beyond the first 5 gets in a queue.

The running and the queued tasks appear in the **Recent Tasks** window at the bottom left of your screen.

Note - In the first installation, you cannot install both the Access Control and Threat Prevention policies on the same gateway at the same time. You must install one and then the other.

Accelerated Install Policy

R81 introduces the Accelerated Install Policy feature for the Access Control policy. When the Access Control policy installation is accelerated, the installation duration is decreased significantly.

Policy installation is accelerated depending on the changes that were made to the Access Control policy since the last installation.

For example, creating a Host object and adding it to an Access Control rule triggers *accelerated* policy installation.

For more information about accelerated install policy and a detailed list on the events that trigger accelerated policy installation, see sk169096.

Creating an Access Control Policy

Introducing the Unified Access Control Policy

Define one, unified Access Control Policy. The Access Control Policy lets you create a simple and granular Rule Base that combines all these Access Control features:

- Firewall - Control access to and from the internal network.
- Application & URL Filtering - Block applications and sites.
- Content Awareness - Restrict the Data Types that users can upload or download.
- IPsec VPN and Mobile Access - Configure secure communication with Site-to-Site and Remote Access VPN.
- Identity Awareness - Identify users, computers, and networks.

There is no need to manage separate Rule Bases. For example, you can define one, intuitive rule that: Allows users in specified networks, to use a specified application, but prevents downloading files larger than a specified size. You can use all these objects in one rule:

- Security Zones
- Services
- Applications and URLs
- Data Types
- Access Roles

Information about these features is collected in one log:

- Network
- Protocol
- Application
- User
- Accessed resources
- Data Types

The Columns of the Access Control Rule Base

The Columns of the Access Control Rule Base

These are the columns of the rules in the Access Control policy. Not all of these are shown by default. To select a column that does not show, right-click on the header of the Rule Base, and select it.

Column	Description
No	Rule number in the Rule Base Layer.
Hits	Number of times that connections match a rule (see *"Analyzing the Rule Base Hit Count" on page 232*).
Name	Name that the system administrator gives this rule.
Source **Destination**	Network objects that define ■ Where the traffic starts ■ The destination of the traffic (see *"Source and Destination Column" on the next page*)
VPN	The VPN Community to which the rule applies. (see *"VPN Column" on the next page*).
Services & Applications	Services, Applications, Categories, and Sites. If Application & URL Filtering is not enabled, only Services show. (see *"Services & Applications Column" on page 186*)
Content	The data asset to protect, for example, credit card numbers or medical records. You can set the direction of the data to Download Traffic (into the organization), Upload Traffic (out of the organization), or Any Direction. (see *"Content Column" on page 189*)
Action	Action that is done when traffic matches the rule. Options include: Accept, Drop, Ask, Inform (UserCheck message), Inline Layer, and Reject. (see *"Actions" on page 190*)
Track	Tracking and logging action that is done when traffic matches the rule. (see *"Tracking Column" on page 193*)
Install On	Network objects that will get the rule(s) of the policy. (see *"Installing the Access Control Policy" on page 230*)
Time	Time period that this rule is enforced.
Comment	An optional field that lets you summarize the rule.

Source and Destination Column

In the Source and Destination columns of the Access Control Policy Rule Base, you can add Network objects including groups of all types. Here are some of the network objects you can include:

- Network (see *"Networks" on page 161* and *"Network Groups" on page 161*)
- Host
- Zones (see *"Security Zones" on page 170*)
- Dynamic Objects (see *"Dynamic Objects" on page 169*)
- Domain Objects (see *"Domains" on page 167*)
- Access Roles
- Updatable Objects (see *"Updatable Objects" on page 168*)

To Learn More About Network Objects

You can add network objects to the **Source** and **Destination** columns of the Access Control Policy. See *"Managing Objects" on page 159*.

VPN Column

You can configure rules for Site-to-Site VPN, Remote Access VPN, and the Mobile Access Portal and clients.

To make a rule for a VPN Community, add a Site-to-Site Community or a Remote Access VPN Community object to this column, or select **Any** to make the rule apply to all VPN Communities.

When you enable Mobile Access on a Security Gateway, the Security Gateway is automatically added to the Remote Access VPN Community. Include that Community in the **VPN** column of the rule or use **Any** to make the rule apply to Mobile Access Security Gateways. If the Security Gateway was removed from the VPN Community, the **VPN** column must contain **Any**.

IPsec VPN

The IPsec VPN solution lets the Security Gateway encrypt and decrypt traffic to and from other Security Gateways and clients. Use SmartConsole SmartConsole to easily configure VPN connections between Security Gateways and remote devices.

For Site-to-Site Communities, you can configure Star and Mesh topologies for VPN networks, and include third-party gateways.

The VPN tunnel guarantees:

- Authenticity - Uses standard authentication methods
- Privacy - All VPN data is encrypted
- Integrity - Uses industry-standard integrity assurance methods

IKE and IPsec

The Check Point VPN solution uses these secure VPN protocols to manage encryption keys, and send encrypted packets. IKE (Internet Key Exchange) is a standard key management protocol that is used to create the VPN tunnels. IPsec is protocol that supports secure IP communications that are authenticated and encrypted on private or public networks.

Mobile Access to the Network

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the **Mobile Application** in the **Services & Applications** column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the **Source** column of a rule.

To Learn More About VPN

To learn more about Site-to-Site VPN and Remote Access VPN, see these guides:

- *R81 Site to Site VPN Administration Guide*
- *R81 Remote Access VPN Administration Guide*
- *R81 Mobile Access Administration Guide*

Services & Applications Column

In the **Services & Applications** column of the Access Control Rule Base, define the applications, sites, and services that are included in the rule. A rule can contain one or more:

- Services
- Applications
- Mobile Applications for Mobile Access
- Web sites
- Default categories of Internet traffic
- Custom groups or categories that you create, that are not included in the Check Point Application Database.

Service Matching

The Security Gateway identifies (*matches*) a service according to *IP protocol*, TCP and UDP *port number*, and *protocol signature*.

To make it possible for the Security Gateway to match services by protocol signature, you must enable **Application & URL Filtering** on the Security Gateway and on the Ordered Layer. (see *"Enabling Access Control Features" on page 212*).

You can configure TCP and UDP services to be matched by *source port*.

Application Matching

If an application is *allowed* in the policy, the rule is matched only on the **Recommended** services of the application. This default setting is more secure than allowing the application on all services. For example: a rule that allows Facebook, allows it only on the Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.

If an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can change the default match settings for applications.

Configuring Matching for an Allowed Application

You can configure how a rule matches an application or category that is *allowed* in the policy. You can configure the rule to match the application in one of these ways:

- On any service
- On a specified service

To do this, change the **Match Settings** of the application or category. The application or category is changed everywhere that it is used in the policy.

To change the matched services for an allowed application or category:

1. In a rule which has applications or categories in the **Services & Applications** column, double-click an application or category.
2. Select **Match Settings**.
3. Select an option:
   - The default is **Recommended** services. The defaults for Web services are the Application Control **Web Browsing Services**.
   - To match the application with all services, click **Any**.
   - To match the application on specified services, click **Customize**, and add or remove services.
   - To match the application with all services and exclude specified services, click **Customize**, add the services to exclude, and select **Negate**.
4. Click **OK**.

Configuring Matching for Blocked Applications

By default, if an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can configure the matching for blocked applications so that they are matched on the recommended services. For Web applications, the recommended services are the *Application Control Web browsing services*.

If the match settings of the application are configured to **Customize**, the blocked application is matched on the customized services service. *It is not matched on all ports.*

To configure matching for blocked applications:

1. In SmartConsole, go to **Manage & Settings** > **Blades** > **Application & URL Filtering** > **Advanced Settings** > **Application Port Match**
2. Configure **Match application on 'Any' port when used in 'Block' rule**:
   - Selected - This is the default. If an application is *blocked* in the Rule Base, the application is matched to *Any* port.
   - Not selected - If an application is *blocked* in the Rule Base, the application is matched to the services that are configured in the application object of the application. However, some applications are still matched on Any. These are applications (Skype, for example) that do not limit themselves to a standard set of services.

Summary of Application Matching in a "Block" Rule

Application - Match Setting	Checkbox: Match web application on 'Any' port when used in 'Block' rule	Blocked Application is Matched on Service
Recommended services (default)	Selected (default)	Any
Recommended services (default)	Not selected	Recommended services
Customize	*Not relevant*	Customized
Any	*Not relevant*	Any

Adding Services, Applications, and Sites to a rule

You can add services, applications and sites to a rule.

Note - Rules with applications or categories do not apply to connections from or to the Security Gateway.

To add services, applications or sites to a rule:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. To add applications to a rule, select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.
4. Search for the services, sites, applications, or categories.
5. Click the **+** next to the ones you want to add.

Creating Custom Applications, Categories, and Groups

You can create custom applications, categories or groups, which are not included in the Check Point Application Database.

To create a new application or site:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.

   The Application viewer window opens.
4. Click **New** > **Custom Applications/Site** > **Application/Site**.
5. Enter a name for the object.
6. Enter one or more URLs.

   If you used a regular expression in the URL, click **URLs are defined as Regular Expressions**.

   Note - If the application or site URL is defined as a regular expression you must use the correct syntax.
7. Click **OK**.

To create a custom category

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.

   The Application viewer window opens.
4. Click **New** > **Custom Applications/Site** > **User Category**.
5. Enter a name for the object.
6. Enter a description for the object.
7. Click **OK**.

Services and Applications on R77.30 and Lower Security Gateways, and after Upgrade

For Security Gateways R77.30 and lower:

- The Security Gateway matches TCP and UDP services by *port* number. The Security Gateway cannot match services by protocol signature.
- The Security Gateway matches applications by the application signature.

When you upgrade the Security Management Server to R80 and higher and the Security Gateways to R80.10 and higher, this change of behavior occurs:

- Applications that were defined in the Application & URL Filtering Rule Base are accepted on their recommended ports

Content Column

You can add Data Types to the Content column of rules in the Access Control Policy.

To use the Content column, you must enable **Content Awareness**, in the General Properties page of the Security Gateway, and on the Layer.

A Data Type is a classification of data. The Security Gateway classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

You can set the direction of the data in the Policy to **Download Traffic** (into the organization), **Upload Traffic** (out of the organization), or **Any Direction**.

There are two kinds of Data Types: *Content Types* (classified by analyzing the file content) and *File Types* (classified by analyzing the file ID).

Content Type examples:

- PCI - credit card numbers
- HIPAA - Medical Records Number - MRN
- International Bank Account Numbers - IBAN
- Source Code - JAVA
- U.S. Social Security Numbers - According to SSA
- Salary Survey Terms

File type examples:

- Viewer File - PDF
- Executable file
- Database file
- Document file
- Presentation file
- Spreadsheet file

Note these limitations:

- Websocket content is not inspected.
- HTTP connections that are not RFC-compliant are not inspected.

To learn more about the Data Types, open the Data Type object in SmartConsole and press the **?** button (or **F1** key) to see the Help.

Note - Content Awareness and Data Loss Prevention (DLP) both use Data Types. However, they have different features and capabilities. They work independently, and the Security Gateway enforces them separately.

To learn more about DLP, see the *R81 Data Loss Prevention Administration Guide*.

Actions

Action	Meaning
Accept	Accepts the traffic

Action	Meaning
Drop	Drops the traffic. The Security Gateway does not send a response to the originating end of the connection and the connection eventually does a time-out. If no UserCheck object is defined for this action, no page is displayed.
Ask	Asks the user a question and adds a confirmatory check box, or a reason box. Uses a UserCheck object.
Inform	Sends a message to the user attempting to access the application or the content. Uses a UserCheck object.
To see these actions, right-click and select More:	
Reject	Rejects the traffic. The Security Gateway sends an RST packet to the originating end of the connection and the connection is closed.
UserCheck Frequency	Configure how often the user sees the configured message when the action is ask, inform, or block.
Confirm UserCheck	Select the action that triggers a UserCheck message: ■ **Per rule** - UserCheck message shows only once when traffic matches a rule. ■ **Per category** - UserCheck message shows for each matching category in a rule. ■ **Per application/Site** - UserCheck message shows for each matching application/site in a rule. ■ **Per Data type** - UserCheck message shows for each matching data type.
Limit	Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for uploads and downloads. **Important** : After policy installation, a bandwidth limit is not enforced on a connection that is matched to an Access Control rule with the Action "**Limit**" in one of these scenarios: ■ The '**Keep all connections**' option is selected in the security object ■ The '**Keep connections open after the policy has been installed**' option is selected in the Service object used in this rule

Action	Meaning
Enable Identity Captive Portal	Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.
	 **Important** - A rule that drops traffic, with the **Source** and **Destination** parameters defined as **Any**, also drops traffic to and from the Captive Portal.

UserCheck Actions

UserCheck lets the Security Gateways send messages to users about possible non-compliant or dangerous Internet browsing. In the Access Control Policy, it works with URL Filtering, Application Control, and Content Awareness. (You can also use UserCheck in the Data Loss Prevention Policy, in SmartConsole). Create UserCheck objects and use them in the Rule Base, to communicate with the users. These actions use UserCheck objects:

- **Inform**
- **Ask**
- **Drop**

UserCheck on a Security Gateway

When UserCheck is enabled, the user's Internet browser shows the UserCheck messages in a new window.

You can enable UserCheck on Security Gateways that use:

- Access Control features:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention features:
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
  - Threat Extraction
- Data Loss Prevention

UserCheck on a computer

The UserCheck client is installed on endpoint computers. This client:

- Sends messages for applications that are not based on Internet browsers, such as Skype and iTunes, and Internet browser add-ons and plug-ins.
- Shows a message on the computer when it cannot be shown in the Internet browser.

Tracking Column

These are some of the **Tracking** options:

- **None** - Do not generate a log.
- **Log** -This is the default **Track** option. It shows all the information that the Security Gateway used to match the connection.
- **Accounting** - Select this to update the log at 10 minute intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

To Learn More About Tracking

To learn more about Tracking options, see the *R81 Logging and Monitoring Administration Guide*.

Rule Matching in the Access Control Policy

The Security Gateway determines the rule to apply to a connection. This is called *matching* a connection. Understanding how the Security Gateway matches connections will help you:

- Get better performance from the Rule Base.
- Understand the logs that show a matched connection.

Examples of Rule Matching

These example Rule Bases show how the Security Gateway matches connections.

Note that these Rule Bases intentionally do not follow the best practices for Access Control Rules (see *"Best Practices for Access Control Rules" on page 228*). This is to make the explanations of rule matching clearer.

Rule Base Matching - Example 1

For this Rule Base:

No	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	ftp-pasv	Download executable file	Drop
2	Any	Any	Any	Executable file	Accept
3	Any	Any	Gambling (Category)	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure for an FTP connection:

Part of connection	Security Gateway action	Inspection result
SYN	Run the Rule Base: Look for the first rule that matches: ■ Rule 1 - Match.	Final match (drop on rule 1). Shows in the log. The Security Gateway does not turn on the inspection engines for the other rules.

Rule Base Matching - Example 2

For this Rule Base:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (category)	Any	Drop
3	Any	Any	ftp	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure when browsing to a file sharing Web site. Follow the rows from top to bottom. Follow each row from left to right:

Part of connection	Security Gateway action	Inspection result
SYN	Run the Rule Base. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - Possible match. ■ Rule 3 - No match. ■ Rule 4 - Match.	Possible match (Continue to inspect the connection).
HTTP Header	The Security Gateway turns on inspection engines to examine the data in the connection. In this example turn on the: ■ URL Filtering engine - Is it a gambling site? ■ Content Awareness engine - Is it an executable file?	Application: File sharing (category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - No match. ■ Rule 3 - No match. ■ Rule 4 - Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Data: PDF file.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - No match. ■ Rule 2 - No match. ■ Rule 3 - No match. ■ Rule 4 - Match.	Final match (accept on rule 4). Shows in the log.

Rule Base Matching - Example 3

For this Rule Base:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (Category)	Any	Drop
3	Any	Any	Any	Any	Accept

This is the matching procedure when downloading an executable file from a business Web site. Follow the rows from top to bottom. Follow each row from left to right:

Part of connection	Security Gateway action	Inspection result
SYN	Run the Rule Base. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - Possible match. ■ Rule 3 - Match.	Possible match (Continue to inspect the connection).
HTTP Header	The Security Gateway turns on inspection engines to examine the content in the connection. In this example turn on the: ■ URL Filtering engine - Is it a gambling site? ■ Content Awareness engine - Is it an executable file?	Application: Business (Category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - No match. ■ Rule 3 - Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Content: Executable file.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Match. ■ Rule 2 - No match. ■ Rule 3 - Match.	Final match (accept on rule 1). Shows in the log.

The matching examples show that:

- The Security Gateway sometimes runs the Rule Base more than one time. Each time it runs, the Security Gateway optimizes the matching, to find the first rule that applies to the connection.
- If the rule includes an application, or a site, or a service with a protocol signature (in the **Application and Services** column), or a Data Type (in the **Content** column), the Security Gateway:
  - Turns on one or more inspection engines.
  - Postpones making the final match decision until it has inspected the body of the connection.
- The Security Gateway searches for the first rule that applies to (*matches*) a connection. If the Security Gateway does not have all the information it needs to identify the matching rule, it continues to inspect the traffic.

Creating a Basic Access Control Policy

A Security Gateway controls access to computers, clients, servers, and applications using a set of rules that make up an Access Control Rule Base. You need to configure a Rule Base with secure Access Control and optimized network performance.

A strong Access Control Rule Base:

- Allows only authorized connections and prevents vulnerabilities in a network.
- Gives authorized users access to the correct internal resources.
- Efficiently inspects connections.

Basic Rules

Best Practice - These are basic Access Control rules we recommend for all Rule Bases:

- **Stealth rule** that prevents direct access to the Security Gateway
- **Cleanup rule** that drops all traffic that is not matched by the earlier rules in the policy

Use Case - Basic Access Control

This use case shows a Rule Base for a simple Access Control security policy. (The **Hits**, **VPN** and **Content** columns are not shown.)

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Admin Access to Security Gateways	Admins (Access Role)	Group of Security Gateways	Any	Accept	Log	Policy Targets
2	Stealth	Any	Group of Security Gateways	Any	Drop	Alert	Policy Targets
3	Critical subnet	Internal	Finance HR R&D	Any	Accept	Log	CorpGW
4	Tech support	TechSupport	Remote1-web	HTTP	Accept	Alert	Remote1GW
5	DNS server	Any	DNS	Domain UDP	Accept	None	Policy Targets
6	Mail and Web servers	Any	DMZ	HTTP HTTPS SMTP	Accept	Log	Policy Targets

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
7	SMTP	Mail	NOT Internal net group	SMTP	Accept	Log	Policy Targets
8	DMZ & Internet	IntGroup	Any	Any	Accept	Log	Policy Targets
9	Cleanup rule	Any	Any	Any	Drop	Log	Policy Targets

Explanations for rules:

Rule	Explanation
1	**Admin Access to Gateways** - SmartConsole administrators are allowed to connect to the Security Gateways.
2	**Stealth** - All internal traffic that is NOT from the SmartConsole administrators to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.
3	**Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and R&D.
4	**Tech support** - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.
5	**DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.
6	**Mail and Web servers** - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.
7	**SMTP** - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.
8	**DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.
9	**Cleanup rule** - Drops all traffic that does not match one of the earlier rules.

Use Case - Inline Layer for Each Department

This use case shows a basic Access Control Policy with a sub-policy for each department. The rules for each department are in an Inline Layer. An Inline Layer is independent of the rest of the Rule Base. You can delegate ownership of different Layers to different administrators.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Critical subnet	Internal	Finance HR	Any	Any	Accept	Log
2	SMTP	Mail	NOT internal network (Group)	smtp	Any	Accept	Log
3	R&D department	R&D Roles	Any	Any	Any	TechSupport Layer	N/A
3.1	R&D servers	Any	R&D servers (Group) QA network	Any	Any	Accept	Log
3.2	R&D source control	InternalZone	Source control servers (Group)	ssh http https	Any	Accept	Log
---	---	---	---	---	---	---	---
3.X	Cleanup rule	Any	Any	Any	Any	Drop	Log
4	QA department	QA network	Any	Any	Any	QA Layer	N/A
4.1	Allow access to R&D servers	Any	R&D Servers (Group)	Web Services	Any	Accept	Log
---	---	---	---	---	---	---	---
4.Y	Cleanup rule	Any	Any	Any	Any	Drop	Log
5	Allow all users to access employee portal	Any	Employee portal	Web Services	Any	Accept	None
---	---	---	---	---	---	---	---
9	Cleanup rule	Any	Any	Any	Any	Drop	Log

Explanations for rules:

Rules	Explanation
1 2	General rules for the whole organization.
3 3.1 3.2 --- 3.X	An Inline Layer for the R&D department. Rule 3 is the parent rules of the Inline Layer. The **Action** is the name of the Inline Layer. **If a packet does not match on parent rule 3:** Matching continues to the next rule outside the Inline Layer (rule 4). **If a packet matches on parent rule 3:** Matching continues to 3.1, first rule inside the Inline Layer. If a packet matches on this rule, the rule action is done on the packet. If a packet does not match on rule 3.1, continue to the next rule inside the Inline Layer, rule 3.2. If there is no match, continue to the remaining rules in the Inline Layer. --- means one or more rules. The packet is matched only inside the inline layer. It never leaves the inline layer, because the inline layer has an implicit cleanup rule. It is not matched on rules 4, 5 and the other rules in the Ordered Layer. Rule 3.X is a **cleanup rule**. It drops all traffic that does not match one of the earlier rules in the Inline Layer. This is a default explicit rule. You can change or delete it. **Best Practice** - Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.
4 4.1 --- 4.Y	Another Inline Layer, for the QA department.
5	More general rules for the whole organization.
--	One or more rules.
9	**Cleanup rule** - Drop all traffic that does not match one of the earlier rules in the Ordered Layer. This is a default explicit rule. You can change or delete it. **Best Practice** - Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.

Creating Application Control and URL Filtering Rules

Create and manage the Policy for Application Control and URL Filtering in the Access Control Policy, in the Access Control view of SmartConsole. Application Control and URL Filtering rules define which users can use specified applications and sites from within your organization and what application and site usage is recorded in the logs.

To learn which applications and categories have a high risk, look through the **Application Wiki** in the **Access Tools** part of the **Security Policies** view. Find ideas for applications and categories to include in your Policy.

To see an overview of your Access Control Policy and traffic, see the Access Control view in **Logs & Monitor** > **New Tab** > **Views**.

Best Practice - Do not use Application Control and URL Filtering in the same rule, this may lead to wrong rule matching. Use Application Control and URL Filtering in separate rules. This makes sure that the URL Filtering rule is used as soon as the category is identified. For more information, see sk174045.

Monitoring Applications

Scenario: I want to monitor all Facebook traffic in my organization. How can I do this?

To monitor all Facebook application traffic:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Click one of the **Add rule** toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
4. Create a rule that includes these components:
   - **Name** - Give the rule a name, such as **Monitor Facebook**.
   - **Source** - Keep it as **Any** so that it applies to all traffic from the organization.
   - **Destination** - Keep it as **Internet** so that it applies to all traffic going to the internet or DMZ.
   - **Services & Applications** - Click the plus sign to open the Application viewer. Add the **Facebook** application to the rule:
     - Start to type "face" in the Search field. In the Available list, see the **Facebook** application.
   - Click each item to see more details in the description pane.
   - Select the items to add to the rule.

Note - Applications are matched by default on their **Recommended** services. You can change this (see *"Configuring Matching for an Allowed Application" on page 187*). Each service runs on a specific port. The recommended **Web Browsing Services** are `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.

   - **Action** - Select **Accept**
   - **Track** - Select **Log**

- **Install On** - Keep it as **Policy Targets** for or all Security Gateways, or choose specific Security Gateways, on which to install the rule

The rule allows all Facebook traffic but logs it. You can see the logs in the **Logs & Monitor** view, in the **Logs** tab. To monitor how people use Facebook in your organization, see the Access Control view (SmartEvent Server required).

Blocking Applications and Informing Users

Scenario: I want to block pornographic sites in my organization, and tell the user about the violation. How can I do this?

To block an application or category of applications and tell the user about the policy violation:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Create a rule that includes these components:
   - **Services & Applications** - Select the **Pornography** category.
   - **Action** - **Drop**, and a UserCheck **Blocked Message - Access Control**

     The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.
   - **Track** - **Log**

Note - This Rule Base example contains only those columns that are applicable to this subject.

Name	Source	Destination	Services & Applications	Action	Track	Install On
Block Porn	Any	Internet	Pornography (category)	Drop Blocked Message	Log	Policy Targets

The rule blocks traffic to pornographic sites and logs attempts to access those sites. Users who violate the rule receive a UserCheck message that informs them that the application is blocked according to company security policy. The message can include a link to report if the website is included in an incorrect category.

Important - A rule that blocks traffic, with the **Source** and **Destination** parameters defined as **Any**, also blocks traffic to and from the Captive Portal.

Limiting Application Traffic

Scenario: I want to limit my employees' access to streaming media so that it does not impede business tasks.

If you do not want to block an application or category, there are different ways to set limits for employee access:

- Add a **Limit** object to a rule to limit the bandwidth that is permitted for the rule.
- Add one or more **Time** objects to a rule to make it active only during specified times.

The example rule below:

- Allows access to streaming media during non-peak business hours only.
- Limits the upload throughput for streaming media in the company to 1 Gbps.

To create a rule that allows streaming media with time and bandwidth limits:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base.
4. Create a rule that includes these components:
   - **Services & Applications** - **Media Streams** category.

     Note - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this, see *"Services & Applications Column" on page 186*.
   - **Action** - Click **More** and select **Action**: *Accept*, and a **Limit** object.
   - **Time** - Add a **Time** object that specifies the hours or time period in which the rule is active.

     Note - The **Time** column is not shown by default in the Rule Base table. To see it, right-click on the table header and select **Time**.

Name	Source	Destination	Services and Applications	Action	Track	Install On	Time
Limit Streaming Media	Any	Internet	Media Streams (Category)	Accept Upload_1Gbps	Log	All	Off-Work

Note - In ClusterXL Load Sharing modes, the specified bandwidth limit is divided between all defined cluster members, regardless of the cluster state. For example, if a rule sets a 1Gbps limit in a cluster with three members, each member has a fixed limit of 333 Mbps.

Using Identity Awareness Features in Rules

Scenario: I want to allow a Remote Access application for a specified group of users and block the same application for other users. I also want to block other Remote Access applications for everyone. How can I do this?

If you enable Identity Awareness on a Security Gateway, you can use it together with Application Control to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role **Identified_Users** that represents all identified users in the organization. You can use this to allow access to applications only for users who are identified on the Security Gateway.
- You want to allow access to the Radmin Remote Access tool for all identified users.
- You want to block all other Remote Access tools for everyone within your organization. You also want to block any other application that can establish remote connections or remote control.

To do this, add two new rules to the Rule Base:

1. Create a rule and include these components:
   - **Source** - The **Identified_Users** access role
   - **Destination** -**Internet**
   - **Services & Applications - Radmin**
   - **Action** -**Accept**
2. Create another rule below and include these components:
   - **Source** - **Any**
   - **Destination** - **Internet**
   - **Services & Applications** - The category: **Remote Administration**
   - **Action** - **Block**

Name	Source	Destination	Services & Applications	Action	Track	Install On
Allow Radmin to Identified Users	Identified_ Users	Internet	Radmin	Allow	Log	All
Block other Remote Admins	Any	Internet	Remote Administration	Block	Log	All

Notes on these rules::

- Because the rule that allows Radmin is above the rule that blocks other Remote Administration tools, it is matched first.
- The Source of the first rule is the **Identified_Users** access role. If you use an access role that represents the Technical Support department, then only users from the technical support department are allowed to use Radmin.
- Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

For more about Access Roles and Identity Awareness, see the *R81 Identity Awareness Administration Guide*.

Blocking Sites

Scenario: I want to block sites that are associated with categories that can cause liability issues. Most of these categories exist in the Application Database but there is also a custom defined site that must be included. How can I do this?

You can do this by creating a *custom group* and adding all applicable categories and the site to it. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created
  - An Access Role that represents all identified users in the organization (*Identified_Users*).
  - A custom application for a site named *FreeMovies*.
- You want to block sites that can cause liability issues for everyone within your organization.
- You will create a custom group that includes Application Database categories as well as the previously defined custom site named *FreeMovies*.

To create a custom group

1. In the Object Explorer, click **New > More > Custom Application/Site > Application/Site Group**.
2. Give the group a name. For example, *Liability_Sites*.
3. Click **+** to add the group members:
   - Search for and add the custom application *FreeMovies*.
   - Select **Categories**, and add the ones you want to block (for example *Anonymizer*, *Critical Risk*, and *Gambling*)
   - Click **Close**
4. Click **OK**.

You can now use the *Liability_Sites* group in the Access Control Rule Base.

In the Rule Base, add a rule similar to this

In the Security Policies view of SmartConsole, go to the Access Control Policy.

- **Source** - The **Identified_Users** access role
- **Destination** - **Internet**
- **Services & Applications** - *Liability_Sites*
- **Action** - **Drop**

Note - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

Name	Source	Destination	Services & Applications	Action	Track
Block sites that may cause a liability	Identified_Users	Internet	Liability_Sites	Drop	Log

Blocking URL Categories

Scenario: I want to block pornographic sites. How can I do this?

You can do this by creating a rule that blocks all sites with pornographic material with the *Pornography category*. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role (*Identified_Users*) that represents all identified users in the organization.
- You want to block sites related to pornography.

The procedure is similar to *"Blocking Applications and Informing Users" on page 203*.

Ordered Layers and Inline Layers

A policy is a set of rules that the Security Gateway enforces on incoming and outgoing traffic. There are different policies for Access Control and for Threat Prevention.

You can organize the Access Control rules in more manageable subsets of rules using Ordered Layers and Inline Layers.

The Need for Ordered Layers and Inline Layers

Ordered Layers and Inline Layers helps you manage your cyber security more efficiently. You can:

- Simplify the Rule Base, or organize parts of it for specific purposes.
- Organize the Policy into a hierarchy, using Inline Layers, rather than having a flat Rule Base.

  An Inline Layer is a *sub-policy* which is independent of the rest of the Rule Base.
- Reuse Ordered Layers in multiple Policy packages, and reuse Inline Layers in multiple Layers.
- Simplify the management of the Policy by delegating ownership of different Layers to different administrators.
- Improve performance by reducing the number of rules in a Layer.

Order of Rule Enforcement in Inline Layers

The Ordered Layer can contain Inline Layers.

This is an example of an Inline Layer:

No.	Source	Destination	VPN	Services	Action
1					
2	Lab_network	Any	Any	Any	Lab_rules
2.1	Any	Any	Any	https http	Allow
2.2	Any	Any	Any	Any	Drop
3					

The Inline Layer has a parent rule (Rule 2 in the example), and sub rules (Rules 2.1 and 2.2). The Action of the parent rule is the name of the Inline Layer.

If the packet does not match the parent rule of the Inline Layer, the matching continues to the next rule of the Ordered Layer (Rule 3).

If a packet matches the parent rule of the Inline Layer (Rule 2), the Security Gateway checks it against the sub rules:

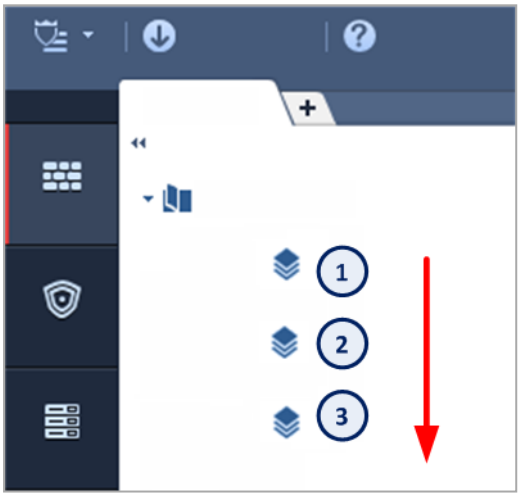
- If the packet matches a sub rule in the Inline Layer (Rule 2.1), no more rule matching is done.
- If none of the higher rules in the Ordered Layer match the packet, the explicit **Cleanup Rule** is applied (Rule 2.2). If this rule is missing, the **Implicit Cleanup Rule** is applied (see *"Types of Rules in the Rule Base" on page 213*). No more rule matching is done.

Important - Always add an explicit **Cleanup Rule** at the end of each Inline Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Order of Rule Enforcement in Ordered Layers

When a packet arrives at the Security Gateway, the Security Gateway checks it against the rules in the first Ordered Layer, sequentially from top to bottom, and enforces the first rule that matches a packet.

If the **Action** of the matching rule is **Drop**, the Security Gateway stops matching against later rules in the Policy Rule Base and drops the packet. If the **Action** is **Accept**, the Security Gateway continues to check rules in the next Ordered Layer.



Item	Description
1	Ordered Layer 1
2	Ordered Layer 2
3	Ordered Layer 3

If none of the rules in the Ordered Layer match the packet, the explicit **Default Cleanup Rule** is applied. If this rule is missing, the **Implicit Cleanup Rule** is applied (see *"Types of Rules in the Rule Base" on page 213*).

Every Ordered Layer has its own implicit cleanup rule. You can configure the rule to *Accept* or *Drop* in the **Layer settings**. (see *"Configuring the Implicit Cleanup Rule" on page 215*).

Important - Always add an explicit **Cleanup Rule** at the end of each Ordered Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Creating an Inline Layer

An Inline Layer is a *sub-policy*, which is independent of the rest of the Rule Base.

The workflow for making an Inline Layer is:

1. Create a *parent* rule for the Inline Layer. Make a rule that has one or more properties that are the same for all the rules in the Inline Layer. For example, rules that have the same source, or service, or group of users.
2. Create *sub-rules* for the Inline Layer. These are rules that define in more detail what to do if the Security Gateway matches a connection to the parent rule. For example, each sub-rule can apply to specified hosts, or users, or services, or Data Types.

To create an Inline Layer

1. Add a rule to the Ordered Layer. This is the *parent* rule.
2. In the **Source**, **Destination**, **VPN**, and **Services & Applications** cells, define the match conditions for the Inline Layer.
3. Click the **Action** cell of the rule. Instead of selecting a standard action, select **Inline Layer** > **New Layer**.
4. The **Layer Editor** window opens.
5. Configure the properties of the Inline Layer:
   a. Enable one or more of these **Blades** for the rules of Inline Layer:
      - Firewall
      - Application & URL Filtering
      - Content Awareness
      - Mobile Access
   b. **Optional**: It is a best practice to share Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer**.
   c. Click **Advanced**.
   d. Configure the **Implicit Cleanup Rule** to *Drop* or *Accept* (see *"Types of Rules in the Rule Base" on page 213*).
   e. Click **OK**.

   The name of the Inline Layer shows in the **Action** cell of the rule.
6. Under the parent rule of the Inline Layer, add *sub-rules*.
7. Make sure there is an explicit cleanup rule as the last rule of the Inline Layer. (see *"Types of Rules in the Rule Base" on page 213*).

Creating an Ordered Layer

To create an Ordered Layer

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.

You will see a list of the Layers. You can select **Show only shared Layers**.

3. Click the **New** icon in the upper toolbar.
4. Configure the settings in the **Layer Editor** window.
5. **Optional**: It is a best practice to share Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer**.
6. Click **OK**.
7. Click **Close**.
8. Publish the SmartConsole session.

   This Ordered Layer is not yet assigned to a Policy Package.

To add an Ordered Layer to the Access Control Policy

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the Access Control Policy section and select **Edit Policy**.

   The **Policy** window opens.
3. In the Access Control section, click the plus sign.

   You will see a list of the Layers that you can add. These are Layers that have **Multiple policies can use this layer** enabled.
4. Select the Layer.
5. Click **OK**.
6. Publish the SmartConsole session.

Security Gateways R77.30 or lower: To create a Layer for URL Filtering and Application Control

1. In SmartConsole, click Security Policies.
2. Right-click a Layer in the Access Control Policy section and select **Edit Policy**.

   The **Policy** window opens.
3. In the Access Control section, click the plus sign.
4. Click **New Layer**.

   The **Layer Editor** window opens and shows the **General** view.
5. Enable Application & URL Filtering on the Layer.
   a. Enter a name for the Layer.

      We recommend the name **Application**.
   b. In the **Blades** section, select **Application & URL Filtering**.
   c. Click **OK** and the **Layer Editor** window closes.
   d. Click **OK** and the **Policy** window closes.
6. Publish the SmartConsole session.

Enabling Access Control Features

Before creating the Access Control Policy, you must enable the Access Control features that you will use in the Policy.

Enable the features on the:

- Security Gateways, on which you will install the Policy.
- Ordered Layers and Inline Layers of the Policy. Here you can enable:
  - Firewall. This includes VPN (see *"VPN Column" on page 185*).
  - Application & URL Filtering (see *"Services & Applications Column" on page 186*).
  - Content Awareness (see *"Content Column" on page 189*).
  - Mobile Access (see *"Mobile Access to the Network" on page 286*).

Enabling Access Control Features on a Security Gateway

1. In SmartConsole, from the left navigation panel, click **Gateways & Servers** and double-click the Security Gateway object.

   The **General Properties** window of the Security Gateway opens.
2. From the navigation tree, click **General Properties**.
3. In the **Network Security** tab, select one or more of these Access Control features:
   - IPsec VPN
   - Mobile Access
   - Application Control
   - URL Filtering
   - Content Awareness
   - Identity Awareness
4. Click **OK**.

Enabling Access Control Features on a Layer

To enable the Access Control features on an Ordered Layer:

1. In SmartConsole, click **Security Policies**.
2. Under Access Control, right-click **Policy** and select **Edit Policy**.
3. Click options  for the Layer.
4. Click **Edit Layer**.

   The **Layer Editor** window opens and shows the **General** view.
5. Enable the **Blades** that you will use in the Ordered Layer:

- Firewall.
- Application & URL Filtering
- Content Awareness
- Mobile Access

6. Click **OK**.

To enable the Access Control features on an Inline Layer

1. In SmartConsole, click **Security Policies**.
2. Select the Ordered Layer.
3. In the parent rule of the Inline Layer, right-click the **Action** column, and select **Inline Layer** > **Edit Layer**.
4. Enable the **Blades** that you will use in the Inline Layer:
   - Firewall
   - Application & URL Filtering
   - Content Awareness
   - Mobile Access

   Note - Do not enable a Blade that is not enabled in the Ordered Layer.

5. Click **OK**.

Types of Rules in the Rule Base

There are three types of rules in the Rule Base- **explicit**, **implied** and **implicit**.

Explicit rules

The rules that the administrator configures explicitly, to allow or to block traffic based on specified criteria.

Important - The **default Cleanup rule** is an explicit rule that is added by default to every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit Cleanup rule as the last rule in each layer.

Implied rules

The default rules that are available as part of the **Global properties** configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- **First** - Applied first, before all other rules in the Rule Base - explicit or implied
- **Last** - Applied last, after all other rules in the Rule Base - explicit or implied, but before the **Implicit Cleanup Rule**
- **Before Last** - Applied before the last explicit rule in the Rule Base

Implied rules are configured to allow connections for different services that the Security Gateway uses. For example, the **Accept Control Connections** rules allow packets that control these services:

- Installation of the security policy on a Security Gateway
- Sending logs from a Security Gateway to the Security Management Server
- Connecting to third party application servers, such as RADIUS and TACACS authentication servers

Implicit cleanup rule

The default "catch-all" rule for the Layer that deals with traffic that does not match any explicit or implied rules in the Layer. It is made automatically when you create a Layer.

Implicit cleanup rules do not show in the Rule Base.

For Security Gateways R80.10 and higher, the default implicit cleanup rule action is **Drop**. This is because most Policies have Whitelist rules (the Accept action). If the Layer has Blacklist rules (the Drop action), you can change the action of the implicit cleanup rule to **Accept** in the Layer Editor.

For Security Gateways R77.30 and lower, the action of the implicit rule depends on the Ordered Layer:

- **Drop** - for the **Network** Layer
- **Accept** - for a Layer with **Applications and URL Filtering** enabled

Note - If you change the default values, the policy installation fails on Security Gateway R77.30 or lower.

Order in which the Security Gateway applies the rules

1. **First Implied Rule** - No explicit rules can be placed before it.
2. **Explicit Rules** - These are the rules that you create.
3. **Before Last Implied Rules** - Applied before the last explicit rule.
4. **Last Explicit Rule** - We recommend that you use a **Cleanup rule** as the last explicit rule.

   Note - If you use the **Cleanup rule** as the last explicit rule, the **Last Implied Rule** and the **Implicit Cleanup Rule** are not enforced.

5. **Last Implied Rule** - Remember that although this rule is applied after all other explicit and implied rules, the Implicit Cleanup Rule is still applied last.
6. **Implicit Cleanup Rule** - The default rule that is applied if none of the rules in the Layer match.

Configuring the Implied Rules

Some of the implied rules are enabled by default. You can change the default configuration as necessary.

To configure the implied rules:

1. In SmartConsole, select the Access Control Policy.
2. From the toolbar above the policy, select **Actions** > **Implied Rules**.

The **Implied Policy** window opens.

3. In the left pane, click **Configuration**.
4. Select a rule to enable it, or clear a rule to disable it.
5. For the enabled rules, select the position of the rules in the Rule Base: **First**, **Last**, or **Before Last** (see *"Types of Rules in the Rule Base" on page 213*).
6. Click **OK** and install the policy.

Showing the Implied Rules

In SmartConsole, from the **Security Policies** View, select **Actions** > **Implied Rules**.

The **Implied Policy** window opens.

It shows only the implied rules, not the explicit rules.

Configuring the Implicit Cleanup Rule

To configure the Implicit Cleanup Rule:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.
3. Select a Layer and click **Edit**.

   The **Layer Editor** opens.
4. Click **Advanced**
5. Configure the **Implicit Cleanup Rule** to *Drop* or *Accept*.
6. Click **OK**.
7. Click **Close**.
8. Publish the SmartConsole session.

Administrators for Access Control Layers

You can create administrator accounts dedicated to the role of Access Control, with their own installation and SmartConsole Read/Write permissions.

You can also delegate ownership of different Layers to different administrators. See *"Configuring Permissions for Access Control Layers" on page 117*.

Sharing Layers

You may need to use the same rules in different parts of a Policy, or have the same rules in multiple Policy packages.

There is no need to create the rules multiple times. Define an Ordered Layer or an Inline Layer one time, and mark it as shared. You can then reuse the Inline Layer or Ordered layer in multiple policy packages or use the Inline Layer in multiple places in an Ordered Layer. This is useful, for example, if you are an administrator of a corporation and want to share some of the rules among multiple branches of the corporation:

- It saves time and prevents mistakes.
- To change a shared rule in all of the corporation's branches, you must only make the change once.

To mark a Layer as shared

1. In SmartConsole, click **Menu** > **Manage policies and layers**.
2. In the left pane, click **Layers**.
3. Select a Layer in Access Control or in Threat Prevention.
4. Right-click and select **Edit Layer**.
5. Configure the settings in the **Layer Editor** window.
6. In **General**, select **Multiple policies and rules can use this layer**.
7. Click **OK**.
8. Click **Close**.
9. Publish the SmartConsole session.

To reuse a Threat Prevention Ordered Layer

1. In SmartConsole, go to **Menu** > **Manage policies and layers** > **Policies**.
2. Right-click the required policy and click **Edit**. The policy properties window opens.
3. In the Threat Prevention box, click the **+** sign.
4. Select the layer you want to include in this policy package.
5. Click **OK**.
6. Close the policy properties window.
7. In SmartConsole, install the policy.
8. Repeat this procedure for all policy packages.

For examples of Inline Layers and Ordered Layer, see *" Use Cases for the Unified Rule Base" on page 218*.

Visual Division of the Rule Base with Sections

To better manage a policy with a large number of rules, you can use **Sections** to divide the Rule Base into smaller, logical components. The division is only visual and does not make it possible to delegate administration of different **Sections** to different administrators.

Exporting Layer Rules to a .CSV File

You can export Layer rules to a .CSV file. You can open and change the .CSV file in a spreadsheet application such as Microsoft Excel.

To export Layer rules to a .CSV file:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.

   The **Manage Layers** window opens.
2. Click **Layers**.

3. Select a Layer, and then click **Actions** > **Export selected Layer**.
4. Enter a path and file name.

Managing Policies and Layers

To work with Ordered Layers and Inline Layers in the Access Control Policy, select **Menu** > **Manage policies and layers** in SmartConsole.

The **Manage policies and layers** window shows.

To see the Layer in the policy package and their attributes:

In the **Layers** pane of the window, you can see:

- **Name** - Layer name
- **Number of Rules** - Number of rules in the Layer
- **Modifier** - The administrator who last changed the Layer configuration.
- **Last Modified** -Date the Layer was changed.
- **Show only Shared Layers** - A shared Layer has the **Multiple policies and rules can use this Layer** option selected. (see *"Sharing Layers" on page 215*).
- **Layer Details**
  - **Used in policies** - Policy packages that use the Layer
  - **Mode**:
    - **Ordered** - An Ordered Layer. In a Multi-Domain Security Management environment, it includes global rules and a placeholder for local, Domain rules.
    - **Inline** - An Inline Layer, also known as a Sub-Policy.
    - **Not in use** - A Layer that is not used in a Policy package.

To see the rules in the Layer:

1. Select a Layer.
2. Right-click and select **Open layer in policy**.

Use Cases for the Unified Rule Base

Here are some use cases that show examples of rules that you can define for the Access Control Policy.

Use Case - Application Control and Content Awareness Ordered Layer

This use case shows an example unified Access Control Policy. It controls applications and content in one Ordered Layer.

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
General compliance (1)								
1	Block categories	Any	Internet	Any	Anonymizer Critical Risk	Any	Drop Block Message	Log
Block risky executables (2)								
2	Block download of executable files from uncategorized and high risk sites	InternalZone	Internet	Any	Uncategorized High Risk	Download Traffic Executable File	Drop	Log
Credit card data (3-4)								
3	Allow uploading of credit cards numbers, by finance, and only over HTTPS	Finance (Access Role)	Web Servers	Any	https	Upload Traffic PCI - Credit Card Numbers	Accept	Log

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
4	Block other credit cards from company Web servers	Any	Web Servers	Any	Any	Any Direction PCI - Credit Card Numbers	Drop	Log
Inform about sensitive data over VPN (5)								
5	Inform the user about sensitive data from VPN sites	Any	Any	RemoteAccess	Any	Any Direction Salary Survey Report	Inform	Log
Cleanup (6)								
6	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Explanations for rules:

Rule	Explanation
1	**General Compliance** section - Block access to unacceptable Web sites and applications.
2	**Block risky executables** section - Block downloading of high risk executable files.
3-4	**Credit card data** section - Allow uploading of credit cards numbers only by the finance department, and only over HTTPS. Block other credit cards.
5	**Block sensitive data over VPN** section - A remote user that connects over the organization's VPN sees an informational message.
6	**cleanup rule** - Accept all traffic that does not match one of the earlier rules.

Use Case - Inline Layer for Web Traffic

This use case shows an example Access Control Policy that controls Web traffic. The Web server rules are in an Inline Layer.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Headquarter WEB traffic - via proxy	HQ	Proxy	Web Proxy	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
2	Allow Proxy to the Internet	Proxy	Internet	Web	Any	Accept	None
3	Allow local branch to access the internet directly	Local Branch	Internet	Web	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
4	Web Servers	InternalZone	Web Servers	Web	Any	Web Servers protection	N/A
4.1	Block browsing with unapproved browsers	Any	Any	NEGATED Google Chrome Internet Explorer 11 Firefox Safari	Any	Drop	Log
4.2	Inform user when uploading Credit Cards only over HTTPS	Any	Any	https	Upload Traffic PCI - Credit Card Numbers	Inform Access Noti... once a day per applic...	Log

No	Name	Source	Destination	Services & Applications	Content	Action	Track
4.3	Block Credit Cards	Any	Any	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
4.4	Block downloading of sensitive content	Any	Any	Any	Download Traffic HIPAA - Medical Record Headers	Drop	Log
4.5	Cleanup rule	Any	Any	Any	Any	Accept	None
5	Ask user when sending credit cards to PayPal	InternalZone	Internet	PayPal	Any Direction PCI - Credit Card Numbers	Ask Company Policy Access Noti... once a day per applic...	Log
6	Cleanup rule	Any	Any	Any	Any	Drop	Log

Explanations for rules:

Rule	Explanation
4	This is the parent rule of the Inline Layer. The **Action** is the name of the Inline Layer. If a packet matches on the parent rule, the matching continues to rule 4.1 of the Inline Layer. If a packet does not match on the parent rule, the matching continues to rule 5.
4.1 -4.4	If a packet matches on rule 4.1, the rule action is done on the packet, and no more rule matching is done. If a packet does not match on rule 4.1, continue to rule 4.2. The same logic applies to the remaining rules in the Inline Layer.
4.5	If none of the higher rules in the Ordered Layer match the packet, the explicit *Cleanup Rule* is applied. The *Cleanup rule* is a default explicit rule. You can change or delete it. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.

Use Case - Content Awareness Ordered Layer

This use case shows a Policy that controls the upload and download of data from and to the organization.

There is an explanation of some of the rules below the Rule Base.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
Regulatory compliance							
1	Block the download of executable files	InternalZone	Internet	Any	Download Traffic Executable file	Drop	Log
2	Allow uploading of credit cards numbers by finance users, only over HTTPS	Finance (Access Role)	Web Servers	https	Upload Traffic PCI - Credit Card Numbers	Accept	Log
3	Block other credit cards from company Web servers	InternalZone	Web Servers	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
Personally Identifiable Information							
4	Matches U.S. Social Security Numbers (SSN) allocated by the U.S. Social Security Administration (SSA).	InternalZone	Internet	Any	Upload Traffic U.S. Social Security Numbers - According to SSA	Inform Access Notifi... once a day per applicati...	Log
5	Block downloading of sensitive medical information	InternalZone	Internet	Any	Download Traffic HIPAA - Medical Records Headers	Drop Block Message	Log
Human Resources							

No	Name	Source	Destination	Services & Applications	Content	Action	Track
6	Ask user when uploading documents containing salary survey reports.	InternalZone	Internet	Any	Upload Traffic Salary Survey Report	Ask Company Policy once a day per applicati...	Log
Intellectual Property							
7	Matches data containing source code	InternalZone	Internet	Any	Any Direction Source Code	Restrict source code	N/A
7.1		Any	Any	Any	Download Traffic Source Code	Accept	Log
7.2		Any	Any	Any	Upload Traffic Source Code	Ask Company Policy once a day per applicati...	Log
7.3	Cleanup Inline Layer	Any	Any	Any	Any	Drop Block Message	Log

Explanations for rules:

Rule	Explanation
1-3	**Regulatory Compliance** section - Controls the upload and download of executable files and credit cards. You can set the direction of the **Content**. In rule 1 it is **Download Traffic**, in rule 2 it is **Upload Traffic**, and in rule 3 it is **Any Direction**. Rule 1 controls executable files, which are File Types. The File Type rule is higher in the Rule Base than rules with Content Types (Rules 2 to 7). This improves the efficiency of the Rule Base, because File Types are matched sooner than Content Types.
4-5	**Personally Identifiable Information** section - Controls the upload and download of social security number and medical records. The rule Action for rule 4 is **Inform**. When an internal user uploads a file with a social security number, the user sees a message.

Rule	Explanation
6	**Human resources** section - Controls the sending of salary survey information outside of the organization. The rule action is **Ask**. If sensitive content is detected, the user must confirm that the upload complies with the organization's policy.
7	**Intellectual Property** section - A group of rules that control how source code leaves the organization. Rule 7 is the parent rule of an Inline Layer (see *"Ordered Layers and Inline Layers" on page 208*). The **Action** is the name of the Inline Layer. If a packet matches on rule 7.1, matching stops. If a packet does not match on rule 7.1, continue to rule 7.2. In a similar way, if there is no match, continue to 7.3. The matching stops on the last rule of the Inline Layer. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer

Use Case - Application & URL Filtering Ordered Layer

This use case shows some examples of URL Filtering and Application Control rules for a typical policy that monitors and controls Internet browsing. (The **Hits, VPN** and **Install On** columns are not shown.)

No.	Name	Source	Destination	Services & Applications	Action	Track	Time
1	Liability sites	Any	Internet	Potential liability (group)	Drop Blocked Message	Log	Any
2	High risk applications	Any	Internet	High Risk iTunes Anonymizer (category)	Drop Blocked Message	Log	Any
3	Allow IT department Remote Admin	IT (Access Role)	Any	Radmin	Allow	Log	Work-Hours
4	Allow Facebook for HR	HR (Access Role)	Internet	Facebook	Allow Download_1Gbps	Log	Any
5	Block these categories	Any	Internet	Streaming Media Protocols Social Networking P2P File Sharing Remote Administration	Drop Blocked Message	Log	Any

No.	Name	Source	Destination	Services & Applications	Action	Track	Time
6	Log all applications	Any	Internet	Any	Allow	Log	Any

Explanations for rules:

Rule	Explanation
1	**Liability sites** - Blocks traffic to sites and applications in the custom *Potential_liability* group. The UserCheck *Blocked Message* is shown to users and explains why their traffic is blocked. See *"Blocking Sites" on page 206*. *Scenario: I want to block sites that are associated with categories that can cause liability issues. Most of these categories exist in the Application Database but there is also a custom defined site that must be included. How can I do this?* You can do this by creating a *custom group* and adding all applicable categories and the site to it. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object. In this example: ■ You have already created • An Access Role that represents all identified users in the organization (*Identified_Users*). • A custom application for a site named *FreeMovies*. ■ You want to block sites that can cause liability issues for everyone within your organization. ■ You will create a custom group that includes Application Database categories as well as the previously defined custom site named *FreeMovies*. **To create a custom group:** 1. In the Object Explorer, click **New > More > Custom Application/Site > Application/Site Group**. 2. Give the group a name. For example, *Liability_Sites*. 3. Click **+** to add the group members: ■ Search for and add the custom application *FreeMovies*. ■ Select **Categories**, and add the ones you want to block (for example *Anonymizer*, *Critical Risk*, and *Gambling*) ■ Click **Close** 4. Click **OK**. You can now use the *Liability_Sites* group in the Access Control Rule Base. **In the Rule Base, add a rule similar to this:** In the Security Policies view of SmartConsole, go to the Access Control Policy. ■ **Source** - The **Identified_Users** access role ■ **Destination** - **Internet** ■ **Services & Applications** - *Liability_Sites* ■ **Action** -**Drop**  **Note** - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

<table>
<tr><th>Rule</th><th>Explanation</th></tr>
<tr><td></td><td>
<table>
<tr><th>Name</th><th>Source</th><th>Destination</th><th>Services & Applications</th><th>Action</th><th>Track</th></tr>
<tr><td>Block sites that may cause a liability</td><td>Identified_ Users</td><td>Internet</td><td>Liability_Sites</td><td>Drop</td><td>Log</td></tr>
</table>
</td></tr>
<tr><td>2</td><td>High risk applications - Blocks traffic to sites and applications in the High Risk category and blocks the iTunes application. The UserCheck Block Message is shown to users and explains why their traffic is blocked.</td></tr>
<tr><td>3</td><td>Allow IT department Remote Admin - Allows the computers in the <code>IT</code> department network to use the Radmin application. Traffic that uses Radmin is allowed only during the Work-Hours (set to 8:00 through 18:30, for example).</td></tr>
<tr><td>4</td><td>Allow Facebook for HR - Allows computers in the <code>HR</code> network to use Facebook. The total traffic downloaded from Facebook is limited to 1 Gbps, there is no upload limit.</td></tr>
<tr><td>5</td><td>Block these categories - Blocks traffic to these categories: Streaming Media, Social Networking, P2P File Sharing, and Remote Administration. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.
  Note - The Remote Administration category blocks traffic that uses the <code>Radmin</code> application. If this rule is placed before rule 3, then this rule can also block Radmin for the IT department.</td></tr>
<tr><td>6</td><td>Log all applications - Logs all traffic that matches any of the URL Filtering and Application Control categories.</td></tr>
</table>

Best Practices for Access Control Rules

1. Make sure you have these rules:
   - Stealth rule that prevents direct access to the Security Gateway
   - Cleanup rule that drops all traffic that is not allowed by the earlier rules in the policy.
2. Use Layers to add structure and hierarchy of rules in the Rule Base.
3. Add all rules that are based only on source and destination IP addresses and ports, in a Firewall/Network Ordered Layer at the top of the Rule Base.
4. Create Firewall/Network rules to explicitly accept safe traffic, and add an *explicit cleanup rule* at the bottom of the Ordered Layer to drop everything else.
5. Create an Application Control Ordered Layer after the Firewall/Network Ordered Layer. Add rules to explicitly drop unwanted or unsafe traffic. Add an explicit cleanup rule at the bottom of the Ordered Layer to accept everything else.

   Alternatively, put Application Control rules in an Inline Layer as part of the Firewall/Network rules. In the parent rule of the Inline Layer, define the Source and Destination.
6. Share Ordered Layers and Inline Layers when possible.
7. For Security Gateways R80.10 and higher: If you have one Ordered Layer for Firewall/Network rules, and another Ordered Layer for Application Control - Add all rules that examine applications, Data Type, or Mobile Access elements, to the Application Control Ordered Layer, or to an Ordered Layer after it.
8. Turn off the XFF inspection, unless the Security Gateway is behind a proxy server. For more, see sk92839.
9. Disable a rule when working on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Security Gateway. To disable a rule, right-click in the **No** column of the rule and select **Disable**.

Best Practices for Efficient rule Matching

1. Place rules that check the source, destination, and port (network rules) higher in the Rule Base.

   Reason: Network rules are matched sooner, and turn on fewer inspection engines.
2. Place rules that check applications and content (Data Types) below network rules.
3. Do not define a rule with *Any* in the Source and in the Destination, and with an Application or a Data Type. For example these rules are not recommended:

Source	Destination	Services & Applications	Content
Any	Any	Facebook	
Any	Any		Credit Card numbers

   Instead, define one of these recommended rules:

Source	Destination	Services & Applications	Content
Any	Internet	Facebook	
Any	Server		Credit Card numbers

Reason for 2 and 3: Application Control and Content Awareness rules require content inspection. Therefore, they:

- Allow the connection until the Security Gateway has inspected connection header and body.
- May affect performance.

4. For rules with Data Types: Place rules that check File Types higher in the Rule Base than rules that check for Content Types. See *"Content Column" on page 189*.

   Reason: File Types are matched sooner than Content Types.

5. Do not use Application Control and URL Filtering in the same rule, this may lead to wrong rule matching. Use Application Control and URL Filtering in separate rules. This makes sure that the URL Filtering rule is used as soon as the category is identified. For more information, see sk174045.

To see examples of some of these best practices, see the *" Use Cases for the Unified Rule Base" on page 218* and *"Creating a Basic Access Control Policy" on page 198*.

Installing the Access Control Policy

1. On the Global Toolbar, click **Menu** > **Install Policy**.

   The **Install Policy** window opens showing the Security Gateways.

2. If there is more than one Policy package: From the **Policy** drop-down list, select a policy package.
3. Select **Access Control**. You can also select other Policies.
4. If there is more than one Security Gateway: Select the Security Gateways, on which to install the policy.
5. Select the **Install Mode**:

   - **Install on each selected gateway independently** - Install the policy on each target Security Gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target Security Gateways.

     Note - If you select **For Gateway Clusters, if installation on a cluster member fails, do not install on that cluster**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.

   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target Security Gateways. If the policy fails to install on one of the Security Gateways, the policy is not installed on other target Security Gateways.

6. Click **Install**.

Pre-R80.10 Gateways and the Unified Access Control Policy

When you upgrade an R77.30 or lower Security Management Server, which manages R77.30 or lower Security Gateways, to R80.10 or higher, the existing Access Control policies are converted in this way:

- The pre-R80.10 **Firewall** policy is converted into the **Network Policy Layer** of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Drop** all traffic that is not matched by any rule in this Layer.
- The pre-R80.10 **Application & URL Filtering** policy is converted into the **Application** Policy Layer, which is the second Layer of the R80.x Access Control Policy. The implicit cleanup rule for it is set to **Accept** all traffic that is not matched by any rule in this Layer.

Important - After upgrade, do not change the **Action** of the implicit cleanup rules, or the order of the Policy Layers. If you do, the policy installation will fail.

New Access Control Policy for pre-R80.10 Security Gateways on an R80.x Security Management Server must have this structure:

1. The first Policy Layer is the Network Layer (with the **Firewall** blade enabled on it).
2. The second Policy Layer is the Application & URL Filtering Layer (with the **Application & URL Filtering** blade enabled on it).
3. There are no other Policy Layers.

If the Access Control Policy has a different structure, the policy will fail to install.

You can change the names of the Layers, for example, to make them more descriptive.

Each new Policy Layer will have the explicit default rule, added automatically and set to **Drop** all the traffic that does not match any rule in that Policy Layer. We recommend that the **Action** is set to **Drop** for the Network Policy Layer and **Accept** for the Application Control Policy Layer.

If you remove the default rule, the **Implicit Cleanup Rule** will be enforced. The **Implicit Cleanup Rule** is configured in the Policy configuration window and is not visible in the Rule Base table. Make sure the **Implicit Cleanup Rule** is configured to **Drop** the unmatched traffic for the Network Policy Layer and to **Accept** the unmatched traffic for the Application Control Policy Layer.

Analyzing the Rule Base Hit Count

Use the Hit Count feature to show the number of connections that each rule matches. Use the Hit Count data to:

- Analyze a Rule Base - You can delete rules that have no matching connection

  Note - If you see a rule with a zero hit count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. There can be matching connections on other Security Gateways.

- Better understand the behavior of the Access Control Policy

The Hit Count value appears as:

- The percentage of the rule hits from total hits
- The indicator level (very high, high, medium, low, or zero)

The percentage and indicator level are configured in the Access Control Policy Rule Base.

When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways (version R75.40 and higher). Hit Count works independently from logging and tracks the hits even if the **Track** option is **None**.

Note - From R81, Hit Count is also supported in the NAT Rule Base.

Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways. The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways.

After you enable or disable Hit Count you must install the Policy for the Security Gateway to start or stop collecting data.

To enable or disable Hit Count globally

1. In SmartConsole, click **Menu** > **Global properties**.
2. Select **Hit Count** from the tree.
3. Select the options:
   - **Enable Hit Count** - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.
   - **Keep Hit Count data up to** - Select one of the time range options. The default is 3 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.
4. Click **OK**.
5. Install the Policy.

To enable or disable Hit Count on each Security Gateway:

1. From the **Gateway Properties** for the Security Gateway, select **Hit Count** from the navigation tree.
2. Select **Enable Hit Count** to enable the feature or clear it to disable Hit Count.
3. Click **OK**.
4. Install the Policy.

Hit Count Display

Configuring the Hit Count Display

These are the options you can configure for how matched connection data is shown in the **Hits** column:

- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total hit count for:
  - Security Gateways that are not supported
  - Security Gateways that have disabled the hit count feature

  The values are shown with these letter abbreviations:
  - K = 1,000
  - M = 1,000,000
  - G = 1,000,000,000
  - T = 1,000,000,000,000

  For example, 259K represents 259 thousand connections and 2M represents 2 million connections.
- **Percentage** -Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.
- **Level** -The hit count level is a label for the range of hits according to the table.

  The hit count range = Maximum hit value - Minimum hit value (does not include zero hits)

Hit Count Level	Icon	Range
Zero		0 hits
Low		Less than 10 percent of the hit count range
Medium		Between 10 - 70 percent of the hit count range
High		Between 70 - 90 percent of the hit count range
Very High		Above 90 percent of the hit count range

To show the Hit Count in the Rule Base:

Right-click the heading row of the Rule Base and select **Hits**.

To configure the Hit Count in a rule

1. Right-click the rule number of the rule.
2. Select **Hit Count** and one of these options (you can repeat this action to configure more options):
   - **Timeframe** - Select **All**, **1 day**, **7 days**, **1 month**, or **3 months**
   - **Display** - Select **Percentage**, **Value**, or **Level**

To update the Hit Count in a rule

1. Right-click the rule number of the rule.
2. Select **Hit Count > Refresh**.

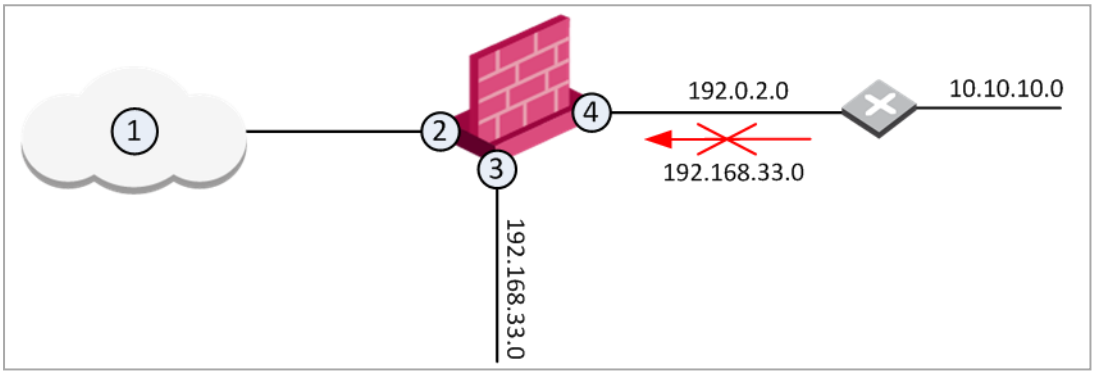
Preventing IP Spoofing

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks that packet.

Example:

The diagram shows a Security Gateway with interfaces 2 and 3, and 4, and some example networks behind the interfaces.



For the Security Gateway, Anti-Spoofing makes sure that:

- All incoming packets to 2 come from the Internet (1)
- All incoming packets to 3 come from 192.168.33.0
- All incoming packets to 4 come from 192.0.2.0 or 10.10.10.0

If an incoming packet to B has a source IP address in network 192.168.33.0, the packet is blocked, because the source address is spoofed.

When you configure Anti-Spoofing protection on a Check Point Security Gateway interface, the Anti-Spoofing is done based on the interface topology. The interface topology defines where the interface **Leads To** (for example, **External** (Internet) or **Internal**), and the **Security Zone** of interface.

Configuring Anti-Spoofing

Make sure to configure Anti-Spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

To configure Anti-Spoofing for an interface:

1. In SmartConsole, from the left navigation panel, click **Gateways & Servers** and double-click the Security Gateway object.

   The **Gateway Properties** window opens.
2. From the navigation tree, select **Network Management**.
3. Click **Get Interfaces**.
4. Click **Accept**.

The Security Gateway network topology shows. If SmartConsole fails to automatically retrieve the topology, make sure that the details in the **General Properties** section are correct and the Security Gateway, the Security Management Server, and the SmartConsole can communicate with each other.

5. Select an interface and click **Edit**.

   The interface properties window opens.

6. From the navigation tree, click **General**.

7. In the **Topology** section of the page, click **Modify**.

   The **Topology Settings** window opens.

8. In the **Leads To** section, select the type of network, to which this interface leads:

   - **Internet (External)** - This is the default setting. It is automatically calculated from the topology of the Security Gateway. To update the topology of an internal network after changes to static routes, click **Network Management** > **Get Interfaces** in the **Gateway Properties** window.
   - **Override** - Override the default setting.

   If you **Override** the default setting:

   - **Internet (External)** - All external/Internet addresses
   - **This Network (Internal)** -
     - **Not Defined** - All IP addresses behind this interface are considered a part of the internal network that connects to this interface
     - **Network defined by the interface IP and Net Mask** - Only the network that directly connects to this internal interface
     - **Network defined by routes** - The Security Gateway dynamically calculates the topology behind this interface. If the network of this interface changes, there is no need to click **Get Interfaces** and install a policy. For more, see *"Dynamically Updating the Security Gateway Topology" on page 128*.
     - **Specific** - A specific object (a Network, a Host, an Address Range, or a Network Group) behind this internal interface
     - **Interface leads to DMZ** - The DMZ that directly connects to this internal interface

9. **Optional:** In the **Security Zone** section, select **User defined**, check **Specify Security Zone** and choose the zone of the interface.

10. Configure **Anti-Spoofing** options (see *"Anti-Spoofing Options" on the next page*). Make sure that **Perform Anti-Spoofing based on interface topology** is selected.

11. Select an **Anti-Spoofing action**:

    - **Prevent** - Drops spoofed packets
    - **Detect** - Allows spoofed packets. To monitor traffic and to learn about the network topology without dropping packets, select this option together with the **Spoof Tracking Log** option.

12. Configure Anti-Spoofing exceptions (optional). For example, configure addresses, from which packets are not inspected by Anti-Spoofing:

    a. Select **Don't check packets from**.

    b. Select an object from the drop-down list, or click **New** to create a new object.

13. Configure **Spoof Tracking** - select the tracking action that is done when spoofed packets are detected:
    - **Log** - Create a log entry (default)
    - **Alert** - Show an alert
    - **None** - Do not log or alert
14. Click **OK** twice to save Anti-Spoofing settings for the interface.

For each interface, repeat the configuration steps. When finished, install the Access Control policy.

Anti-Spoofing Options

- **Perform Anti-Spoofing based on interface topology** - Select this option to enable spoofing protection on this external interface.
- **Anti-Spoofing action is set to** - Select this option to define if packets will be rejected (the Prevent option) or whether the packets will be monitored (the Detect option). The Detect option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually preventing packets from passing.
- **Don't check packets from** - Select this option to make sure anti-spoofing does not take place for traffic from internal networks that reaches the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object. The anti-spoofing enforcement mechanism disregards objects selected in the **Don't check packets from** drop-down menu.
- **Spoof Tracking** - Select a tracking option.

Multicast Access Control

Multicast IP transmits one copy of each datagram (IP packet) to a multicast address, where each recipient in the group takes their copy. The routers in the network forward the datagrams only to routers and hosts with access to receive the multicast packets.

To configure multicast access control

1. Open a Security Gateway object.
2. On the **Network Management** page, select an interface and click **Edit**.
3. On **Interface** > **Advanced**, click **Drop Multicast packets by the following conditions**.
4. Select a multicast policy for the interface:
   - **Drop multicast packets whose destination is in the list**
   - **Drop all multicast packets except those whose destination is in the list**

   When access is denied to a multicast group on an interface for outbound IGMP packets, inbound packets are also denied.

   If you do not define access restrictions for multicast packets, multicast datagrams to one interface of the Security Gateway are allowed out of all other interfaces.
5. Click **Add**.

   The **Add Object** window opens, with the **Multicast Address Ranges** object selected.
6. Click **New** > **Multicast Address Range**.

   The **Multicast Address Range Properties** window opens.
7. Enter a name for this range.
8. Define an **IP address Range** or a **Single IP Address** in the range: **224.0.0.0** - **239.255.255.255**.

   Class D IP addresses are reserved for multicast traffic and are allocated dynamically. The multicast address range `224.0.0.0` - `239.255.255.255` is used only for the destination address of IP multicast traffic.

   Every IP datagram whose destination address starts with `1110` is an IP multicast datagram. The remaining 28 bits of the multicast address range identify the group to which the datagram is sent.

   The `224.0.0.0` - `224.0.0.255` range is reserved for LAN applications that are never forwarded by a router. These addresses are permanent host groups. For example: an ICMP request to `224.0.0.1` is answered by all multicast capable hosts on the network, `224.0.0.2` is answered by all routers with multicast interfaces, and `224.0.0.13` is answered by all PIM routers. To learn more, see the IANA website.

   The source address for multicast datagrams is always the unicast source address.
9. Click **OK**.
10. In the **Add Object** window, Click **OK**.
11. In the **Interface Properties** window, Click **OK**.
12. In the Security Gateway window, Click **OK**.
13. In the Rule Base, add a rule that allows the multicast address range as the **Destination**.

14. In the **Services** of the rule, add the multicast protocols.
    - **Multicast routing protocols** - For example: Protocol-Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Extensions to OSPF (MOSPF).
    - **Dynamic registration** -Hosts use the Internet Group Management Protocol (IGMP) to let the nearest multicast router know they want to belong to a specified multicast group. Hosts can leave or join the group at any time.
15. Install the policy.

Configuring the NAT Policy

Translating IP Addresses

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. NAT protects the identity of a network and does not show internal IP addresses to the Internet. You can also use NAT to supply more IPv4 and IPv6 addresses for the network.

The Security Gateway can change both the source and destination IP addresses in a packet. For example, when an internal computer sends a packet to an external computer, the Security Gateway translates the source IP address to a new one. The packet comes back from the external computer; the Security Gateway translates the new IP address back to the original IP address. The packet from the external computer goes to the correct internal computer.

SmartConsole gives you the flexibility to make necessary configurations for your network:

- Easily enable the Security Gateway to translate all traffic that goes to the internal network.
- SmartConsole can automatically create Static and Hide NAT rules that translate the applicable traffic.
- You can manually create NAT rules for different configurations and deployments.

How Security Gateways Translate Traffic

A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Security Gateway can allow external traffic to access internal resources.

  The configuration of static NAT on a *range* results in the translation of the IP addresses in the range into a *range of the same size, starting with the IP address specified.*

- **Hide NAT** - The Security Gateway uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers; external computers CANNOT access internal servers. The Security Gateway can translate up to 50,000 connections at the same time from external computers and servers.
- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Security Gateway uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules to use Port Translation (see *"NAT Rules" on page 242*).

Using Hide NAT

For each SmartConsole object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object

Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- `rlogin` (destination port 512)
- `rshell` (destination port 513)
- `rexec` (destination port 514)

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Sample NAT Deployments

Static NAT

Firewalls that do Static NAT, translate each internal IP address to a different external IP address.

Item	Description
3	External computers and servers in the Internet
2	Security Gateway configured with Static NAT
1	Internal computers

Sample Static NAT Workflow

An external computer in the Internet sends a packet to 192.0.2.5. The Security Gateway translates the IP address to 10.10.0.26 and sends the packet to internal computer A. Internal computer A sends back a packet to the external computer. The Security Gateway intercepts the packet and translates the source IP address to 192.0.2.5.

Internal computer B (10.10.0.37) sends a packet to an external computer. The Security Gateway intercepts the packet translates the source IP address to 192.0.2.16.

Internet sends packet to 192.0.2.5 → Security Gateway translates this address to **10.10.0.26** → Internal computer A receives packet

Internal computer A (10.10.0.26) sends packet to Internet → Security Gateway translates this address to **192.0.2.5** → Internet receives packet from 192.0.2.5

Internal computer B (10.10.0.37) sends packet to Internet → Security Gateway translates this address to **192.0.2.16** → Internet receives packet from 192.0.2.16

Hide NAT

Firewalls that do Hide NAT use different port numbers to translate internal IP address to one external IP address. External computers cannot start a connection to an internal computer.

Item	Description
1	Internal computers
2	Security Gateway configured with Hide NAT
3	External computers and servers in the Internet

Sample Hide NAT Workflow

Internal computer A (10.10.0.26) sends a packet to an external computer. The Security Gateway intercepts the packet and translates the source IP address to 192.0.2.1 port 11000. The external computer sends back a packet to 192.0.2.1 port 11000. The Security Gateway translates the packet to 10.10.0.26 and sends it to internal computer A.

Internal computer A (10.10.0.26) sends packet to Internet → Security Gateway translates this address to **192.0.2.1 port 11000** → Internet receives packet from 192.0.2.1 port 11000

Internet sends back packet to 192.0.2.1 port 11000 → Security Gateway translates this address to **10.10.0.26** → Internal computer A receives packet

NAT Rules

The NAT Rule Base has two sections that specify how the IP addresses are translated:

- **Original Packet**
- **Translated Packet**

Each section in the NAT Rule Base is divided into cells that define the **Source**, **Destination**, and **Service** for the traffic.

This is how a NAT Rule Base looks:

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for X (Y-Z)								
1	Object1	Object2	Any	= Original	= Original	= Original	Policy Targets	
2	Object3	Object4	Any	S Object5	S Object6	= Original	Policy Targets	
3	Object7	Object8	Any	H Object9	H Object10	= Original	Policy Targets	

Automatic and Manual NAT Rules

There are two types of NAT rules for network objects:

- Rules that SmartConsole automatically creates and adds to the NAT Rule Base
- Rules that you manually create and then add to the NAT Rule Base

When you create manual NAT rules, it can be necessary to create the translated NAT objects for the rule.

Using Automatic Rules

You can enable automatic NAT rules for these SmartConsole objects:

- Security Gateways
- Hosts
- Networks
- Address Ranges

SmartConsole creates two automatic rules for Static NAT, to translate the source and the destination of the packets.

For Hide NAT, one rule is created to translate the source of the packets.

For network and address range objects, SmartConsole creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the NAT automatic rules:

Type of Traffic	Static NAT	Hide NAT
Internal to external	Rule translates source IP address	Rule translates source IP address
External to internal	Rule translates destination IP address	N/A (External connections are not allowed)
Intranet (for network and address range objects)	Rule does not translate IP address	Rule does not translate IP address

Order of NAT Rule Enforcement

The Firewall enforces the NAT Rule Base in a sequential manner. Automatic and manual rules are enforced differently. Automatic rules can use bidirectional NAT to let two rules be enforced for a connection.

- **Manual rules** - The first manual NAT rule that matches a connection is enforced. The Firewall does not enforce a different NAT rule that can be more applicable.
- **Automatic rules** - Two automatic NAT rules that match a connection, one rule for the **Source** and one for the **Destination** can be enforced. When a connection matches two automatic rules, those rules are enforced.

SmartConsole organizes the automatic NAT rules in this order:

1. Static NAT rules for Firewall, or host (computer or server) objects
2. Hide NAT rules for Firewall, or host objects
3. Static NAT rules for network or address range objects
4. Hide NAT rules for network or address range objects

Sample Automatic Rules

Here are some sample automatic rules.

Static NAT for a Network Object

1. Intranet connections in the HR network are not translated. The Firewall does not translate a connection between two computers that are part of the HR object.

   The Firewall does not apply rules 2 and 3 to traffic that matches rule 1.
2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.
3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.

Hide NAT for Address Range

1. Intranet connections in the Sales address range are not translated. The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.

   The Firewall does not apply rule 2 to traffic that matches rule 1.
2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

Configuring Static and Hide NAT

You can enable and configure NAT for SmartConsole objects.

Configuring Static NAT

When you enable Static NAT, each object is translated to a different IP address. SmartConsole can automatically create the NAT rules, or you can create them manually.

Configuring Hide NAT

Hide NAT uses different port numbers to identify the internal IP addresses. When you enable Hide NAT mode, the Firewall can translates the IP address to:

- The IP address of the external Security Gateway interface
- The IP address for the object

Note - You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Enabling Automatic NAT

SmartConsole can automatically create and configure the NAT rules for a network. Enable automatic NAT for every object, for which you are translating the IP address. Then configure the Access Control Rule Base to allow traffic to the applicable objects.

To enable automatic NAT

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.

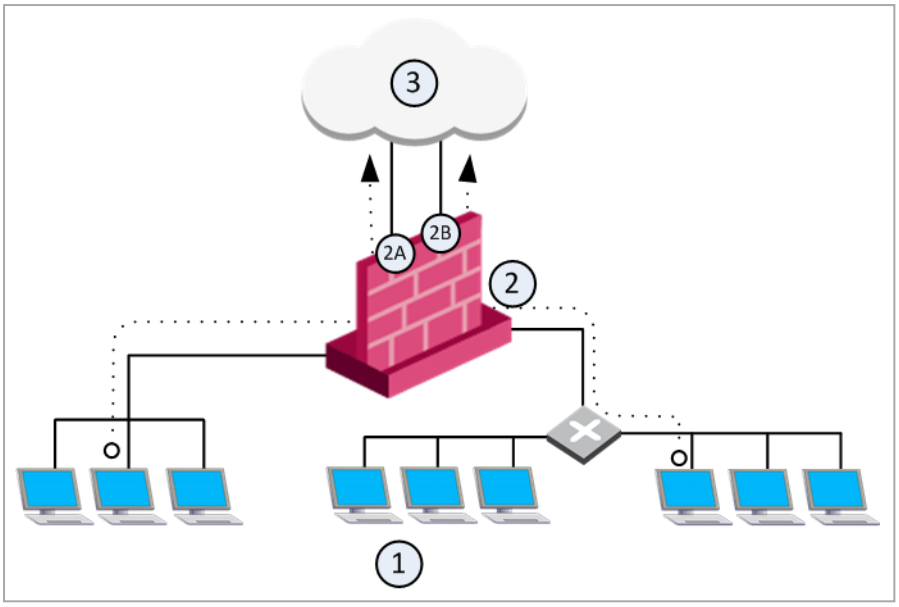
   The **General Properties** window of the gateway opens.
2. From the navigation tree, select **NAT** > **Advanced**.
3. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
4. Select the **Translation method**: **Hide** or **Static**.
5. Configure the NAT IP address for the object.
   - **Hide behind Gateway** - Use the IP address of the Security Gateway
   - **Hide behind IP address** - Enter the IP address.
6. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
7. Click **OK**.
8. Install the Access Control Policy.

After you enable and configure NAT on all applicable gateways, install the policy.

Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses. An easy alternative is to enable a Firewall to automatically Hide NAT for all traffic with external networks. The Firewall translates all traffic that goes through an external interface to the valid IP address of that interface.

In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of an external interface.



Item	Description
1	Internal networks
2	Security Gateway - Firewall is configured with automatic Hide NAT.
2A and 2B	Two external interfaces 192.0.2.1 and 192.0.2.100.
1 -->3	External computers and servers on the Internet

Source IP addresses are translated to the applicable external interface IP address: **192.0.2.1** or **192.0.2.100**.

Note - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.

To enable automatic Hide NAT

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.

   The **General Properties** window of the gateway opens.
2. From the navigation tree, select **NAT**.
3. Select **Hide internal networks behind the Gateway's external IP**.
4. Click **OK**.
5. Install the Access Control Policy.

Enabling Manual NAT

For some deployments, it is necessary to manually define the NAT rules. Create SmartConsole objects that use the **valid** (NATed) IP addresses. Create NAT rules to translate the original IP addresses of the objects to valid IP addresses. Then configure the Firewall Rule Base to allow traffic to the applicable translated objects with these valid IP addresses.

Note - For manual NAT rules, it is necessary to configure Proxy ARP entries to associate the translated IP address. See *" Advanced NAT Settings " on page 274* - section "*Automatic and Proxy ARP*".

These are some situations that must use manual NAT rules:

- Rules that are restricted to specified destination IP addresses and to specified source IP addresses
- Translate both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translate services (destination ports)
- Rules that only use specified services (ports)
- Translate IP addresses for dynamic objects

This procedure explains how to configure manual Static NAT for a web server. You can also configure manual Hide NAT for SmartConsole objects. See *"Sample Deployment (Manual Rules for Port Translation)" on page 249*.

To enable manual Static NAT, follow this workflow

1. Create a clone from the network object, for example, the Web server.
2. Add a NAT rule that maps the original object to the NATed one.
3. Add Access Control rules that allow traffic to the new NATed objects.

To create a clone network object

1. In SmartConsole, right-click the object and select **Clone**.

   The **General Properties** window of the new object opens.
2. Enter the **Name**. We recommend that you name the object **<name>_valid_address**.
3. Enter the NATed IP address.
4. Click **OK**.

To add a NAT rule to the Rule Base

1. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.
2. Add a manual rule above the automatic NAT rules.
3. Configure the manual rule to translate the IP address. For example:
   - **Original Source** - **WebServer**
   - **Translated Source** - **WebServer_valid_address**

To add Access Control rules

1. In SmartConsole, go to **Security Policies** > **Access Control** > **Policy**.
2. Add rules that allow traffic to the applicable NATed objects.

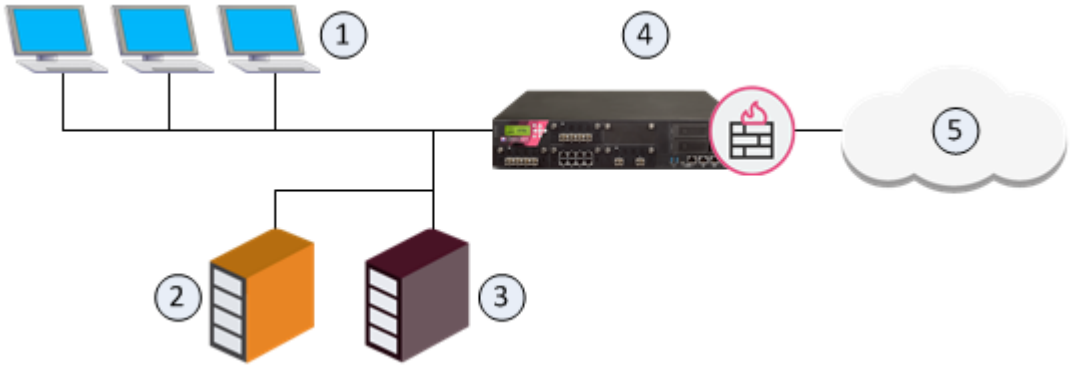
   These objects are the cloned objects that are called **<name>_valid_address**.

3. Install the policy.

Sample Deployment (Static and Hide NAT)

The goal for this sample deployment is to configure:

- Static NAT for the SMTP and the HTTP servers on the internal network. These servers can be accessed from the Internet using public addresses.
- Hide NAT for the users on the internal network that gives them Internet access. This network cannot be accessed from the Internet.



Item	Description
1	Internal computers (Alaska_LAN 2001:db8::/64)
2	Web server (Alaska.Web 2001:db8:0:10::5 translated to 2001:db8:0:a::5)
3	Mail server (Alaska.Mail 2001:db8:0:10::6 translated to 2001:db8:0:a::6)
4	Security Gateway (External interface 2001:db8:0:a::1)
5	External computers and servers in the Internet

To configure NAT for the network

1. **Enable automatic Static NAT for the web server.**
   a. Double-click the **Alaska.Web** object and select **NAT**.
   b. Select **Add Automatic Address Translation Rules**.
   c. In **Translation method**, select **Static**.
   d. Select **Hide behind IP Address** and enter **2001:db8:0:a::5**.
   e. Click **OK**.
2. **Enable automatic Static NAT for the mail server.**
   a. Double-click the **Alaska.Mail** object and select **NAT**.
   b. Select **Add Automatic Address Translation Rules**.

c. In **Translation method**, select **Static**.

d. Select **Hide behind IP Address** and enter **2001:db8:0:a::6**.

e. Click **OK**.

3. **Enable automatic Hide NAT for the internal computers.**

   a. Double-click the **Alaska_LAN** object and select **NAT**.

   b. Select **Add Automatic Address Translation Rules**.

   c. In **Translation method**, select **Hide**.

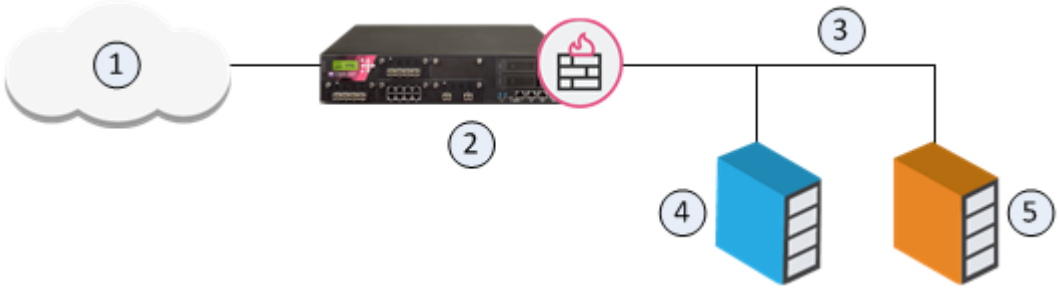
   d. Select **Hide behind Gateway**.

4. Click **OK**.

5. Install the Access Control Policy.

Sample Deployment (Manual Rules for Port Translation)

The goal for this sample configuration is to let external computers access a web and mail server in a DMZ network from one IP address. Configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.



Item	Description
1	External computers and servers in the Internet
2	Security Gateway (Alaska_GW external interface 2001:db8:0:c::1)
3	DMZ network (Alaska_DMZ 2001:db8:a::/128)
4	Web server (Alaska_DMZ_Web 2001:db8:a::35:5 translated to 2001:db8:0:c::1)
5	Mail server (Alaska_DMZ_Mail 2001:db8:a::35:6 translated to 2001:db8:0:c::1)

To configure NAT for the DMZ servers

1. **Enable automatic Hide NAT for the DMZ network.**

   a. Double-click the **Alaska_DMZ** object and select **NAT**.

   b. Select **Add Automatic Address Translation Rules**.

   c. In **Translation method**, select **Hide**.

d. Select **Hide behind Gateway**.

e. Click **OK**.

2. **Create a manual NAT rule that translates HTTP traffic from the Security Gateway to the web server.**

   a. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.

   b. Add a rule below the automatic rules.

   c. Right-click the cell and select **Add new items** to configure these settings:

      - **Original Destination** - **Alaska_GW**
      - **Original Service** - **HTTP**
      - **Translated Destination** - **Alaska_DMZ_Web**

3. **Create a manual NAT rule that translates SMTP traffic from the Security Gateway to the mail server.**

   a. Add a rule below the automatic rules.

   b. Right-click the cell and select **Add new items** to configure these settings:

      - **Original Destination** - **Alaska_GW**
      - **Original Service** - **SMTP**
      - **Translated Destination** - **Alaska_DMZ_Web**

4. **Create a rule in the Firewall Rule Base that allows traffic to the servers.**

   a. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.

   b. Add a rule to the Rule Base.

   c. Right-click the cell and select **Add new items** to configure these settings:

      - **Destination** - **Alaska_DMZ**
      - **Service** - **HTTP, SMTP**
      - **Action** - **Allow**

5. Install the Access Control Policy.

NAT Rule Base for Manual Rules for Port Translation Sample Deployment

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	Original	Original	Original	All	Automatic rule

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	Original	Original	All	Automatic rule
3	Any	Alaska_GW	http	Original	S Alaska_DMZ_Web	Original	Policy Targets	
4	Any	Alaska_GW	smtp	Original	S Alaska_DMZ_Mail	Original	Policy Targets	

Configuring Stateful NAT64 (IPv6 to IPv4 translation)

Background:

NAT64 translation (RFC 6146) lets **IPv6-only client** communicate with **IPv4-only server** using **unicast** UDP, TCP, or ICMP.

IPv6-only client is one of these:

- A host with a networking stack that implements only IPv6.
- A host with a networking stack that implements both IPv4 and IPv6 protocols, but with only IPv6 connectivity.
- A host that runs an IPv6-only client application.

IPv4-only server is one of these:

- A host with a networking stack that implements only IPv4.
- A host with a networking stack that implements both IPv4 and IPv6 protocols, but with only IPv4 connectivity.
- A host that runs an IPv4-only server application.

The translation of IP addresses is done by translating the packet headers according to the IP/ICMP Translation Algorithm defined in RFC 6145. The IPv4 addresses of IPv4 hosts are translated to and from IPv6 addresses using the algorithm defined in RFC 6052, and an IPv6 prefix assigned to the stateful NAT64 for this specific purpose.

Note - For information about DNS64, see RFC 6147.

Properties of Stateful NAT64:

- Performs N:M translation:

- N must be greater than M
- If M=1, performs a Hide NAT behind a single IPv4 address.
- If M>1, performs a Hide NAT behind a range of IPv4 addresses.

- Gives good IPv4 address preservation (multiplexed using ports).
- Saves connection states and binding.
- There are no requirements on the assignment of IPv6 addresses to IPv6 clients. Any mode of IPv6 address assignment is legitimate (Manual, DHCP6, SLAAC).
- It is a scalable solution.

NAT64 use case scenarios:

- [IPv6 Network] --- (Internet) --- [Security Gateway] --- [internal IPv4 Network]

  Common use case for Content Providers. DNS64 is not needed.
- [internal IPv6 Network] --- [Security Gateway] --- (Internet) --- [IPv4 Network]

  Common use case for Carriers, ISPs, Enterprises. DNS64 is required.
- [IPv6 Network] --- [Security Gateway] --- [IPv4 Network]

  Common use case for Enterprises. DNS64 is required.

These standards are supported for NAT64:

- RFC 6144 - Framework for IPv4/IPv6 Translation
- RFC 6146 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC 6052 - IPv6 Addressing of IPv4/IPv6 Translators
- RFC 6145 - IP/ICMP Translation Algorithm
- RFC 2428 - FTP Extensions for IPv6 and NATs
- RFC 6384 - An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation

These features are not supported for NAT64:

- VoIP traffic.
- HTTPS Inspection.
- SSL de-multiplexer.
- Security Gateway in HTTP Proxy mode.
- IPS protection "HTTP Header Spoofing".

Workflow for configuring NAT64 rules:

1. Prepare your Security Gateway for NAT64
2. Define the NAT64 rules.
3. Configure the additional settings for NAT64.

Preparing Security Gateway for NAT64

Note - In cluster, do these steps on *each* cluster member.

Procedure

Step	Instructions
1	Make sure that an IPv6 address is assigned to the interface that connects to the destination IPv4 network, and the IPv6 network prefix length is equal to, or less than **96**. **Note** - This can be any valid IPv6 address with the IPv6 network prefix length equal to, or less than **96**. ■ In Gaia Portal: Click **Network Management > Network Interfaces**. ■ In Gaia Clish: Run: `show interface <Name of Interface> ipv6-address` If such IPv6 address is not assigned yet, assign it now. For details, see *R81 Gaia Administration Guide* - Chapter *Network Management* - Section *Network Interfaces* - Section *Physical Interfaces*.

Step	Instructions
2	Make sure that the IPv6 routing is configured to send the traffic that is destined to the NATed IPv6 addresses (defined in the *Original Destination* column in the NAT64 rule) through the interface that connects to the destination IPv4 network. ■ In Gaia Portal: Click **Advanced Routing > Routing Monitor**. ■ In Gaia Clish: Run: `show ipv6 route` If such route does not already exist, add it in Gaia Clish. For details, see *R81 Gaia Administration Guide*. Run these commands in Gaia Clish: 1. Add the static route: `set ipv6 static-route <NATed Destination IPv6 Addresses>/<96 or less> nexthop gateway <Any IPv6 Address from the IPv6 subnet of the Interface that connects to the destination real IPv4 network> on` Example topology: [IPv6 Client] --- (NATed IPv6 of IPv4 side are 1111:2222::/96) [Security Gateway] (eth3 with IPv6 3333:4444::1) --- [IPv4 Server] In such case, configure the IPv6 route using this command: `set ipv6 static-route 1111:2222::/96 nexthop gateway 3333:4444::10 on` 2. Save the configuration: `save config`

Step	Instructions
3	Make sure that the number of IPv6 CoreXL Firewall instances is **equal** to the number of IPv4 CoreXL Firewall instances. a. Connect to the command line on the Security Gateway. b. Log in to Gaia Clish, or Expert mode. c. Show the number of IPv6 CoreXL Firewall instances: `fw6 ctl multik stat` d. Show the number of IPv4 CoreXL Firewall instances: `fw ctl multik stat` e. If the number of IPv6 CoreXL Firewall instances is less than the number of IPv4 CoreXL Firewall instances, then do these steps: i. Run: `cpconfig` ii. Select **Check Point CoreXL** iii. Select **Change the number of IPv6 firewall instances** iv. Configure the number of IPv6 CoreXL Firewall instances to be the same as the number of IPv4 CoreXL Firewall instances v. Select **Exit** vi. Reboot the Security Gateway f. Connect to the command line on the Security Gateway. g. Log in to Gaia Clish, or Expert mode. h. Show the number of IPv6 CoreXL Firewall instances: `fw6 ctl multik stat` i. Show the number of IPv4 CoreXL Firewall instances: `fw ctl multik stat` Example output: `[Expert@GW:0]# fw ctl multik stat` `ID | Active | CPU | Connections | Peak` `----------` ` 0 | Yes | 3 | 10 | 14` ` 1 | Yes | 2 | 6 | 15` ` 2 | Yes | 1 | 7 | 15` `[Expert@GW:0]#` `[Expert@GW:0]# fw6 ctl multik stat` `ID | Active | CPU | Connections | Peak` `----------` ` 0 | Yes | 3 | 0 | 0` ` 1 | Yes | 2 | 0 | 4` ` 2 | Yes | 1 | 0 | 2` `[Expert@GW:0]#`

Defining NAT64 Rules

Define NAT64 rules as Manual NAT rules in the Access Control Policy. Make sure that you add access rules that allow this NAT traffic.

Do these steps in SmartConsole to define NAT64 rules

1. Define a source IPv6 Network object.

   This object represents the source IPv6 addresses, which you translate to source IPv4 addresses.

2. Define a translated destination IPv6 Network object with an IPv4-embedded IPv6 address, or a translated destination IPv6 Host object with a static IPv6 address.

   This object represents the translated destination IPv6 address, to which the IPv6 sources connect.

3. Define a translated source IPv4 Address Range object.

   This object represents the translated source IPv4 addresses, to which you translate the original source IPv6 addresses.

4. Create a Manual NAT64 rule.

5. Install the Access Control Policy.

To define a source IPv6 Network object that represents the source IPv6 address, which you translate to source IPv4 addresses

1. Click **Objects** menu > **New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.

6. In the **IPv6** section:

   a. In the **Network address** field, enter the IPv6 address of your IPv6 network, which you translate to source IPv4 addresses.

   b. In the **Prefix** field, enter the prefix of your IPv6 network.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a translated destination IPv6 Network object with IPv4-embedded IPv6 address that represents the IPv6 addresses, to which the IPv6 sources connect

1. Click **Objects** menu > **New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.

6. In the **IPv6** section:

a. In the **Network address** field, enter the destination *IPv4-embedded* IPv6 address (also called *IPv4-mapped* IPv6 address), to which the IPv6 sources connect.

Such IPv6 address contains (from left to right) 80 "zero" bits, followed by 16 "one" bits, and then the 32 bits of the IPv4 address - 0:0:0:0:0:FFFF:X.Y.Z.W, where X.Y.Z.W are the four octets of the destination IPv4 address.

For example, for IPv4 network 192.168.3.0, the IPv4-embedded IPv6 address is 0:0:0:0:0:FFFF:192.168.3.0, or 0:0:0:0:0:FFFF:C0A8:0300. For more information, see RFC 6052.

These IPv4-embedded IPv6 addresses are published by an external DNS64 server.

b. In the **Prefix** field, enter the applicable IPv6 prefix.

Note - You can define IPv4-embedded IPv6 addresses only for these object types: Address Range, Network, and Host.

7. On the **NAT** page of this object:

Do not configure anything.

8. Click **OK**.

To define a translated destination IPv6 Host object with static IPv6 address that represents the IPv6 address, to which the IPv6 sources connect

1. Click **Objects** menu > **New Host**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

Do not enter anything.

6. In the **IPv6** section:

In the **Network address** field, enter the destination static IPv6 address, to which the IPv6 sources connect.

7. On the **NAT** page of this object:

Do not configure anything.

8. Configure the applicable settings on other pages of this object.
9. Click **OK**.

To define a translated source IPv4 Address Range object that represents the IPv4 addresses, to which you translate the source IPv6 addresses

1. Click **Objects** menu > **More object types** > **Network Object** > **Address Range** > **New Address Range**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.

5. In the **IPv4** section:
   a. In the **First IP address** field, enter the first IPv4 address of your IPv4 addresses range, to which you translate the source IPv6 addresses.
   b. In the **Last IP address** field, enter the last IPv4 address of your IPv4 addresses range, to which you translate the source IPv6 addresses.

   Notes:
   - This IPv4 addresses range must not use private IPv4 addresses (see RFC 1918 and **Menu** > **Global properties** > **Non Unique IP Address Range**
   - This IPv4 addresses range must not be used on the IPv4 side of the network.
   - We recommend that you define a large IPv4 addresses range for more concurrent NAT64 connections.
6. In the **IPv6** section:

   Do not enter anything.
7. On the **NAT** page of this object:

   Do not configure anything.
8. Click **OK**.

To create a Manual NAT64 rule

1. From the left Navigation Toolbar, click **Security Policies**.
2. In the top **Access Control** section, click **NAT**.
3. Right-click on the **Manual Lower Rules** section title, and near the **New Rule**, click **Above** or **Below**.

   Configure this Manual NAT64 rule:

   Important - Some combinations of object types are not supported in the *Original Source* and *Original Destination* columns. See the summary table with the supported NAT rules at the bottom of this section.
   a. In the **Original Source** column, add the IPv6 object for your original source IPv6 addresses.

      In this rule column, NAT64 rules support only these types of objects:
      - `*Any`
      - Host with a static IPv6 address
      - Address Range with IPv6 addresses
      - Network with IPv6 address

b. In the **Original Destination** column, add a translated destination IPv6 object with an IPv4-embedded IPv6 address.

   In this rule column, NAT64 rules support only these types of objects:

   - Host with a static IPv6 address
   - Address Range with IPv4-embedded IPv6 addresses
   - Network with an IPv4-embedded IPv6 address

c. In the **Original Services** column, you must leave the default **Any**.

d. In the **Translated Source** column, add the IPv4 **Address Range** object for your translated source IPv4 addresses range.

   In this rule column, NAT64 rules support only these types of objects:

   - Host with a static IPv4 address, only if in the **Original Source** column you selected a Host with a static IPv6 address
   - Address Range with IPv4 addresses

e. In the **Translated Source** column, right-click the IPv4 **Address Range** object > click **NAT Method** > click **Stateful NAT64**:

   - The **Translated Packet Destination** column shows **= Embedded IPv4 Address**.
   - The **64** icon shows in both the **Translated Source** and **Translated Destination** columns.

   In this rule column, NAT64 rule supports only these types of objects:

   - Host with a static IPv4 address, only if in the **Original Source** column you selected a Host with a static IPv6 address
   - Embedded IPv4 Address

f. In the **Translated Services** column, you must leave the default **= Original**.

4. Install the Access Control Policy.

To summarize, you must configure only these Manual NAT64 rules (rule numbers are for convenience only):

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	`*Any`	IPv6 *Host* object with a static IPv6 address	`*Any`	IPv4 *Address Range* object	IPv4 *Host* object	`= Original`
2	`*Any`	IPv6 *Address Range* object with an IPv4-embedded IPv6 addresses	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
3	*Any	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
4	IPv6 *Host* object with a static IPv6 address	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Host* object	IPv4 *Host* object	= Original
5	IPv6 *Host* object with a static IPv6 address	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
6	IPv6 *Host* object with a static IPv6 address	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
7	IPv6 *Address Range* object	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Address Range* object	IPv4 *Host* object	= Original
8	IPv6 *Address Range* object	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
9	IPv6 *Address Range* object	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
10	IPv6 *Network* object	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Address Range* object	IPv4 *Host* object	= Original
11	IPv6 *Network* object	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
12	IPv6 *Network* object	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original

Configuring the Additional Settings for NAT64

You can configure the additional settings that control the NAT64 translation mechanism. These settings are compliant with RFC 6145.

> **Best Practice** - We recommend that you change the default settings only if you are familiar with the technology.

Procedure

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with GuiDBedit Tool (see sk13009) to the applicable Security Management Server or Domain Management Server.
3. In the top left section, click **Table > Global Properties > properties**.
4. In the top right section, click **firewall_properties**.
5. In the bottom section, scroll to these **Field Names**:

- `nat64_add_UDP_checksum`
- `nat64_avoid_PMTUD_blackhole`
- `nat64_copy_type_of_service`
- `nat64_error_message_on_dropped_packets`

6. Right-click on the applicable Field Name and click **Edit**.
7. Select the applicable **Value** (**true**, or **false**). Click **OK**.

Field Name	Description
`nat64_add_UDP_checksum`	This setting controls whether the translator should calculate and add a valid UDP checksum value to a packet, if the packet checksum value is zero. This is important because, by default, an IPv4 UDP packet with a checksum value of zero is dropped on the IPv6 side. **Default:** false
`nat64_avoid_PMTUD_blackhole`	This setting controls whether to allow packet fragmentation on the IPv4 (destination) side during PMTU discovery. Enable this setting if some equipment combinations cause PMTU discovery to fail. **Default:** false
`nat64_copy_type_of_service`	This setting controls whether to copy the traffic **Class Field** to the **Type Of Service** field, and set the **Type Of Service** field in the translated packet to zero. **Default:** true
`nat64_error_message_on_dropped_packets`	This setting controls whether to generate an audit log after a connection is closed. For each closed connection, the log shows: ■ Connection information (source and destination IP address, source port, and service). ■ Translated source IP address and source port. ■ Start time and end time. ■ If the connection was closed because the connection expired, log shows additional information in the **TCP End Reason** field. If this field does not show in the log, the connection was closed with a TCP RST, or with a TCP FIN, and did not expire. **Default:** true

8. Save the changes (click **File > Save All**).
9. Close the GuiDBedit Tool.
10. Connect with the SmartConsole to the applicable Security Management Server or Domain Management Server.
11. Install the Access Control Policy.

Logging of NAT64 traffic

In the Security Gateway log for NAT64 connection, the source and destination IPv6 addresses show in their original IPv6 format. To identify a NAT64 entry, look in the **More** section of the **Log Details** window.

Field in Log	Description
Xlate (NAT) Source IP	Shows the translated source IPv4 address, to which the Security Gateway translated the original source IPv6 address
Xlate (NAT) Destination IP	Shows the translated destination IPv4 address, to which the Security Gateway translated the original destination IPv6 address
More	Identifies the entry as NAT64 traffic (`Nat64 enabled`)

Example of NAT64 Translation Flow

Example topology

[IPv6 Client] --- (interface) [Security Gateway] (internal) --- [IPv4 Server]

Where:

Item	Description
IPv6 Client	IPv6 real address is 1111:1111::0100/96
Security Gateway external interface	IPv6 address is 1111:1111::1/96
Security Gateway internal interface	IPv4 address is 10.0.0.1/24 IPv6 address is 3333:4444::1/96
IPv4 Server	IPv4 real address is 10.0.0.100/24 IPv6 NATed address is 1111:2222::0A00:0064/96
IPv6 NATed network	IPv6 address of the network on the external Security Gateway side is 1111:2222::/96 These IPv6 addresses are used to translate the IPv4 address of the IPv4 Server to the IPv6 address
IPv4 NATed network	IPv4 address of the network on the internal Security Gateway side is 1.1.1.0/24 These IPv4 addresses are used to translate the IPv6 address of the IPv6 Client to the IPv4 address

Traffic flow

1. IPv6 Client opens an IPv6 connection to the NATed IPv6 address of the IPv4 Server:

   From the IPv6 Client's IPv6 real address 1111:1111::0100 to the IPv4 Server's NATed IPv6 address 1111:2222::0A00:0064

   Where:

   The "1111:2222::" part is the NATed IPv6 subnet

   The "0A00:0064" part is 10.0.0.100

2. Security Gateway performs these NAT translations:

   a. Translate the IPv6 Client's *source* address from the real IPv6 address 1111:1111::0100 to the special concatenated *source* IPv6 address 0064:FF9B::0101:01X

      Where:

      The "0064:FF9B::" part is a well-known prefix reserved for NAT64 (as defined by the RFC)

      The "0101:01XX" part is 1.1.1.X

   b. Translate the IPv6 Client's *source* address from the special concatenated *source* IPv6 address 0064:FF9B::0101:01XX to the *source* IPv4 address 1.1.1.X

   c. Translate the IPv6 Client's NATed *destination* address from the IPv6 address 1111:2222::0A00:0064 to the NATed destination IPv4 address 10.0.0.100

3. IPv4 Server receives this request connection as from the *source* IPv4 address 1.1.1.X to the *destination* IPv4 address 10.0.0.100

4. IPv4 Server replies to this connection from the *source* IPv4 address 10.0.0.100 to the *destination* IPv4 address 1.1.1.X

5. Security Gateway performs these NAT translations:

   a. Translate the IPv4 Server's *source* real IPv4 address 10.0.0.100 to the *source* NATed IPv6 address 1111:2222::0A00:0064

   b. Translate the IPv6 Client's NATed *destination* IPv4 address 1.1.1.X to the *destination* special concatenated IPv6 address 0064:FF9B::0101:01X

      Where:

      The "64:FF9B::" part is a well-known prefix reserved for NAT64 (as defined by the RFC)

      The "0101:01XX" part is 1.1.1.X

   c. Translate the IPv6 Client's *destination* special concatenated IPv6 address 0064:FF9B::0101:01XX to the *destination* IPv6 real address 1111:1111::0100

6. IPv6 Client receives this reply connection as from the *source* IPv6 address 1111:2222::0A00:0064 to the *destination* IPv6 address 1111:1111::0100

Summary

- *Request*: [IPv6 Client] ---> [Security Gateway] ---> [IPv4 Server]

Field in packet	Original IPv6 packet	NATed IPv4 packet
Source IP	1111:1111::0100 / 96	1.1.1.X / 24
Destination IP	1111:2222::0A00:0064 / 96	10.0.0.100 / 24

- *Reply*: [IPv6 Client] <--- [Security Gateway] <--- [IPv4 Server]

Field in packet	Original IPv4 packet	NATed IPv6 packet
Source IP	10.0.0.100 / 24	1111:2222::0A00:0064 / 96
Destination IP	1.1.1.X / 24	1111:1111::0100 / 96

Configuring Stateless NAT46 (IPv4 to IPv6 translation)

NAT46 rules are only supported on Security Gateways and Cluster Members R80.20 and higher.

Background:

NAT46 translation lets an **IPv4** network communicate with an **IPv6** network without maintaining any session information on Security Gateway.

Properties of Stateless NAT46:

- Performs 1:1 IP address mapping.
- The system generates the translated source IPv6 address as a combination of these two parts:
  1. A user-defined Network object with an IPv6 address defined with the 96-bit prefix.
  2. The source IPv4 address, which is added as a 32-bit suffix.

NAT46 use case scenarios:

- [IPv4 Network] --- (Internet) --- [Security Gateway] --- [IPv6 Network]

  Common use case for Content Providers.
- [IPv4 Network] --- [Security Gateway] --- (Internet) --- [IPv6 Network]

  Common use case for Enterprises.

These features are not supported for NAT46:

- VoIP traffic.
- FTP traffic.
- Any protocols that require state information between Control and Data connections.

Preparing Security Gateway for NAT46

Note - In cluster, do these steps on *each* cluster member.

Procedure

Step	Instructions
1	Make sure that an IPv6 address is assigned to the interface that connects to the destination IPv6 network, and the IPv6 network prefix length is equal to 96. **Note** - This can be any valid IPv6 address with the IPv6 network prefix length equal to **96**. ■ In Gaia Portal: Click **Network Management > Network Interfaces**. ■ In Gaia Clish: Run: `show interface <Name of Interface> ipv6-address` If such IPv6 address is not assigned yet, assign it now. For details, see *R81 Gaia Administration Guide* - Chapter *Network Management* - Section *Network Interfaces* - Section *Physical Interfaces*.
2	Make sure that the routing is configured to send the traffic that is destined to the NATed IPv4 addresses (defined in the *Translated Destination* column in the NAT46 rule) through the interface that connects to the destination IPv6 network. ■ In Gaia Portal: Click **Advanced Routing > Routing Monitor**. ■ In Gaia Clish: Run: `show route` If such route does not already exist, add it in Gaia Clish. For details, see *R81 Gaia Administration Guide*. Run these commands in Gaia Clish: 1. Add the static route: `set static route <NATed Destination IPv4 Addresses>/<NATed IPv4 Net Mask> nexthop gateway logical <Name of Interface that connects to the real IPv6 Network> on` Example topology: [IPv4 Client] --- (NATed IPv4 of IPv6 side are 1.1.1.0/24) [Security Gateway] (eth3) --- [IPv6 Server] In such case, configure the IPv4 route using this command: `set static route 1.1.1.0/24 nexthop gateway logical eth3 on` 2. Save the configuration: `save config`

Step	Instructions
3	Make sure that the number of IPv6 CoreXL Firewall instances is **equal** to the number of IPv4 CoreXL Firewall instances. 1. Connect to the command line on the Security Gateway. 2. Log in to Gaia Clish, or Expert mode. 3. Show the number of IPv6 CoreXL Firewall instances: `fw6 ctl multik stat` 4. Show the number of IPv4 CoreXL Firewall instances. Run: `fw ctl multik stat` 5. If the number of IPv6 CoreXL Firewall instances is less than the number of IPv4 CoreXL Firewall instances, then do these steps: a. Run: `cpconfig` b. Select **Check Point CoreXL** c. Select **Change the number of IPv6 firewall instances** d. Configure the number of IPv6 CoreXL Firewall instances to be the same as the number of IPv4 CoreXL Firewall instances e. Select **Exit** f. Reboot the Security Gateway 6. Connect to the command line on the Security Gateway. 7. Log in to Gaia Clish, or Expert mode. 8. Show the number of IPv6 CoreXL Firewall instances. Run: `fw6 ctl multik stat` 9. Show the number of IPv4 CoreXL Firewall instances. Run: `fw ctl multik stat` Example output: `[Expert@GW:0]# fw6 ctl multik stat` `ID | Active | CPU | Connections | Peak` `0 | Yes | 3 | 0 | 0` `1 | Yes | 2 | 0 | 4` `2 | Yes | 1 | 0 | 2` `[Expert@GW:0]#` `[Expert@GW:0]# fw ctl multik stat` `ID | Active | CPU | Connections | Peak` `0 | Yes | 3 | 10 | 14` `1 | Yes | 2 | 6 | 15` `2 | Yes | 1 | 7 | 15` `[Expert@GW:0]#`

Defining NAT46 Rules

Define NAT46 rules as Manual NAT rules in the Access Control Policy. Make sure that you add access rules that allow this NAT traffic.

Do these steps in SmartConsole to define NAT46 rules

1. Define an applicable source IPv4 object (IPv4 Host, IPv4 Address Range, or IPv4 Network).
2. Define a destination IPv4 Host object.

   This object represents the destination IPv4 address, to which the IPv4 sources connect.
3. Define a translated source IPv6 Network object with an IPv6 address defined with the 96-bit prefix.

   This object represents the translated source IPv6 addresses, to which you translate the source IPv4 addresses.
4. Define a translated destination IPv6 Host object.

   This object represents the translated destination IPv6 address, to which the translated IPv4 sources connect.
5. Create a Manual NAT46 rule.
6. Install the Access Control Policy.

To define a source IPv4 Host object

1. Click **Objects** menu > **New Host**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4 address** field, enter the source IPv4 address.
6. In the **IPv6** section:

   Do not enter anything
7. On the **NAT** page of this object:

   Do not configure anything.
8. Configure the applicable settings on other pages of this object.
9. Click **OK**.

To define a source IPv4 Network object

1. Click **Objects** menu > **New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:
   a. In the **Network address** field, enter the IPv4 address of your source IPv4 network.
   b. In the **Net mask** field, enter the net mask of your source IPv4 network.
6. In the **IPv6** section:

Do not enter anything.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a source IPv4 Address Range object

1. Click **Objects** menu > **More object types** > **Network Object** > **Address Range** > **New Address Range**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:
   a. In the **First IP address** field, enter the first IPv4 address of your IPv4 addresses range.
   b. In the **Last IP address** field, enter the last IPv4 address of your IPv4 addresses range.
6. In the **IPv6** section:

   Do not enter anything.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a translated destination IPv4 Host object

1. Click **Objects** menu > **New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:
   a. In the **Network address** field, enter the IPv4 address of your destination IPv4 network.
   b. In the **Net mask** field, enter the net mask of your destination IPv4 network.
6. In the **IPv6** section:

   Do not enter anything.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a translated source IPv6 Network object with an IPv6 address defined with the 96-bit prefix

1. Click **Objects** menu > **New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.
6. In the **IPv6** section:
   a. In the **Network address** field, enter the translated source IPv6 address.
   b. In the **Prefix** field, enter the number **96**.
7. On the **NAT** page of this object:

   Do not configure anything.
8. Click **OK**.

To define a translated destination IPv6 Host object

1. Click **Objects** menu > **New Host**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.
6. In the **IPv6** section:

   In the **Network address** field, enter the destination static IPv6 address.
7. On the **NAT** page of this object:

   Do not configure anything.
8. Configure the applicable settings on other pages of this object.
9. Click **OK**.

To create a Manual NAT46 rule

1. From the left Navigation Toolbar, click **Security Policies**.
2. In the top **Access Control** section, click **NAT**.
3. Right-click on the **Manual Lower Rules** section title, and near the **New Rule**, click **Above** or **Below**.

   Configure this NAT46 rule:

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
***Any** or Source IPv4 **Host** object or Source IPv4 **Address Range** object or Source IPv4 **Network** object	IPv4 **Host** object	***Any**	IPv6 **Network** object with an IPv6 address defined with the 96-bit prefix	IPv6 **Host** object	**= Original**

Do these steps:

a. In the **Original Source** column, add the applicable IPv4 object.

   In this rule column, NAT46 rules support only these types of objects:

   - `*Any`
   - Host with a static IPv4 address
   - Address Range with IPv4 addresses
   - Network with IPv4 address

b. In the **Original Destination** column, add the IPv4 **Host** object that represents the destination IPv4 address, to which the IPv4 sources connect.

   In this rule column, NAT46 rules support only IPv4 Host objects.

c. In the **Original Services** column, you must leave the default **Any**.

d. In the **Translated Source** column, add the IPv6 **Network object** with an IPv6 address defined with the 96-bit prefix.

   In this rule column, NAT64 rules support only IPv6 Network objects with an IPv6 address defined with the 96-bit prefix.

e. In the **Translated Source** column, right-click the IPv6 **Network object** with the 96-bit prefix > click **NAT Method** > click **Stateless NAT46**.

   The **46** icon shows in the **Translated Source** column.

f. In the **Translated Destination** column, add the IPv6 **Host** object represents the translated destination IPv6 address, to which the translated IPv4 sources connect.

In this rule column, NAT46 rule supports only an IPv6 Host objects.

g. In the **Translated Services** column, you must leave the default **= Original**.

To summarize, you must configure only these NAT46 rules (rule numbers are for convenience only):

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	`*Any`	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`
2	IPv4 *Host* object with a static IPv4 address	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`
3	IPv4 *Address Range* object	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`
4	IPv4 *Network* object	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`

4. Install the Access Control Policy.

Logging of NAT46 traffic

In the Security Gateway log for NAT64 connection, the source and destination IPv6 addresses show in their original IPv6 format. To identify a NAT46 entry, look in the **More** section of the **Log Details** window.

Field in Log	Description
Xlate (NAT) Source IP	Shows the translated source IPv6 address, to which the Security Gateway translated the original source IPv4 address
Xlate (NAT) Destination IP	Shows the translated destination IPv6 address, to which the Security Gateway translated the original destination IPv4 address
More	Identifies the entry as NAT46 traffic (`Nat46 enabled`)

Example of NAT46 Translation Flow

Example topology

[IPv4 Client] --- (internal) [Security Gateway] (external) --- [IPv6 Server]

Where:

Item	Description
IPv4 Client	IPv4 real address is 192.168.2.55 IPv6 NATed address is 2001:DB8:90::192.168.2.55**/96**
Security Gateway internal interface	IPv4 address is 192.168.2.1/24
Security Gateway external interface	IPv6 address is 2001:DB8:5001::1/**96**
IPv6 Server	IPv6 real address is 2001:DB8:5001::30/96 IPv4 NATed address is 1.1.1.66/24
IPv6 NATed network	IPv6 address of the network on the external Security Gateway side is 2001:DB8:90::/96 These IPv6 addresses are used to translate the IPv4 address of the IPv4 Client to IPv6 address
IPv4 NATed network	IPv4 address of the network on the internal Security Gateway side is 1.1.1.0/24 These IPv4 addresses are used to translate the IPv6 address of the IPv6 Server to IPv4 address

Traffic flow

1. IPv4 Client opens an IPv4 connection to the NATed IPv4 address of the IPv6 Serve

   From IPv4 address 192.168.2.55 to IPv4 address 1.1.1.66
2. Security Gateway performs these NAT translations:

a. From the source IPv4 address 192.168.2.55 to the source IPv6 address 2001:DB8:90::192.168.2.55/96

b. From the destination IPv4 address 1.1.1.66 to the destination IPv6 address 2001:DB8:5001::30

3. IPv6 Server receives this request connection as from the IPv6 address 2001:DB8:90::192.168.2.55/96 to the IPv6 address 2001:DB8:5001::30
4. IPv6 Server replies to this connection from the IPv6 address 2001:DB8:5001::30 to the IPv6 address 2001:DB8:90::192.168.2.55/96
5. Security Gateway performs these NAT translations:

   a. From the source IPv6 address 2001:DB8:5001::30 to the source IPv4 address 1.1.1.66

   b. From the destination IPv6 address 2001:DB8:90::192.168.2.55/96 to the destination IPv4 address 192.168.2.55
6. IPv4 Client receives this reply connection as from the IPv4 address 1.1.1.66 to the IPv4 address 192.168.2.55

To summarize:

- Request: [IPv4 Client] ---> [Security Gateway] ---> [IPv6 Server]

Field in packet	Original IPv4 packet	NATed IPv6 packet
Source IP	192.168.2.55 / 24	2001:DB8:90::192.168.2.55 / 96
Destination IP	1.1.1.66 / 24	2001:DB8:5001::30 / 96

- Reply: [IPv4 Client] <--- [Security Gateway] <--- [IPv6 Server]

Field in packet	Original IPv6 packet	NATed IPv4 packet
Source IP	2001:DB8:5001::30 / 96	192.168.2.55 / 24
Destination IP	2001:DB8:90::192.168.2.55 / 96	1.1.1.66 / 24

Advanced NAT Settings

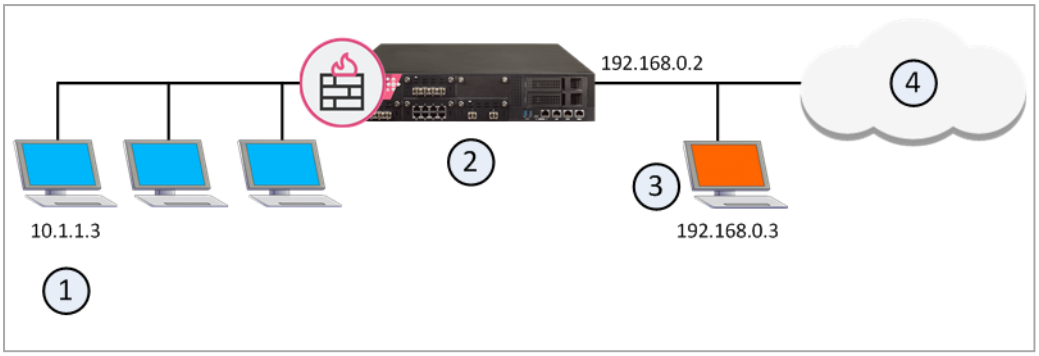
This section includes advanced NAT settings.

Deployment Configurations

This section discusses how to configure NAT in some network deployments.

Automatic and Proxy ARP

Giving a computer on the internal network an IP address from an external network using NAT makes that computer appear on the external network. When NAT on the Security Gateway is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP Requests that are sent from the external network for the IP address of the internal computer.



Item	Description
1	Computer on the internal network with IP address 10.1.1.3
2	Security Gateway with external interface IP address 192.168.0.2 responds to ARP Requests on behalf of translated internal objects
3	Translated IP Address 192.168.0.3 on the external network
4	External network

If you are using manual NAT rules, you must configure Proxy ARP entries to associate the translated IP address with the MAC address of the Security Gateway interface that is on the same network as the translated IP addresses.

See sk30197 for more information about configuring:

- Proxy ARP for IPv4 Manual NAT
- Proxy ARP for Scalable Platforms

See sk91905 for more about configuring Proxy NDP for IPv6 Manual NAT.

NAT and Anti-Spoofing

NAT is performed after Anti-Spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT.

Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is normally not necessary to perform NAT. You can disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule slows down the performance of the VPN.

Connecting Translated Objects on Different Interfaces

The following sections describe how to allow connections in both directions between statically translated objects (hosts, networks or address ranges) on different Security Gateway interfaces.

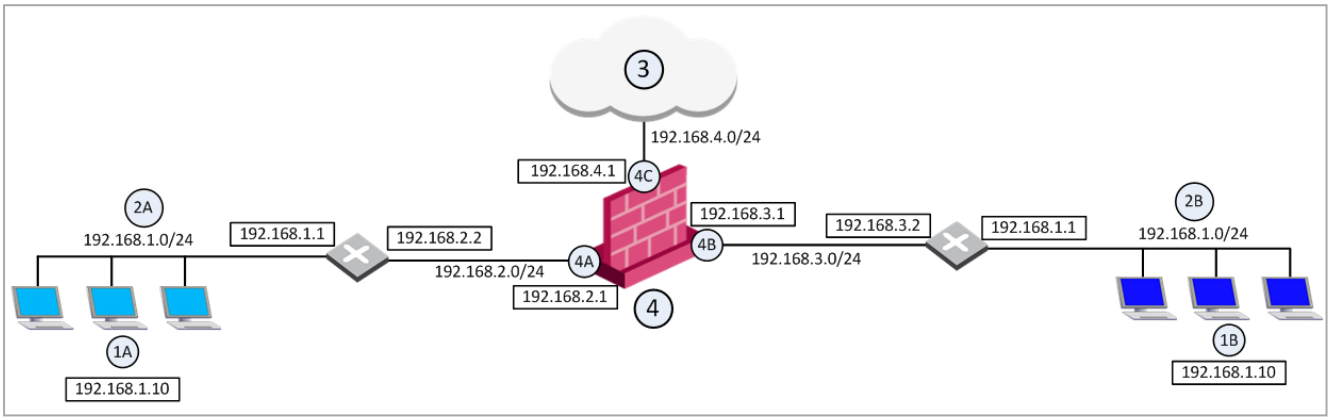
If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

Internal Communication with Overlapping Addresses

If two internal networks have overlapping (or partially overlapping) IP addresses, Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each overlapping internal network.

Network Configuration



For example, assume both Network 2A and Network 2B share the same address space (**192.168.1.0/24**), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.

Users in Network 2A who want to communicate with users in Network 2B must use the **192.168.30.0/24** network as a destination. Users in Network 2B who want to communicate with users in Network 2A must use the **192.168.20.0/24** network as a destination.

The Security Gateway (4) translates the IP addresses in the following way for each individual interface:

Interface 4A

- Inbound source IP addresses are translated to the virtual network **192.168.20.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

Interface 4B

- Inbound source IP addresses are translated to the network **192.168.30.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

Interface 4C

Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface's IP address (**192.168.4.1**).

Communication Examples

This section describes how to enable communication between internal networks, and between an internal network and the Internet

Communication Between Internal Networks

If user 1A, at IP address **192.168.1.10** in Network 2A, wants to connect to user 1B, at IP address **192.168.1.10** (the same IP address) in Network 2B, user 1A opens a connection to the IP address **192.168.30.10**.

Communication Between Internal Networks

Step	Source IP address	Destination IP address
Interface 4A - before NAT	**192.168.1.10**	**192.168.30.10**
Interface 4A - after NAT	**192.168.20.10**	**192.168.30.10**
Security Gateway enforces the security policy for packets from network **192.168.20.0/24** to network **192.168.30.0/24**.		
Interface 4B - before NAT	**192.168.20.10**	**192.168.30.10**
Interface 4B - after NAT	**192.168.20.10**	**192.168.1.10**

Communication Between an Internal Network and the Internet

If user 1A, at IP address **192.168.1.10** in network 2A, connects to IP address **192.0.2.10** on the Internet (3).

Communication Between an Internal Network and the Internet

Step	Source IP address	Destination IP address
Interface 4A - before NAT	**192.168.1.10**	**192.0.2.10**
Interface 4A - after NAT	**192.168.20.10**	**192.0.2.10**
The Security Gateway (4) enforces the security policy for packets from network **192.168.20.0/24** to the Internet (3).		
Interface 4C - before NAT	**192.168.20.10**	**192.0.2.10**
Interface 4C - after NAT Hide	**192.168.4.1**	**192.0.2.10**

Routing Considerations

To allow routing from Network 2A to Network 2B, routing must be configured on the Security Gateway.

These sections contain sample routing commands for Windows and Linux operating systems (for other operating systems, use the equivalent commands).

On Windows

- **route add 192.168.30.0 mask 255.255.255.0 192.168.3.2**
- **route add 192.168.20.0 mask 255.255.255.0 192.168.2.2**

On Linux

- **route add -net 192.168.30.0/24 gw 192.168.3.2**
- **route add -net 192.168.20.0/24 gw 192.168.2.2**

Object Database Configuration

To activate the overlapping NAT feature, use GuiDBedit Tool (see sk13009), or the `dbedit` command (see skI3301). In the sample network configuration, the per interface values for interface 4A and interface 4B are set in the following way:

Sample Network Configuration: Interface Configuration

Parameter	Value
enable_ overlapping_ nat	**true**
overlap_nat_ dst_ipaddr	The overlapping IP addresses (before NAT). In the sample network configuration, **192.168.1.0** for both interfaces.
overlap_nat_ src_ipaddr	The IP addresses after NAT. In the sample network configuration, **192.168.20.0** for interface 4A, and **192.168.30.0** for interface 4B.
overlap_nat_ netmask	The net mask of the overlapping IP addresses. In the sample network configuration, **255.255.255.0**.

Security Management Behind NAT

The Security Management Server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

NAT (Static or Hide) for the Security Management Server IP address can be configured in one click, while still allowing connectivity with managed Security Gateways. All Security Gateways can be controlled from the Security Management Server, and logs can be sent to the Security Management Server. NAT can also be configured for a Management High Availability server and a Log Server.

Note - Security Management behind NAT is not supported for deployments where the Security Management Server also acts as a Security Gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management Server (1) is in a network on which Network Address Translation is performed (the "NATed network"). The Security Management Server can control Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.

Item	Description
1	Primary_Security_Management object with IP address 10.0.0.1. Translated address 192.168.55.1

In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A Security Gateway. However, when using Hide NAT on the Security Management Server, Security Gateways can send logs to the Security Management Server.

When using the Security Management behind NAT feature, the remote Security Gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

To enable NAT for the Security Management Server:

- From the **NAT** page of the Security Management Server object, define NAT and select **Apply for Security Gateway control connections**.

Non-Corresponding Security Gateway Addresses

Sometimes the Security Gateway contacts the Security Management Server with an address that does not correspond to the deployment of the remote Security Gateway.

For example:

- When the automatic selection of the Security Gateway does not conform with the routing of the deployment of the Security Gateway. In this case, define the masters and loggers manually, to allow the remote Security Gateway to contact the Security Management Server using the required address. When an inbound connection from a managed Security Gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management Server.

To define masters and loggers, select **Use local definitions for Log Servers** and **Use local definitions for Masters** and specify the correct IP addresses on the Security Gateway.

This solution encompasses different scenarios:

- The remote Security Gateway addresses the NATed IP when you want it to address the real IP.
- The remote Security Gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management Server in the masters file.

Notes:

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management Server or as a Log Server.
- Ensure that you properly define the Topology settings on all Security Gateways. All workarounds required for previous versions still function with no changes in their behavior.

Configuring the Security Management Server Object

To configure the Security Management Server object:

1. From the **NAT** page on the Primary_Security_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select **Hide behind IP Address**, for example, **192.168.55.1**. Do not select **Hide behind Gateway** (address **0.0.0.0**).
2. Select **Install on Gateway** to protect the NATed objects or network. Do not select **All**.
3. Select **Apply for Security Gateway control connections**.

Configuring the Security Gateway Object

To configure the Security Gateway object:

1. Open the Security Gateway**Network Management** page
2. Create the Interface. Click **Actions** > **New interface**.
3. In the **General** page of the **Interface** window, define the **IP** address and the Net Mask.
4. In the **Topology** section, click **Modify**.
5. Select **Override**.
6. Select **Network defined by the interface IP and Net Mask**.

IP Pool NAT

An IP Pool is a range of IP addresses (an address range, a network or a group of one of these objects) that is routable to the Security Gateway. IP Pool NAT ensures proper routing for encrypted connections for the following two connection scenarios:

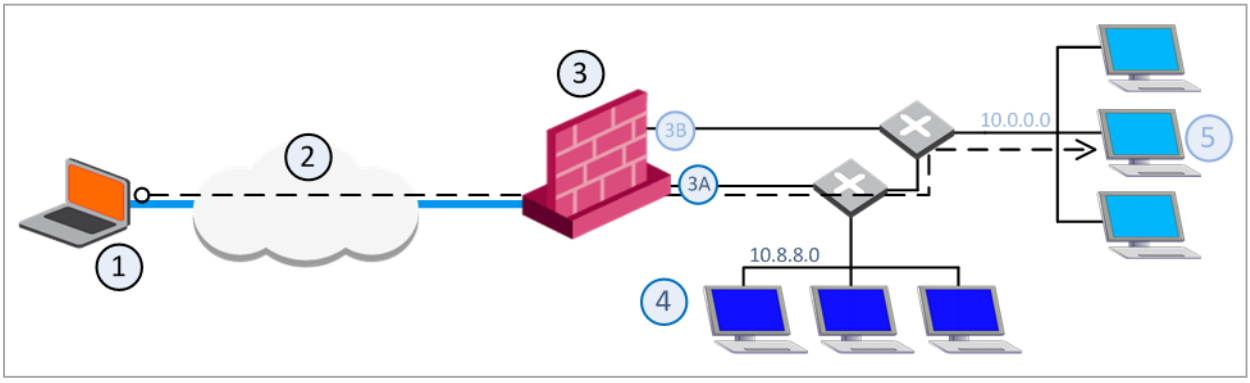
- Remote Access Client to MEP (Multiple Entry Point) Security Gateways
- Security Gateway to MEP Security Gateways

When a connection is opened from a Remote Access Client or a client behind a gateway, to a server behind the MEP Security Gateways, the packets are routed through one of the MEP Security Gateways. Return packets in the connection must be routed back through the same Security Gateway in order to maintain the connection. To ensure that this occurs, each of the MEP Security Gateways maintains a pool of IP addresses that are routable to the Security Gateway. When a connection is opened to a server, the Security Gateway substitutes an IP address from the IP pool for the source IP address. Reply packets from the server return to the Security Gateway, which restores the original source IP address and forwards the packets to the source.

IP Pool Per Interface

You can define a separate IP address pool on one or more of the Security Gateway interfaces instead of defining a single pool of IP addresses for the Security Gateway.

Defining an IP pool per interface solves routing issues that occur when the Security Gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the Security Gateway through the same Security Gateway interface. This illustration shows one of the MEP Security Gateways in a Remote Access Client to MEP (Multiple Entry Point) Security Gateway deployment.



Item	Description
1	Packets from source host: Source: Original Destination:
2	VPN tunnel through the Internet
3	MEP Security Gateway
3A	IP Pool 1 packets: Source: 10.55.8.x Destination:
3B	IP Pool 2 packets: Source: 10.55.10.x Destination:
4	Internal network 10.8.8.0
5	Target host in internal network 10.10.10.0

If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct Security Gateway interface through the use of static IP pool NAT addresses.

The remote client's IP address is NATed to an address in the IP pool on one of the Security Gateway interfaces. The addresses in the IP pool can be routed only through that Security Gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the Security Gateway interface, the Security Gateway restores the remote peer's source IP address.

The routing tables on the routers that lie behind the Security Gateway must be edited so that addresses from a Security Gateway IP pool are returned to the correct Security Gateway interface.

Switching between IP Pool NAT per Security Gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.

NAT Priorities

IP Pool NAT can be used both for encrypted (VPN) and non-encrypted (decrypted by the Security Gateway) connections.

Note - To enable IP Pool NAT for clear connections through the Security Gateway, configure INSPECT changes in the **user.def** file (see sk98239). Contact *Check Point Support*.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPsec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

The order of NAT priorities are:

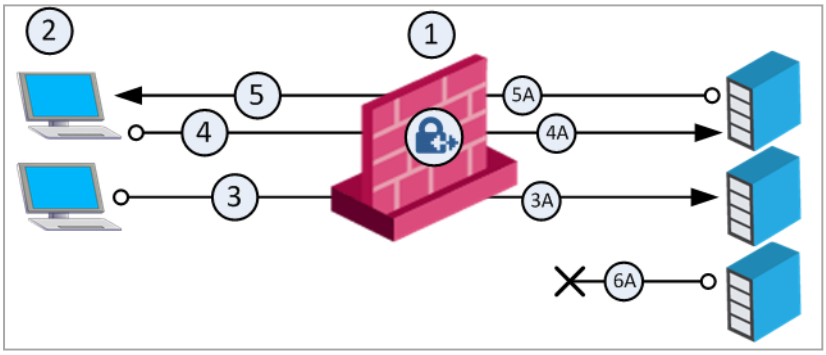
1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

Reusing IP Pool Addresses For Different Destinations

IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

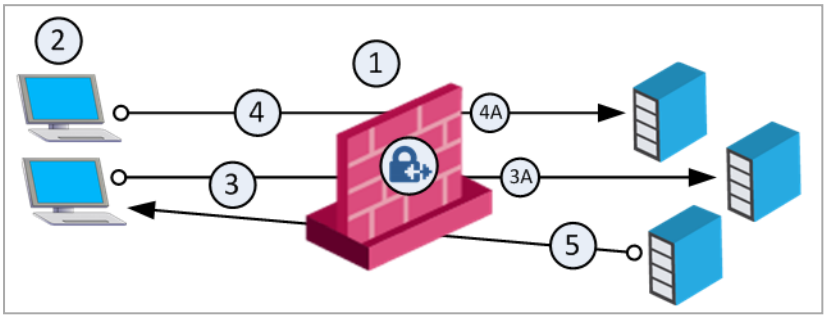
Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers (connections 1 and 2). When reusing addresses from the IP Pool, back connections are supported from the original server only (connection 3). This means that connections back to the client can be opened only from the specific server to which the connection was opened.



Item	Description
1	Security Gateway with IP Pool addresses A to Z
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: A Destination:
5A	NATed packet from reply connection 5. Source: Original Destination: A

Item	Description
6A	This server cannot open a connection with Destination A back to the client.

The default **Do not reuse IP Pool NAT** behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in the following illustration). In this mode, if an IP pool contains 20 addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client (connection 3).



Item	Description
1	Security Gateway with IP Pool addresses A to Z.
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: Z Destination:
5	Connection. Source: Original Destination: A

Switching between the **Reuse** and **Do not reuse** modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

Configuring IP Pool NAT

To configure IP Pool NAT:

1. From the SmartConsole **Menu**, select **Global properties**.
2. In the **Global properties** > **NAT** page, select **Enable IP Pool NAT** and the required tracking options.
3. In the Security Gateway's **General Properties** page, ensure the Security Gateway version is specified correctly.

4. For each Security Gateway or Security Gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range.

   For example, for an address range, do the following:

   a. From the **Objects Bar (F11)**, In the network objects tree, select **New > More > Network Object > Address Range > Address Range**.

      The **Address Range Properties** window opens.

   b. In the **General** tab, enter the first and last IP of the address range.

   c. Click **OK**. The new address range appears in the **Address Ranges** branch of the network objects tree.

5. Edit the Security Gateway object, and select **NAT** > **IP Pool NAT**.

6. In the **IP Pool NAT** page, select one of the following:

   a. **Allocate IP Addresses from** and then select the address range you created to configure IP Pool NAT for the whole Security Gateway, or

   b. **Define IP Pool NAT on Gateway interfaces** to configure IP Pool NAT per interface.

7. If required, select one or more of the following options:

   a. **Use IP Pool NAT for VPN client connections**

   b. **Use IP Pool NAT for gateway to gateway connections**

   c. **Prefer IP Pool NAT over Hide NAT** to specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

8. Click **Advanced**.

   a. **Return unused addresses to IP Pool after**:

      Addresses in the pool are reserved for 60 minutes (default), even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the time-out to prevent the IP Pool from being depleted.

   b. **Reuse IP addresses from the pool for different destinations**:

      This is a good option unless it is necessary to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.

9. Click **OK**.

10. Edit the routing table of each internal router so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway or, if using IP Pools per interface, the appropriate Security Gateway interface.

IP Pool NAT for Clusters

IP Pools for clusters are configured in two places in SmartConsole:

- In the Cluster object > **NAT > IP Pool NAT** page, select the connection scenario.
- In the Cluster Member object > **IP Pool NAT** page, define the IP Pool on the Cluster Member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each Cluster Member interface.

Mobile Access to the Network

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the **Mobile Application** in the **Services & Applications** column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the **Source** column of a rule.

Check Point Mobile Access Solutions

Check Point Mobile Access has a range of flexible clients and features that let users access internal resources from remote locations. All these solutions include these features:

- Enterprise-grade, secure connectivity to corporate resources
- Strong user authentication
- Granular access control

For more information about the newest versions of Mobile Access solutions and clients, go to sk67820.

Client-Based vs. Clientless

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. The client supplies access to most types of corporate resources according to the access privileges of the user.
- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

Mobile Access Clients

- Capsule Workspace - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
- Capsule Connect - A full L3 tunnel app that gives users network access to all mobile applications.
- Check Point Mobile for Windows - A Windows IPsec VPN client that supplies secure IPsec VPN connectivity and authentication.

Mobile Access Web Portal

The Mobile Access Portal is a clientless SSL VPN solution that supplies secure access to web-based resources. After users authenticate to the portal, they can access Mobile Access applications such as Outlook Web App and a corporate wiki.

SSL Network Extender

SSL Network Extender is an on-demand SSL VPN client and is installed on the computer or mobile device from an Internet browser. It supplies secure access to internal network resources.

Configuring Mobile Access to Network Resources

Sample Mobile Access Workflow

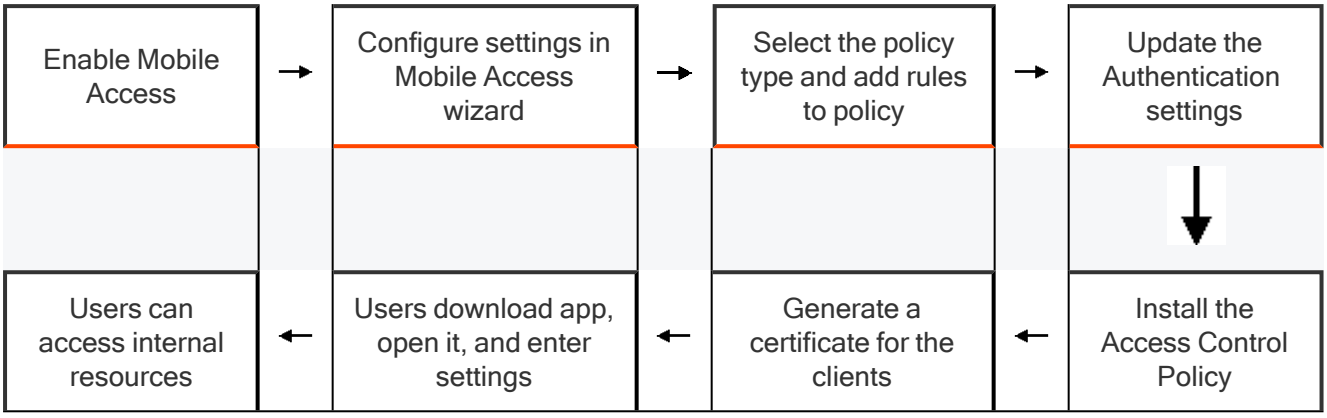
This is a high-level workflow to configure remote access to Mobile Access applications and resources.

1. Use SmartConsole to enable the Mobile Access Software Blade on the Security Gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
    a. Select mobile clients.
    b. Define the Mobile Access Portal.
    c. Define applications, for example Outlook Web App.
    d. Connect to the AD server for user information.
3. Select the policy type:
    - The default is to use the Legacy Policy, configured in the Mobile Access tab in SmartConsole.
    - To include Mobile Access in the **Unified Access Control Policy**, select this in **Gateway Properties** > **Mobile Access**.
4. Add rules to the Policy:
    - For Legacy Policy: Add rules in SmartConsole. Select **Security Policies** > **Shared Policies**> Mobile Access > **Open Mobile Access Policy in SmartConsole**
    - For Unified Access Control Policy: Add rules in SmartConsole > **Security Policies Access Control Policy**.
5. Configure the authentication settings in **Gateway Properties** > Mobile Access > **Authentication**.
6. Install the Access Control Policy on the Security Gateway.

    Users can access mobile applications through the configured Mobile Access Portal with the defined authentication method.
7. Optional: Give secure access to users through the Capsule Workspace app with certificate authentication.
    a. In the Security Gateway object > Mobile Access > **Authentication**, click **Settings**, and select **Require client certificate**.
    b. Use the Certificate Creation and Distribution Wizard (in the **Security Policies** view > **Client Certificates** > **New**).

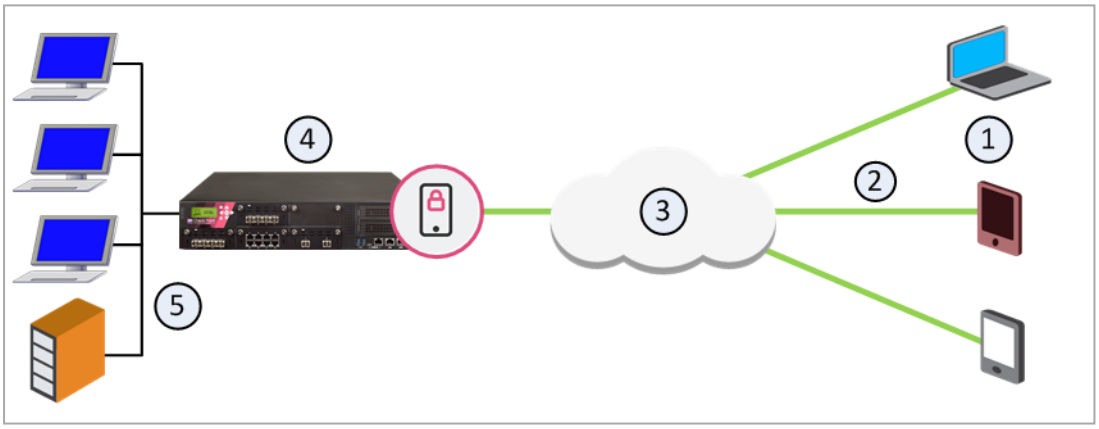
c. Users download the Capsule Workspace app.

d. Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.



Sample Mobile Access Deployment

This is a sample deployment of a Mobile Access Security Gateway with an AD and Exchange server in the internal network.



Item	Description
1	Mobile devices
2	Mobile Access tunnels
3	Internet (external networks)
4	Mobile Access Security Gateway
5	Internal network resources, AD and Exchange servers

In this sample Mobile Access deployment, a mobile device uses a Mobile Access tunnel to connect to the internal network. The Mobile Access Security Gateway decrypts the packets and authenticates the user. The connection is allowed and the mobile device connects to the internal network resources.

Using the Mobile Access Configuration Wizard

This procedure describes how to enable and configure the Mobile Access Software Blade on a Security Gateway with the Configuration wizard. For this sample configuration, the AD user group Mobile Access contains all the users that are allowed to connect to the internal network. The deployment is based on the Sample Mobile Access Deployment.

This configuration lets these clients connect to internal resources:

- Android and iOS mobile devices
- Windows and Mac computers
- Internet browsers can open a SSL Network Extender connection to the internal network

To configure Mobile Access:

1. In SmartConsole, go to Gateways & Servers and double-click the Security Gateway object.

   The **General Properties** window opens.

2. In the **General Properties** > **Network Security** section, select Mobile Access.

   The Mobile Access page of the **Mobile Access Configuration Wizard** opens.

3. Configure the Security Gateway to allow connections from the Internet and mobile devices. Select these options:
   - **Web**
   - **Mobile Devices** - Select the required options.
   - **Desktops/Laptops** -Select the required options.

4. Click **Next**.

   The **Web Portal** page opens.

5. Enter the primary URL for the Mobile Access Portal.

   The default is: `https://<IPv4 Address of Security Gateway>/sslvpn`

6. Click **Next**.

   The **Applications** page opens.

7. Configure the applications to show:
   a. In **Web Applications**, make sure **Demo web application (World Clock)** is selected.
   b. In **Mail/Calendar/Contacts**, enter the domain for the Exchange server and select:
      - **Mobile Mail (including push mail notifications)**
      - **ActiveSync Applications**
      - **Outlook Web App**

      The Mobile Access Portal shows links to the Demo web and Outlook Web App applications. The client on the mobile device shows links to the other applications.

8. Click **Next**.

   The **Active Directory** page opens.

9. Select the AD domain and enter the user name and password.
10. Click **Connect**.

    The Security Gateway makes sure that it can connect to the AD server.
11. Click **Next**.

    The **Users** page opens.

    Click **Add** and then select the group Mobile Access.
12. Click **Next** and then click **Finish**.

    The **Mobile Access Configuration Wizard** closes.
13. Click **OK**.

    The **Gateway Properties** window closes.

Allowing Mobile Connections

The Mobile Access Configuration Wizard enables and configures the Mobile Access Software Blade. It is necessary to add Firewall rules to allow connections from the VPN clients on the computers and devices. Create a Host Node object for the Exchange server, all of the other objects are predefined.

Name	Source	Destination	VPN	Service	Action	Install On	Track
Mobile Access Users	Any	ExchngSrvr	RemoteAccess	HTTP HTTPS MSExchange	Accept	Mobile Access GW	Log

All connections from the `RemoteAccess` VPN community to the Exchange server are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and MS Exchange. This rule is installed on Security Gateway in the `MobileAccessGW` group.

Defining Access to Applications

Use the **Security Policies** page in SmartConsole to define rules that let users access Mobile Access applications. The applications that are selected in the Configuration Wizard are automatically added to this page. You can also create and edit the rules that include these SmartConsole objects:

- Users and user groups
- Mobile Access applications
- Mobile Access Security Gateways

Activating Single Sign-On

Enable the SSO (Single Sign-On) feature to let users authenticate one time for applications that they use during Mobile Access sessions. The credentials that users enter to log in to the Mobile Access Portal can be re-used automatically to authenticate to different Mobile Access applications. SSO user credentials are securely stored on the Mobile Access Security Gateway for that session and are used again if users log in from different remote devices. After the session is completed, the credentials are stored in a database file.

By default, SSO is enabled on new Mobile Access applications that use HTTP. Most Web applications authenticate users with specified Web forms. You can configure SSO for an application to use the authentication credentials from the Mobile Access Portal. It is not necessary for users to log in again to each application.

To configure SSO

1. In SmartConsole, go to **Security Policies > Shared Policies > Mobile Access**.
2. Click **Open Mobile Access Policy in SmartDashboard**.
3. In the Mobile Access tab, select **Additional Settings** > Single Sign-On.

   The Single Sign-On page opens.
4. Select an application and click **Edit**.

   The application properties window opens and shows the **Single Sign On** page.

For Web form applications

1. In the **Application Single Sign-On Method** section, select **Advanced** and click **Edit**.

   The **Advanced** window opens.
2. Select **This application reuses the portal credentials. Users are not prompted**.
3. Click **OK**.
4. Select **This application uses a Web form to accept credentials from users**.
5. Click **OK**.
6. Install the policy.

Connecting to a Citrix Server

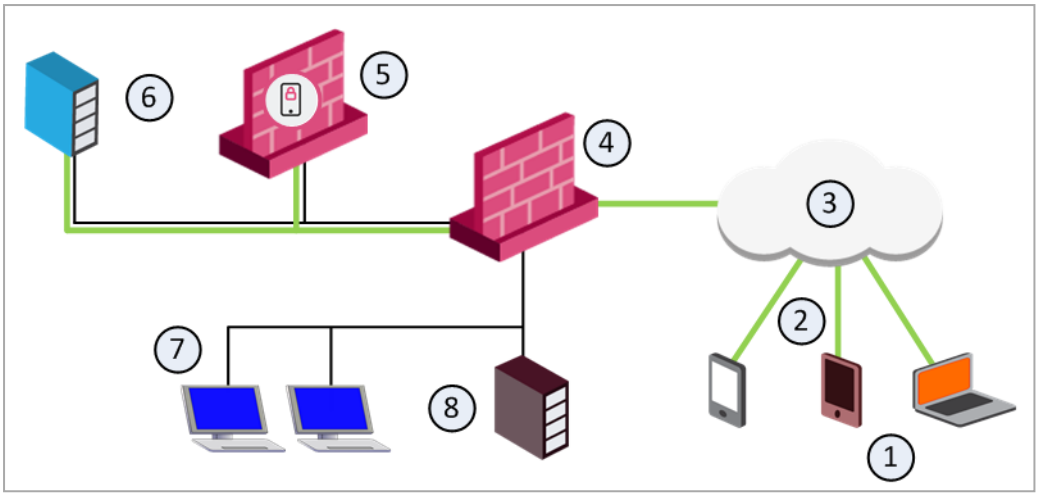
Citrix Services

The Mobile Access Software Blade integrates the Citrix clients and services. It is not necessary to use STA (Secure Ticketing Authority) servers in a Mobile Access Security Gateways deployment because Mobile Access uses its own STA engine. You can also use Mobile Access in a deployment with STA and CSG (Citrix Secure Gateway) servers.

The Mobile Access server certificate must use a FQDN (Fully Qualified Domain Name) that is issued to the FQDN of the Mobile Access Security Gateway.

Sample Deployment with Citrix Server

This is a sample deployment of a Mobile Access Security Gateway and a Citrix web server in the DMZ. The Citrix XenApp server is connected to the internal network.



Item	Description
1	Mobile devices
2	Mobile Access tunnels
3	Internet (external networks)
4	Security Gateway for the internal network
5	Mobile Access Security Gateway in the DMZ
6	Citrix web interface
7	Internal network resources
8	Citrix XenApp (MetaFrame) server

Configuring Citrix Services for Mobile Access

This procedure describes how to configure Mobile Access to let remote users connect to Citrix applications. The deployment is based on the Sample Deployment with Citrix Server (see *"Sample Deployment with Citrix Server" on the previous page*).

To configure Citrix services:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access, click **Configure in SmartDashboard**.
3. In the Mobile Access tab, click **Applications** > **Citrix Services**.
4. Click **New**.

   The **General Properties** page of the **Citrix Service** window opens.
5. Enter the **Name** for the Citrix server object.
6. From the navigation tree, click **Web Interface**.
7. Create a new object for the Citrix web interface server, in **Servers**, click **Manage** > **New** > **Host**.

The **Host Node** window opens.

8. Enter the settings for the Citrix web interface server.
9. Click **OK**.
10. In Services, select one or more of these services that the Citrix web interface server supports:
    - HTTP
    - HTTPS
11. From the navigation tree, click **Link in Portal**.
12. Configure the settings for the link to the Citrix services in the Mobile Access Portal:
    - **Link text** - The text that is shown for the Citrix link
    - **URL** - The URL for the directory or subdirectory of the Citrix application
    - **Tooltip** - Text that is shown when the user pauses the mouse pointer above the Citrix link
13. From the navigation tree, select **Additional Settings** > **Single Sign On**.
14. Enable Single Sign On for Citrix services, select these options:
    - **Turn on single Sign On for this application**
    - **Prompt users for their credentials, and store them for future use**
15. Click **OK**.

    The Citrix server object is added to **Defined Citrix Services**.
16. From the Mobile Access navigation tree, select **Policy**.
17. Add the Citrix services object to the applicable rules.
    a. Right-click on the Applications cell of a rule and select **Add Applications**.
    b. Select the Citrix services object.
18. Install the policy.

Compliance Check

The Mobile Access Software Blade lets you use the Endpoint Security on Demand feature to create compliance policies and add more security to the network. Mobile devices and computers are scanned one time to make sure that they are compliant before they can connect to the network.

The compliance scanner is installed on mobile devices and computers with ActiveX (for Internet Explorer on Windows) or Java. The scan starts when the Internet browser tries to open the Mobile Access Portal.

Compliance Policy Rules

The compliance policy is composed of different types of rules. You can configure the security and compliance settings for each rule or use the default settings.

These are the rules for a compliance policy:

- Windows security - Microsoft Windows hotfixes, patches and Service Packs.
- Anti-Spyware protection - Anti-Spyware software.
- Anti-Virus protection - Anti-Virus software version and virus signature files.

- Firewall - Personal Firewall software.
- Spyware scan - Action that is done for different types of spyware.
- Custom - Compliance rules for your organization, for example: applications, files, and registry keys.
- OR group - A group of the above rules. An endpoint computer is compliant if it meets one of the rules in the group.

Creating a Compliance Policy

By default, Endpoint Security on Demand only allows endpoint computers that are compliant with the compliance policy log in to the Mobile Access Portal.

To create a compliance policy:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.
1. In the Mobile Access tab, select **Endpoint Security on Demand** > **Endpoint Compliance**.
2. Click **Edit policies**.

   The **Policies** window opens.
3. Click **New Policy**.

   The **Policies** > **New Policy** window opens.
4. Enter the **Name** and **Description** for the policy.
5. Click **Add**.

   The **Add Enforcement Rules** window opens.
6. Select rules for the policy.

   You can also create new rules - click **New Rule**, and configure the rule settings.
7. Click **OK**.

   The **Policies** > **New Policy** window shows the rules for the policy.
8. Select **Bypass spyware scan** if necessary.

   When selected, the scan for endpoint computers that are compliant with the Anti-Virus or Anti-Spyware settings is changed. These computers do not scan for spyware when they connect to a Mobile Access Security Gateway.
9. Click **OK**.

   The **Policies** window opens.
10. Click **OK**.

Configuring Compliance Settings for a Security Gateway

The Firewall on a Mobile Access Security Gateway only allows access to endpoint computers that are compliant with the compliance policy.

This procedure shows how to configure the Laptop Computer policy for a Security Gateway (see *"Compliance Policy Rules" on the previous page*).

To configure the compliance settings:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.
1. In the Mobile Access tab, select **Endpoint Security on Demand > Endpoint Compliance**.
2. Select the Security and click **Edit**.

   The **Endpoint Compliance** page of the Security Gateway properties window opens.
3. Select **Scan endpoint machine when user connects**.
4. Select **Threshold policy** and from the drop-down menu select **Laptop Computer**.
5. Click **OK**.
6. Install the policy on the Mobile Access Security Gateway.

Secure Workspace

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the "real" workspace. Users can only send data from this secure environment through the Mobile Access Portal. Secure Workspace users can only access permitted applications, files, and other resources from the virtual workspace.

Secure Workspace creates an encrypted folder on the computer called **My Secured Documents** and can be accessed from the virtual desktop. This folder contains temporary user files. When the session terminates, Secure Workspace deletes this folder and all other session data.

For more about configuring Secure Workspace and Mobile Access VPN, see the *R81 Mobile Access Administration Guide*.

To enable Secure Workspace on a Mobile Access Security Gateway

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.

   Legacy SmartDashboard opens.
3. In the Mobile Access tab, click **Endpoint Security on Demand** > **Secure Workspace**.
4. Select the Security Gateway and click **Edit**.

   The **Check Point Secure Workspace** page of the Security Gateway properties window opens.
5. Select **This gateway supports access to applications from within Check Point Secure Workspace**.
6. Click **OK**.
7. Install the policy.

Secure Workspace

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the "real" workspace. Users can only send data from this secure environment through the Mobile Access Portal. Secure Workspace users can only access permitted applications, files, and other resources from the virtual workspace.

Secure Workspace creates an encrypted folder on the computer called **My Secured Documents** and can be accessed from the virtual desktop. This folder contains temporary user files. When the session terminates, Secure Workspace deletes this folder and all other session data.

For more about configuring Secure Workspace and Mobile Access VPN, see the *R81 Mobile Access Administration Guide*.

To enable Secure Workspace on a Mobile Access Security Gateway

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.

   Legacy SmartDashboard opens.
3. In the Mobile Access tab, click **Endpoint Security on Demand** > **Secure Workspace**.
4. Select the Security Gateway and click **Edit**.

   The **Check Point Secure Workspace** page of the Security Gateway properties window opens.
5. Select **This gateway supports access to applications from within Check Point Secure Workspace**.
6. Click **OK** and then install the policy.

To Learn More About Mobile Access

To learn more about Mobile Access VPN, see the *R81 Mobile Access Administration Guide*.

Site-to-Site VPN

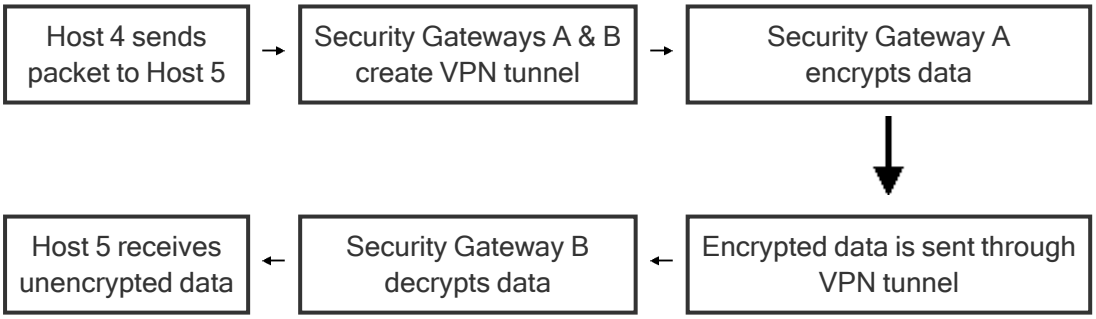
The basis of Site-to-Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

Sample Site-to-Site VPN Deployment

Item	Description
A, B	Security Gateways
2	VPN tunnel
3	Internal network in VPN domain
4	Host 4
5	Host 5

In this sample VPN deployment, Host 4 and Host 5 securely send data to each other. The Security Gateways perform IKE negotiation and create a VPN tunnel. They use the IPsec protocol to encrypt and decrypt data that is sent between Host 4 and Host 5.

VPN Workflow

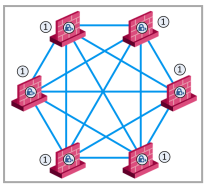


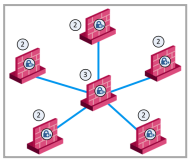
VPN Communities

A VPN Domain is a collection of internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community - collection of VPN tunnels and their attributes. Network resources of different VPN Domains can securely communicate with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN tunnels between each pair of Security Gateway. In a Star community, each satellite Security Gateway has a VPN tunnel to the central Security Gateway, but not to other Security Gateways in the community.

Mesh Topology **Star Topology**





Item	Description
1	Security Gateway
2	Satellite Security Gateways
3	Central Security Gateway

Sample Star Deployment

This section explains how to configure a VPN star community. This deployment lets the satellite Security Gateways connect to the internal network of the central Security Gateway. The internal network object is named: **Internal-network**.

To create a new VPN Star Community:

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Access Tools** section, click **VPN Communities**.
3. Click **New** and select **Star Community**.

   The **New Star Community** window opens.
4. Enter the name for the community.
5. From the navigation tree, select **Encryption**.
6. Configure the VPN encryption methods and algorithms for the VPN community.
7. Click **OK**.

To configure star VPN for the Security Gateways

For each Security Gateway in the VPN community, follow these configuration steps.

1. In SmartConsole, go to the **Gateways & Servers** page and double-click the Security Gateway object.

   The Security Gateway properties window opens.
2. In the **Network Security** section of the **General Properties** page, select **IPsec VPN**.
3. From the navigation tree, go to **Network Management > VPN Domain**.
   - For the central Security Gateway, click **Manually defined** and select the **Internal-network** object
   - For a satellite Security Gateway, select **All IP addresses**
4. From the navigation tree, click **IPsec VPN**.
5. Configure the Security Gateway as a member of a VPN star community.

a. In the **This Security Gateway participates in the following VPN Communities** section, click **Add**.

   The **Add this Gateway to Community** window opens.

b. Select the VPN Community.

c. Click **OK**.

6. Click **OK**.

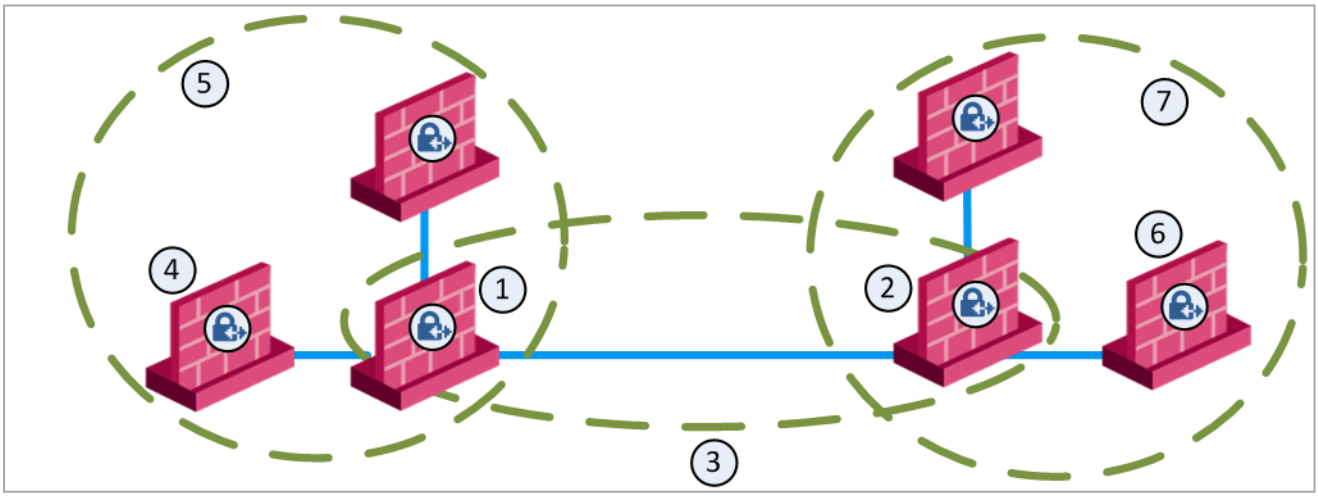
After you create a community and configure Security Gateways, add those Security Gateways to the community as a center or as a satellite Security Gateway.

To add a Security Gateway to a new star community

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Access Tools** section, click **VPN Communities**.
3. Select the new star community and click **Edit**.

   The **Star Community** window opens.
4. In the **Gateways** page, add Security Gateways to the community:
   - **Center Gateways** - Click **Add** and select center Security Gateways. Select **Mesh center gateways**, if necessary.
   - **Satellite Gateways** - Click **Add** and select satellite Security Gateways.
5. Click **OK**.

Sample Combination VPN Community



Item	Description
1	London Security Gateway
2	New York Security Gateway
3	London - New York Mesh community

Item	Description
4	London company partner (external network)
5	London Star community
6	New York company partner (external network)
7	New York Star community

This deployment is composed of a Mesh community for London and New York Security Gateways that share internal networks. The Security Gateways for external networks of company partners do not have access to the London and New York internal networks. However, the Star VPN communities let the company partners access the internal networks of the sites that they work with.

Allowing VPN Connections

To allow VPN connections between Security Gateways in specific VPN communities, add Access Control rules that accept such connections.

To allow all VPN traffic to hosts and clients on the internal networks of a specific VPN community, select these options in the **Encrypted Traffic** section of the properties configuration window for that VPN Community:

- For a meshed community: **Accept all encrypted traffic**
- For a Star Community: **Accept all encrypted traffic on Both center and satellite gateways**, or **Accept all encrypted traffic on Satellite gateways only**.

Sample VPN Access Control Rules

This table shows sample VPN rules for an Access Control Rule Base. (The **Action**, **Track** and **Time** columns are not shown. **Action** is set to **Allow**, **Track** is set to **Log**, and **Time** is set to **Any**.)

No.	Name	Source	Destination	VPN	Service	Install On
1	-	Any	**NEGATED** Member Security Gateways	BranchOffices LondonOffices	Any	BranchOffices LondonOffices
2	Site-to-site VPN	Any	Any	All_GwToGw	FTP-port HTTP HTTPS SMTP	Policy Targets
3	Remote access	Any	Any	RemoteAccess	HTTP HTTPS IMAP	Policy Targets

1. Automatic rule that SmartConsole adds to the top of the *Implied Rules* when the **Accept All Encrypted Traffic** configuration option is selected for the `BranchOffices` VPN community and the `LondonOffices` VPN community. This rule is installed on all the Security Gateways in these communities. It allows all VPN traffic to hosts and clients on the internal networks of these communities. Traffic that is sent to the Security Gateways in these VPN communities is dropped.

   Note - This automatic rule can apply to more than one VPN community.

2. **Site-to-site VPN** - Connections between hosts in the VPN Domains of all Site-to-Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

3. **Remote access** - Connections between hosts in the VPN Domains of Remote Access VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

To Learn More About Site-to-Site VPN

To learn more about site-to-Site VPN, see the *R81 Site to Site VPN Administration Guide*.

Remote Access VPN

If employees remotely access sensitive information from different locations and devices, system administrators must make sure that this access does not become a security vulnerability. Check Point's Remote Access VPN solutions let you create a VPN tunnel between a remote user and the internal network. The Mobile Access Software Blade extends the functionality of Remote Access solutions to include many clients and deployments.

VPN Connectivity Modes

When securely connecting remote clients with the internal resources, organizations face connectivity challenges, such as these:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a LAN with internal IP addresses (such as, at hotels)
- It is necessary for the remote client to use protocols that are not supported

The Check Point IPsec VPN Software Blade provides these VPN connectivity modes to help organizations resolve those challenges:

- **Office Mode**

  Remote users can be assigned the same or non-routable IP addresses from the local ISP. Office Mode solves these routing problems and encapsulates the IP packets with an available IP address from the internal network. Remote users can send traffic as if they are in the office and avoid VPN routing problems.

- **Visitor Mode**

  Remote users can be restricted to using only HTTP and HTTPS protocols. Visitor Mode lets these users tunnel all protocols through regular TCP connections on port 443.

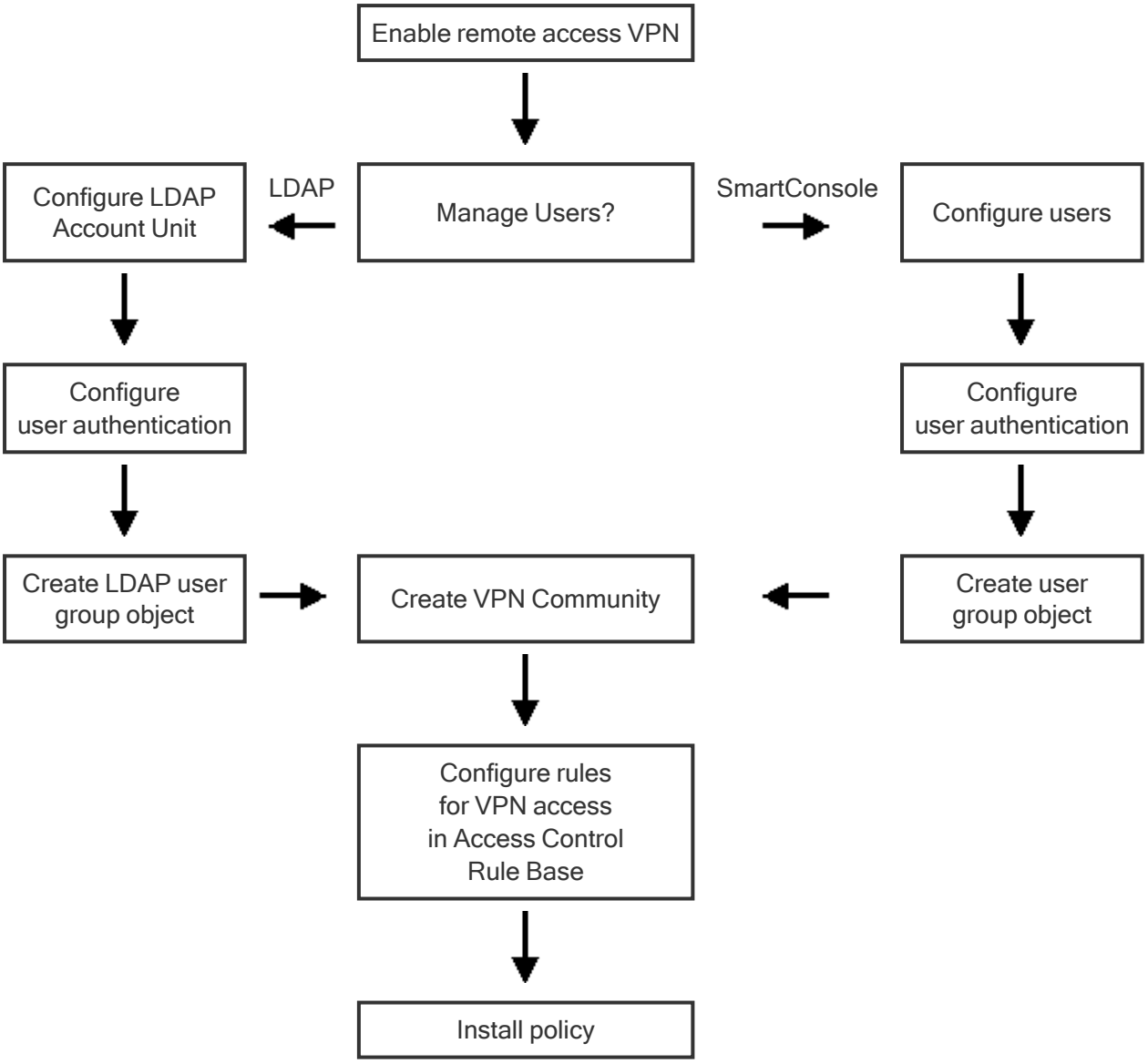
Sample Remote Access VPN Workflow

Here is an example of a Remote Access VPN workflow:

1. Use SmartConsole to enable Remote Access VPN on the Security Gateway.
2. Add the remote user information to the Security Management Server:
   - Create and configure an LDAP Account Unit
   - Enter the information in the SmartConsole user database

   Optional: Configure the Security Gateway for remote user authentication.
3. Define the Access Control and encryption rules for the Security Gateway.
4. Create the group objects to use in the Security Gateway rules:
   - **LDAP Group** object - for an LDAP Account Unit
   - **User Group** object - for users configured in the SmartConsole user database
5. Create and configure the encryption settings for the VPN community object in Menu > **Global properties** > **Remote Access** > **VPN - Authentication and Encryption**.

6. Add Access Control rules to the Access Control Rule Base to allow VPN traffic to the internal networks.



Configuring the Security Gateway for a Remote Access Community

Make sure that the VPN Software Blade is enabled before you configure the Remote Access community.

To configure the Security Gateway for Remote Access

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway object opens and shows the **General Properties** page.
2. From the navigation tree, click **IPsec VPN**.

   The page shows the VPN communities that the Security Gateway is participating.
3. To add the Security Gateway to a Remote Access community:

a. Click **Add**.
b. Select the community.
c. Click **OK**.

4. From the navigation tree, click **Network Management > VPN Domain**.
5. Configure the VPN Domain.

To configure the settings for Visitor Mode

1. From the navigation tree, click **VPN Clients > Office Mode**.
2. Configure the settings for Office Mode.

   Note - Office Mode support is mandatory on the Security Gateway side.
3. Click **OK**.
4. Publish the SmartConsole session.

To Learn More About Remote Access VPN

See the *R81 Remote Access VPN Administration Guide*.

Creating a New Threat Prevention Policy

To learn about configuring a Threat Prevention Policy, see the *R81 Threat Prevention Administration Guide*.

HTTPS Inspection

HTTPS Internet traffic uses the TLS (Transport Layer Security) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new TLS connections with the external site or server. The Security Gateways are then able to decrypt and inspect HTTPS traffic that uses the new TLS connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.
- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that arrive from the Internet or an external network.

The Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

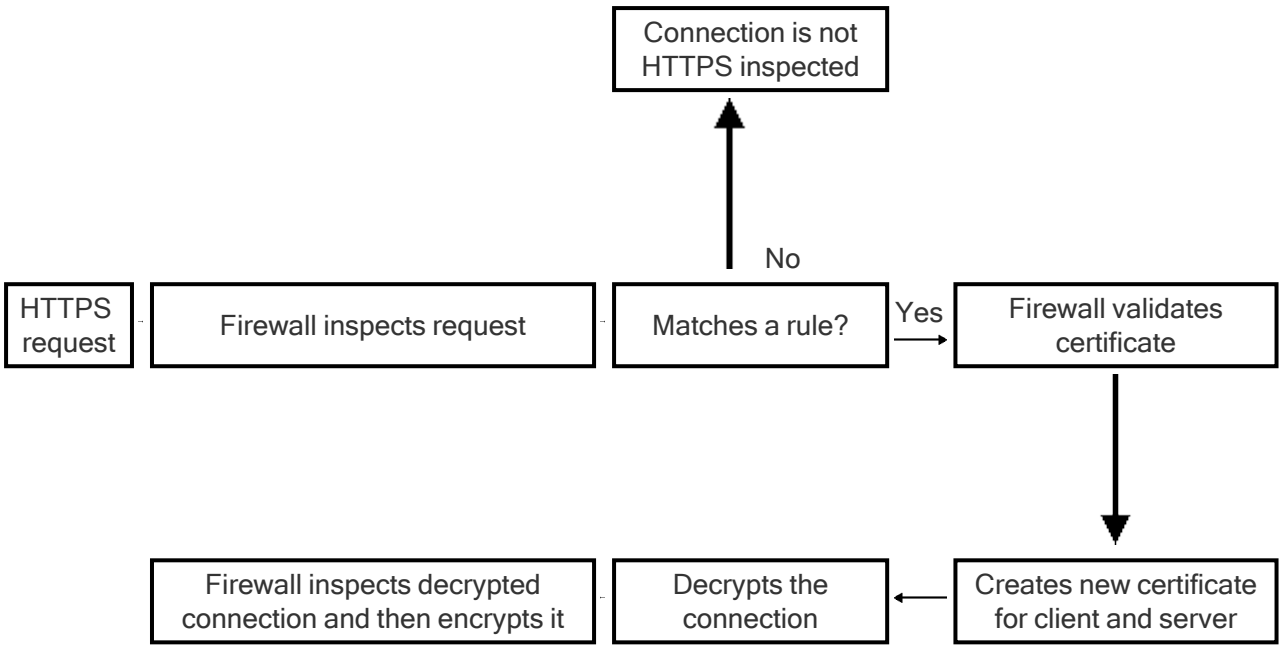
Inspecting HTTPS Packets

Outbound Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to the Internet. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not HTTPS inspected and not logged.

If the request matches an HTTPS Inspection rule, the Security Gateway validates the certificate from the server (on the Internet). The Security Gateway validates the certificate using the Online Certificate Status Protocol (OCSP) standard. OCSP is faster and uses much less memory than CRL Validation, which is used for certificate validation in releases lower than R80.10. For a new HTTPS connection to the server, the Security Gateway creates and uses a new certificate. There are two HTTPS connections, one to the internal client and one to the external server. It can then decrypt and inspect the packets according to the Security Policy. The packets are encrypted again and sent to the destination.

Outbound connection flow

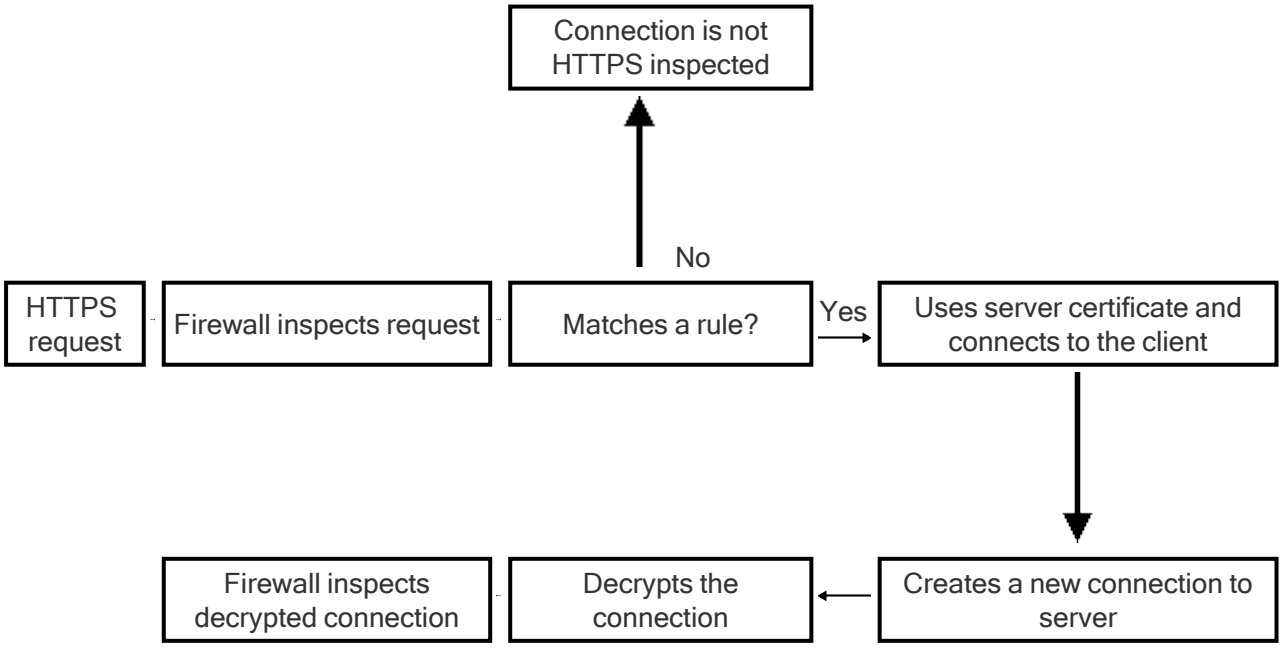


Inbound Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not HTTPS inspected and not logged.

If the request matches an HTTPS Inspection rule, the Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Security Gateway has a secure connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the Security Policy.

Inbound connection flow



Configuring Security Gateways to inspect outbound and inbound HTTPS traffic

This section gives an example of how to configure a Security Gateway to inspect outbound and inbound HTTPS traffic.

Workflow overview

Step	Instructions
1	Enable HTTPS Inspection on the Security Gateway.
2	Configure the Security Gateway to use the certificate. ■ **Outbound Inspection** - Generate a new certificate for the Security Gateway ■ **Inbound Inspection** - Import the certificate for the internal server
3	Configure the HTTPS Inspection Rule Base.
4	Install the Access Control Policy.

Enabling HTTPS Inspection

You must enable HTTPS Inspection on each Security Gateway.

To enable HTTPS Inspection on a Security Gateway

Step	Instructions
1	From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2	Click **HTTPS Inspection** > **Step 3**.
3	Select **Enable HTTPS Inspection**.

The first time you enable HTTPS Inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS Inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Creating an Outbound CA Certificate

The outbound CA certificate is saved with a CER file extension and uses a password to encrypt the private key of the file. The Security Gateways use this password to sign certificates for the sites accessed. You must keep the password because it is also used by other Security Management Servers that import the CA certificate to decrypt the file.

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive TLS error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections.

After you create the outbound CA certificate, a certificate object named Outbound Certificate is created. Use this object in rules that inspect outbound HTTPS traffic in the HTTPS Inspection Rule Base.

To create an outbound CA certificate

Step	Instructions
1	In SmartConsole **Gateways & Servers** view, right-click the Security Gateway object and select **Edit**. The **Gateway Properties** window opens.
2	In the navigation tree, select HTTPS Inspection.
3	In **Step 1** of the HTTPS Inspection page, click **Create**. The **Create** window opens.
4	Enter the necessary information: ■ **Issued by (DN)** - Enter the domain name of your organization. ■ **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate. ■ **Retype private key password** - Retype the password. ■ **Valid from** - Select the date range for which the CA certificate is valid.
5	Click **OK**.
6	Export and deploy the CA certificate, (see *"Exporting and Deploying the Generated CA" on page 311*).

Importing an Outbound CA Certificate

You can import a CA certificate that is already deployed in your organization or import a CA certificate created on one Security Management Server to another Security Management Server.

Best Practice - Use *private* CA Certificates.

For each Security Management Server that has Security Gateways enabled with HTTPS Inspection, you must:

- Import the CA certificate.
- Enter the password the Security Management Server uses to decrypt the CA certificate file and sign the certificates for users. Use this password only when you import the certificate to a new Security Management Server.

To import a CA certificate

Step	Instructions
1	If the CA certificate was created on another Security Management Server, export the certificate from the Security Management Server, on which it was created (see *"Exporting a Certificate from the Security Management Server" on the next page*).
2	In the SmartConsole Gateways & Servers view, right-click the Security Gateway object and select **Edit**. The **Gateway Properties** window opens.
3	In the navigation tree, select HTTPS Inspection.
4	In **Step 1** of the HTTPS Inspection page, click **Import**. The **Import Outbound Certificate** window opens.
5	Browse to the certificate file.
6	Enter the **private key password**.
7	Click **OK**.
8	If the CA certificate was created on another Security Management Server, deploy it to clients (see *"Exporting and Deploying the Generated CA" on the next page*).

Exporting a Certificate from the Security Management Server

If you use more than one Security Management Server in your organization, you must *first* export the CA certificate with the `export_https_cert` CLI command from the Security Management Server on which it was created before you can import it to other Security Management Servers.

Command syntax

```
export_https_cert [-local] | [-s server] [-f certificate file name under FWDIR/tmp][-help]
```

To export the CA certificate

On the Security Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f [certificate file name under FWDIR/tmp]
```

Example:

```
$FWDIR/bin/export_https_cert -local -f mycompany.cer
```

Exporting and Deploying the Generated CA

To prevent users from getting warnings about the generated CA certificates that HTTPS Inspection uses, install the generated CA certificate used by HTTPS Inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.

When users run standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

To distribute a certificate with a GPO

Step	Instructions
1	From the HTTPS Inspection window of the Security Gateway, click **Export certificate**.
2	Save the CA certificate file.
3	Use the Group Policy Management Console to add the certificate to the Trusted Root Certification Authorities certificate store, (see *"Deploying Certificates by Using Group Policy" on the next page*).
4	Push the Policy to the client computers in the organization. **Note** - Make sure that the CA certificate is pushed to the client computer organizational unit.
5	Test the distribution by browsing to an HTTPS site from one of the clients. Also, verify that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

Deploying Certificates by Using Group Policy

You can use this procedure to deploy a certificate to multiple client machines with Active Directory Domain Services and a Group Policy Object (GPO). A GPO can contain multiple configuration options, and is applied to all computers in the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.

To deploy a certificate using Group Policy

Step	Instructions
1	On the Microsoft Windows Server, open the **Group Policy Management Console**.
2	Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3	Right-click the GPO and select **Edit**. The **Group Policy Management Editor** opens and shows the contents of the policy object.
4	Open **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Publishers**.
5	Click **Action** > **Import**.
6	Do the instructions in the **Certificate Import Wizard** to find and import the certificate you exported from SmartConsole.
7	In the navigation pane, click **Trusted Root Certification Authorities** and repeat steps 5-6 to install a copy of the certificate to that store.

Configuring Inbound HTTPS Inspection

Configure the Security Gateway for inbound HTTPS Inspection.

To enable inbound HTTPS traffic inspection

Step	Instructions
1	From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2	Click HTTPS Inspection > **Step 3**.
3	Select **Enable HTTPS Inspection**.
4	Import server certificates for servers behind the organization Security Gateway.
5	Define an HTTPS Inspection policy: ■ Create rules ■ Add a sever certificate to the **Certificate** column of each rule.

The first time you enable HTTPS Inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS Inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Assigning a Server Certificate for Inbound HTTPS Inspection

Add the server certificates to the Security Gateway. This creates a server certificate object.

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the traffic. The Security Gateway inspects the inbound traffic and creates a new HTTPS connection from the gateway to the internal server. To allow HTTPS Inspection, the Security Gateway must use the original server certificate and private key. The Security Gateway uses this certificate and the private key for TLS connections to the internal servers.

After you import a server certificate (with a CER file extension) to the Security Gateway, add the object to the HTTPS Inspection Policy.

Do this procedure for all servers that receive connection requests from clients outside of the organization.

To add a server certificate for inbound HTTPS Inspection

Step	Instructions
1	In SmartConsole, go to **Security Policies** > **HTTPS Inspection** > **HTTPS Tools** > **Additional Settings**.
2	Click **Open HTTPS Inspection Policy In SmartDashboard**. SmartDashboard opens.
3	Click **Server Certificates**.
4	Click **Add**. The **Import Inbound Certificate** window opens.
5	Enter a **Certificate name** and a **Description** (optional).
6	Browse to the certificate file.
7	Enter the **Private key password**. Enter the same password that was used to protect the private key of the certificate on the server.
8	Click **OK**.

The **Successful Import** window opens the first time you import a server certificate. It shows you where to add the object in the HTTPS Inspection Rule Base. Click **Don't show this again** if you do not want to see the window each time you import a server certificate and **Close**.

HTTPS Inspection Policy

The HTTPS Inspection rules define how the Security Gateways inspect HTTPS traffic. The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection rules are applied to all the Software Blades that have HTTPS Inspection enabled.

These are the Software Blades that support HTTPS Inspection:

- Access Control:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention:
  - IPS
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
- Data Loss Prevention

Starting from R81, the HTTPS Inspection policy is in SmartConsole > the **Security Policies** view > **HTTPS Inspection**. Starting from R80.40 you can create different HTTPS Inspection layers per different policy packages. When you create a new policy package, you can use the pre-defined HTTPS Inspection layer, or customize the HTTPS Inspection layer to fit your security needs.

You can share an HTTPS Inspection layer across multiple policy packages.

Fields

These are the fields that manage the rules for the HTTPS Inspection Security Policy.

Field	Description
No.	Rule number in the HTTPS Inspection Rule Base.
Name	Name that the system administrator gives this rule.
Source	Network object that defines where the traffic starts.
Destination	Network object that defines the destination of the traffic.
Services	The network services that are inspected or bypassed. By default, the services `HTTPS` on port 443 and `HTTP_and_HTTPS proxy` on port 8080 are inspected. You can add or delete services from the list.
Site Category	Categories for applications or web sites that are inspected or bypassed.

Field	Description
Action	Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (**Bypass**).
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that will enforce the HTTPS Inspection Policy. You can only select Security Gateways that have HTTPS Inspection enabled (by default, the gateways which appear in the Install On column have HTTPS inspection enabled).
Certificate	The certificate that is used for this rule. ■ Inbound HTTPS Inspection - Select the certificate that the internal server uses. You can create server certificates from the SmartDashboard > **HTTPS Inspection** > **Server Certificates** > **Add**. ■ Outbound HTTPS Inspection - Select the Outbound Certificate object that you are using for the computers in the network. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client.
Comment	An optional field that lets you summarize the rule.

Configuring HTTPS Inspection Rules

Create different HTTPS Inspection rules for outbound and inbound traffic.

The outbound rules use the certificate that was generated for the Security Gateway.

The inbound rules use a different certificate for each internal server.

You can also create bypass rules for traffic that is sensitive and should not be inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

After creating the rules, install the Access Control Policy.

Sample HTTPS Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy (The **Track** and **Install On** columns are not shown. **Track** is set to **Log** and **Install On** is set to **HTTPS policy targets**.)

No	Name	Source	Destination	Services	Site Category	Action	Blade	Certificate
1	Inbound traffic	Any	WebCalendar Server	HTTPS	Any	Inspect	Any	WebCalendarServer CA
2	Financial sites	Any	Internet	HTTPS HTTP_HTTPS_proxy	Financial Services	Bypass	Any	Outbound CA
3	Outbound traffic	Any	Internet	HTTPS HTTP_HTTPS_proxy	Any	Inspect	Any	Outbound CA

1. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.
2. **Financial sites** - This is a bypass rule that does not inspect HTTPS traffic to websites that are defined in the Financial Services category.
3. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

Bypassing HTTPS Inspection for Software Update Services

Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.

To bypass HTTPS Inspection for software updates

Step	Instructions
1	In SmartConsole, go to Security Policies > **HTTPS Inspection**> **HTTPS Tools** > **Additional Settings** > **Open HTTPS Inspection Policy in SmartDashboard**.
2	In SmartDashboard, click the HTTPS Inspection tab.
3	Click **HTTPS Validation**.
4	Go to **Whitelisting** and select **Bypass HTTPS Inspection of traffic to well-known software update services (list is dynamically updated)**. This option is selected by default.
5	Click **list** to see the list of approved domain names.

Managing Certificates by Gateway

The Gateways pane in the HTTPS Inspection tab in SmartDashboard lists the gateways with HTTPS Inspection enabled.

In the CA Certificate section, in the lower part of the Gateways pane, you can **Renew** the certificate validity date range if necessary and **Export** it for distribution to the organization client machines.

If the Security Management Server which manages the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**.

- You can import a CA certificate already deployed in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export it from the Security Management Server on which it was created (see *"Exporting and Deploying the Generated CA" on page 311*).

Adding Trusted CAs for Outbound HTTPS Inspection

When a client initiates an HTTPS connection to a website server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the Security Gateway to the designated server.

When the Security Gateway establishes a secure connection (a TLS tunnel) to the designated website, it must validate the site server certificate.

HTTPS Inspection comes with a preconfigured list of trusted CAs. This list is updated by Check Point when necessary and is automatically downloaded to the Security Gateway. After you install the update, make sure to install the policy. You can select to disable the automatic update option and manually update the Trusted CA list.

If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates.

Saving a CA Certificate

You can save a selected certificate in the trusted CAs list to the local file system.

To export a CA certificate

Step	Instructions
1	In SmartDashboard, go to the HTTPS Inspection tab > **Trusted CAs**.
2	Click **Actions** > **Export to file**.
3	Browse to a location, enter a file name and click **Save**. A `*.cer` file is created.

HTTPS Validation

In the HTTPS Validation page of SmartDashboard you can set options for

- Fail mode
- HTTPS site categorization mode
- Server validation
- Certificate blacklisting
- Whitelisting
- Troubleshooting

To learn more about these options, see the Help. Click the **?** symbol in the **HTTPS Validation** page.

Showing HTTPS Inspection Logs

The predefined log query for HTTPS Inspection shows all HTTPS traffic that matched the HTTPS Inspection policy, and was configured to be logged.

To see HTTPS Inspection Logs

Step	Instructions
1	In the SmartConsole Logs & Monitor view, go to the **Logs** tab, and click **Queries**.
2	Select the HTTPS Inspection query.

The **Logs** tab includes an **HTTP Inspection Action** field. The field value can be *inspect* or *bypass*. If HTTPS Inspection was not done on the traffic, this field does not show in the log.

SNI support for Site Categorization

Starting from R80.30, a new functionality allows the categorization of HTTPS sites before the HTTPS Inspection begins, and prevents connectivity failure if the inspection does not succeed.

SNI is an extension to the TLS protocol, which indicates the hostname at the start of the TLS handshaking process.

The categorization is performed by examining the SNI field in the client hello message at the beginning of the TLS handshaking process. To make sure that you reached the right site, the SNI is verified against the Subject Alternative Name of the host, which appears in the certificate.

After the identity of the host is known and verified, the site is categorized, and it is determined whether the connection should be inspected or not.

SNI support is enabled by default.

HTTPS Inspection on Non-Standard Ports

Applications that use HTTP normally send the HTTP traffic on TCP port 80. Some applications send HTTP traffic on other ports also. You can configure some Software Blades to only inspect HTTP traffic on port 80, or to also inspect HTTP traffic on non-standard ports.

The security policies inspect all HTTP traffic, even if it is sent using nonstandard ports. This option is selected by default. You can configure this option in the **Manage & Settings** view > **Blades > Threat Prevention > Advanced Settings**.

Configuring Security Gateways to Inspect TLS v1.3 Traffic

From R81, Check Point Security Gateway can inspect the Transport Layer Security (TLS) v1.3 traffic (see RFC 8446).

To inspect TLS v1.3 traffic

Important:

- By default, this feature is disabled.
- In a Cluster, you must configure all the Cluster Members in the same way.

1. Make sure the Security Gateway (Cluster Member) supports the User-space Firewall (USFW) mode.

   For the list of supported platforms, see sk167052.

2. Enable the inspection of the TLS 1.3 traffic:
   a. Connect to the command line on the Security Gateway (Cluster Member).
   b. Log in to the Expert mode.
   c. Back up the `$FWDIR/boot/modules/fwkern.conf` file:

   ```
   cp -v $FWDIR/boot/modules/fwkern.conf{,_BKP}
   ```

   d. Edit the `$FWDIR/boot/modules/fwkern.conf` file:

   ```
   vi $FWDIR/boot/modules/fwkern.conf
   ```

   e. Set the value of the kernel parameter **fwtls_enable_tlsio** to 1 (see sk26202).

   Add this line (without spaces):

   ```
   fwtls_enable_tlsio=1
   ```

   f. Save the changes in the file and exit the editor.
   g. Reboot.
3. Make sure the Security Gateway (Cluster Member) enabled the feature:

a. Connect to the command line on the Security Gateway (Cluster Member).

b. Log in to Gaia Clish or the Expert mode.

c. Examine the value of the kernel parameter **fwtls_enable_tlsio** (see sk26202):

```
fw ctl get int fwtls_enable_tlsio
```

Expected output:

```
fwtls_enable_tlsio = 1
```

Note - To disable the inspection of the TLS v1.3 traffic, set the value of the kernel parameter **fwtls_enable_tlsio** to **0** and reboot.

Client Certificates for Smartphones and Tablets

To allow your users to access their resources using their handheld devices, make sure they can authenticate to the Security Gateway with client certificates.

In many organizations, the daily task of assigning and maintaining client certificates is done by a different department than the one that maintains the Security Gateways. The computer help desk, for example. You can create an administrator that is allowed to use SmartConsole to create client certificates, while restricting other permissions (see *"Giving Permissions for Client Certificates" on page 326*).

To configure client certificates, open SmartConsole and go to **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.

To configure the Mobile Access policy, go to **Manage & Settings** > **Blades** > **Mobile Access** > **Configure in SmartDashboard**. The **Client Certificates** page in SmartConsole is a shortcut to the SmartDashboard **Mobile Access** tab, **Client Certificates** page.

Managing Client Certificates

Check Point Mobile Apps for mobile devices can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

Manage client certificates in **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**..

The page has two panes.

- In the **Client Certificates** pane:
  - Create, edit, and revoke client certificates.
  - See all certificates, their status, expiration date and enrollment key. By default, only the first 50 results show in the certificate list. Click **Show more** to see more results.
  - Search for specified certificates.
  - Send certificate information to users.
- In the **Email Templates for Certificate Distribution** pane:
  - Create and edit email templates for client certificate distribution.
  - Preview email templates.

Creating Client Certificates

Note - If you use LDAP or AD, creation of client certificates does not change the LDAP or AD server. If you get an error message regarding LDAP/AD write access, ignore it and close the window to continue.

To create and distribute certificates with the client certificate wizard

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. In the **Client Certificates** pane, click **New**.

   The **Certificate Creation and Distribution** wizard opens.
3. In the **Certificate Distribution** page, select how to distribute the enrollment keys to users. You can select one or both options.
   a. **Send an email containing the enrollment keys using the selected email template** -Each user gets an email, based on the template you choose, that contains an enrollment key.
      - **Template** - Select the email template that is used.
      - **Site** - Select the Security Gateway, to which users connect.
      - **Mail Server** - Select the mail server that sends the emails.

      You can click **Edit** to view and change its details.
   b. **Generate a file that contains all of the enrollment keys** - Generate a file for your records that contains a list of all users and their enrollment keys.
4. **Optional:** To change the expiration date of the enrollment key, edit the number of days in **Users must enroll within x days**.
5. **Optional:** Add a comment that will show next to the certificate in the certificate list on the **Client Certificates** page.
6. Click **Next**.

   The **Users** page opens.
7. Click **Add** to add the users or groups that require certificates.
   - Type text in the search field to search for a user or group.
   - Select a type of group to narrow your search.
8. When all included users or groups show in the list, click **Generate** to create the certificates and send the emails.
9. If more than 10 certificates are being generated, click **Yes** to confirm that you want to continue.

   A progress window shows. If errors occur, an error report opens.
10. Click **Finish**.
11. Click **Save**.
12. In SmartConsole, install the Policy.

Revoking Certificates

If the status of a certificate is Pending Enrollment, after you revoke it, the certificate does not show in the **Client Certificate** list.

To revoke one or more certificates

1. Select the certificate or certificates from the **Client Certificate** list.
2. Click **Revoke**.
3. Click **OK**.

After you revoke a certificate, it does not show in the **Client Certificate** list.

Creating Templates for Certificate Distribution

To create or edit an email template

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. To create a new template: In the **Email Templates for Certificate Distribution** pane, select **New**.

   To edit a template: In the **Email Templates for Certificate Distribution** pane, double-click a template.

   The **Email Template** opens.
3. Enter a **Name** for the template.
4. **Optional:** Enter a **Comment**. Comments show in the Mail Template list on the **Client Certificates** page.
5. **Optional:** Click **Languages** to change the language of the email.
6. Enter a **Subject** for the email. Click **Insert Field** to add a predefined field, such as a Username.
7. In the message body add and format text. Click **Insert Field** to add a predefined field, such as Username, Registration Key, or Expiration Date.
8. Click inside the E-mail Template body.
9. Click **Insert Link** and select the type of link to add (link or QR code).
   - **Site and Certificate Creation**

     For users who already have a Check Point app installed.

     When users scan the QR code or go to the link, it creates the site and registers the certificate.

     Select the client type that will connect to the site- Select one client type that users will have installed:

     - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
     - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.

- **Download Application**

  Direct users to download a Check Point App for their mobile devices.

  Select the client device operating system:

  - **iOS**
  - **Android**

  Select the client type that will connect to the site- Select one client type that users will have installed:

  - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.

- **Custom URL**

  Lets you configure your own URL.

For each link type, you can select which elements are added to the mail template

- **Link URL** - Enter the full link address.
- **QR Code** - When enabled, users scan the code with their mobile devices.
- **HTML Link** - When enabled, users tap the link on their mobile devices.

  You can select both **QR Code** and **HTML Link** to include both in the email.
- **Display Text** - Enter the text for the link title.

10. Click **OK**.
11. **Optional:** Click **Preview in Browser** to see a preview of how the email will look.
12. Click **OK**.
13. Publish the changes

Cloning a Template

Clone an email template to create a template that is similar to one that already exists.

To create a clone of an email template

1. Select a template from the template list in the **Client Certificates** page.
2. Click **Clone**.
3. A new copy of the selected template opens for you to edit.

Giving Permissions for Client Certificates

You can create an administrator that is allowed to use SmartConsole to create client certificates, and restrict other permissions.

To make an administrator for client certificates

1. Define an administrator (see *"Creating, Changing, and Deleting an Administrator Account" on page 110*).
2. Create a customized profile for the administrator, with permission to handle client certificates. Configure this in the **Others** page of the Administrator Profile. Restrict other permissions (see *"Creating, Changing, and Deleting an Administrator Account" on page 110*).

See *"Managing Administrator Accounts" on page 103*.

Preferences and Management Settings

Database Revisions

The Security Management architecture has built-in revisions. Each publish operation creates a new revision which contains only the changes from the previous revisions.

Benefits of the revision architecture:

- Safe recovery from a crisis, restoring a database to a good known revision.
- Fast policy verification, based on the differences between installed versions
- More efficient Management High Availability.

Important - Before using the revision feature consider these limitations:

- Reverting a to previous revision is an irreversible operation, newer revisions than the target revision are lost.
- Changes apply to objects only and not to the file system.
- Tasks, SIC and Licenses are not reverted.
- The revert action disconnects all other connected users and discards all of their private sessions.
- Revision is not supported in these scenarios:
  - The Endpoint Security Management Server is enabled.
  - If SmartConsole and the Security Management Server are connected through a proxy server, the GUI for this feature is not supported. In this case, use the applicable API command.
  - VSX configuration or related networks differ between the source and target revisions.
  - A new Multi-Domain Server, a Security Management Server or a Check Point object was created or deleted after the target revision date.
  - The corresponding revision of the Global Domain, or the IPS or Application Control components was purged.

Best Practices:

1. We recommend to update the IPS and Application Control signatures and install the policy after the revert. Install policy if changes to log destinations are applied.
2. If you need a full environment restore to a certain point in time, use **Restore Backup**. All work done after the backup is lost. To learn more, see the: *R81 Gaia Administration Guide*
3. We recommend to purge irrelevant revisions. Accumulating too many revisions can create a heavy load on the server, which may cause disk and performance issues.

To see saved database versions:

In SmartConsole, go to **Manage & Settings** > **Sessions** > **Revisions**.

To open a specific revision:

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.

   The bottom pane shows the audit logs of the changes made in the revision.
2. **Optional:** Click **View**.

   A separate read-only SmartConsole session opens.

To compare between two revisions:

1. In **SmartConsole**, go to **Manage & Settings** > **Sessions** > **Revisions**.
2. Select a revision.
3. In the toolbar, click **Changes**.
4. Select the revision to compare to:
   - The current revision

     Or
   - A previous revision in the list. If you select this option, select the applicable revision from the list.

   A changes report is generated. The report shows a comparison between the two selected revisions.

To revert to an earlier revision

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.
2. In **Actions**, click **Revert to this Revision**.

   The **Revert to Revision** wizard opens.

To delete all versions of the database that are older than the selected version:

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.
2. In **Actions**, click **Purge**.
3. In the confirmation window that opens, click **Yes**.

Important - Purge is irreversible. When you purge, that revision and older revisions are deleted.

Notes:

- When connected with SmartConsole to a Security Management Server, sessions that were published through the Management API in the system Domain are not shown in the **Revisions** view.
- When connecting with the Management API to the Domain of a Security Management Server and running the *show sessions* API command with *view-published-sessions* set to *true*, sessions that were published through SmartConsole are not returned, even if they include changes in the system Domain.

Setting IP Address Versions of the Environment

Many objects and rules use IP addresses. Configure the version that your environment uses to see only relevant options.

To set IP address version

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. Select the IP address version that your environment uses: **IPv4**, **IPv6**, or **IPv4 and IPv6**.
4. Select how you want to see subnets: **Mask Length** or **Subnet Mask**.

Restoring Window Default

Some windows in the SmartConsole offer administrators the option to not see the window again. You can undo this selection, and restore all windows to show again.

This option is available only if administrators selected **do not show** in a window.

To restore windows from "do not show"

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. In the **User Preferences** area, click **Restore All Messages**.

Configuring the Login Window

Administrators in your environment use SmartConsole daily. Customize the Login window, to set the environment to comply with your organization's culture.

To customize the Login window

1. Click **Manage & Settings**.
2. Click **Preferences** > **Login Message**.

   The **Login Message** window opens.
3. Select **Show custom message during login**.
4. In **Customize Message**, enter a **Header** and **Message** for administrators to see.

   The default suggestion is:
   ```
   Warning
   This system is for authorized use only
   ```
5. If you want the message to have a warning icon, in **Customize Layout**, select **Add warning sign**.
6. If you want the Login window to show your organization's logo, in **Customize Layout**, select **Add logo** and then **Browse** to an image file.

Synchronization with UserCenter

You can add information regarding your environment to User Center, such as Security Gateway name, version, and active blades. Check Point uses this additional information for better inventory management, pro-active support, and more efficient ticket resolution.

To learn more, see sk94064.

To sync with User Center

1. In SmartConsole, click **Manage & Settings**.
2. Click **Sync with User Center**
3. Select **Synchronize information once a day**.

Inspection Settings

You can configure inspection settings for the Security Gateway:

- Deep packet inspection settings
- Protocol parsing inspection settings
- VoIP packet inspection settings

The Security Management Server comes with two preconfigured inspection profiles for the Security Gateway:

- **Default Inspection**
- **Recommended Inspection**

When you configure a Security Gateway, the **Default Inspection** profile is enabled for it. You can also assign the **Recommended Inspection** profile to the Security Gateway, or to create a custom profile and assign it to the Security Gateway.

To activate the Inspection Settings, install the Access Control Policy.

Note - In SmartDashboardR77.30 and lower, **Inspection Settings** are configured as **IPS Protections**.

Configuring Inspection Settings

To configure Inspection Settings

1. In SmartConsole, go to the **Manage & Settings** > **Blades** view.
2. In the **General** section, click **Inspection Settings**.

   The **Inspection Settings** window opens.

You can:

- Edit inspection settings.
- Edit user-defined **Inspection Settings** profiles. You cannot change the **Default Inspection** profile and the **Recommended Inspection** profile.
- Assign **Inspection Settings** profiles to Security Gateways.
- Configure exceptions to settings.

To edit a setting

1. In the **Inspection Settings** > **General** view, select a setting.
2. Click **Edit**.
3. In the window that opens, select a profile, and click **Edit**.

   The settings window opens.
4. Select the **Main Action:**
   - **Default Action** - preconfigured action
   - **Override with Action** - from the drop-down menu, select an action with which to override the default - **Accept**, **Drop**, **Inactive** (the setting is not activated)
5. Configure the **Logging Settings**

   Select **Capture Packets**, if you want to be able to examine packets that were blocked in Drop rules.
6. Click **OK**.
7. Click **Close**.

For advanced configuration of SYN attacks, see sk120476.

To view settings for a certain profile

1. In the **Inspection Settings** > **General** view, click **View** > **Show Profiles**.
2. In the window that opens, select **Specific Inspection settings profiles**.
3. Select profiles.
4. Click **OK**.

   Only settings for the selected profiles are shown.

You can add, edit, clone, or delete custom Inspection Settings profiles.

To edit a custom Inspection Settings profile

1. In the **Inspection Settings** > **Profiles** view, select a profile.
2. Click **Delete**, to remove it, or click **Edit** to change the profile name, associated color, or tag.
3. If you edited the profile attributes, Click **OK** to save the changes.

To add a new Inspection Settings profile

1. In the **Profiles** view, click **New**.
2. In the **New Profile** window that opens, edit the profile attributes:

3. Click **OK**.

To assign an Inspection Settings profile to a Security Gateway

1. In the **Inspection Settings** > **Gateways** view, select a Security Gateway, and click **Edit**.
2. In the window that opens, select an Inspection Settings profile.
3. Click **OK**.

To configure exceptions to inspection settings

1. In the **Inspection Settings** > **Exceptions** view, click **New** to add a new exception, or select an exception and click **Edit** to modify an existing one.

   The **Exception Rule** window opens.
2. Configure the exception settings:
   - **Apply To** - select the **Profile** to which to apply the exception
   - **Protection** - select the setting
   - **Source** - select the source **Network Object**, or select **IP Address** and enter a source IP address
   - **Destination** - select the destination **Service Object**
   - **Service** - select **Port/Range**, **TCP** or **UDP**, and enter a destination port number or a range of port numbers
   - **Install On** - select a Security Gateway, on which to install the exception
3. Click **OK**.

To enforce the changes, install the Access Control Policy.

SmartTasks

Management SmartTasks let you configure automatic actions according to different triggers in the system. A SmartTask is a combination of trigger and action.

- **Triggers** are events – currently defined in terms of existing management operations, such as installing a policy or publishing a session.
- **Actions** are automatic responses that take place after the trigger event , such as running a script, posting a web request or sending email.

Available Triggers

- **Before Publish** - Fired when an administrator publishes a session. The SmartTask passes the sessions meta-data (publishing administrator, domain information and session name) to the action. If the local Management API server is available, the session changes about to be published are formatted as a response to the "show changes" API.
- **After Publish** - Fired after an administrator successfully publishes a session. The SmartTask passes the same information to the action as the **Before Publish** trigger.

- **After Install Policy** - Fired after a policy has been installed. The SmartTask passes to the action information related to the policy installation task, such as the package installed, the administrator who initiated the installation and the task's result.

Available Actions

- **Run Script** - Runs a pre-defined Repository Script. The script gets the trigger's data as the first parameter. The trigger's data is passed as Base64 encoded JSON data, which can be decoded to implement custom business logic.

  For SmartTasks configured to run with "Before" operation triggers, the repository script can signal whether to abort or continue the operation by printing a JSON object with the "result" and optional "message" fields and then exit with code 0. If the value of the "result" field is "failure" the operation aborts.

  For SmartTasks configured to run with other triggers, exit code 0 is treated as success. Any other exit code is treated as failure.

  Note - By default, Repository Scripts run on the local Security Management Server although this can be customized using the Web API.

- **Web Request** - Executes an HTTPS POST web request to the configured URL. The trigger's data is passed as JSON data to the request's payload.

  Notes:

  - The configured URL must start with HTTPS and the target web server capable of handling such requests.
  - For web servers with self-signed SSL certificates, establish trust by specifying the certificate's fingerprint. You can get the fingerprint by clicking **Get Fingerprint** in the SmartTask editor or by viewing the certificate in a web browser.

  For SmartTasks configured to run with "Before" operation triggers, the repository script can signal whether to abort or continue the operation by responding with JSON object "result" and optional "message" fields and a status of 200 OK. If the value of the "result" field is "failure" the operation aborts.

  For SmartTasks configured to run with other triggers, a 200 OK return code is treated as success. Any other exit code is treated as failure.

Configuring SmartTask Properties

1. Enter a unique name for the SmartTask - The name property is required and case sensitive.
2. Switch the SmartTask **ON** or **OFF** using the toggle button.
3. Optional - Enter a description for the SmartTask.
4. Select a trigger for the SmartTask.
5. Select an action that will happen once the trigger is fired.
6. Custom Data – You can add additional information to the JSON data sent with the trigger information by adding a JSON object to the **Custom Data** field. The JSON custom data is concatenated to the trigger's payload and passed to the action.
7. Optional - Add tags for the SmartTask object.

SmartTask Advanced Properties

The available advanced options depend on the action selected on the **General** tab.

Send Web Request

- **Time-out** – Number of seconds before the request times out and the request aborted.
- **If the HTTPS request times out** - Treat the time-out as an error and abort the event or continue normally.
- **X-chkp-shared-secret** – Enter a shared secret that can be used by the target web server to identify the Security Management Server. The value is sent as part of the request in the *X-chkp-shared-secret* header in the out-going web request.

Run script

- **Time-out** – Number of seconds before the request times out and the request aborted.
- **If the script fails to run or times-out** – Treat time-out (or execution failure) as an error and abort the event or continue normally.

Example

Use Case:

A company policy dictates that the publish operation must be used with a service request number as a prefix to the session name before saving any changes to the database, so the administrators can see what the rationale for changing the security policy was.

Procedure:

Add the *Validate Session Name Prefix* to the **Scripts Repository**.

1. Save the script in the repository.

   #### Instructions

   a. Click **Gateways & Servers** > **Scripts** > **Scripts Repository** > **New** (✳)

   b. Give the script a name.

   c. In the **Content** text box, paste the script code below.

   d. Click **OK** to save the script in the repository.

Script code

```
#!/bin/bash
JQ=${CPDIR}/jq/jq
data=`echo $1 | base64 --decode -i`

# Extracting the required session name prefix for the session name based on the input JSON
sessionNamePrefix=`echo $data | $JQ -r  .\"custom-data\".\"session-name-prefix\"`

# If there's no input session name prefix, publish is allowed
if [[ $sessionNamePrefix = "null" ]] || [[ -z "$sessionNamePrefix" ]]; then
    printf '{"result":"success"}\n'
    exit 0
fi

# Extracting the actual session name
sessionName=`echo $data | $JQ -r .session.\"session-name\"`

# Abort the publish if the session doesn't contain a name at all
if [[ $sessionName = "null" ]]; then
    m1="Corporate Policy requires you to use a service request number for the session's name
prefix."
    m2="For example: ${sessionNamePrefix}######"
    m3="Session name is missing. Please change your session's name to meet the requirements
and try to publish again."
    printf '{"result":"failure","message":"%s %s %s"}\n' "$m1" "$m2" "$m3"
    exit 0
fi

# Abort the publish if the session name doesn't match the expected prefix
if [[ ! $sessionName == $sessionNamePrefix* ]]; then
    m1="Corporate Policy requires you to use a ticket number as the session's name."
    m2="For example: ${sessionNamePrefix}###### "
    m2=${m2//\"/\\\"}
    m3="Please change your session's name to meet the requirements and publish again."
    printf '{"result":"failure","message":"%s %s %s"}\n' "$m1" "$m2" "$m3"
    exit 0
else
    # Session name matches the expected prefix, publish is allowed
    printf '{"result":"success"}\n'
    exit 0
fi
```

2. Create a SmartTask to run the session validation script.

   ### Instructions

   a. Go to **Manage & Settings** > **Tasks** > **SmartTasks** > **New** (✦).

   b. Give the new SmartTask a name (you can call it "`Validate Session Name Before Publish`")

   c. In the **Trigger and Action** section, select from the drop down menu:

      Before Publish and **Run Script**.

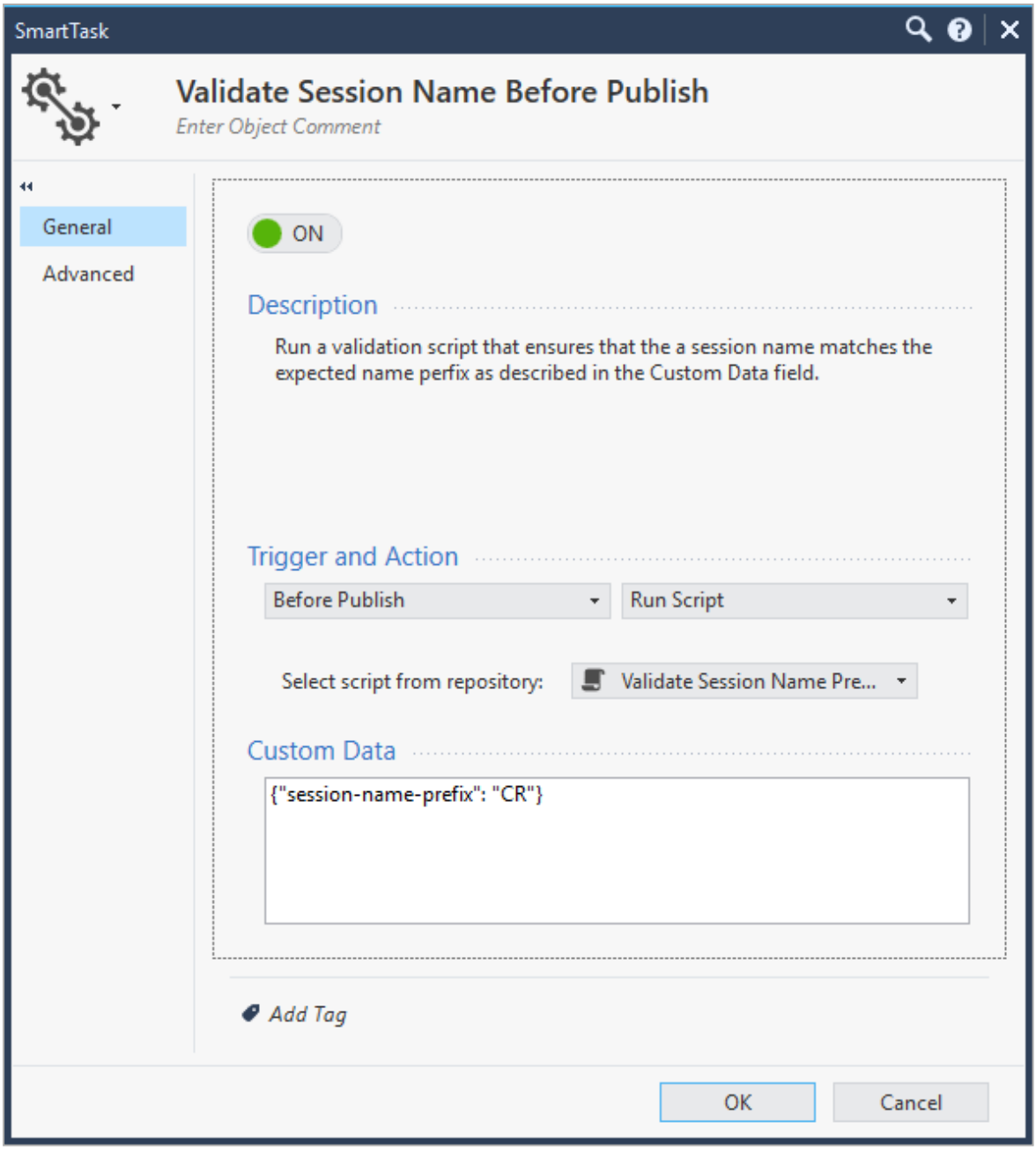
   d. In the **Select script from repository** drop down, select the script saved in Step 1.

   e. In the **Custom Data** field, enter this string:

      {"session-name-prefix": "CR"}

      Note - The variable "**session-name-prefix**" correlates to the variable used at the beginning of the script in Step 1. If these are not identical, this script cannot work and the process fails.



3. Publish the SmartConsole session.
4. Add a network object.
5. Publish the changes using the required prefix.

Note - If you publish the session without using the prefix, the process fails.

Network Security for IoT Devices

Introduction

The complexity of using IoT devices in the modern work environment such as hospitals, industries, and smart-buildings has, at cost, exposed them to ill-natured and harmful cyber attacks. Malicious cyber invasions into IoT devices have caused considerable financial loss to a number of enterprises. In addition to monetary loss and physical damage, these attacks can lead to data breaches, data tampering, ransomware, and even denial of service.

Common IoT devices susceptible to attack:

Smart Buildings/Offices	Healthcare	Industry
HVAC	HVAC	HVAC
Printers, copiers, fax machines	Printers, copiers, fax machines	Printers, copiers, fax machines
Elevators	Elevators	Elevators
Surveillance Cameras	Surveillance Cameras	Surveillance Cameras
Unhardened kiosk connected to a LAN	Unhardened kiosk connected to a LAN	Unhardened kiosk connected to a LAN
Access control points	Access control points	Access control points
Programmable logic controllers (PLCs)	Programmable logic controllers (PLCs)	Programmable logic controllers (PLCs)
Thermostats	Thermostats	Thermostats
Lighting	Lighting	Lighting
Residential smart meters	MRI machines	--
Fire alarms	Fire alarms	Fire alarms
N/A	Ultrasound machines	--
--	C-arms	--
--	Infusion pumps	--
--	Blood glucose meter	--
--	Patient monitor	--

What makes IoT devices so vulnerable:

- Outdated software, legacy OS, or no OS
- Basic Micro Controllers
- No Security-by-Design
- Lack of device management
- Shadow Devices
- Operational Limitations

Check Point's Infinity for IoT provides comprehensive network security for enterprise IT and IoT devices, smart building devices, industrial IoT, and connected medical equipment in these ways:

1. Prevent malicious intents and unauthorized access to IoT devices by analyzing multiple threat indicators from various resources.
2. Prevent infected devices from compromising other network elements.
3. Minimize the attack surface through internal network segmentation.
4. Provide deep insight information per IoT device.
5. Uses 3rd party discovery engine for IoT assets discovery.
6. Create separated IoT policy layer, using the discovered IoT device's attributes.

Note - Enforcement of IoT assets in the Access Control policy is not supported on Centrally Managed Quantum Spark appliances running Gaia Embedded operating system.

Prerequisites

- Check Point certified IoT Discovery Service installed on the network with a connection to the Management Server.
- Discovery Service
  - Industrial / Enterprise:
    - Armis
    - Claroty
    - Indegy
    - Ordr
    - SAM
    - SCADAfence
  - Medical:
    - Medigate
    - CyberMDX
    - Cynerio
- Identity Awareness Web API must be activated on the enforcing Security Gateway (the configuration is done automatically).
- Security Gateway version R80.10 and above

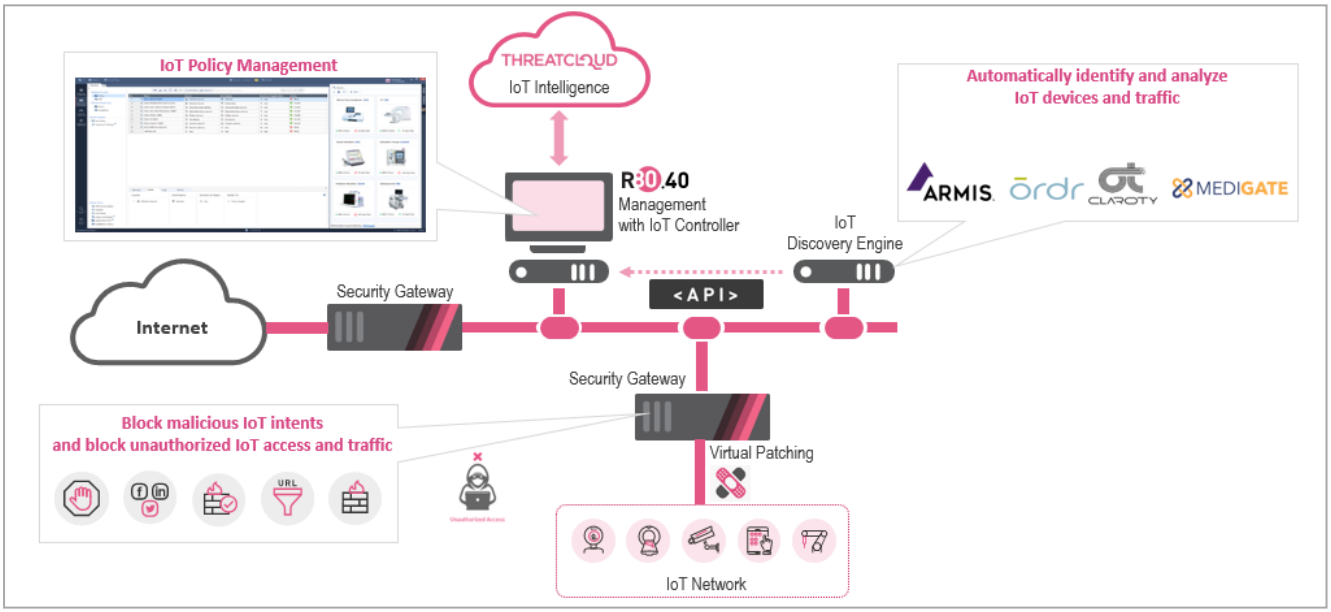
Note - Enforcement of IoT assets in the Access Control policy is not supported on Centrally Managed Quantum Spark appliances running Gaia Embedded operating system.

Network Overview

Check Point's Infinity for IoT delivers comprehensive IoT cyber-security by applying granular IoT-based policies. Check Point's IoT protection solution mobilizes hospitals, industries, smart buildings and offices to reduce and even eliminate IoT attacks.

- Identify and analyze IoT devices and traffic
- Deploy IoT policy enforcement points
- Identify and block IoT malicious intents

Network Diagram



Configuring the IoT Controller

Before Check Point Infinity for IoT can protect IoT devices from malicious attacks, you need to configure the IoT Discovery Service. The IoT Discovery Service is a 3rd party source that provides the necessary device attributes for each IoT device to the firewall.

To define the IoT Discovery Service

Step	Instructions
1	Go to **SmartConsole** > **Objects** > **New** > **More** > **IoT Discovery Service**. The **New IoT Discovery Service** window opens.

Step	Instructions
2	To configure the **General tab:** a. Enter the **Hostname**, **Port**, and **Pre-shared Key**. The pre-shared key must be provided from the certified IoT discovery service, and used for authorizing and authenticating the IoT discovery service. b. Click **OK.** The **Certificate Trust** window opens. Before verifying, check that the certificate is valid, and that the IoT discovery service is the certified owner. Infinity for IoT utilizes the Identity Awareness API. For easy activation, select the gateways where IoT enforcement will be done. To configure the **Gateways** tab: ■ Select the enforcing gateway for IoT traffic. To configure the **Policies** tab: a. Select the **Policy** to be applied on the **IoT layer**. b. Click **OK**.
3	Publish the SmartConsole session.
4	Install Policy.

Configuring a new IoT controller generates a new IoT policy layer on the selected profiles, a new Threat Prevention profile, and a new rule in the Threat Prevention policy.

Adding IoT Assets to the Policy

After setting up the IoT policy, you can add IoT assets to the policy manually.

The policy is divided into three categories:

Category	Description
User-Defined	Used by administrators.
Auto-Generated	Rules generated from network traffic and IoT network patterns.
Cleanup	A set of rules for detected anomalies.

To define an IoT Access Rule

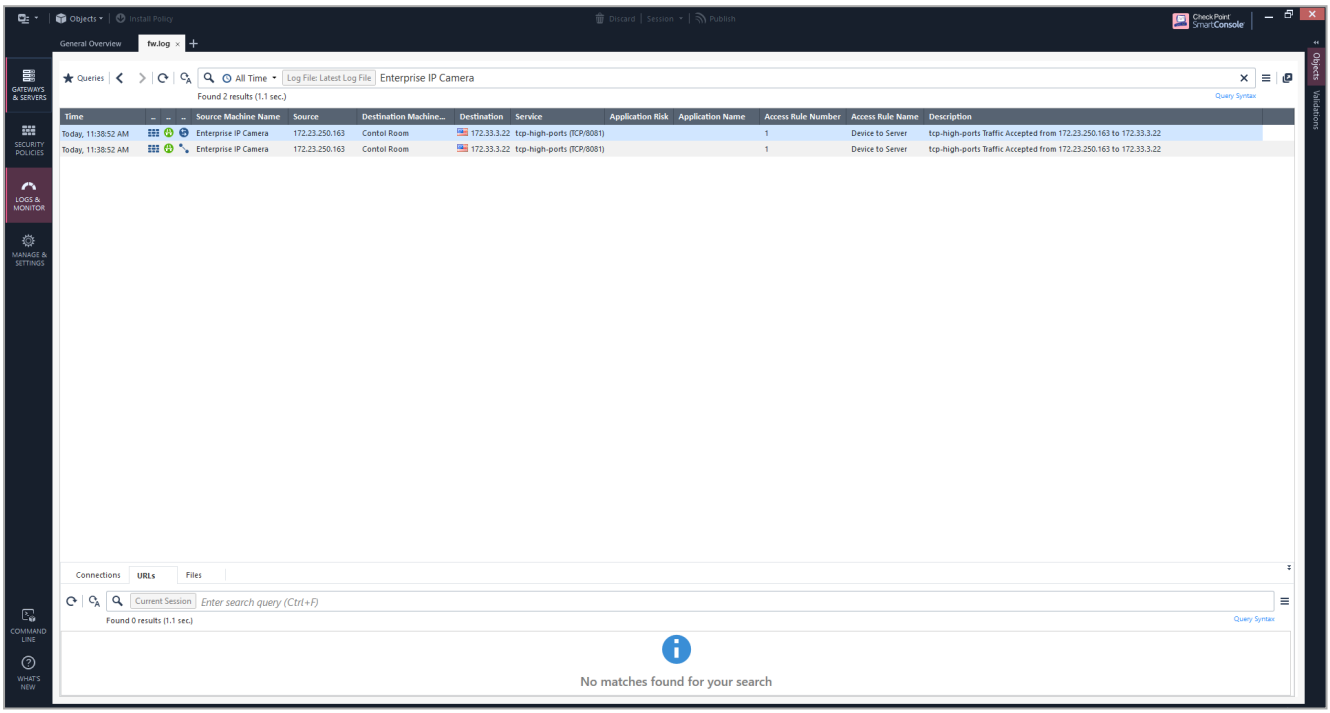
Step	Instructions
1	From **Security Policies** > **Access Control**, select the **IoT Layer**.
2	Click **User-Defined Section**, and then click the plus sign.
3	In the **Source and/or Destination field**, click the plus sign > **Add new item...**. The **Add new item** window opens.
4	Select **Import** > **IoT Controllers**, and then choose the IoT asset to be add to the rule.

Infinity for IoT Logs

Using Check Point's IoT Security Manager, security teams can see detailed IoT device information such as the manufacture's name, model, serial number, and its location. With a thorough log they gain a clearer, contextual understanding about the device's behavior and forensics for event investigation.

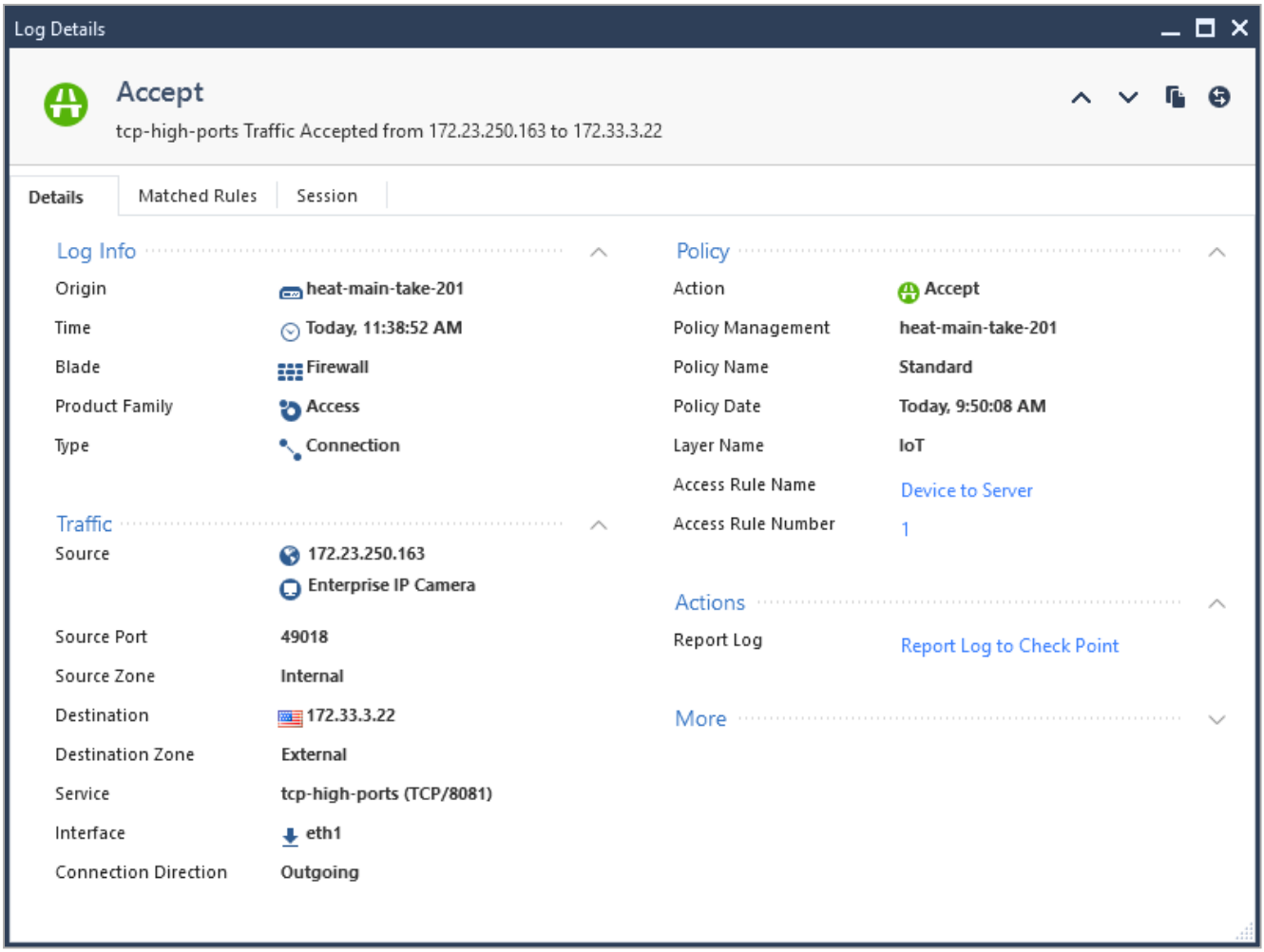
Example 1 - Log Search by IoT Asset Information

Advanced log search using the enriched log data to simplify log filtering.



Example 2 - Extended Log Data

IoT log data contains enriched information that helps identify the IoT assets in the log.



Management High Availability

This chapter descibes the configuration of Management High Availability.

Overview of Management High Availability

High Availability is redundancy and database backup for management servers. Synchronized servers have the same policies, rules, user definitions, network objects, and system configuration settings.

Management High Availability uses the built-in revisions technology and allows the High Availability procedure to synchronize only the changes done since the last synchronization. This provides:

- Real-time updates between management peers.
- Minimal effect on the management server resources.

The first management server installed is the primary. If the primary Security Management Server fails, or is off line for maintenance, the administrator can initiate a changeover, so that the secondary server takes over.

Notes:

- For High Availability (and Load Sharing) environments for Security Gateways, see the *R81 ClusterXL Administration Guide*.
- For High Availability environments for Endpoint Security, see the *R81 Endpoint Security Server Administration Guide*.

The High Availability Environment

A Management High Availability environment includes:

- One Active Security Management Server
- One or more Standby Security Management Server

For full redundancy, the active management server at intervals synchronizes its database with the secondary server or servers.

Active vs. Standby

In a standard High Availability configuration there is one Active server at a time. The administrator uses the Active server manage the High Availability configuration. The Active server automatically synchronizes the standby server(s) at regular intervals. You can open a Standby server only in Read Only mode. If the Active server fails, you can initiate a changeover to make a Standby server become the Active server. If communication with the Active server fails, there may be more than one Active server. This is called Collision Mode.

Primary Server vs. Secondary Server

The sequence in which you install management servers defines them as Primary or Secondary. The first management server installed becomes the Primary active server. When you install more Security Management Servers, you define them as Secondary. Secondary servers are Standby servers by default.

Important notes about backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81 Gaia Administration Guide*.
- About the "`migrate export`" and "`migrate import`" commands, see the *R81 CLI Reference Guide*.
- About the "`mds_backup`" and "`mds_restore`" commands, see the *R81 CLI Reference Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Configuring a Secondary Security Management Server in SmartConsole

How to configure a Secondary Security Management Server in SmartConsole.

In the SmartConsole connected to the Primary Security Management Server, create a Check Point Host object for the Secondary Security Management Server. After you publish the SmartConsole session, synchronization starts between the Primary and Secondary Security Management Servers.

To configure the Secondary Security Management Server in SmartConsole:

1. Connect with SmartConsole to the Primary Security Management Server.
2. In **Object Categories**, click **New > More > Network Object > Gateways and Servers > Check Point Host**.
3. On the **General Properties** page, enter a unique name and IP address for the Secondary Security Management Server.
4. In the **Software Blades** section, select the **Management** tab.
5. Select **Network Policy Management**.

   This automatically selects the **Secondary Server**, **Logging and Status**, and **Provisioning**.
6. Create SIC trust between the Secondary Security Management Server and the Primary:
   a. Click **Communication**.
   b. Enter the SIC Activation Key of the secondary server.
   c. Click **Initialize**.
   d. Click **Close**.
7. Click **OK**.
8. Publish the SmartConsole session to save these session changes to the database.

   The initialization and synchronization between the Security Management Servers start.

9. Monitor these tasks in the Task List, in the SmartConsole System Information area. Wait for the Task List to show that a full sync has completed.
10. Open the **High Availability Status** window and make sure there is one Active Security Management Server, and one Standby Security Management Server.

Synchronizing Active and Standby Servers

At intervals, the Active server synchronizes with the standby server or servers, and when you publish the SmartConsole session. Sessions that are not published are not synchronized.

Monitoring High Availability

The **High Availability Status** window shows the status of each Security Management Server in the High Availability configuration.

To see the server status in your High Availability environment:

1. Open SmartConsole and connect to a primary or secondary server.
2. On the **Menu**, click **High Availability**.

The **High Availability Status** window opens.

For the management server and its peer or peers in the High Availability configuration, the **High Availability Status** window shows:

- A Warning or Error message - The message shows if there is a problem between the High Availability peers.
- **Connected To** - The server that SmartConsole is connected to. Also, the High Availability mode of the server (Active or Standby), and the synchronization status and actions of the server.
- **Peers** - The servers that the connected server sees. Also, the High Availability mode of each server (Active or Standby), and the synchronization status and actions of each server.

Monitoring Synchronization Status and Actions

Status messages can be general, meaning that they apply to the full system, or they can apply to a specified active or standby server. General messages show in the yellow overview banner.

General Status messages in overview banner	Description
	The database of the primary Security Management Server is identical with the database of the secondary.
Some servers could not be synchronized	A communication issue prevents synchronization, or some other synchronization issue exists.
	The active and standby servers are not communicating.
Communication Problem	Some services are down or cannot be reached.
Collision or HA conflict	More than one management server configured as active. Two active servers cannot sync with each other.

When connected to a specified *active* management server:

Status window area:	Peer Status	Additional Information
Connected to:	Active	SmartConsole is connected to the active management server.
Peers	Standby	The peer is in standby. The message can also show: ■ Sync problem, last time sync ■ Synchronized successfully. Last sync time: <time> ■ No communication
	Not communicating, last sync time	
	Active	A state of collision exists between two servers both defined as active.

When connected to a specified *Standby* Management Server:

Status window area:	Peer Status	Description
Connected to:	Standby	Also shows: last sync time.
Peers	Active	The peer is on standby. The message can also show: ■ No communication, last sync time ■ OK., last sync time: <time> ■ Sync problem, last sync time (in any direction)
	Standby *or* Unknown	Can also show: no communication.

Changing a Server to Active or Standby

The Active server synchronizes with the Standby server or servers at intervals, and when you publish the session. Sessions that are not published are not synchronized.

Changeover between the primary (active) and secondary (standby) management server is not automatic. If the Active fails or it is necessary to change the Active to a Standby, you must do this manually. When the management server becomes Standby it becomes Read Only, and gets all changes from the new Active server.

When you initiate changeover, all public data is synchronized from the new Active to the new Standby server after the Standby becomes Active. Data from the new Active overrides the data on the new Standby. *Unpublished* changes are not synchronized.

> **Best Practice** - We recommend that you publish the SmartConsole session before initiating a changeover to the Standby Security Management Server.

To Interchange the Active and Standby

1. Connect with SmartConsole to the Standby Security Management Server.
2. Click the Menu button and select **High Availability**.

   The **High Availability Status** window opens.
3. Use the **Action** buttons to change the Standby server to Active.

This changes the previous Active server to Standby.

Working in Collision Mode

You can make more than one server Active. You may need to do that if there is no connectivity to the primary. When you change the Standby to Active, it becomes Active without telling the current Active server to become Standby. This is known as *collision mode*. You can later change one of the Active servers to Standby, and return to the standard configuration.

When in collision mode, the Active servers do not sync even if they have network connectivity. When you change one of them to Standby, sync starts and overwrites the data on the Standby server with the remaining Active data.

Changeover Between Active and Standby

Changeover between the primary (active) and secondary (standby) management server is not automatic. If the Active fails or it is necessary to change the Active to a Standby, you must do this manually. When the management server becomes Standby it becomes Read Only, and gets all changes from the new Active server.

High Availability Troubleshooting

These error messages show in the **High Availability Status** window when synchronization fails:

Not Communicating

Solution:

1. Check connectivity between the servers.
2. Test SIC.

Collision or HA Conflict

More than one management server is configured as active.

Solution:

1. From the main SmartConsole menu, select **Management High Availability**.

   The **High Availability Status** window opens.
2. Use the **Actions** button to set one of the active servers to standby.

   Warning - When this server becomes the Standby, all its data is overwritten by the active server.

Sync Error

Solution:

Do a manual sync.

Unlocking the Administrator

In a High Availability environment, if an administrator is locked on the Standby Management Server, the administrator is not locked and does not appear as locked on the Active Management Server. Therefore, you cannot unlock the administrator on the Active Management Server.

To unlock the administrator:

Use the API command `unlock-administrator` on the Standby Management Server. See the *Check Point Management API Reference*.

Environments with Endpoint Security

Environments that include Endpoint Security require additional steps and information.

For details, see *High Availability* in the *R81 Endpoint Security Server Administration Guide*.

High Availability Disaster Recovery

If the primary management server becomes permanently unavailable:

- Create a new Primary server with the IP address of the original Primary server (see *"Creating a New Primary Management Server" below*).

  Note - This is not supported for environments with Endpoint Security.

- Promote the Secondary Management Server to Primary and create new licenses.

  Important - Check Point product licenses are linked to IP addresses. At the end of the disaster recovery you must make sure that licenses are correctly assigned to your servers.

Creating a New Primary Management Server

1. Change the Secondary Management Server from Standby to Active.
2. Promote the Secondary Management Server to be Primary. Follow the procedure of promoting a Secondary Management Server (See *"Promoting a Secondary Management Server to Primary" on the next page* - no need to remove instances of the old Primary Management object and install database).
3. Install the new Secondary Management Server with the IP of the old Primary Management Server.
4. Reset SIC and connect with SIC to the new Secondary Management Server.

To set the old Primary Management Server as the new Primary Management Server

1. Change the new Secondary Management Server from Standby to Active.
2. Promote the new Secondary Management Server to be the Primary Management Server. Follow the procedure of promoting a Secondary Management Server (See *"Promoting a Secondary Management Server to Primary" below* - no need to remove instances of the old Primary Management object and install database).
3. Create the Secondary Management Server on the old Secondary Management Server with the original IP of the old Secondary Management Server.
4. Reset SIC and connect with SIC to the Secondary Management Server.

Promoting a Secondary Management Server to Primary

The first management server installed is the Primary Server and all servers installed afterwards are Secondary servers. The Primary server acts as the synchronization master. When the Primary server is down, secondary servers cannot synchronize their databases until a Secondary is promoted to Primary and the initial syncs completes.

Note This is the disaster recovery method supported for High Availability environments with Endpoint Security.

To promote a Secondary Management Server to become the Primary Management Server

Before you start - make sure that the primary server is offline.

1. Set the Secondary server to Active.
2. On the Secondary Management Server that you will promote, run:

   ```
   #$FWDIR/bin/promote_util
   #cpstop
   ```

3. Remove the `$FWDIR/conf/mgha*` files. They contain information about the current Secondary settings. These files will be recreated when you start the Check Point services.
4. Make sure you have a `mgmtha` license on the newly promoted server.

   Note - All licenses must have the IP address of the promoted Security Management Server.

5. Run `cpstart` on the promoted server.
6. Open SmartConsole, and:
   a. Remove all instances of the old Primary Management object. To see all of the instances, right-click the object and select **Where Used**.

      Note - When you remove the old Primary Management Server, all previous licenses are revoked.

   b. Install database.

The ICA Management Tool

The ICA Management Tool lets you:

- Manage certificates
- Run searches
- Recreate CRLs
- Configure the ICA
- Remove expired certificates

Note - The ICA Management Tool supports TLS.

Check Point ICA is fully compliant with X.509 standards for both certificates and CRLs. See the related X.509 and PKI documentation, and RFC 2459 for more information.

For more information, see:

- sk30501: Setting up the ICA Management Tool
- sk102837: Best Practices - ICA Management Tool configuration
- sk39915: Invoking the ICA Management Tool

Using the ICA Management Tool

Use the ICA management tool for user certificate operations only, such as certificate creation. Do not use the ICA management tool to change SIC certificates or VPN certificates. Change SIC and VPN certificates in SmartConsole.

To use the ICA management tool, you must first enable it on the Security Management Server.

Enabling and Connecting to the ICA Management Tool

The ICA Management Tool is disabled by default.

To enable the ICA Management tool

Run this command on the Security Management Server:

```
cpca_client [-d] set_mgmt_tool on|off [-p <ca_port>] [-a|-u
"administrator|user DN" ... ]
```

The command options are:

Option	Description
on	Starts the ICA Management Tool (by opening port 18265)
off	Stops the ICA Management Tool (by closing port 18265)
-p	Changes the port used to connect to the CA (if the default port is not being used)
-a "administrator DN" ...	Sets the DNs of the administrators that will be allowed to use the ICA Management Tool
-u "user DN" ...	Sets the DNs of users allowed to use the ICA Management Tool. An option intended for administrators with limited privileges.

Note - If `cpca_client` is run without `-a` or `-u` parameters, the list of the allowed users and administrators remains unchanged.

To Connect to the ICA Management Tool

1. Add the administrator's certificate to the browser's certificate repository.
2. Open the ICA Management tool from the browser using this address:

   `https://<Management_Host_Name>:18265`

   Authenticate when requested.

The ICA Management Tool GUI

Item	Description
1	**Menu Pane** Shows a list of operations
2	**Operations Pane** **Manage certificates**. The window divides into **Search attributes configuration** and **Bulk operation configuration**. **Create Certificates**. **Configure the CA**. Contains configuration parameters You can also view the CA's time, name, and the version and build number of the Security Management Server. **Manage CRLs**. Download, publish, and recreate CRLs.
3	**Search Results Pane**. The results of the applied operation show in this pane. This window consists of a table with a list of certificates and certificate attributes.

Connect to the ICA Management tool using a browser and HTTPS connection.

User Certificate Management

Internally managed User Certificates can be initialized, revoked or have their registrations removed using the ICA Management Tool. User Certificates of users managed on an LDAP server can only be managed using the ICA Management Tool.

This table shows User Certificate attributes that can be configured using the ICA Management Tool

Attributes	Default	Configurable	Comments
validity	2 years	yes	
key size	2048 bits	yes	Can be set to 4096 bits
DN of User certificates managed by the internal database	CN=user name, OU=users	no	This DN is appended to the DN of the ICA
DN of User certificates managed on an LDAP server		yes	Depends on LDAP branch
KeyUsage	5	yes	Digital signature and Key encipherment
ExtendedKeyUsage	0 (no KeyUsage)	yes	

Modifying the Key Size for User Certificates

If the user completes the registration from the Remote Access machine, the key size can be configured in the **Advanced Configuration** page in SmartConsole.

To configure the key size

1. From the **Menu**, select **Global Properties**.
2. Go to Advanced, and in the **Advanced Configuration** section, click **configure**.

   The **Advanced Configuration** window opens.
3. Go to the **Certificates and PKI properties** page.
4. Set the new key size for this property: `user_certs_key_size`.
5. Click **OK**.

You can also change the key size using the GuiDBedit Tool (see sk13009). Change the key size as it is listed in `users_certs_key_size Global Property`. The new value is downloaded when you update the site.

Performing Multiple Simultaneous Operations

The ICA Management Tool can do multiple operations at the same time. For example:

- Run an LDAP query for the details of all the organization's employees
- Create a file out of this data, and then use this file to:
  - Start (initialize) the creation of certificates for all employees
  - Send a notification about the new certificates to each of those employees

These operations can be done simultaneously:

- Start (initialize) user certificates
- Revoke user certificates
- Send mail to users
- Remove expired certificates
- Remove certificates for which the registration procedure was not completed

ICA Administrators with Reduced Privileges

The ICA Management Tool supports administrators with limited privileges. These administrators cannot execute multiple concurrent operations, and their privileges include only these:

- Basic searches
- Initialization of certificates for new users

Operations with Certificates

Management of SIC Certificates

SIC certificates are managed using SmartConsole.

Management of Security Gateway VPN Certificates

VPN certificates are managed in the **VPN** page of the corresponding network object. These certificates are issued automatically when the IPSec VPN blade is defined for the Check Point Security Gateway or host. This definition is specified in the **General Properties** window of the corresponding network object.

If a VPN certificate is revoked, a new one is issued automatically.

Management of User Certificates in SmartConsole

The user certificates of users that are managed on the internal database are managed in SmartConsole.

For more information, see *User Certificates* in the *R81 Remote Access VPN Administration Guide*.

Notifying Users about Certificate Initialization

The ICA Management Tool can be configured to send a notification to users about certificate initialization.

To send mail notifications:

1. In the Menu pane, click **Configure the CA**.
2. In the **Management Tool Mail Attributes** area, configure:
   - The mail server
   - The mail "`From`" address
   - An optional "`To`" address, which can be used if the users' address is not know

     The administrator can use this address to get the certificates on the user's behalf and forward them later.
3. Click **Apply**.

Retrieving the ICA Certificate

For trust purposes, some Security Gateways and Remote Access clients, such as peer gateways that are not managed by the Security Management Server or clients using Clientless VPN, must retrieve the ICA certificate.

To retrieve the ICA Certificate

1. Open a browser and enter the applicable URL.

   Use this format:

   `http://<IP address of Management Server>:18264`

   The **Certificate Services** window opens.
2. Use the links to download the CA certificate to your computer or (in Windows) install the CA certification path.

Searching for a Certificate

There are two search options:

- A basic search that includes only the user name, type, status and the serial number
- An advanced search that includes all the search fields (can only be performed by administrators with unlimited privileges)

To do a certificate search:

In the **Manage Certificates** page, enter the search parameters, and click **Search**.

Basic Search Parameters

- **User Name** - Username string (by default, this field is empty)
- **Type** - Drop-down list with these options:
  - *Any* (default)
  - *SIC*

- *Gateway*
- *Internal User* or *LDAP user*

- **Status** - Drop-down list with these options:
  - *Any* (default)
  - *Pending*
  - *Valid*
  - *Revoked*
  - *Expired*
  - *Renewed (superseded)*
- **Serial Number** - Serial number of the requested certificate (by default, this field is empty)

Advanced Search Attributes

In addition to the parameters of the basic search, specify these parameters:

- **Sub DN** - DN substring (by default, this field is empty)
- **Valid From** - Date, from which the certificate is valid, in the format dd-mmm-yyyy [hh:mm:ss] (for example 15-Jan-2003) (by default, this field is empty)
- **Valid To** - Date until which the certificate is valid, in the format dd-mmm-yyyy [hh:mm:ss] (for example 14-Jan-2003 15:39:26) (by default, this field is empty)
- **CRL Distribution Point** - Drop-down list with these options:
  - *Any* (default)
  - *No CRL Distribution Point* (for certificates issued before the management upgrade - old CRL mode certificates)

  The list also shows all available CRL numbers.

The Search Results

The results of a search show in the **Search Results** pane. This pane consists of a table with a list of searched certificate attributes such as:

- **(SN) Serial Number** - The SN of the certificate
- **User Name (CN)** - The string between the first equals sign ("=") and the next comma (",")
- **DN**
- **Status** - One of these: *Pending, Valid, Revoked, Expired, Renewed (superseded)*
- The date, from which certificates are valid until the date they expire

Note - The status bar shows search statistics after each search.

Viewing and Saving Certificate Details

You can view or save the certificate details that show in the search results.

To view and save certificate details

Click on the **DN** link in the **Search Results** pane.

- If the status is *pending*, the certificate information together with the registration key shows, and a log entry is created and shows in SmartConsole > **Logs & Monitor** > **Logs**.
- If the certificate was already created, you can save it on a disk or open directly (if the operating system recognizes the file extension)

Removing and Revoking Certificates and Sending Email Notifications

1. In the Menu pane, click **Manage Certificates**.
2. Search for a Certificate with set attributes (see *"Searching for a Certificate" on page 354*).

   The results show in the **Search Results** pane.
3. Select the certificates, as needed, and click one of these options:
   - **Revoke Selected** - revokes the selected certificates and removes pending certificates from the CA's database
   - **Remove Selected** - removes the selected certificates from the CA's database and from the CR

     Note - You can only remove expired or pending certificates.
   - **Mail to Selected** - sends mail for all selected *pending* certificate

     The mail includes the authorization codes. Messages to users that do not have an email defined are sent to a default address. For more information, see *"Notifying Users about Certificate Initialization" on page 353*.

Submitting a Certificate Request to the CA

There are three ways to submit certificate requests to the CA:

- **Initiate** - A registration key is created on the CA and used once by a user to create a certificate
- **Generate** - A certificate file is created and associated with a password which must be entered when the certificate is accessed
- **PKCS#10** - When the CA receives a PKCS#10 request, the certificate is created and delivered to the requester

To initiate a certificate

1. In the Menu pane, select **Create Certificates > Initiate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form:
   - **Certificate Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two weeks from the date of creation)
3. Click **Go**.

A registration key is created and show in the **Results** pane.

If necessary, click **Send mail to user** to email the registration key. The number of characters in the email is limited to 1900.

4. The certificate becomes usable after entering the correct registration key.

To generate a certificate

1. In the Menu pane, select **Create Certificates > Generate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form:
   - **Certificate Expiration Date** - Select a date or enter the date in the format `dd-mm-yyyy [hh:mm:ss]` (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format `dd-mm-yyyy [hh:mm:ss]` (the default value is two weeks from the date of creation)
3. Enter a password.
4. Click **Go**.
5. Save the P12 file, and supply it to the user.

To create a PKCS#10 certificate

1. In the Menu pane, select **Create Certificates > PKCS#10**.
2. Paste into the space the encrypted base-64 buffer text provided.

   You can also click on **Browse for a file to insert (IE only)** to import the request file.
3. Click **Create** and save the created certificate.
4. Supply the certificate to the requester.

Initializing Multiple Certificates Simultaneously

You can initialize a batch of certificates at the same time.

To initialize several certificates simultaneously

1. Create a file with the list of DNs to initialize.

   Note - There are two ways to create this file - through an LDAP query or a non-LDAP query.

2. In the Menu pain, go to **Create Certificates > Advanced**.
3. Browse to the file you created.
   - To send registration keys to the users, select **Send registration keys via email**
   - To receive a file that lists the initialized DNs with their registration keys, select **Save results to file**

     This file can later be used in a script.
4. Click **Initiate from file**.

Files created through LDAP Queries

The file initiated by the LDAP search has this format:

- Each line after a blank line or the first line in the file represents one DN to be initialized
- If the line starts with "`mail=`", the string continues with the mail of the use

  If no email is given, the email address will be taken from the ICA's "Management Tool Mail To Address" attribute.
- If there is a line with the `not_after` attribute, then the value at the next line is the Certificate Expiration Date.

  The date is given in seconds from now.
- If there is a line with the is `otp_validity` attribute, then the value at the next line is the Registration Key Expiration Date.

  The date is given in seconds from now.

Here is an example of an LDAP Search output:

```
not_after
86400
otp_validity
3600
uid=user_1,ou=People,o=intranet,dc=company,dc=com
mail=user_1@company.com
<blank_line>
...
uid=...
```

For more information, see *"LDAP and User Directory" on page 66*.

Files created through a Simple Non-LDAP Query

It is possible to create a simple (non-LDAP) query by configuring the DN + email in a file using this format:

```
<email address> space <DN>
... blank line as a separator ...
<email address> space <DN>
```

CRL

CRL Management

By default, the CRL is valid for one week. This value can be configured. New CRLs are issued:

- When approximately 60% of the CRL validity period has passed
- Immediately following the revocation of a certificate

It is possible to recreate a specified CRL using the ICA Management Tool. The utility acts as a recovery mechanism in the event that the CRL is deleted or corrupted. An administrator can download a DER encoded version of the CRL using the ICA Management Tool.

CRL Modes

The ICA can issue multiple CRLs. Multiple CRLs prevent one CRL from becoming larger than 10K. If the CRL exceeds 10K, IKE negotiations can fail when trying to open VPN tunnels.

Multiple CRLs are created by attributing each certificate issued to a specified CRL. If revoked, the serial number of the certificate shows in the specified CRL.

The CRL Distribution Point (CRLDP) extension of the certificate contains the URL of the specified CRL. This ensures that the correct CRL is retrieved when the certificate is validated.

CRL Operations

You can download, update, or recreate CRLs through the ICA management tool.

To do operations with CRLs

1. In the Menu pane, select **Manage CRLs**.
2. From the drop-down box, select one or more CRLs.
3. Select an action:
   - Click **Download** to download the CRL.
   - Publish the SmartConsole session to renew the CRL after changes have been made to the CRL database.

     This operation is done at an interval set by the **CRL Duration** attribute.
   - Click **Recreate** to recreate the CRL.

CA Procedures

CA Cleanup

To clean up the CA, you must remove the expired certificates. Before you do that, make sure that the time set on the Security Management Server is correct.

To remove the expired certificates:

In the Menu pane, select **Manage CRLs > Clean the CA's Database and CRLs from expired certificates**.

Configuring the CA

To configure the CA

1. In the Menu pane, select **Configure the CA**.
2. Edit the *"CA Data Types and Attributes" on the next page* as necessary.
3. In the **Operations** pane, select an operation:

- **Apply** - Save and enter the CA configuration settings.

  If the values are valid, the configured settings become immediately effective. All non-valid strings are changed to the default values.

- **Cancel** - Reset all values to the values in the last saved configuration.
- **Restore Default** - Revert the CA to its default configuration settings.

  Entering the string `Default` in one of the attributes will also reset it to the default after you click **Configure**. Values that are valid will be changed as requested, and others will change to default values.

CA Data Types and Attributes

The CA data types are:

- **Time** - displayed in the format: `<number> days <number> seconds`, for example: `CRL Duration: 7 days 0 seconds`

  You can enter the values in the format in which they are displayed (`<number> days <number> seconds`) or as a number of seconds.

- **Integer** - a regular integer, for example: `SIC Key Size: 2048`
- **Boolean** - the values can be true or false (not case sensitive), for example: `Enable renewal: true`
- **String** - an alphanumeric string, for example: `Management Tool DN prefix: cn=tests`

These are the CA attributes, in alphabetical order:

Attribute	Comment	Values	Default
Authorization Code Length	The number of characters of the authorization codes.	min-6 max-12	6
CRL Duration	The period of time for which the CRL is valid.	min-5 minutes max-1 year	1 week
Enable Renewal	For User certificates. This is a Boolean value setting which stipulates whether to enable renewal or not.	true or false	true
Grace Period Before Revocation	The amount of time the old certificate will remain in Renewed (superseded) state.	*min-0* *max-5 years*	1 week
Grace Period Check Period	The amount of time between sequential checks of the *Renewed (superseded)* list in order to revoke those whose duration has passed.	min-10 minutes max-1 week	1 day

Attribute	Comment	Values	Default
IKE Certificate Validity Period	The amount of time an IKE certificate will be valid.	min - 10 minutes max: ■ 3 years starting from R81Jumbo Hotfix Accumulator Take 42 ■ 20 years in lower takes and GA	■ 1 year starting from R81Jumbo Hotfix Accumulator Take 42 ■ 5 years in lower takes and GA
IKE Certificate Extended Key Usage	Certificate purposes for describing the type of the extended key usage for IKE certificates. Refer to RFC 2459.		means no KeyUsage
IKE Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459.		Digital signature and Key encipherment
Management Tool DN prefix	Determines the DN prefix of a DN that will be created when entering a user name.	possible values CN= UID=	CN=
Management Tool DN suffix	Determines the DN suffix of a DN that will be created when entering a user name.		ou=users
Management Tool Hide Mail Button	For security reasons the mail sending button after displaying a single certificate can be hidden.	true or false	false
Management Tool Mail Server	The SMTP server that will be used in order to send registration code mails. It has no default and must be configured in order for the mail sending option to work.		-
Management Tool Registration Key Validity Period	The amount of time a registration code is valid when initiated using the Management Tool.	min-10 minutes max-2 months	2 weeks
Management Tool User Certificate Validity Period	The amount of time that a user certificate is valid when initiated using the Management Tool.	min-one week max-20 years	2 years

Attribute	Comment	Values	Default
Management Tool Mail From Address	When sending mails this is the email address that will appear in the **from** field. A report of the mail delivery status will be sent to this address.		-
Management Tool Mail Subject	The email subject field.		-
Management Tool Mail Text Format	The text that appears in the body of the message. 3 variables can be used in addition to the text: `$REG_KEY` (user's registration key); `$EXPIRE` (expiration time); `$USER` (user's DN).		Registration Key: `$REG_KEY` `Expiration: $EXPIRE`
Management Tool Mail To address	When the **send** mail option is used, the emails to users that have no email address defined will be sent to this address.		-
Max Certificates Per Distribution Point	The maximum capacity of a CRL in the new CRL mode.	min-3 max-400	400
New CRL Mode	A Boolean value describing the CRL mode.	0 for old CRL mode 1 for new mode	true
Number of certificates per search page	The number of certificates that will be displayed in each page of the search window.	min-1 max-approx 700	approx 700
Number of Digits for Serial Number	The number of digits of certificate serial numbers.	min-5 max-10	5
Revoke renewed certificates	This flag determines whether to revoke an old certificate after it has been renewed. The reason for not revoking this is to prevent the CRL from growing each time a certificate is renewed. If the certificate is not revoked the user may have two valid certificates.	true or false	true

Attribute	Comment	Values	Default
SIC Key Size	The key size in bits of keys used in SIC.	possible values: 1024 2048 4096	2048
SIC Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459.		Digital signature and Key encipherment
SIC Certificate Validity Period	The amount of time a SIC certificate will be valid.	min-10 minutes max-20 years	5 years
User Certificate Extended Key Usage	Certificate purposes for describing the type of the extended key usage for User certificates. Refer to RFC 2459.		means no KeyUsage
User Certificate Key Size	The key size in bits of the user's certificates.	Possible values: 1024 2048 4096	2048
User Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459		Digital signature and Key encipherment

Certificate Longevity and Statuses

Certificates issued by the ICA have a defined validity period. When period ends, the certificate *expires*.

SIC certificates, VPN certificates for Security Gateways and User certificates can be created in one step in SmartConsole. User certificates can also be created in two steps using SmartConsole or the ICA Management Tool. The two steps are:

- Initialization - during this step a registration code is created for the user. When this is done, the certificate status is *pending*
- Registration - when the user completes the registration procedure in the remote client. After entering the registration code the certificate becomes *valid.*

The advantages are:

Enhanced security

- The private key is created and stored on the user's machine
- The certificate issued by the ICA is downloaded securely to the client.

Pre-issuance automatic and administrator-initiated certificate removal

If a user does not complete the registration procedure in a given period (two weeks by default), the registration code is automatically removed. An administrator can remove the registration key before the user completes the registration procedure. After that, the administrator can revoke the user certificate.

Explicit or Automatic Renewal of User certificates ensuring continuous User connectivity

A user certificate of type PKCS12 can be renewed explicitly by the user. A PKCS12 certificate can also be set to renew automatically when it is about to expire. This renewal operation ensures that the user can continuously connect to the organization's network. The administrator can choose when to set the automatic revoke old user certificates.

One more advantage is:

Automatic renewal of SIC certificates ensuring continuous SIC connectivity

SIC certificates are renewed automatically after 75% of the validity time of the certificate has passed. If, for example, the SIC certificate is valid for five years. After 3.75 years, a new certificate is created and downloaded automatically to the SIC entity. This automatic renewal ensures that the SIC connectivity of the Security Gateway is continuous. The administrator can revoke the old certificate automatically or after a set period of time. By default, the old certificate is revoked one week after certificate renewal.

Gaia API Proxy

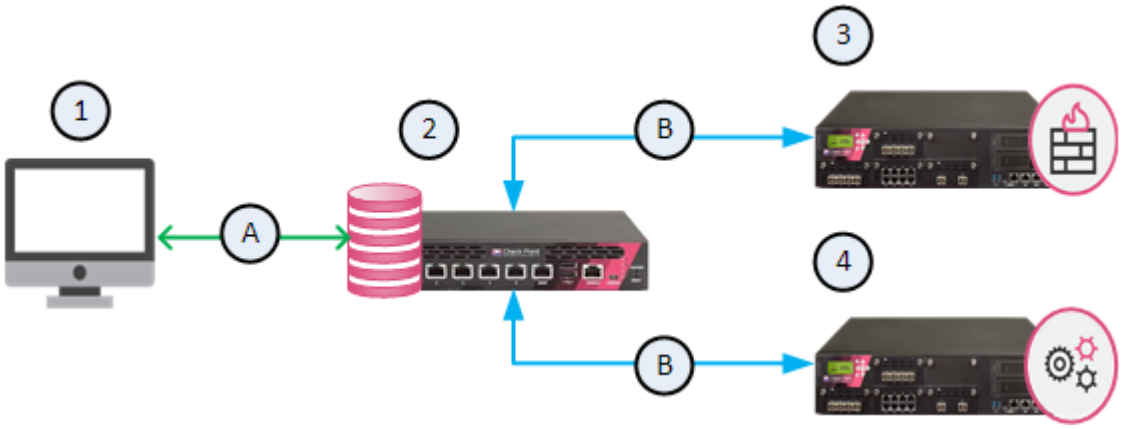
Check Point products support API commands. See the *Check Point API Reference*.

With the Gaia API Proxy feature on a Management Server, you run the Gaia API commands on managed Security Gateways and Cluster Members:

1. An administrator connects with an API Client to a Management Server.
2. From the Management Server, an administrator runs the Gaia API commands on managed Security Gateways and Cluster Members.

The Gaia API Proxy feature on the R81 Management Server works with all managed Security Gateways and Cluster Members that support the Gaia API.

Example diagram



Item	Description
1	An API Client
2	A Management Server with the Gaia API Proxy feature
3	A managed Security Gateway
4	A managed ClusterXL
A	Management API communication
B	Gaia API communication

Workflow:

1. **Run the Management API "`login`" command to log in to the Management Server**

   When you work with an API Client, run the Check Point API "`login`" command to log in to the Management Server (see the *Check Point Management API Reference*).

   Important - The administrator that logs in must have the **Run One Time Script** permission enabled in the assigned permission profile. See *"Assigning Permission Profiles to Administrators" on page 114*.

2. **Run the Gaia API commands on managed Security Gateways and Cluster Members**

   The Management API "`login`" command returns the Session Unique Identifier (SID) token.

   In the same API Client, use this SID token in the "`X-chkp-sid`" field of the Gaia API commands you run on managed Security Gateways and Cluster Members.

   Gaia API Syntax:

   ```
   POST https://<IP Address of Management Server>/web_api/gaia-api/<Gaia API Version>/<Gaia API Command>
   ```

   See the *Check Point Gaia API Reference*.

   The body of the Gaia API command must identify the managed Security Gateway or Cluster Member by one of these parameters:

   - Object name
   - Object primary IP address
   - Object UID

3. **The Gaia API Proxy logs in to the specified Security Gateway or Cluster Member**

   The Gaia API Proxy on the Management Server interprets the Gaia API command and logs in to the specified Security Gateway or Cluster Member.

   a. This login returns the SID for the Security Gateway or Cluster Member.

   b. The Gaia API Proxy uses this SID to run the Gaia API commands.

   c. The Gaia API Proxy saves this SID in its database:

      - The SID timeout is 580 seconds on the Management Server.
      - The SID timeout is 10 minutes on a Security Gateway or Cluster Member.

4. **The Gaia API Proxy forwards the response from the Security Gateway or Cluster Member to the API client**

   - To increase performance, the Gaia API Proxy saves the response in the Gaia API Proxy cache on the Management Server.
   - If the Gaia API Proxy gets the same Gaia API request during the cache timeout, it returns the Gaia API response from its cache and updates the cache.

- An administrator can configure these cache parameters in the `$FWDIR/api/conf/cache.conf` file on the Management Server:

Note - After you change the `$FWDIR/api/conf/cache.conf` file, you must reload the API server configuration with the "`api reconf`" command in the Expert mode.

Parameter	Accepted Values	Description
`timeout`	0, or greater	Specifies the time, after which the next Gaia API command triggers a cache update for that Gaia API command: • `0` - The Gaia API proxy does not use cache • `<integer>` - The Gaia API proxy saves the Gaia API responses in its cache for the specified number of seconds (default: 60 seconds)
`total_ gateways`	integer	Specifies the number of unique Security Gateways and Cluster Members, from which to save the Gaia API responses.
`maximum_ entries`	integer	Specifies the number of unique Gaia API commands to save for each Security Gateway and Cluster Member.

Important - The Gaia API Proxy sends Gaia API command over HTTPS. The Access Control policy for the Security Gateway or ClusterXL must explicitly allow HTTPS traffic from the Management Server to the Security Gateway or Cluster Members.

Examples

Gaia API command "show-hostname"

In this example, we identify the managed Security Gateway by the object primary IP address.

Request

```
POST https://<IP Address of Management Server>/gaia-api/show-hostname
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "192.168.1.1"
}
```

Response

```
{
  "command-name" : "show-hostname",
  "response-message" : {
    "name" : "gw-832546"
  }
}
```

Gaia API command "show-interface"

In this example, we identify the managed Security Gateway by the object name.

Request

```
POST https://<IP Address of Management Server>/gaia-api/v1.4/show-
interfaces
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "gw-832546",
  "name" : "eth0"
}
```

Response

```
{
  "command-name" : "v1.4/show-interfaces",
  "response-message" : {
    "ipv6-local-link-address": "Not Configured",
    "type": "physical",
    "name": "eth0",
    "ipv6-mask-length": "Not-Configured",
    "ipv6-address": "Not-Configured",
    "ipv6-autoconfig": "Not configured",
    "ipv4-address": "192.168.1.1",
    "enabled": true,
    "comments": "",
    "ipv4-mask-length": "24"
  }
}
```

Gaia API command "show-diagnostics"

In this example, we identify the managed Security Gateway by the object UID.

Request

```
POST https://<IP Address of Management Server>/gaia-api/v1.4/show-
diagnostics
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "52048978-c507-8243-9d84-074d11154616",
  "category" : "os",
  "topic" : "disk"
}
```

Response

```
{
  "command-name" : "v1.4/show-diagnostics",
  "response-message" : {
    "to": 3,
    "total": 3,
    "from": 1,
    "objects": [
      {
      "total": "34342961152",
      "partition": "/",
      "used": "5718065152",
      "free": "28624896000"
      },
      {
      "total": "304624640",
      "partition": "/boot",
      "used": "26991616",
      "free": "277633024"
      },
      {
      "total": "34342961152",
      "partition": "/var/log",
      "used": "455684096",
      "free": "33887277056"
      }
    ]
  }
}
```

Command Line Reference

See the *R81 CLI Reference Guide*.

Below is a limited list of applicable commands.

Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description
TAB	Shows the available nested subcommands: `main command` `→ nested subcommand 1` `→ → nested subsubcommand 1-1` `→ → nested subsubcommand 1-2` `→ nested subcommand 2` Example: `cpwd_admin` `config` `-a <options>` `-d <options>` `-p` `-r` `del <options>` Meaning, you can run only **one** of these commands: ■ This command: `cpwd_admin config -a <options>` ■ Or this command: `cpwd_admin config -d <options>` ■ Or this command: `cpwd_admin config -p` ■ Or this command: `cpwd_admin config -r` ■ Or this command: `cpwd_admin del <options>`
Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

contract_util

Description

Works with the Check Point Service Contracts.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d]
    check <options>
    cpmacro <options>
    download <options>
    mgmt
    print <options>
    summary <options>
    update <options>
    verify
```

Parameters

Parameter	Description
`check <options>`	Checks whether the Security Gateway is eligible for an upgrade. See *"contract_util check" on page 374*.
`cpmacro <options>`	Overwrites the current `cp.macro` file with the specified `cp.macro` file. See *"contract_util cpmacro" on page 375*.
`download <options>`	Downloads all associated Check Point Service Contracts from the User Center, or from a local file. See *"contract_util download" on page 376*.
`mgmt`	Delivers the Service Contract information from the Management Server to the managed Security Gateways. See *"contract_util mgmt" on page 378*.
`print <options>`	Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not. See *"contract_util print" on page 379*.
`summary <options>`	Shows post-installation summary. See *"contract_util summary" on page 380*.
`update <options>`	Updates Check Point Service Contracts from your User Center account. See *"contract_util update" on page 381*.
`verify`	Checks whether the Security Gateway is eligible for an upgrade. This command also interprets the return values and shows a meaningful message. See *"contract_util verify" on page 382*.

contract_util check

Description

Checks whether the Security Gateway is eligible for an upgrade.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util check
    {-h | -help}
    hfa
    maj_upgrade
    min_upgrade
    upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`hfa`	Checks whether the Security Gateway is eligible for an upgrade to a higher Hotfix Accumulator.
`maj_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Major version.
`min_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Minor version.
`upgrade`	Checks whether the Security Gateway is eligible for an upgrade.

contract_util cpmacro

Description

Overwrites the current `cp.macro` file with the specified `cp.macro` file, if the specified is newer than the current file.

For more information about the `cp.macro` file, see sk96217: What is a cp.macro file?

Syntax

```
contract_util cpmacro /<path_to>/cp.macro
```

This command shows one of these messages:

Message	Description
`CntrctUtils_Write_cp_macro returned -1`	The `contract_util cpmacro` command failed: ■ Failed to create a temporary file. ■ Failed to write to a temporary file. ■ Failed to replace the current file.
`CntrctUtils_Write_cp_macro returned 0`	The `contract_util cpmacro` command was able to overwrite the current file with the specified file, because the specified file is newer.
`CntrctUtils_Write_cp_macro returned 1`	The `contract_util cpmacro` command did not overwrite the current file, because it is newer than the specified file.

contract_util download

Description

Downloads all associated Check Point Service Contracts from User Center, or from a local file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util download
      {-h | -help}
      local
            {-h | -help}
            [{hfa | maj_upgrade | min_upgrade | upgrade}] <Service Contract
File>
      uc
            {-h | -help}
            [-i] [{hfa | maj_upgrade | min_upgrade | upgrade}] <Username>
<Password> [<Proxy Server> [<Proxy Username>:<Proxy Password>]]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-i`	Interactive mode - prompts the user for the User Center credentials and proxy server settings.
`local`	Specifies to download the Service Contract from the local file. This is equivalent to the "`cplic contract put`" command (see *"cplic contract" on page 433*).
`uc`	Specifies to download the Service Contract from the User Center.
`hfa`	Downloads the information about a Hotfix Accumulator.
`maj_upgrade`	Downloads the information about a Major version.
`min_upgrade`	Downloads the information about a Minor version.
`upgrade`	Downloads the information about an upgrade.
<Username>	Your User Center account e-mail address.
<Password>	Your User Center account password.
<Proxy Server> `[`*<Proxy Username>*`:`*<Proxy Password>*`]`	Specifies that the connection to the User Center goes through the proxy server. ■ *<Proxy Server>* - IP address of resolvable hostname of the proxy server ■ *<Proxy Username>* - Username for the proxy server. ■ *<Proxy Password>* - Password for the proxy server. Note - If you do not specify the proxy server explicitly, the command uses the proxy server configured in the management database.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your User Center account.

contract_util mgmt

Description

Delivers the Service Contract information from the Management Server to the managed Security Gateways.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util mgmt
```

contract_util print

Description

Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not.

This command can show which licenses are not recognized by the Service Contract file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d] print
      {-h | -help}
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Shows a formatted table header and more information.
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util summary

Description

Shows post-installation summary and whether this Check Point computer is eligible for upgrades.

Syntax

```
contract_util summary
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util update

Description

Updates the Check Point Service Contracts from your User Center account.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util update
      [-proxy <Proxy Server>:<Proxy Port>]
      [-ca_path <Path to ca-bundle.crt File>]
```

Parameters

Parameter	Description
`update`	Updates Check Point Service Contracts (attached to pre-installed licenses) from your User Center account.
`-proxy <Proxy Server>:<Proxy Port>`	Specifies that the connection to the User Center goes through the proxy server: ■ `<Proxy Server>` - IP address of resolvable hostname of the proxy server. ■ `<Proxy Port>` - The applicable port on the proxy server. Note - If you do not specify the proxy explicitly, the command uses the proxy configured in the management database.
`-ca_path <Path to ca-bundle.crt File>`	Specifies the path to the Certificate Authority Bundle file (`ca-bundle.crt`).  **Note** - If you do not specify the path explicitly, the command uses the default path.

contract_util verify

Description

Checks whether the Security Gateway is eligible for an upgrade.

This command is the same as the *"contract_util check" on page 374* command, but it also interprets the return values and shows a meaningful message.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util verify
```

cp_conf

Description

Configures or reconfigures a Check Point product installation.

Note - The available options for each Check Point computer depend on the configuration and installed products.

Syntax on a Management Server

```
cp_conf
      -h
      admin <options>
      auto <options>
      ca <options>
      client <options>
      finger <options>
      lic <options>
      snmp <options>
```

Parameters

Parameter	Description
`-h`	Shows the entire built-in usage.
`admin <options>`	Configures Check Point system administrators for the Security Management Server. See *"cp_conf admin" on page 385*.
`auto <options>`	Shows and configures the automatic start of Check Point products during boot. See *"cp_conf auto" on page 388*.
`ca <options>`	■ Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN). ■ Initializes the Internal Certificate Authority (ICA). See *"cp_conf ca" on page 389*.
`client <options>`	Configures the GUI clients that can use SmartConsole to connect to the Security Management Server. See *"cp_conf client" on page 390*.
`finger <options>`	Shows the ICA's Fingerprint. See *"cp_conf finger" on page 393*.
`lic <options>`	Manages Check Point licenses. See *"cp_conf lic" on page 394*.

Parameter	Description
`snmp <options>`	Do **not** use these outdated commands. To configure SNMP, see the *R81 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.

cp_conf admin

Description

Configures Check Point system administrators for the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- Only one administrator can be defined in the *"cpconfig" on page 425* menu.
  To define additional administrators, use SmartConsole.
- This command corresponds to the option **Administrator** in the *"cpconfig" on page 425* menu.

Syntax

```
cp_conf admin
      -h
      add [<UserName> <Password> {a | w | r}]
      add -gaia [{a | w | r}]
      del <UserName1> <UserName2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add [<UserName> <Password> {a | w | r}]`	Adds a Check Point system administrator: ■ `<UserName>` - Specifies the administrator's username ■ `<Password>` - Specifies the administrator's password ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`add -gaia [{a | w | r}]`	Adds the Gaia administrator user `admin`: ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`del <UserName1> <UserName2> ...`	Deletes the specified system administrators.
`get`	Shows the list of the configured system administrators.
`get -gaia`	Shows the management permissions assigned to the Gaia administrator user `admin`.

Example 1 - Adding a Check Point system administrator

```
[Expert@MGMT:0]# cp_conf admin add
Administrator name: admin
Administrator admin already exists.
Do you want to change Administrator's Permissions (y/n) [n] ? y

Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w

Administrator admin was modified successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; )
[Expert@MGMT:0]#
```

Example 2 - Adding the Gaia administrator user

```
[Expert@MGMT:0]# cp_conf admin add -gaia
Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w
Administrator admin was added successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get -gaia

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; ) - Gaia admin
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia a
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products with Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia w
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products without Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia r
Administrator admin already exists.

Administrator admin was modified successfully and has
Read Only Permission for all products
[Expert@MGMT:0]#
```

cp_conf auto

Description

Shows and controls which of Check Point products start automatically during boot.

Note - This command corresponds to the option **Automatic start of Check Point Products** in the *"cpconfig" on page 425* menu.

Syntax

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`{enable | disable} <Product1> <Product2> ...`	Controls whether the installed Check Point products start automatically during boot. This command is for Check Point use only.
`get all`	Shows which of these Check Point products start automatically during boot: ■ Check Point Security Gateway ■ QoS (former FloodGate-1) ■ SmartEvent Suite

Example from a Security Management Server

```
[Expert@MGMT:0]# cp_conf auto get all
Check Point Security Gateway is not installed

QoS is not installed

The SmartEvent Suite will start automatically at boot time.

[Expert@MGMT:0]#
```

cp_conf ca

Description

- Initializes the Internal Certificate Authority (ICA).
- Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN).

Note - On a Security Management Server, this command corresponds to the option **Certificate Authority** in the *"cpconfig" on page 425* menu.

Syntax

```
cp_conf ca
       -h
       fqdn <FQDN Name>
       init
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`fqdn <FQDN Name>`	Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN). `<FQDN Name>` is the text string *hostname.domainname*
`init`	Initializes the Internal Certificate Authority (ICA).

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cp_conf ca fqdn MyMGMT.checkpoint.com
Trying to contact Certificate Authority. It might take a while...
Certificate was created successfully
MyMGMT.checkpoint.com was successfully set to the Internal CA
[Expert@MyMGMT:0]#
```

cp_conf client

Description

Configures the GUI clients that are allowed to connect with SmartConsoles to the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- This command corresponds to the option **GUI Clients** in the *"cpconfig" on page 425* menu.

Syntax

```
cp_conf client
      add <GUI Client>
      createlist <GUI Client 1> <GUI Client 2> ...
      del <GUI Client 1> <GUI Client 2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
<GUI Client>	*<GUI Client>* can be one of these: ■ One IPv4 address (for example, 192.168.10.20), or one IPv6 address (for example, 3731:54:65fe:2::a7) ■ One hostname (for example, MyComputer) ■ `"Any"` - To denote all IPv4 and IPv6 addresses without restriction ■ A range of IPv4 addresses (for example, 192.168.10.0/255.255.255.0), or a range of IPv6 addresses (for example, 2001::1/128) ■ IPv4 address wildcard (for example, 192.168.10.*)
`add` *<GUI Client>*	Adds a GUI client.
`createlist` *<GUI Client 1> <GUI Client 2> ...*	Deletes the current allowed GUI clients and creates a new list of allowed GUI clients.
`del` *<GUI Client 1> <GUI Client 2> ...*	Deletes the specified the GUI clients.
`get`	Shows the allowed GUI clients.

Examples

Example 1 - Configure one IPv4 address

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.15
172.20.168.15 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.15
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.15
172.20.168.15 was deleted successfully
[Expert@MGMT:0]#
```

Example 2 - Configure one hostname

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add MySmartConsoleHost
MySmartConsoleHost was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
MySmartConsoleHost
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del MySmartConsoleHost
MySmartConsoleHost was deleted successfully
[Expert@MGMT:0]#
```

Example 3 - Configure "Any"

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add "Any"
Any was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del "Any"
Any was deleted successfully
[Expert@MGMT:0]#
```

Example 4 - Configure a range of IPv4 addresses

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was deleted successfully
[Expert@MGMT:0]#
```

Example 5 - Configure IPv4 address wildcard

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.*
172.20.168.* was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.*
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.*
172.20.168.* was deleted successfully
[Expert@MGMT:0]#
```

Example 6 - Delete the current list and create a new list of allowed GUI clients

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist 192.168.40.0/255.255.255.0 172.30.40.55
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
192.168.40.0/255.255.255.0
172.30.40.55
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist "Any"
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#
```

cp_conf finger

Description

Shows the Internal Certificate Authority's Fingerprint.

This fingerprint is a text string derived from the ICA certificate on the Security Management Server, Multi-Domain Server, or Domain Management Server.

This fingerprint verifies the identity of the Security Management Server, Multi-Domain Server, or Domain Management Server when you connect to it with SmartConsole.

Note - This command corresponds to the option **Certificate's Fingerprint** in the *"cpconfig" on page 425* menu.

Syntax

```
cp_conf finger
      -h
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`get`	Shows the ICA's Fingerprint.

Example

```
[Expert@MGMT:0]# cp_conf finger get
EDNA COCO MOLE ATOM ASH MOT SAGE NINE ILL TINT HI CUBE
[Expert@MGMT:0]#
```

cp_conf lic

Description

Shows, adds and deletes Check Point licenses.

Note - This command corresponds to the option **Licenses and contracts** in the *"cpconfig" on page 425* menu.

Syntax

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add -f <Full Path to License File>`	Adds a license from the specified Check Point license file. You get this license file in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 435*.
`add -m <Host> <Date> <Signature Key> <SKU/Features>`	Adds the license manually. You get these license details in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 435*.
`del <Signature Key>`	Delete the license based on its signature. This is the same command as the *"cplic del" on page 440*.
`get [-x]`	Shows the local installed licenses. If you specify the "`-x`" parameter, output also shows the signature key for every installed license. This is the same command as the *"cplic print" on page 443*.

Example 1 - Adding the license from the file

```
[Expert@HostName:0]#  cp_conf lic add -f ~/License.lic
License was installed successfully.
[Expert@HostName:0]#

[Expert@HostName:0]# cp_conf lic get
Host             Expiration   Signature                                 Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx      CPMP-XXX
[Expert@HostName:0]#
```

Example 2 - Adding the license manually

```
[Expert@MyHostName:0]# cp_conf lic add -m MyHostName 25Aug2019 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX
License was successfully installed
[Expert@MyHostName:0]#

[Expert@MyHostName:0]# cp_conf lic get
Host             Expiration   Signature                                 Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx      CPMP-XXX
[Expert@MyHostName:0]#
```

cp_log_export

Description

Exports Check Point logs over syslog.

For more information, see sk122323 and *R81 Logging and Monitoring Administration Guide*.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cp_log_export
```

```
cp_log_export <command-name> help
```

Parameters

Parameter	Description
No Parameters	Shows the built-in general help.
`<command-name> help`	Shows the built help for the specified internal command.

Internal Commands

Name	Description
`add`	Deploy a new Check Point Log Exporter.
`delete`	Remove an existing Log Exporter.
`reexport`	Reset the current position and export all logs again based on the configuration.
`restart`	Restart a Log Exporter process.
`set`	Update an existing Log Exporter configuration.
`show`	Print the current Log Exporter configuration.
`start`	Start an existing Log Exporter process.
`status`	Show a Log Exporter overview status.
`stop`	Stop an existing Log Exporter process.

Internal Command Arguments

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "show", "status", "start", "stop", "restart" command	Required for "reexport" command
`--apply-now`	Applying any change that was done immediately.	Optional	Optional	**Mandatory**	N/A	**Mandatory**
`ca-cert`	Full path to the CA certificate file `*.pem`. Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N/A	N/A	N/A
`client-cert`	Full path to the client certificate `*.p12`. Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N/A	N/A	N/A
`client-secret`	The challenge phrase used to create the client certificate `*.p12`. Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N/A	N/A	N/A
`domain-server`	The name or IP address of the applicable Domain Management Server or Domain Log Server.	**Mandatory**	**Mandatory**	**Mandatory**	Optional. By default, applies to all.	**Mandatory**
`enabled`		Optional	Optional	N/A	N/A	N/A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "show", "status", "start", "stop", "restart" command	Required for "reexport" command
`encrypted`	Use TSL (SSL) encryption to send the logs.	Optional	Optional	N/A	N/A	N/A
`export-attachment-ids`	Add a field to the exported log that represents the ID of log's attachment (if exists).	Optional	Optional	N/A	N/A	N/A
`export-attachment-link`	Add a field to the exported log that represents a link to SmartView that shows the log card and automatically opens the attachment.	Optional	Optional	N/A	N/A	N/A
`export-link`	Add a field to the exported log that represents a link to SmartView that shows the log card.	Optional	Optional	N/A	N/A	N/A
`export-link-ip`	Make the links to SmartView use a custom IP address (for example, for a Log Server behind NAT).	Optional	Optional	N/A	N/A	N/A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "show", "status", "start", "stop", "restart" command	Required for "reexport" command
`filter-action-in`	Export all logs with a specific action. The value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma.  **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.	Optional	Optional	N/A	N/A	N/A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "show", "status", "start", "stop", "restart" command	Required for "reexport" command
`filter-blade-in`	Export all logs that belong to a specific Software Blade. The value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma. Predefined blade families can be selected (**Access**, **TP**, **Endpoint**, **Mobile**). **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.	Optional	Optional	N/A	N/A	N/A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "show", "status", "start", "stop", "restart" command	Required for "reexport" command
`filter-origin-in`	Export all logs from a specific origin. The value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma.  **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.	Optional	Optional	N/A	N/A	N/A
`format`	The format, in which the logs are exported.	Optional	Optional	N/A	N/A	N/A
`name`	Unique name of the exporter configuration.	**Mandatory**	**Mandatory**	**Mandatory**	Optional. By default, applies to all.	**Mandatory**
`protocol`	Layer 4 Transport protocol to use (TCP or UDP).	**Mandatory**	Optional	N/A	N/A	N/A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "show", "status", "start", "stop", "restart" command	Required for "reexport" command
`read-mode`	Configure the mode, in which the log files are read and exported.	Optional	Optional	N/A	N/A	N/A
`reconnect-interval`	Schedule a reconnection to the target server after the connection is lost.	Optional	Optional	N/A	N/A	N/A
`target-port`	The listening port on the target server, to which you export the logs.	**Mandatory**	Optional	N/A	N/A	N/A
`target-server`	The IP address or FQDN of the target server, to which you export the logs.	**Mandatory**	Optional	N/A	N/A	N/A

cpca_client

Description

Execute operations on the Internal Certificate Authority (ICA).

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d]
      create_cert <options>
      double_sign <options>
      get_crldp <options>
      get_pubkey <options>
      init_certs <options>
      lscert <options>
      revoke_cert <options>
      revoke_non_exist_cert <options>
      search <options>
      set_mgmt_tool <options>
      set_sign_hash <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`create_cert <options>`	Issues a SIC certificate for the Security Management Server or Domain Management Server. See *"cpca_client create_cert" on page 405*.
`double_sign <options>`	Creates a second signature for a certificate. See *"cpca_client double_sign" on page 406*.
`get_crldp <options>`	Shows how to access a CRL file from a CRL Distribution Point. See *"cpca_client get_crldp" on page 408*.
`get_pubkey <options>`	Saves the encoding of the public key of the ICA's certificate to a file. See *"cpca_client get_pubkey" on page 409*.

Parameter	Description
`init_certs <options>`	Imports a list of DNs for users and creates a file with registration keys for each user. See *"cpca_client init_certs" on page 410*.
`lscert <options>`	Shows all certificates issued by the ICA. See *"cpca_client lscert" on page 411*.
`revoke_cert <options>`	Revokes a certificate issued by the ICA. See *"cpca_client revoke_cert" on page 413*.
`revoke_non_exist_cert <options>`	Revokes a non-existent certificate issued by the ICA. See *"cpca_client revoke_non_exist_cert" on page 416*.
`search <options>`	Searches for certificates in the ICA. See *"cpca_client search" on page 417*.
`set_mgmt_tool <options>`	Controls the ICA Management Tool. See *"cpca_client set_mgmt_tool" on page 419*.
`set_sign_hash <options>`	Sets the hash algorithm that the CA uses to sign the file hash. See *"cpca_client set_sign_hash" on page 422*.

cpca_client create_cert

Description

Issues a SIC certificate for the Security Management Server or Domain Management Server.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] create_cert [-p <CA port number>] -n "CN=<Common Name>" -f
<Full Path to PKCS12 file> [-w <Password>] [-k {SIC | USER | IKE | ADMIN_
PKG}] [-c "<Comment for Certificate>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-n "CN=<Common Name>"`	Sets the CN to the specified `<Common Name>`.
`-f <Full Path to PKCS12 file>`	Specifies the PKCS12 file, which stores the certificate and keys.
`-w <Password>`	Optional. Specifies the certificate password.
`-k {SIC | USER | IKE | ADMIN_PKG}`	Optional. Specifies the certificate kind.
`-c "<Comment for Certificate>"`	Optional. Specifies the certificate comment (must enclose in double quotes).

Example

```
[Expert@MGMT:0]# cpca_client create_cert -n "cn=cp_mgmt" -f $CPDIR/conf/sic_cert.p12
```

cpca_client double_sign

Description

Creates a second signature for a certificate.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] double_sign [-p <CA port number>] -i <Certificate File in
PEM format> [-o <Full Path to Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-i <Certificate File in PEM format>`	Imports the specified certificate (only in PEM format).
`-o <Full Path to Output File>`	Optional. Saves the certificate into the specified file.

Example

```
[Expert@MGMT:0]# cpca_client double_sign -i certificate.pem

 Requesting Double Signature for the following Certificate:
        refCount: 1
        Subject: Email=example@example.com,CN=http://www.example.com/,OU=ValiCert Class 2 Policy Validation
Authority,O=exampleO\, Inc.,L=ExampleL Validation Network

 Double Sign of Cert:
 ======================
 (
        : (
                :dn ("Email=example@example.com,CN=http://www.example.com/,OU=exampleOU Class 2 Policy
Validation Authority,O=exampleO\, Inc.,L=exampleL Validation Network")
                :doubleSignCert (52016390... ... ...ebb67e96)
                :return_code (0)
        )
)

[Expert@MGMT:0]#
```

cpca_client get_crldp

Description

Shows how to access a CRL file from a CRL Distribution Point.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_crldp [-p <CA port number>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

Example

```
[Expert@MGMT:0]# cpca_client get_crldp
192.168.3.51
[Expert@MGMT:0]
```

cpca_client get_pubkey

Description

Saves the encoding of the public key of the ICA's certificate to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_pubkey [-p <CA port number>] <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`<Full Path to Output File>`	Saves the encoding of the public key of the ICA's certificate to the specified file.

Example

```
[Expert@MGMT:0]# cpca_client get_pubkey /tmp/key.txt[Expert@MGMT:0]#
[Expert@MGMT:0]# cat /tmp/key.txt
3082010a... ... ...f98b8910
[Expert@MGMT:0]#
```

cpca_client init_certs

Description

Imports a list of Distinguished Names (DN) for users and creates a file with registration keys for each user.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] init_certs [-p <CA port number>] -i <Full Path to Input File> -o <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-i <Full Path to Input File>`	Imports the specified file. Make sure to use the full path. Make sure that there is an empty line between each DN in the specified file. Example: `...CN=test1,OU=users...` `<Empty Line>` `...CN=test2,OU=users...`
`-o <Full Path to Output File>`	Saves the registration keys to the specified file. This command saves the error messages in the `<Name of Output File>.failures` file in the same directory.

cpca_client lscert

Description

Shows all certificates issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] lscert [-dn <SubString>] [-stat {Pending | Valid | Revoked | Expired | Renewed}] [-kind {SIC | IKE | User | LDAP}] [-ser <Certificate Serial Number>] [-dp <Certificate Distribution Point>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <SubString>`	Optional. Filters the search results to those with a DN that matches the specified `<SubString>`. This command does not support multiple values.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Filters the search results to those with certificate status that matches the specified status. This command does not support multiple values.
`-kind {SIC | IKE | User | LDAP}`	Optional. Filters the search results to those with certificate kind that matches the specified kind. This command does not support multiple values.
`-ser <Certificate Serial Number>`	Optional. Filters the search results to those with certificate serial number that matches the specified serial number. This command does not support multiple values.
`-dp <Certificate Distribution Point>`	Optional. Filters the search results to the specified Certificate Distribution Point (CDP). This command does not support multiple values.

Example

```
[Expert@MGMT:0]# cpca_client lscert -stat Revoked
Operation succeeded. rc=0.
5 certs found.

Subject = CN=VSX2,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 5521   DP = 0
Not_Before: Sun Apr  8 14:10:01 2018   Not_After: Sat Apr  8 14:10:01 2023

Subject = CN=VSX1,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 9113   DP = 0
Not_Before: Sun Apr  8 14:09:02 2018   Not_After: Sat Apr  8 14:09:02 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#


[Expert@MGMT:0]# cpca_client lscert -kind IKE
Operation succeeded. rc=0.
3 certs found.

Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 27214   DP = 1
Not_Before: Wed Apr 11 17:26:02 2018   Not_After: Tue Apr 11 17:26:02 2023

Subject = CN=VSX_Cluster VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 64655   DP = 1
Not_Before: Mon Apr  9 19:36:31 2018   Not_After: Sun Apr  9 19:36:31 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#
```

cpca_client revoke_cert

Description

Revokes a certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_cert [-p <CA port number>] -n "CN=<Common Name>" -s
<Certificate Serial Number>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-n "CN=<Common Name>"`	Specifies the certificate CN. To get the CN, run the *"cpca_client lscert" on page 411* command and examine the text that you see between the "`Subject =`" and the "`,O=...`". **Example** From this output: `Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x` `Status = Valid Kind = IKE Serial = 27214 DP = 1` `Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023` you get this syntax: `-n "CN=VS1 VPN Certificate` **Note** - You can use the parameter '`-n`' only, or together with the parameter "`-s`".
`-s <Certificate Serial Number>`	Specifies the certificate serial number. To see the serial number, run the *"cpca_client lscert" on page 411* command. **Note** - You can use the parameter "`-s`" only, or together with the parameter "`-n`".

Example 1 - Revoking a certificate specified by its CN

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -n "CN=VS1 VPN Certificate"
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

Example 2 - Revoking a certificate specified by its serial number.

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -s 27214
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

cpca_client revoke_non_exist_cert

Description

Revokes a non-existent certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_non_exist_cert -i <Full Path to Input File>
```

Parameters

Parameter	Description
`-d`	Runs the `cpca_client` command under debug.
`-i <Full Path to Input File>`	Specifies the file that contains the list of the certificate to revoke. You must create this file in the same format as the *"cpca_client lscert" on page 411* command prints its output. **Example** `Subject = CN=cp_mgmt,O=MGMT.5p72vp` `Status = Valid  Kind = SIC  Serial = 30287  DP = 0` `Not_Before: Sat Apr  7 19:40:12 2018  Not_After: Fri Apr  7 19:40:12 2023` `<Empty Line>` `Subject = CN=cp_mgmt,O=MGMT.5p72vp` `Status = Valid  Kind = SIC  Serial = 60870  DP = 0` `Not_Before: Sat Apr  7 19:40:13 2018  Not_After: Fri Apr  7 19:40:13 2023`

Note - This command saves the error messages in the `<Name of Input File>.failures` file.

cpca_client search

Description

Searches for certificates in the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] search <String> [-where {dn | comment | serial | device_
type | device_id | device_name}] [-kind {SIC | IKE | User | LDAP}] [-stat
{Pending | Valid | Revoked | Expired | Renewed}] [-max <Maximal Number of
Results>] [-showfp {y | n}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<String>	Specifies the text to search in the certificates. You can enter only one text string that does not contain spaces.
`-where {dn | comment | serial | device_ type | device_id | device_name}`	Optional. Specifies the certificate's field, in which to search for the string: ■ `dn` - Certificate DN ■ `comment` - Certificate comment ■ `serial` - Certificate serial number ■ `device_type` - Device type ■ `device_id` - Device ID ■ `device_name` - Device Name The default is to search in all fields.

Parameter	Description
`-kind {SIC | IKE | User | LDAP}`	Optional. Specifies the certificate kind to search. You can enter multiple values in this format: `-kind <Kind1> <Kind2> <Kind3>` The default is to search for all kinds.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Specifies the certificate status to search. You can enter multiple values in this format: `-stat <Status1> <Status2> <Status3>` The default is to search for all statuses.
`-max <Maximal Number of Results>`	Optional. Specifies the maximal number of results to show. ■ Range: 1 and greater ■ Default: 200
`-showfp {y | n}`	Optional. Specifies whether to show the certificate's fingerprint and thumbprint: ■ `y` - Shows the fingerprint and thumbprint (this is the default) ■ `n` - Does not show the fingerprint and thumbprint

Example 1

```
[Expert@MGMT:0]# cpca_client search samplecompany -where comment -kind SIC LDAP -stat Pending Valid Renewed
```

Example 2

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dnOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
Fingerprint = XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX
Thumbprint = xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
[Expert@MGMT:0]#
```

Example 3

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dn -showfp nOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
[Expert@MGMT:0]#
```

cpca_client set_mgmt_tool

Description

Controls the ICA Management Tool.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

See:

- sk30501: Setting up the ICA Management Tool
- sk39915: Invoking the ICA Management Tool
- sk102837: Best Practices - ICA Management Tool configuration

Syntax

```
cpca_client [-d] set_mgmt_tool {on | off | add | remove | clean | print} [-p <CA port number>] {[-a <Administrator DN>] | [-u <User DN>] | [-c <Custom User DN>]}
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`on`	Starts the ICA Management Tool.
`off`	Stops the ICA Management Tool.
`add`	Adds the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`remove`	Removes the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`clean`	Removes all administrators, users, or custom users that are permitted to use the ICA Management Tool.
`print`	Shows the configured administrators, users, or custom users that are permitted to use the ICA Management Tool.

Parameter	Description
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18265.
`-a <Administrator DN>`	Optional. Specifies the DN of the administrator that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-a "CN=ICA_Tool_Admin,OU=users,O=MGMT.s6t98x"`
`-u <User DN>`	Optional. Specifies the DN of the user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole: **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-u "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Parameter	Description
`-c <Custom User DN>`	Optional. Specifies the DN for the custom user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole. **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-c "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Note - If you run the "`cpca_client set_mgmt_tool`" command without the parameter "`-a`" or "`-u`", the list of the permitted administrators and users is not changed. The previously defined permitted administrators and users can start and stop the ICA Management Tool.

cpca_client set_sign_hash

Description

Sets the hash algorithm that the CA uses to sign the file hash. Also, see sk103840.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] set_sign_hash {sha1 | sha256 | sha384 | sha512}
```

Important - After this change, you must restart the Check Point services with these commands:

- On Security Management Server, run:
  1. `cpstop`
  2. `cpstart`
- On a Multi-Domain Server, run:
  1. `mdsstop_customer <Name or IP Address of Domain Management Server>`
  2. `mdsstart_customer <Name or IP Address of Domain Management Server>`

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{sha1 | sha256 | sha384 | sha512}`	The hash algorithms that the CA uses to sign the file hash. The default algorithm is SHA-256.

Example

```
[Expert@MGMT:0]# cpca_client set_sign_hash sha256

You have selected the signature hash function SHA-256
WARNING: This hash algorithm is not supported in Check Point gateways prior to R71.
WARNING: It is also not supported on older clients and SG80 R71.

Are you sure? (y/n)
y
Internal CA signature hash changed successfully.
Note that the signature on the Internal CA certificate has not changed, but this has no security
implications.
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpstop ; cpstart
```

cpca_create

Description

Creates new Check Point Internal Certificate Authority database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_create [-d] -dn <CA DN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <CA DN>`	Specifies the Certificate Authority Distinguished Name (DN).

cpconfig

Description

This command starts the Check Point Configuration Tool.

This utility configures specific settings for the installed Check Point products.

Syntax

```
cpconfig
```

Note - On a Multi-Domain Server, run the "`mdsconfig`" command.

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this server.
Administrator	Configures Check Point system administrators for this server.
GUI Clients	Configures the GUI clients that can use SmartConsole to connect to this server.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R81 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.
Certificate Authority	Initializes the Internal Certificate Authority (ICA) and configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN).
Certificate's Fingerprint	Shows the ICA's Fingerprint. This fingerprint is a text string derived from the server's ICA certificate. This fingerprint verifies the identity of the server when you connect to it with SmartConsole.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

Example - Menu on a Security Management Server

```
[Expert@MyMGMT:0]# cpconfig
This program will let you re-configure
your Check Point Security Management Server configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) Administrator
(3) GUI Clients
(4) SNMP Extension
(5) Random Pool
(6) Certificate Authority
(7) Certificate's Fingerprint
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

cpinfo

Description

A utility that collects diagnostics data on your Check Point computer at the time of execution.

It is mandatory to collect these data when you contact *Check Point Support* about an issue on your Check Point computer.

For more information, see sk92739.

cplic

Description

The `cplic` command manages Check Point licenses.

You can run this command in Gaia Clish or in the Expert mode.

License Management is divided into three types of commands:

Licensing Commands	Applies To	Description
Local licensing commands	Management Servers, Security Gateways and Cluster Members	You execute these commands locally on the Check Point computers.
Remote licensing commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the managed Security Gateways and Cluster Members.
License Repository commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the licenses stored in the local license repository.

Syntax for Local Licensing on a Management Server itself

```
cplic [-d]
      {-h | -help}
      check <options>
      contract <options>
      del <options>
      print <options>
      put <options>
```

Syntax for Remote Licensing on managed Security Gateways and Cluster Members

```
cplic [-d]
      {-h | -help}
      del <options>
      get <options>
      put <options>
      upgrade <options>
```

Syntax for License Database Operations on a Management Server

```
cplic [-d]
      {-h | -help}
      db_add <options>
      db_print <options>
      db_rm <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the applicable built-in usage.
`check <options>`	Confirms that the license includes the feature on the local Security Gateway or Management Server. See *"cplic check" on page 431*.
`contract <options>`	Manages (deletes and installs) the Check Point Service Contract on the local Check Point computer. See *"cplic contract" on page 433*.
`db_add <options>`	Applies only to a Management Server. Adds licenses to the license repository on the Management Server. See *"cplic db_add" on page 435*.
`db_print <options>`	Applies only to a Management Server. Shows the details of Check Point licenses stored in the license repository on the Management Server. See *"cplic db_print" on page 437*.
`db_rm <options>`	Applies only to a Management Server. Removes a license from the license repository on the Management Server. See *"cplic db_rm" on page 439*.
`del <options>`	Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses. See *"cplic del" on page 440*.
`del <Object Name> <options>`	Detaches a Central license from a remote managed Security Gateway or Cluster Member. See *"cplic del <object name>" on page 441*.

Parameter	Description
`get <options>`	Applies only to a Management Server. Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server. See *"cplic get" on page 442*.
`print <options>`	Prints details of the installed Check Point licenses on the local Check Point computer. See *"cplic print" on page 443*.
`put <options>`	Installs and attaches licenses on a Check Point computer. See *"cplic put" on page 445*.
`put <Object Name> <options>`	Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members. See *"cplic put <object name>" on page 447*.
`upgrade <options>`	Applies only to a Management Server. Upgrades licenses in the license repository with licenses in the specified license file. See *"cplic upgrade" on page 450*.

cplic check

Description

Confirms that the license includes the feature on the local Security Gateway or Management Server. See sk66245.

Syntax

```
cplic check {-h | -help}
```

```
cplic [-d] check [-p <Product>] [-v <Version>] [{-c | -count}] [-t <Date>]
[{-r | -routers}] [{-S | -SRusers}] <Feature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <Product>`	Product, for which license information is requested. Some examples of products: ■ `fw1` - FireWall-1 infrastructure on Security Gateway / Cluster Member (all blades), or Management Server (all blades) ■ `mgmt` - Multi-Domain Server infrastructure ■ `services` - Entitlement for various services ■ `cvpn` - Mobile Access ■ `etm` - QoS (FloodGate-1) ■ `eps` - Endpoint Software Blades on Management Server
`-v <Version>`	Product version, for which license information is requested.
`{-c | -count}`	Outputs the number of licenses connected to this feature.
`-t <Date>`	Checks license status on future date. Use the format **ddmmyyyy**. A feature can be valid on a given date on one license, but invalid on another.
`{-r | -routers}`	Checks how many routers are allowed. The `<Feature>` option is not needed.

Parameter	Description
`{-S | -SRusers}`	Checks how many SecuRemote users are allowed.
<Feature>	Feature, for which license information is requested.

Example from a Management Server

```
[Expert@MGMT]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 24Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:comp fw1:6.0:compunlimited fw1:6.0:cluster-1 fw1:6.0:cpxmgmt_qos_u_sites fw1:6.0:sprounl
fw1:6.0:nxunlimit fw1:6.0:swp evnt:6.0:smrt_evnt fw1:6.0:fwc fw1:6.0:ca fw1:6.0:rtmui fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:cmd evnt:6.0:alzd5 evnt:6.0:alzc1
evnt:6.0:alzs1 fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:sme10 etm:6.0:rtm_u fw1:6.0:cep1 fw1:6.0:rt fw1:6.0:cemid fw1:6.0:web_sec_u fw1:6.0:workflow fw1:6.0:raml
fw1:6.0:routers fw1:6.0:supmgmt fw1:6.0:supunlimit fw1:6.0:prov fw1:6.0:atlas-unlimit fw1:6.0:filter fw1:6.0:ui psmp:6.0:psmsunlimited fw1:6.0:vpe_unlimit
fw1:6.0:cluster-u fw1:6.0:remote1 fw1:6.0:aes fw1:6.0:strong fw1:6.0:rdp fw1:6.0:des fw1:6.0:isakmp fw1:6.0:dbvr_unlimit fw1:6.0:cmpmgmt fw1:6.0:rtmmgmt
fw1:6.0:fgmgmt fw1:6.0:blades fw1:6.0:cpipv6 fw1:6.0:mgmtha fw1:6.0:remote
[Expert@MGMT]#
```

Example from a Management Server in High Availability

```
[Expert@MGMT]# cplic check -p fw1 -v 6.0 -c mgmtha
cplic check 'mgmtha': 1 licenses
[Expert@MGMT]#
```

cplic contract

Description

Deletes the Check Point Service Contract on the local Check Point computer.

Installs the Check Point Service Contract on the local Check Point computer.

Note

- For more information about Service Contract files, see sk33089: What is a Service Contract File?
- If you install a Service Contract on a managed Security Gateway / Cluster Member, you must update the license repository on the applicable Management Server - either with the *"cplic get" on page 442* command, or in SmartUpdate.

Syntax

```
cplic contract -h
```

```
cplic [-d] contract
      del
            -h
            <Service Contract ID>
      put
            -h
            [{-o | -overwrite}] <Service Contract File>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`del`	Deletes the Service Contract from the `$CPDIR/conf/cp.contract` file on the local Check Point computer.
`put`	Merges the Service Contract to the `$CPDIR/conf/cp.contract` file on the local Check Point computer.
<Service Contract ID>	ID of the Service Contract.
`{-o | -overwrite}`	Specifies to overwrite the current Service Contract.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your *Check Point User Center* account.

cplic db_add

Description

Adds licenses to the license repository on the Management Server.

When you add Local licenses to the license repository, Management Server automatically attaches them to the managed Security Gateway / Cluster Member with the matching IP address.

When you add Central licenses, you must manually attach them.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic db_add {-h | -help}
```

```
cplic [-d] db_add -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Features>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l <License File>`	Name of the file that contains the license.
<Host>	Hostname or IP address of the Security Management Server / Domain Management Server.
<Expiration Date>	The license expiration date.
<Signature>	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` Case sensitive. Hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example, `CPSUITE-EVAL-3DES-vNG`

Example

If the file `192.0.2.11.lic` contains one or more licenses, the command "`cplic db_add -l 192.0.2.11.lic`" produces output similar to:

```
[Expert@MGMT]# cplic db_add -l 192.0.2.11.lic
Adding license to database ...
Operation Done
[Expert@MGMT]#
```

cplic db_print

Description

Shows the details of Check Point licenses stored in the license repository on the Management Server.

Syntax

```
cplic db_print {-h | -help}
```

```
cplic [-d] db_print {<Object Name> | -all} [{-n | -noheader}] [-x] [{-t | -type}] [{-a | -attached}]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	Prints only the licenses attached to *<Object Name>*. *<Object Name>* is the name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-all`	Prints all the licenses in the license repository.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signatures.
`{-t | -type}`	Prints licenses with their type: Central or Local.
`{-a | -attached}`	Shows to which object the license is attached. Useful, if the parameter "`-all`" is specified.

Example

```
[Expert@MGMT:0]# cplic db_print -all
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX
[Expert@MGMT:0]#

[Expert@MGMT:0]# cplic db_print -all -x -a
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX  MGMT
[Expert@MGMT:0]#
```

cplic db_rm

Description

Removes a license from the license repository on the Management Server.

After you remove the license from the repository, it can no longer use it.

Warning - You can run this command ONLY after you detach the license with the *"cplic del" on page 440* command.

Syntax

```
cplic db_rm {-h | -help}
cplic [-d] db_rm <Signature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Signature>	The signature string within the license. To see the license signature string, run the *"cplic print" on page 443* command.

Example

```
[Expert@MGMT:0]# cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

cplic del

Description

Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses.

This command can delete a license on both local computer, and on remote managed computers.

Syntax

```
cplic del {-h | -help}
cplic [-d] del [-F <Output File>] <Signature> <Object Name>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-F <Output File>`	Saves the command output to the specified file.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 443* command.
`<Object Name>`	The name of the Security Gateway / Cluster Member object as defined in SmartConsole.

cplic del <object name>

Description

Detaches a Central license from a remote managed Security Gateway or Cluster Member.

When you run this command, it automatically updates the license repository.

The Central license remains in the license repository as an unattached license.

Syntax

```
cplic del {-h | -help}
```

```
cplic [-d] del <Object Name> [-F <Output File>] [-ip <Dynamic IP Address>] <Signature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	The name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-F` *<Output File>*	Saves the command output to the specified file.
`-ip` *<Dynamic IP Address>*	Deletes the license on the DAIP Security Gateway with the specified IP address. **Note** - If this parameter is used, then object name must be a DAIP Security Gateway.
<Signature>	The signature string within the license. To see the license signature string, run the *"cplic print" on page 443* command.

cplic get

Description

Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server.

This command helps synchronize the license repository with the managed Security Gateways and Cluster Members.

When you run this command, it updates the license repository with all local changes.

Syntax

```
cplic get {-h | -help}
```

```
cplic [-d] get
      -all
      <IP Address>
      <Host Name>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-all`	Retrieves licenses from all Security Gateways and Cluster Members in the managed network.
<IP Address>	The IP address of the Security Gateway / Cluster Member, from which licenses are to be retrieved.
<Host Name>	The name of the Security Gateway / Cluster Member object as defined in SmartConsole, from which licenses are to be retrieved.

Example

If the Security Gateway with the object name `MyGW` contains four Local licenses, and the license repository contains two other Local licenses, the command "`cplic get MyGW`" produces output similar to this:

```
[Expert@MGMT:0]# cplic get MyGW
Get retrieved 4 licenses.
Get removed 2 licenses.
[Expert@MGMT:0]#
```

cplic print

Description

Prints details of the installed Check Point licenses on the local Check Point computer.

Note - On a Security Gateway / Cluster Member, this command prints all installed licenses (both Local and Central).

Syntax

```
cplic print {-h | -help}
```

```
cplic [-d] print[{-n | -noheader}] [-x] [{-t | -type}] [-F <Output File>]
[{-p | -preatures}] [-D]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signature.
`{-t | -type]`	Prints licenses showing their type: Central or Local.
`-F <Output File>`	Saves the command output to the specified file.
`{-p | -preatures}`	Prints licenses resolved to primitive features.
`-D`	On a Multi-Domain Server, prints only Domain licenses.

Example 1

```
[Expert@HostName:0]# cplic print
Host             Expiration    Features
192.168.3.28     25Aug2019     CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

Example 2

```
[Expert@HostName:0]# cplic print -x
Host             Expiration   Signature                          Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

cplic put

Description

Installs one or more Local licenses on a Check Point computer.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put [{-o | -overwrite}] [{-c | -check-only}] [{-s | -select}] [-F <Output File>] [{-P | -Pre-boot}] [{-k | -kernel-only}] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Features>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-o | -overwrite}`	On a Security Gateway / Cluster Member, this command erases only the local licenses, but not central licenses that are installed remotely.
`{-c | -check-only}`	Verifies the license. Checks if the IP of the license matches the Check Point computer and if the signature is valid.
`{-s | -select}`	Selects only the local license whose IP address matches the IP address of the Check Point computer.
`-F <Output File>`	Saves the command output to the specified file.
`{-P | -Pre-boot}`	Use this option after you have upgraded and before you reboot the Check Point computer. Use of this option will prevent certain error messages.
`{-K | -kernel-only}`	Pushes the current valid licenses to the kernel. For use by Check Point Support only.
`-l <License File>`	Name of the file that contains the license.

Parameter	Description
<Host>	Hostname or IP address of the Security Gateway / Cluster Member for a local license. Hostname or IP address of the Security Management Server / Domain Management Server for a central license.
<Expiration Date>	The license expiration date.
<Signature>	The signature string within the license. Case sensitive. The hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IP address of the external interface (in quad-dot notation). The last part cannot be 0 or 255.
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

Example

```
[Expert@HostName:0]# cplic put -l License.lic
Host Expiration SKU
192.168.2.3 14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
[Expert@HostName:0]#
```

cplic put <object name>

Description

Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members.

When you run this command, it automatically updates the license repository.

Note

- You get the license details in the *Check Point User Center*.
- You can attach more than one license.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put <Object Name> [-ip<Dynamic IP Address> ] [-F <Output File>]
-l <License File> [<Host>] [<Expiration Date>] [<Signature>]
[<SKU/Feature>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	The name of the Security Gateway / Cluster Member object, as defined in SmartConsole.
`-ip` *<Dynamic IP Address>*	Installs the license on the Security Gateway with the specified IP address. This parameter is used to install a license on a Security Gateway with dynamically assigned IP address (DAIP).  **Note** - If you use this parameter, then the object name must be that of a DAIP Security Gateway.
`-F` *<Output File>*	Saves the command output to the specified file.
`-l` *<License File>*	Installs the licenses from the *<License file>*.
<Host>	Hostname or IP address of the Security Management Server / Domain Management Server.
<Expiration Date>	The license expiration date.
<Signature>	The license signature string. Case sensitive. The hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IP address of the external interface (in quad-dot notation). The last part cannot be 0 or 255.
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

cplic upgrade

Description

Upgrades licenses in the license repository with licenses in the specified license file.

Note - You get this license file in the *Check Point User Center*.

Syntax

```
cplic upgrade {-h | -help}
```

```
cplic [-d] upgrade -l <Input File>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-l <Input File>`	Upgrades the licenses in the license repository and Check Point Security Gateways / Cluster Members to match the licenses in the specified file.

Example

This example explains the procedure to upgrade the licenses in the license repository.

There are two Software Blade licenses in the input file:

- One license does not match any license on a remote managed Security Gateway.
- The other license matches an NGX-version license on a managed Security Gateway that has to be upgraded.

Workflow in this example:

1. Upgrade the Security Management Server to the latest version.

   Ensure that there is connectivity between the Security Management Server and the Security Gateways with the previous product versions.

2. Import all licenses into the license repository.

   You can also do this after you upgrade the products on the remote Security Gateways.

3. Run this command:

   ```
   cplic get -all
   ```

Example:

```
[Expert@MyMGMT]# cplic get -all
Getting licenses from all modules ...
MyGW:
Retrieved 1 licenses
```

4. To see all the licenses in the repository, run this command:

   ```
   cplic db_print -all -a
   ```

   Example:

   ```
   [Expert@MyMGMT]# cplic db_print -all -a
   Retrieving license information from database ...

   The following licenses appear in the database:
   ================================================
   Host Expiration Features
   192.0.2.11 Never CPFW-FIG-25-53 CK49C3A3CC7121 MyGW1
   192.0.2.11 26Nov2017 CPSB-SWB CPSB-ADNC-M CK0123456789ab MyGW2
   ```

5. In the *Check Point User Center*, view the licenses for the products that were upgraded from version NGX to a Software Blades license.

   You can also create new upgraded licenses.

6. Download a file containing the upgraded licenses.

   Only download licenses for the products that were upgraded from version NGX to Software Blades.

7. If you did not import the version NGX licenses into the repository, import the version NGX licenses now.

   Use this command:

   ```
   cplic get -all
   ```

8. Run the license upgrade command:

   ```
   cplic upgrade -l <Input File>
   ```

   - The licenses in the downloaded license file and in the license repository are compared.
   - If the certificate keys and features match, the old licenses in the repository and in the remote Security Gateways are updated with the new licenses.
   - A report of the results of the license upgrade is printed.

cppkg

Description

Manages the SmartUpdate software packages repository on the Security Management Server.

Important - Installing software packages with the SmartUpdate is not supported for Security Gateways running on Gaia OS.

Syntax

```
cppkg
      add <options>
      {del | delete} <options>
      get
      getroot
      print
      setroot <options>
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run `mdsenv`).

Parameters

Parameter	Description
`add <options>`	Adds a SmartUpdate software package to the repository. See *"cppkg add" on page 453*.
`{del | delete} <options>`	Deletes a SmartUpdate software package from the repository. See *"ppkg delete" on page 454*.
`get`	Updates the list of the SmartUpdate software packages in the repository. See *"cppkg get" on page 456*.
`getroot`	Shows the path to the root directory of the repository (the value of the environment variable `$SUROOT`). See *"cppkg getroot" on page 457*.
`print`	Prints the list of SmartUpdate software packages in the repository. See *"cppkg print" on page 458*.
`setroot <options>`	Configures the path to the root directory of the repository. See *"cppkg setroot" on page 459*.

cppkg add

Description

Adds a SmartUpdate software package to the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- This command does not overwrite existing packages. To overwrite an existing package, you must first delete the existing package.
- You get the SmartUpdate software packages from the *Check Point Support Center*.

Syntax

```
cppkg add <Full Path to Package | DVD Drive [Product]>
```

Parameters

Parameter	Description
<Full Path to Package>	Specifies the full local path on the computer to the SmartUpdate software package.
DVD Drive `[Product]`	Specifies the DVD root path. Example: `/mnt/CPR80`

Example - Adding R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg add /var/log/CP1100_6.0_4_0_-.tgz
Adding package to the repository
Getting the package type...
Extracting the package files...
Copying package to the repository...
Package was successfully added to the repository
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded        R77.20
[Expert@MGMT:0]#
```

ppkg delete

Description

Deletes SmartUpdate software packages from the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg del ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

```
cppkg delete ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

Parameters

Parameter	Description
`del | delete`	When you do not specify optional parameters, the command runs in the interactive mode. The command shows the menu with applicable options.
`"<Vendor>"`	Specifies the package vendor. Enclose in double-quotes.
`"<Product>"`	Specifies the product name. Enclose in double-quotes.
`"<Major Version>"`	Specifies the package Major Version. Enclose in double-quotes.
`"<OS>"`	Specifies the package OS. Enclose in double-quotes.
`"<Minor Version>"`	Specifies the package Minor Version. Enclose in double-quotes.

Notes:

- To see the values for the optional parameters, run the *"cppkg print" on page 458* command.
- You must specify all optional parameters, or no parameters.

Example 1 - Interactive mode

```
[Expert@MGMT:0]# cppkg delete

Select package:
--------------------
(0) Delete all
(1) CP1100 Gaia Embedded Check Point R77.20 R77.20

(e) Exit

Enter your choice : 1

You chose to delete 'CP1100 Gaia Embedded Check Point R77.20 R77.20', Is this correct? [y/n] : y

Package was successfully removed from the repository
[Expert@MGMT:0]#
```

Example 2 - Manually deleting the specified package

```
Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded        R77.20
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg delete "Check Point" "CP1100" "R77.20" "Gaia Embedded" "R77.20"
Package was successfully removed from the repository
[Expert@MGMT:0]#
```

cppkg get

Description

Updates the list of the SmartUpdate software packages in the SmartUpdate software packages repository based on the real content of the repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg get
```

Example

```
[Expert@MGMT:0]# cppkg get
Update successfully completed
[Expert@MGMT:0]#
```

cppkg getroot

Description

Shows the path to the root directory of the SmartUpdate software packages repository (the value of the environment variable `$SUROOT`)

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg getroot
```

Example

```
[Expert@MGMT:0]# cppkg getroot
[cppkg 7119 4128339728]@MGMT[29 May 19:16:06] Current repository root is set to : /var/log/cpupgrade/suroot
[Expert@MGMT:0]#
```

cppkg print

Description

Prints the list of SmartUpdate software packages in the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg print
```

Example - R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#
```

cppkg setroot

Description

Configures the path to the root directory of the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- The default path is: `/var/log/cpupgrade/suroot`
- When changing repository root directory:
  - This command copies the software packages from the old repository to the new repository. A package in the new location is overwritten by a package from the old location, if the packages have the same name.
  - This command updates the value of the environment variable `$SUROOT` in the Check Point Profile shell scripts (`$CPDIR/tmp/.CPprofile.sh` and `$CPDIR/tmp/.CPprofile.csh`).

Syntax

```
cppkg setroot <Full Path to Repository Root Directory>
```

Example

```
[Expert@MGMT:0]# cppkg setroot /var/log/my_directory

Repository root is set to : /var/log/cpupgrade/suroot

Note : When changing repository root directory :

       1. Old repository content will be copied into the new repository
       2. A package in the new location will be overwritten by a package in the old
          location, if the packages have the same name

Change the current repository root ? [y/n] : y

The new repository directory does not exist. Create it ? [y/n] : y

Repository root was set to : /var/log/my_directory

Notice : To complete the setting of your directory, reboot the machine!
[Expert@MGMT:0]#
```

cpprod_util

Description

This utility works with Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) without manually opening it:

- Shows which Check Point products and features are enabled on this Check Point computer.
- Enables and disables Check Point products and features on this Check Point computer.

Syntax

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}
cpprod_util -dump
```

Parameters

Parameter	Description
`CPPROD_GetValue`	Gets the configuration status of the specified product or feature: ■ 0 - Disabled ■ 1 - Enabled
`CPPROD_SetValue`	Sets the configuration for the specified product or feature.  **Important** - Do not run these commands unless explicitly instructed by Check Point Support or R&D to do so.
"*<Product>*"	Specifies the product or feature.
"*<Parameter>*"	Specifies the configuration parameter for the specified product or feature.
"*<Value>*"	Specifies the value of the configuration parameter for the specified product or feature: ■ One of these integers: 0, 1, 4 ■ A string
`dump`	Creates a dump file of Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) in the current working directory. The name of the output file is `RegDump`.

Notes

- On a Multi-Domain Server, you must run this command in the context of the relevant Domain Management Server.
- If you run the `cpprod_util` command without parameters, it prints:
  - The list of all available products and features (for example, "`FwIsFirewallMgmt`", "`FwIsLogServer`", "`FwIsStandAlone`")
  - The type of the expected argument when you configure a product or feature ("`no-parameter`", "`string-parameter`", or "`integer-parameter`")
  - The type of the returned output ("`status-output`", or "`no-output`")
- To redirect the output of the `cpprod_util` command, it is necessary to redirect the *stderr* to *stdout*:

  ```
  cpprod_util <options> > <output file> 2>&1
  ```

  Example:

  ```
  cpprod_util > /tmp/output_of_cpprod_util.txt 2>&1
  ```

Examples

Example - Showing a list of all installed Check Point Products Packages on a Management Server

```
[Expert@MGMT:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
NGXCMP
EdgeCmp
SFWCMP
SFWR75CMP
SFWR77CMP
FLICMP
R75CMP
R7520CMP
R7540CMP
R76CMP
R77CMP
PROVIDER-1
Reporting Module
SmartLog
CPinfo
VSEC
DIAG
[Expert@MGMT:0]#
```

Example - Checking if this Check Point computer is configured as a Management Server

```
[Expert@MGMT:0]# cpprod_util FwIsFirewallMgmt
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point computer is configured as a Standalone

```
[Expert@MGMT:0]# cpprod_util FwIsStandAlone
0
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as a Primary in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsPrimary
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Active in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsActiveManagement
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Backup in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsSMCBackup
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point computer is configured as a dedicated Log Server

```
[Expert@MGMT:0]# cpprod_util FwIsLogServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartProvisioning blade is enabled

```
[Expert@MGMT:0]# cpprod_util FwIsAtlasManagement
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Server blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Correlation Unit blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerCorrelationUnit
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the Endpoint Policy Management blade is enabled

```
[Expert@MGMT:0]# cpprod_util UepmIsInstalled
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Endpoint Policy Server

```
[Expert@MGMT:0]# cpprod_util UepmIsPolicyServer
0
[Expert@MGMT:0]#
```

cprid

Description

Manages the Check Point Remote Installation Daemon (`cprid`).

This daemon is used for remote upgrade and installation of Check Point products on the managed Security Gateways.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run these commands in the context of the MDS (run `mdsenv`).

Commands

Syntax	Description
`cpridstart`	Starts the Check Point Remote Installation Daemon (`cprid`).
`cpridstop`	Stops the Check Point Remote Installation Daemon (`cprid`).
`run_cprid_restart`	Stops and then starts the Check Point Remote Installation Daemon (`cprid`).

cprinstall

Description

Performs installation of Check Point product packages and associated operations on remote managed Security Gateways.

Important - Installing software packages with this command is not supported for Security Gateways that run on Gaia OS.

Notes:

- This command requires a license for SmartUpdate.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On the remote Security Gateways these are required:
  - SIC Trust must be established between the Security Management Server and the Security Gateway.
  - The `cpd` daemon must run.
  - The `cprid` daemon must run.

Syntax

```
cprinstall
      boot <options>
      cprestart <options>
      cpstart <options>
      cpstop <options>
      delete <options>
      get <options>
      install <options>
      revert <options>
      show <options>
      snapshot <options>
      transfer <options>
      uninstall <options>
      verify <options>
```

Parameters

Parameter	Description
`boot <options>`	Reboots the managed Security Gateway. See *"cprinstall boot" on page 466*.

Parameter	Description
`cprestart <options>`	Runs the `cprestart` command on the managed Security Gateway. See *"cprinstall cprestart" on page 467*.
`cpstart <options>`	Runs the `cpstart` command on the managed Security Gateway. See *"cprinstall cpstart" on page 468*.
`cpstop <options>`	Runs the `cpstop` command on the managed Security Gateway. See *"cprinstall cpstop" on page 469*.
`delete <options>`	Deletes a snapshot (backup) file on the managed Security Gateway. See *"cprinstall delete" on page 470*.
`get <options>`	■ Gets details of the products and the operating system installed on the managed Security Gateway. ■ Updates the management database on the Security Management Server. See *"cprinstall get" on page 471*.
`install <options>`	Installs Check Point products on the managed Security Gateway. See *"cprinstall install" on page 472*.
`revert <options>`	Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway. See *"cprinstall revert" on page 474*.
`show <options>`	Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS. See *"cprinstall show" on page 475*.
`snapshot <options>`	Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway. See *"cprinstall snapshot" on page 476*.
`transfer <options>`	Transfers a software package from the repository to the managed Security Gateway without installing the package. See *"cprinstall transfer" on page 477*.
`uninstall <options>`	Uninstalls Check Point products on the managed Security Gateway. See *"cprinstall uninstall" on page 478*.
`verify <options>`	Confirms these operations were successful: ■ If a specific product can be installed on the managed Security Gateway. ■ That the operating system and currently installed products the managed Security Gateway are appropriate for the software package. ■ That there is enough disk space to install the product the managed Security Gateway. ■ That there is a CPRID connection with the managed Security Gateway. See *"cprinstall verify" on page 480*.

cprinstall boot

Description

Reboots the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall boot <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall boot MyGW
```

cprinstall cprestart

Description

Runs the `cprestart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cprestart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# cprinstall cprestart MyGW
```

cprinstall cpstart

Description

Runs the `cpstart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstart MyGW
```

cprinstall cpstop

Description

Runs the `cpstop` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstop {-proc | -nopolicy} <Object Name>
```

Parameters

Parameter	Description
`-proc`	Kills the Check Point daemons and Security Servers, while it maintains the active Security Policy running in the Check Point kernel. Rules with generic *Allow*, *Drop* or *Reject* action based on services, continue to work.
`-nopolicy`	Kills the Check Point daemons and Security Servers and unloads the Security Policy from the Check Point kernel.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstop -proc MyGW
```

cprinstall delete

Description

Deletes a snapshot (backup) file on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall delete <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Specifies the name of the snapshot (backup) on SecurePlatform OS.

Example

```
[Expert@MGMT]# cprinstall delete MyGW Snapshot25Apr2017
```

cprinstall get

Description

- Gets details of the products and the operating system installed on the managed Security Gateway.
- Updates the management database on the Security Management Server.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall get <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example:

```
[Expert@MGMT]# cprinstall get MyGW
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system   Major Version      Minor Version
-------------------------------------------------------------------------
SecurePlatform     R75.20             R75.20

Vendor             Product            Major Version       Minor Version
-------------------------------------------------------------------------
Check Point        VPN-1 Power/UTM    R75.20              R75.20
Check Point        SecurePlatform     R75.20              R75.20
Check Point        SmartPortal        R75.20              R75.20
[Expert@MGMT]#
```

cprinstall install

Description

Installs Check Point products on the managed Security Gateway.

Important - Installing software packages with this command is not supported for Security Gateways that run Gaia OS.

Notes:

- Before transferring the software package, this command runs the *"cprinstall verify" on page 480* command.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 458* command.

Syntax

```
cprinstall install [-boot] [-backup] [-skip_transfer] <Object Name>
"<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after installing the package. **Note** - Only reboot after ALL products have the same version. Reboot is canceled in certain scenarios.
`-backup`	Creates a snapshot on the managed Security Gateway before installing the package. **Note** - Only on Security Gateways that runs on SecurePlatform OS.
`-skip_ transfer`	Skip the transfer of the package.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double-quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double-quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100` ■ `VPN-1 Power/UTM` ■ `SmartPortal`
"*<Major Version>*"	Specifies the package Major Version. Enclose in double-quotes.
"*<Minor Version>*"	Specifies the package Minor Version. Enclose in double-quotes.

Example

```
[Expert@MGMT]# cprinstall install -boot MyGW "checkpoint" "firewall" "R75" "R75.20"

Installing firewall R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
[Expert@MGMT]#
```

cprinstall revert

Description

Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall revert <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 475* command.

cprinstall show

Description

Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall show <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall show GW1
SU_backup.tzg
[Expert@MGMT]#
```

cprinstall snapshot

Description

Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall snapshot <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 475* command.

cprinstall transfer

Description

Transfers a software package from the repository to the managed Security Gateway without installing the package.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 458* command.

Syntax

```
cprinstall transfer <Object Name> "<Vendor>" "<Product>" "<Major Version>"
"<Minor Version>"
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double-quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double-quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100`
"*<Major Version>*"	Specifies the package major version. Enclose in double-quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double-quotes.

cprinstall uninstall

Description

Uninstalls Check Point products on the managed Security Gateway.

Important - Uninstalling software packages with this command is not supported for Security Gateways running on Gaia OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- Before uninstalling product packages, this command runs the *"cprinstall verify" on page 480* command.
- After uninstalling a product package, you must run the *"cprinstall get" on page 471* command.
- To see the values for the package attributes, run the *"cppkg print" on page 458* command.

Syntax

```
cprinstall uninstall [-boot] <Object Name> "<Vendor>" "<Product>" "<Major
Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after uninstalling the package. **Note** - Reboot is canceled in certain scenarios.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double-quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double-quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100`
"*<Major Version>*"	Specifies the package major version. Enclose in double-quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double-quotes.

Example

```
[Expert@MGMT]# cprinstall uninstall MyGW "checkpoint" "firewall" "R75.20" "R75.20"
Uninstalling firewall R75.20 from MyGW...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
[Expert@MGMT]#
[Expert@MGMT]# cprinstall get
```

cprinstall verify

Description

Confirms these operations were successful:

- If a specific product can be installed on the managed Security Gateway.
- That the operating system and currently installed products the managed Security Gateway are appropriate for the software package.
- That there is enough disk space to install the product the managed Security Gateway.
- That there is a CPRID connection with the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 458* command.

Syntax

```
cprinstall verify <Object Name> "<Vendor>" "<Product>" "<Major Version>"
["<Minor Version>"]
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double-quotes. Example: ■ checkpoint ■ Check Point
"*<Product>*"	Specifies the product name. Enclose in double-quotes. Examples: ■ SVNfoundation ■ firewall ■ floodgate ■ CP1100 ■ VPN-1 Power/UTM ■ SmartPortal
"*<Major Version>*"	Specifies the package major version. Enclose in double-quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double-quotes. This parameter is optional.

Example 1 - Verification succeeds

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

Example 2 - Verification fails

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : SVN Foundation R75 is already installed on 192.0.2.134
Operation Success. Product cannot be installed, did not pass dependency check.
```

cpstart

Description

Manually starts all Check Point processes and applications.

Notes:

- For the `cprid` daemon, use the *"cprid" on page 463* command.
- For manually starting specific Check Point processes, see sk97638.

Syntax

```
cpstart
```

cpstat

Description

Displays the status and statistics information of Check Point applications.

Syntax

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>] [-o
<Polling Interval> [-c <Count>] [-e <Period>]] <Application Flag>
```

Note - You can write the parameters in the syntax in any order.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The output shows the SNMP queries and SNMP responses for the applicable SNMP OIDs.
`-h <Host>`	Optional. When you run this command on a Management Server, this parameter specifies the managed Security Gateway. *<Host>* is an IPv4 address, a resolvable hostname, or a DAIP object name. The default is `localhost`. **Note** - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:`mdsenv <IP Address or Name of Domain Management Server>`.
`-p <Port>`	Optional. Port number of the Application Monitoring (AMON) server. The default port is 18192.
`-s <SICname>`	Optional. Secure Internal Communication (SIC) name of the Application Monitoring (AMON) server.
`-f <Flavor>`	Optional. Specifies the type of the information to collect. If you do not specify a flavor explicitly, the command uses the first flavor in the *<Application Flag>*. To see all flavors, run the `cpstat` command without any parameters.

Parameter	Description
`-o <Polling Interval>`	Optional. Specifies the polling interval (in seconds) - how frequently the command collects and shows the information. Examples: ■ 0 - The command shows the results only once and the stops (this is the default value). ■ 5 - The command shows the results every 5 seconds in the loop. ■ 30 - The command shows the results every 30 seconds in the loop. ■ N - The command shows the results every N seconds in the loop. Use this parameter together with the "`-c <Count>`" parameter and the "`-e <Period>`" parameter. Example: `cpstat os -f perf -o 2`
`-c <Count>`	Optional. Specifies how many times the command runs and shows the results before it stops. You must use this parameter together with the "`-o <Polling Interval>`" parameter. Examples: ■ 0 - The command shows the results repeatedly every `<Polling Interval>` (this is the default value). ■ 10 - The command shows the results 10 times every `<Polling Interval>` and then stops. ■ 20 - The command shows the results 20 times every `<Polling Interval>` and then stops. ■ N - The command shows the results N times every `<Polling Interval>` and then stops. Example: `cpstat os -f perf -o 2 -c 2`
`-e <Period>`	Optional. Specifies the time (in seconds), over which the command calculates the statistics. You must use this parameter together with the "`-o <Polling Interval>`" parameter. You can use this parameter together with the "`-c <Count>`" parameter. Example: `cpstat os -f perf -o 2 -c 2 -e 60`
`<Application Flag>`	Mandatory. See the table below with flavors for the application flags.

These flavors are available for the application flags

Note - The available flags depend on the enabled Software Blades. Some flags are supported only by a Security Gateway, and some flags are supported only by a Management Server.

Feature or Software Blade	Flag	Flavors
List of enabled Software Blades	`blades`	`fw, ips, av, urlf, vpn, cvpn, aspm, dlp, appi, anti_bot, default, content_ awareness, threat-emulation, default`
Operating System	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, raidInfo, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
Firewall	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`
HTTPS Inspection	`https_inspection`	`default, hsm_status, all`
Identity Awareness	`identityServer`	`default, authentication, logins, ldap, components, adquery, idc, muh`
Application Control	`appi`	`default, subscription_status, update_ status, RAD_status, top_last_hour, top_ last_day, top_last_week, top_last_month`
URL Filtering	`urlf`	`default, subscription_status, update_ status, RAD_status, top_last_hour, top_ last_day, top_last_week, top_last_month`
IPS	`ips`	`default, statistics, all`
Anti-Virus	`ci`	`default`
Threat Prevention	`antimalware`	`default, scanned_hosts, scanned_mails, subscription_status, update_status, ab_ prm_contracts, av_prm_contracts, ab_prm_ contracts, av_prm_contracts`

Feature or Software Blade	Flag	Flavors
Threat Emulation	`threat-emulation`	`default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts`
Threat Extraction	`scrub`	`default, subscription_status, threat_extraction_statistics`
Mobile Access	`cvpn`	`cvpnd, sysinfo, products, overall`
VSX	`vsx`	`default, stat, traffic, conns, cpu, all, memory, cpu_usage_per_core`
IPsec VPN	`vpn`	`default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all`
Data Loss Prevention	`dlp`	`default, dlp, exchange_agents, fingerprint`
Content Awareness	`ctnt`	`default`
QoS	`fg`	`all`
High Availability	`ha`	`default, all`
Policy Server for Remote Access VPN clients	`polsrv`	`default, all`
Desktop Policy Server for Remote Access VPN clients	`dtps`	`default, all`

Feature or Software Blade	Flag	Flavors
LTE / GX	`gx`	`default, contxt_create_info, contxt_delete_info, contxt_update_info, contxt_path_mng_info, GXSA_GPDU_info, contxt_initiate_info, gtpv2_create_info, gtpv2_delete_info, gtpv2_update_info, gtpv2_path_mng_info, gtpv2_cmd_info, all`
Management Server	`mg`	`default, log_server, indexer`
Certificate Authority	`ca`	`default, crl, cert, user, all`
SmartEvent	`cpsemd`	`default`
SmartEvent Correlation Unit	`cpsead`	`default`
Log Server	`ls`	`default`
CloudGuard Controller	`vsec`	`default`
SmartReporter	`svr`	`default`
Provisioning Agent	`PA`	`default`
Thresholds configured with the `threshold_config` command	`thresholds`	`default, active_thresholds, destinations, error`
Historical status values	`persistency`	`product, TableConfig, SourceConfig`

Examples

Example - CPU utilization

```
[Expert@HostName:0]# cpstat -f cpu os
CPU User Time (%):   1
CPU System Time (%): 0
CPU Idle Time (%):   99
CPU Usage (%):       1
CPU Queue Length:    -
CPU Interrupts/Sec:  172
CPUs Number:         8

[Expert@HostName:0]#
```

Example - Performance

```
[Expert@HostName:0]# cpstat os -f perf -o 2 -c 2 -e 60

Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741331456
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741331456
Free Real Memory (Bytes):                4489732096
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       0
CPU System Time (%):                     0
CPU Idle Time (%):                       100
CPU Usage (%):                           0
CPU Queue Length:                        -
CPU Interrupts/Sec:                      135
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296


Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741556736
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741556736
Free Real Memory (Bytes):                4489506816
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       3
CPU System Time (%):                     0
CPU Idle Time (%):                       97
CPU Usage (%):                           3
CPU Queue Length:                        -
CPU Interrupts/Sec:                      140
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296

[Expert@HostName:0]#
```

Example - List of current connected sessions on a Management Server

```
[Expert@MGMT:0]# cpstat -f default mg

Product Name:  Check PointSecurity Management Server
Major version: 6
Minor version: 0
Build number:  994000031
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------------
|Client type |Administrator|Host        |Database lock|
-----------------------------------------------------
|SmartConsole|admin        |JOHNDOE-PC  |false        |
-----------------------------------------------------

[Expert@MGMT:0]#
```

cpstop

Description

Manually stops all Check Point processes and applications.

Notes:

- For the `cprid` daemon, use the *"cprid" on page 463* command.
- For manually stopping specific Check Point processes, see sk97638.

Syntax

```
cpstop
```

cpview

Overview of CPView

Description

CPView is a text based built-in utility on a Check Point computer.

CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway).

The CPView continuously updates the data in easy to access views.

On Security Gateway, you can use this statistical data to monitor the performance.

For more information, see sk101878.

Syntax

```
cpview --help
```

CPView User Interface

The CPView user interface has three sections:

Section	Description
Header	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
Navigation	This menu bar is interactive. Move between menus with the arrow keys and mouse. A menu can have sub-menus and they show under the menu bar.
View	This view shows the statistics collected in that view. These statistics update at the refresh rate.

Using CPView

Use these keys to navigate the CPView:

Key	Description
Arrow keys	Moves between menus and views. Scrolls in a view.
Home	Returns to the **Overview** view.
Enter	Changes to the **View Mode**. On a menu with sub-menus, the **Enter** key moves you to the lowest level sub-menu.
Esc	Returns to the **Menu Mode**.
Q	Quits CPView.

Use these keys to change CPView interface options:

Key	Description
R	Opens a window where you can change the refresh rate. The default refresh rate is 2 seconds.
W	Changes between wide and normal display modes. In wide mode, CPView fits the screen horizontally.
S	Manually sets the number of rows or columns.
M	Switches on/off the mouse.
P	Pauses and resumes the collection of statistics.

Use these keys to save statistics, show help, and refresh statistics:

Key	Description
C	Saves the current page to a file. The file name format is: `cpview_<ID of the cpview process>.cap<Number of the capture>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

cpwd_admin

Description

The Check Point WatchDog (`cpwd`) is a process that invokes and monitors critical processes such as Check Point daemons on the local computer, and attempts to restart them if they fail.

Among the processes monitored by Watchdog are `fwm`, `fwd`, `cpd`, `DAService`, and others.

The list of monitored processes depends on the installed and configured Check Point products and Software Blades.

The Check Point WatchDog writes monitoring information to the `$CPDIR/log/cpwd.elg` log file.

The `cpwd_admin` utility shows the status of the monitored processes, and configures the Check Point WatchDog.

There are two types of Check Point WatchDog monitoring

Monitoring	Description
Passive	WatchDog restarts the process only when the process terminates abnormally. In the output of the `cpwd_admin list` command, the `MON` column shows `N` for passively monitored processes.
Active	WatchDog checks the process status every predefined interval. WatchDog makes sure the process is alive, as well as properly functioning (not stuck on deadlocks, frozen, and so on). In the output of the `cpwd_admin list` command, the `MON` column shows `Y` for actively monitored processes. The list of actively monitored processes is predefined by Check Point. Users cannot change or configure it.

Syntax

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 494*.
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 497*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 498*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 499*.
`flist <options>`	Saves the status of all monitored processes to a `$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst` file. See *"cpwd_admin flist" on page 500*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 501*.
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 502*. **Important** - Do not run this command unless explicitly instructed by Check Point Support or R&D to do so.
`list`	Prints the status of all monitored processes on the screen. See *"cpwd_admin list" on page 503*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 505*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 506*.
`start_ monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 508*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 509*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 511*.

cpwd_admin config

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the `cpstop` and cpstart commands (which restart *all* Check Point processes).

Syntax

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters.  **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-p`	Shows the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 2000 ■ Default: 2000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_ startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_ admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`
`sleep_ timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

Description

Temporarily deletes a monitored process from the WatchDog database of monitored processes.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 503* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 482* command.

Syntax on a Management Server

```
cpwd_admin del -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 503* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

Example

```
[Expert@HostName:0]# cpwd_admin del -name FWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

Description

Temporarily detaches a monitored process from the WatchDog monitoring.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 503* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 482* command.

Syntax on a Management Server

```
cpwd_admin detach -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 503* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

Example

```
[Expert@HostName:0]# cpwd_admin detach -name FWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

Description

Checks whether the WatchDog process `cpwd` is alive.

Syntax

```
cpwd_admin exist
```

Example

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

Description

Saves the status of all WatchDog monitored processes to a file.

Syntax on a Management Server

```
cpwd_admin list [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Output

Column	Description
`APP`	Shows the WatchDog name of the monitored process.
`PID`	Shows the PID of the monitored process.
`STAT`	Shows the status of the monitored process: ■ `E` - executing ■ `T` - terminated
`#START`	Shows how many times the WatchDog started the monitored process.
`START_TIME`	Shows the time when the WatchDog started the monitored process for the last time.
`SLP/LIMIT`	In verbose output, shows the values of the `sleep_timeout` and `no_limit` configuration parameters (see *"cpwd_admin config" on page 494*).
`MON`	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 492*): ■ `Y` - Active monitoring ■ `N` - Passive monitoring
`COMMAND`	Shows the command the WatchDog run to start this process.

Example

```
[Expert@HostName:0]# cpwd_admin flist
/opt/CPshrd-R81/tmp/cpwd_list_1564617600.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

Description

Shows the PID of a WatchDog monitored process.

Syntax for a Management Server

```
cpwd_admin getpid -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 503* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

Example

```
[Expert@HostName:0]# cpwd_admin getpid -name FWD
5640
[Expert@HostName:0]#
```

cpwd_admin kill

Description

Terminates the WatchDog process `cpwd`.

Important - Do not run this command unless explicitly instructed by Check Point Support or R&D to do so.
To restart the WatchDog process, you must restart all Check Point services with the *"cpstop" on page 489* and *"cpstart" on page 482* commands.

Syntax

```
cpwd_admin kill
```

cpwd_admin list

Description

Prints the status of all WatchDog monitored processes on the screen.

Syntax on a Management Server

```
cpwd_admin list [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Output

Column	Description
`APP`	Shows the WatchDog name of the monitored process.
`PID`	Shows the PID of the monitored process.
`STAT`	Shows the status of the monitored process: ■ `E` - executing ■ `T` - terminated
`#START`	Shows how many times the WatchDog started the monitored process.
`START_TIME`	Shows the time when the WatchDog started the monitored process for the last time.
`SLP/LIMIT`	In verbose output, shows the values of the `sleep_timeout` and `no_limit` configuration parameters (see *"cpwd_admin config" on page 494*).
`MON`	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 492*): ■ `Y` - Active monitoring ■ `N` - Passive monitoring
`COMMAND`	Shows the command the WatchDog run to start this process.

Examples

Example - Default output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list
APP         PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD     19738  E     1       [17:50:44] 31/5/2019   N    cpviewd
HISTORYD    0      T     0       [17:54:44] 31/5/2019   N    cpview_historyd
CPD         19730  E     1       [17:54:45] 31/5/2019   Y    cpd
SOLR        19935  E     1       [17:50:55] 31/5/2019   N    java_solr /opt/CPrt-R81/conf/jetty.xml
RFL         19951  E     1       [17:50:55] 31/5/2019   N    LogCore
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   N    SmartView
INDEXER     20032  E     1       [17:50:55] 31/5/2019   N    /opt/CPrt-R81/log_indexer/log_indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-R81/smartlog_server
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   N    cp3dlogd
EPM         20251  E     1       [17:50:56] 31/5/2019   N    startEngine
DASERVICE   20404  E     1       [17:50:59] 31/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list -full
APP         PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
CPVIEWD     19738  E     1       [17:50:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R81/bin/cpviewd
            COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD    0      T     0       [17:54:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R81/bin/cpview_historyd
            COMMAND = cpview_historyd
-------------------------------------------------------------------------------
CPD         19730  E     1       [17:54:45] 31/5/2019   60/5       Y
            PATH = /opt/CPshrd-R81/bin/cpd
            COMMAND = cpd
-------------------------------------------------------------------------------
SOLR        19935  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81/bin/java_solr
            COMMAND = java_solr /opt/CPrt-R81/conf/jetty.xml
-------------------------------------------------------------------------------
RFL         19951  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81/bin/LogCore
            COMMAND = LogCore
-------------------------------------------------------------------------------
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81/bin/SmartView
            COMMAND = SmartView
-------------------------------------------------------------------------------
INDEXER     20032  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81/log_indexer/log_indexer
            COMMAND = /opt/CPrt-R81/log_indexer/log_indexer
-------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPSmartLog-R81/smartlog_server
            COMMAND = /opt/CPSmartLog-R81/smartlog_server
            ENV = LANG=C
-------------------------------------------------------------------------------
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R81/bin/cp3dlogd
            COMMAND = cp3dlogd
-------------------------------------------------------------------------------
EPM         20251  E     1       [17:50:56] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R81/bin/startEngine
            COMMAND = startEngine
-------------------------------------------------------------------------------
DASERVICE   20404  E     1       [17:50:59] 31/5/2019   60/5       N
            PATH = /opt/CPda/bin/DAService_script
            COMMAND = DAService_script
[Expert@HostName:0]#
```

cpwd_admin monitor_list

Description

Prints the status of actively monitored processes on the screen.

See the explanation about the active monitoring in *"cpwd_admin" on page 492*.

Syntax

```
cpwd_admin monitor_list
```

Example

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
APP        FILE_NAME                    NO_MSG_TIMES  LAST_MSG_TIME
CPD        CPD_5420_4714.mntr           0/10          [19:00:33] 31/5/2019
[Expert@HostName:0]#
```

cpwd_admin start

Description

Starts a process as monitored by the WatchDog.

Syntax on a Management Server

```
cpwd_admin start -name <Application Name> -path "<Full Path to Executable>"
-command "<Command Syntax>" [-env {inherit | <Env_Var>=<Value>] [-slp_
timeout <Timeout>] [-retry_limit {<Limit> | u}]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name, under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double-quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd`" ■ For CPM: "`/opt/CPsuite-R81/fw1/scripts/cpm.sh`" ■ For SICTUNNEL: "`/opt/CPshrd-R81/bin/cptnl`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double-quotes. Examples: ■ For FWM: "`fwm`" ■ For FWM on Multi-Domain Server: "`fwm mds`" ■ For FWD: "`fwd`" ■ For CPD: "`cpd`" ■ For CPM: "`/opt/CPsuite-R81/fw1/scripts/cpm.sh -s`" ■ For SICTUNNEL: "`/opt/CPshrd-R81/bin/cptnl -c "/opt/CPuepm-R81/engine/conf/cptnl_srv.conf"`"

Parameter	Description
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ `<Env_Var>=<Value>` - Assigns the specified value to the specified environment variable
`-slp_timeout <Timeout>`	Configures the specified value of the "`sleep_timeout`" configuration parameter. See *"cpwd_admin config" on page 494*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 494*. ■ `<Limit>` - Tries to restart the process the specified number of times ■ `u` - Tries to restart the process unlimited number of times

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin start_monitor

Description

Starts the active WatchDog monitoring. WatchDog monitors the predefined processes actively.

See the explanation for the *"cpwd_admin" on page 492* command.

Syntax

```
cpwd_admin start_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

Description

Stops a WatchDog monitored process.

Important - This change does **not** survive reboot.

Syntax on a Management Server

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to Executable>"
-command "<Command Syntax>" [-env {inherit | <Env_Var>=<Value>]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double-quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd_admin`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double-quotes. Examples: ■ For FWM: "`fw kill fwm`" ■ For FWD: "`fw kill fwd`" ■ For CPD: "`cpd_admin stop`"
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ *<Env_Var>=<Value>* - Assigns the specified value to the specified environment variable

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin stop_monitor

Description

Stops the active WatchDog monitoring. WatchDog monitors all processes only passively.

See the explanation for the *"cpwd_admin" on page 492* command.

Syntax

```
cpwd_admin stop_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

dbedit

Description

Edits the management database - the `$FWDIR/conf/objects_5_0.C` file - on the Security Management Server or Domain Management Server. See sk13301.

Important - Do NOT run this command, unless explicitly instructed by Check Point Support or R&D to do so. Otherwise, you can corrupt settings in the management database.

Syntax

```
dbedit -help
```

```
dbedit [-globallock] [{-local | -s <Management_Server>}] [{-u <Username> |
-c <Certificate>}] [-p <Password>] [-f <File_Name> [ignore_script_failure]
[-continue_updating]] [-r "<Open_Reason_Text>"] [-d <Database_Name>] [-
listen] [-readonly] [-session]
```

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Parameters

Parameter	Description
`-help`	Prints the general help.
`-globallock`	When you work with the dbedit utility, it partially locks the management database. If a user configures objects in SmartConsole at the same time, it causes problems in the management database. This option does not let SmartConsole, or a dbedit user to make changes in the management database. When you specify this option, the dbedit commands run on a copy of the management database. After you make the changes with the `dbedit` commands and run the `savedb` command, the dbedit utility saves and commits your changes to the actual management database.
`-local`	Connects to the localhost (127.0.0.1) without using username/password. If you do not specify this parameter, the dbedit utility asks how to connect.
`-s <Management_Server>`	Specifies the Security Management Server - by IP address or HostName. If you do not specify this parameter, the dbedit utility asks how to connect.

Parameter	Description
`-u <Username>`	Specifies the username, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-c <Certificate>`	Specifies the user's certificate file, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-p <Password>`	Specifies the user's password, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" and "`-u <Username>`" parameters.
`-f <File_Name>`	Specifies the file that contains the applicable dbedit internal commands (see the section "*dbedit Internal Commands*" below): ■ `create <object_type> <object_name>` ■ `modify <table_name> <object_name> <field_name> <value>` ■ `update <table_name> <object_name>` ■ `delete <table_name> <object_name>` ■ `print <table_name> <object_name>` ■ `quit` **Note** - Each command is limited to 4096 characters.
`ignore_script_failure`	Continues to execute the dbedit internal commands in the file and ignores errors. You can use it when you specify the "`-f <File_Name>`" parameter.
`-continue_updating`	Continues to update the modified objects, even if the operation fails for some of the objects (ignores the errors and runs the `update_all` command at the end of the script). You can use it when you specify the "`-f <File_Name>`" parameter.
`-r "<Open_Reason_Text>"`	Specifies the reason for opening the database in read-write mode (default mode).
`-d <Database_Name>`	Specifies the name of the database, to which the dbedit utility should connect (for example, `mdsdb`).
`-listen`	The dbedit utility "listens" for changes (use this mode for advanced troubleshooting with the assistance of Check Point Support). The dbedit utility prints its internal messages when a change occurs in the management database.
`-readonly`	Specifies to open the management database in read-only mode.
`-session`	Session Connectivity.

`dbedit` Internal Commands

Note - To see the available tables, class names (object types), attributes and values, connect to Management Server with GuiDBedit Tool (see sk13009).

Command	Description, Syntax, Examples
`-h`	**Description:** Prints the general help. **Syntax:** `dbedit> -h`
`-q` `quit`	**Description:** Quits from dbedit. **Syntax:** `dbedit> -q` `dbedit> quit [-update_all | -noupdate]` **Examples:** ■ Exit the utility and commit the remaining modified objects (interactive mode): `dbedit> quit` ■ Exit the utility and update all the remaining modified objects: `dbedit> quit -update_all` ■ Exit the utility and discard all modifications: `dbedit> quit -no_update`
`update`	**Description:** Saves the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`"). **Syntax:** `dbedit> update <table_name> <object_name>` **Example:** Save the object *My_Service* in the table *services*: `dbedit> update services My_Service`
`update_all`	**Description:** Saves all the modified objects. **Syntax:** `dbedit> update_all`

Command	Description, Syntax, Examples
`_print_set`	**Description:** Prints the specified object from the specified table (for example, "`network_objects`", "`services`", "`users`") as it appears in the `$FWDIR/conf/objects_5_0.C` file (sets of attributes). **Syntax:** `dbedit> _print_set <table_name> <object_name>` **Example:** Print the object *My_Obj* from the table *network_objects*: `dbedit> print network_objects My_Obj`
`print`	**Description:** Prints the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`"). **Syntax:** `dbedit> print <table_name> <object_name>` **Examples:** ■ Print the object *My_Obj* from the table *network_objects* (in "Network Objects"): `dbedit> print network_objects my_obj` ■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"): `dbedit> print properties firewall_properties`
`printxml`	**Description:** Prints in XML format the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`"). You can export the settings from a Management Server to an XML file that you can use later with external automation systems. **Syntax:** `dbedit> printxml <table_name> [<object_name>]` **Examples:** ■ Print the object *My_Obj* from the table *network_objects*: `dbedit> printxml network_objects my_obj` ■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"): `dbedit> printxml properties firewall_properties`

Command	Description, Syntax, Examples
`printbyuid`	**Description:** Prints the attributes of the object specified by its UID (appears in the `$FWDIR/conf/objects_5_0.C` file at the beginning of the object as "`chkpf_uid ({...})`"). **Syntax:** `dbedit> printbyuid {object_id}` **Example:** Print the attributes of the object with the specified UID: `dbedit> printbyuid {D3833F1D-0A58-AA42-865F-39BFE3C126F1}`
`query`	**Description:** Prints all the objects in the specified table. Optionally, you can query for objects with specific attribute and value - query is separated by a comma after "`query <table_name>`" (spaces are not allowed between the `<attribute>` and `'<value>'`). **Syntax:** `dbedit> query <table_name> [ , <attribute>='<value>' ]` **Examples:** ■ Print all objects in the table *users*: `dbedit> query users` ■ Print all objects in the table *network_objects* that are defined as Management Servers: `dbedit> query network_objects, management='true'` ■ Print all objects in the table *services* with the name *ssh*: `command_sdbedit> query services, name='ssh'` ■ Print all objects in the table *services* with the port *22*: `dbedit> query services, port='22'` ■ Print all objects with the IP address *10.10.10.10*: `dbedit> query network_objects, ipaddr='10.10.10.10'`
`whereused`	**Description:** Checks where the specified object used in the database. Prints the number of places, where this object is used and relevant information about each such place. **Syntax:** `dbedit> whereused <table_name> <object_name>` **Example:** Check where the object *My_Obj* is used: `dbedit> whereused network_objects My_Obj`

Command	Description, Syntax, Examples
`create`	**Description:** Creates an object of specified type (with its default values) in the database. Restrictions apply to the object's name: ■ Object names can have a maximum of 100 characters. ■ Objects names can contain only ASCII letters, numbers, and dashes. ■ Reserved words will be blocked by the Management Server (refer to sk40179). **Syntax:** `dbedit> create <object_type> <object_name>` **Example:** Create the service object *My_Service* of the type *tcp_service* (with its default values): `dbedit> create tcp_service my_service`
`delete`	**Description:** Deletes an object from the specified table. **Syntax:** `dbedit> delete <table_name> <object_name>` **Example:** Delete the service object *My_Service* from the table *services*: `dbedit> delete services my_service`

Command	Description, Syntax, Examples
`modify`	**Description:** Modifies the value of specified attribute in the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`") in the management database. **Syntax:** `dbedit> modify <table_name> <object_name> <field_name> <value>` **Examples:** ■ Modify the color to *red* in the object *My_Service* in the table *services*: `dbedit> modify services My_Service color red` ■ Add a comment to the object *MyObj*: `dbedit> modify network_objects MyObj comments "Created by fwadmin with dbedit"` ■ Set the value of the global property *ike_use_largest_possible_subnets* in the table *properties* to *false*: `dbedit> modify properties firewall_properties ike_use_largest_possible_subnets false` ■ Create a new interface on the Security Gateway *My_FW* and modify its attributes - set the IP address / Mask and enable Anti-Spoofing on interface with *"Element Index"=3* (check the attributes of the object *My_FW* in GuiDBedit Tool (see sk13009)): `dbedit> addelement network_objects My_FW interfaces interface` `dbedit> modify network_objects My_FW interfaces:3:officialname NAME_OF_INTERFACE` `dbedit> modify network_objects My_FW interfaces:3:ipaddr IP_ADDRESS` `dbedit> modify network_objects My_FW interfaces:3:netmask NETWORK_MASK` `dbedit> modify network_objects My_FW interfaces:3:security:netaccess:access specific` `dbedit> modify network_objects My_FW interfaces:3:security:netaccess:allowed network_objects:group_name` `dbedit> modify network_objects My_FW interfaces:3:security:netaccess:perform_anti_spoofing true` `dbedit> modify network_objects MyObj FieldA LINKSYS` ■ In the Owned Object *MyObj* change the value of *FieldB* to *NewVal*: `dbedit> modify network_objects MyObj FieldA:FieldB NewVal` ■ In the Linked Object *MyObj* change the value of *FieldA* from *B* to *C*: `dbedit> modify network_objects MyObj FieldA B:C`

Command	Description, Syntax, Examples
`lock`	**Description:** Locks the specified object (by administrator) in the specified table (for example, "`network_objects`", "`services`", "`users`") from being modified by other users. For example, if you connect from a remote computer to this Management Server with *admin1* and lock an object, you are be able to connect with *admin2*, but are not able to modify the locked object, until *admin1* releases the lock. **Syntax:** `dbedit> lock <table_name> <object_name>` **Example:** Lock the object *My_Service_Obj* in the table *services* in the database: `dbedit> lock services My_Service_Obj`
`addelement`	**Description:** Adds a specified multiple field / container (with specified value) to a specified object in specified table. **Syntax:** `dbedit> addelement <table_name> <object_name> <field_name> <value>` **Examples:** ■ Add the element *BranchObjectClass* with the value *Organization* to a multiple field *Read* in the object *My_Obj* in the table *ldap*: `dbedit> addelement ldap My_Obj Read:BranchObjectClass Organization` ■ Add the service *MyService* to the group of services *MyServicesGroup* in the table *services*: `dbedit> addelement services MyServicesGroup '' services:MyService` ■ Add the network *MyNetwork* to the group of networks *MyNetworksGroup* in the table *network_objects*: `dbedit> addelement network_objects MyNetworksGroup '' network_objects:MyNetwork`

Command	Description, Syntax, Examples
`rmelement`	**Description:** Removes a specified multiple field / container (with specified value) from a specified object in specified table. **Syntax:** `dbedit> rmelement <table_name> <object_name> <field_name> <value>` **Examples:** ■ Remove the service *MyService* from the group of services *MyServicesGroup* from the table *services*: `dbedit> rmelement services MyServicesGroup '' services:MyService` ■ Remove the network *MyNetwork* from the group of networks *MyNetworksGroup* from the table *network_objects*: `dbedit> rmelement network_objects MyNetworksGroup '' network_objects:MyNetwork` ■ Remove the element *BranchObjectClass* with the value *Organization* from the multiple field *Read* in the object *My_Obj* in the table *ldap*: `dbedit> rmelement ldap my_obj Read:BranchObjectClass Organization`
`rename`	**Description:** Renames the specified object in specified table. **Syntax:** `dbedit> rename <table_name> <object_name> <new_object_name>` **Example:** Rename the network object *london* to *chicago* in the table *network_objects*: `dbedit> rename network_objects london chicago`
`rmbyindex`	**Description:** Removes an element from a container by element's index. **Syntax:** `dbedit> rmbyindex <table_name> <object_name> <field_name> <index_number>` **Example:** Remove the element *backup_log_servers* from the container *log_servers* by element index *1* in the table *network_objects*: `dbedit> rmbyindex network_objects g log_servers:backup_log_servers 1`

Command	Description, Syntax, Examples
`add_owned_remove_name`	**Description:** Adds an owned object (and removes its name) to a specified owned object field (or container). **Syntax:** `dbedit> add_owned_remove_name <table_name> <object_name> <field_name> <value>` **Example:** Add the owned object *My_Gateway* (and remove its name) to the owned object field (or container) *my_external_products*: `dbedit> add_owned_remove_name network_objects My_Gateway additional_products owned:my_external_products`
`is_delete_allowed`	**Description:** Checks if the specified object can be deleted from the specified table (object cannot be deleted if it is used by other objects). **Syntax:** `dbedit> is_delete_allowed <table_name> <object_name>` **Example:** `dbedit> is_delete_allowed network_objects MyObj` Check if the object *MyObj* can be deleted from the table *network_objects*:
`set_pass`	**Description:** Sets specified password for specified user. **Notes:** ■ The password must contain at least 4 characters and no more than 50 characters. ■ This command cannot change the administrator's password. **Syntax:** `dbedit> set_pass <Username> <Password>` **Example:** Set the password *1234* for the user *abcd*: `dbedit> set_pass abcd 1234`
`savedb`	**Description:** Saves the database. You can run this command only when the database is locked globally (when you start the dbedit utility with the "`dbedit -globallock`" command). **Syntax:** `dbedit> savedb`

Command	Description, Syntax, Examples
`savesession`	**Description:** Saves the session. You can run this command only when you start the dbedit utility in session mode (with the "`dbedit -session`" command). **Syntax:** `dbedit> savesession`

fw

Description

- Performs various operations on Security or Audit log files.
- Kills the specified Check Point processes.
- Manages the Suspicious Activity Monitoring (SAM) rules.
- Manages the Suspicious Activity Policy editor.

Syntax

```
fw [-d]
      fetchlogs <options>
      hastat <options>
      kill <options>
      log <options>
      logswitch <options>
      lslogs <options>
      mergefiles <options>
      repairlog <options>
      sam <options>
      sam_policy <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`fetchlogs <options>`	Fetches the specified Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), from the specified Check Point computer. See *"fw fetchlogs" on page 525*.
`hastat <options>`	Shows information about Check Point computers in High Availability configuration and their states. See *"fw hastat" on page 527*.
`kill <options>`	Kills the specified Check Point process. See *"fw kill" on page 528*.
`log <options>`	Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw log" on page 529*.

Parameter	Description
`logswitch` *<options>*	Switches the current active Check Point log file - Security (`$FWDIR/log/fw.log`) or Audit (`$FWDIR/log/fw.adtlog`). See *"fw logswitch" on page 537*.
`lslogs` *<options>*	Shows a list of Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), located on the local computer or a remote computer. See *"fw lslogs" on page 540*.
`mergefiles` *<options>*	Merges several Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`), into a single log file. See *"fw mergefiles" on page 543*.
`repairlog` *<options>*	Rebuilds pointer files for Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw repairlog" on page 546*.
`sam` *<options>*	Manages the Suspicious Activity Monitoring (SAM) rules. See *"fw sam" on page 547*.
`sam_policy` *<options>* or `samp` *<options>*	Manages the Suspicious Activity Policy editor that works with these type of rules: ■ Suspicious Activity Monitoring (SAM) rules. ■ Rate Limiting rules. See *"fw sam_policy" on page 553*.

fw fetchlogs

Description

Fetches the specified Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) from the specified Check Point computer.

Syntax

```
fw [-d] fetchlogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]... [-f <Name of Log File N>] <Target>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File N>`	Specifies the name of the log file to fetch. Need to specify name only. **Notes:** ■ If you do not specify the log file name explicitly, the command transfers all Security log files (`$FWDIR/log/*.log*`) and all Audit log files (`$FWDIR/log/*.adtlog*`). ■ The specified log file name can include wildcards * and ? (for example, `2017-0?-*.log`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the `-f` parameter for each log file name pattern. ■ This command also transfers the applicable log pointer files.
`<Target>`	Specifies the remote Check Point computer, with which this local Check Point computer has established SIC trust. ■ If you run this command on a Security Management Server or Domain Management Server, then `<Target>` is the applicable object's name or main IP address of the Check Point Computer as configured in SmartConsole. ■ If you run this command on a Security Gateway or Cluster Member, then `<Target>` is the main IP address of the applicable object as configured in SmartConsole.

Notes:

- This command moves the specified log files from the `$FWDIR/log/` directory on the specified Check Point computer. Meaning, it deletes the specified log files on the specified Check Point computer after it copies them successfully.
- This command moves the specified log files to the `$FWDIR/log/` directory on the local Check Point computer, on which you run this command.
- This command cannot fetch the *active* log files `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`.

  To fetch these active log files:

  1. Perform log switch on the applicable Check Point computer:

     ```
     fw logswitch [-audit] [-h <IP Address or Hostname>]
     ```

  2. Fetch the rotated log file from the applicable Check Point computer:

     ```
     fw fetchlogs -f <Log File Name> <IP Address or Hostname>
     ```

- This command renames the log files it fetched from the specified Check Point computer. The new log file name is the concatenation of the Check Point computer's name (as configured in SmartConsole), two underscore (_) characters, and the original log file name (for example: `MyGW__2019-06-01_000000.log`).

Example - Fetching log files from a Management Server

```
[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      5796KB 2019-06-01_000000.log
      4610KB fw.log
[Expert@HostName:0]#

[Expert@HostName:0]# fw fetchlogs -f 2019-06-01_000000 MyGW
File fetching in process. It may take some time...
File MyGW__2019-06-01_000000.log was fetched successfully
[Expert@HostName:0]#

[Expert@HostName:0]# ls $FWDIR/log/MyGW*
/opt/CPsuite-R81/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R81/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R81/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R81/fw1/log/MyGW__2019-06-01_000000.logptr
[Expert@HostName:0]#

[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      4610KB fw.log
[Expert@HostName:0]#
```

fw hastat

Description

Shows information about Check Point computers in High Availability configuration and their states.

Note - This command is outdated. On Management Servers, run the *"cpstat" on page 483* command.

Syntax

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

Parameters

Parameter	Description
<Target1> *<Target2>* ... *<TargetN>*	Specifies the Check Point computers to query. If you run this command on the Management Server, you can enter the applicable IP address, or the resolvable HostName of the managed Security Gateway or Cluster Member. If you do not specify the target, the command queries the local computer.

Example - Querying the cluster members from the Management Server

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

fw kill

Description

Kills the specified Check Point processes.

Important - Make sure the killed process is restarted, or restart it manually. See sk97638.

Syntax

```
fw [-d] kill [-t <Signal Number>] <Name of Process>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-t <Signal Number>`	Specifies which signal to send to the Check Point process. For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). **Note** - Processes can ignore some signals.
`<Name of Process>`	Specifies the name of the Check Point process to kill. To see the names of the processes, run the `ps auxwf` command.

Example

```
fw kill fwd
```

fw log

Description

Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`).

Syntax

```
fw log {-h | -help}
```

```
fw [-d] log [-a] [-b "<Start Timestamp>" "<End Timestamp>"] [-c <Action>]
[{-f | -t}] [-g] [-H] [-h <Origin>] [-i] [-k {<Alert Name> | all}] [-l] [-m
{initial | semi | raw}] [-n] [-o] [-p] [-q] [-S] [-s "<Start Timestamp>"]
[-e "<End Timestamp>"] [-u <Unification Scheme File>] [-w] [-x <Start Entry
Number>] [-y <End Entry Number>] [-z] [-#] [<Log File>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the built-in usage. **Note** - The built-in usage does not show some of the parameters described in this table.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-a`	Shows only Account log entries.
`-b "<Start Timestamp>" "<End Timestamp>"`	Shows only entries that were logged between the specified start and end times. ■ The *<Start Timestamp>* and *<End Timestamp>* may be a date, a time, or both. ■ If date is omitted, then the command assumes the current date. ■ Enclose the "*<Start Timestamp>*" and "*<End Timestamp>* in single or double quotes (`-b 'XX' 'YY'`, or `-b "XX" "YY"`). ■ You cannot use the "`-b`" parameter together with the "`-s`" or "`-e`" parameters. ■ See the date and time format below.

Parameter	Description
`-c <Action>`	Shows only events with the specified action. One of these: ■ `accept` ■ `drop` ■ `reject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl` **Notes:** ■ The `fw log` command always shows the **Control** (`ctl`) actions. ■ For *login* action, use the `authcrypt`.
`-e "<End Timestamp>"`	Shows only entries that were logged before the specified time. **Notes:** ■ The *<End Timestamp>* may be a date, a time, or both. ■ Enclose the *<End Timestamp>* in single or double quotes (`-e '...'`, or `-e "..."`). ■ You cannot use the "`-e`" parameter together with the "`-b`" parameter. ■ See the date and time format below.
`-f`	This parameter: 1. Shows the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-g`	Does not show delimiters. The default behavior is: ■ Show a colon (`:`) after a field name ■ Show a semi-colon (`;`) after a field value
`-H`	Shows the High Level Log key.
`-h <Origin>`	Shows only logs that were generated by the Security Gateway with the specified IP address or object name (as configured in SmartConsole).
`-i`	Shows log UID.

Parameter	Description
`-k {<Alert Name> | all}`	Shows entries that match a specific alert type: ■ `<Alert Name>` - Show only entries that match a specific alert type: • `alert` • `mail` • `snmp_trap` • `spoof` • `user_alert` • `user_auth` ■ `all` - Show entries that match all alert types (this is the default).
`-l`	Shows both the date and the time for each log entry. The default is to show the date only once above the relevant entries, and then specify the time for each log entry.
`-m`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command shows one unified log entry for each ID. This is the default. If you also specify the `-f` parameter, then the output does not show any updates, but shows only entries that relate to the start of new connections. To shows updates, use the `semi` parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, the output shows an entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. The output shows all log entries.
`-n`	Does not perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.
`-o`	Shows detailed log chains - shows all the log segments in the log entry.
`-p`	Does not perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-q`	Shows the names of log header fields.
`-S`	Shows the Sequence Number.
`-s "<Start Timestamp>"`	Shows only entries that were logged after the specified time. **Notes:** ■ The `<Start Timestamp>` may be a date, a time, or both. ■ If the date is omitted, then the command assumed the current date. ■ Enclose the `<Start Timestamp>` in single or double quotes (`-s '...'`, or `-s "..."`). ■ You cannot use the "`-s`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-t`	This parameter: 1. Does not show the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-w`	Shows the flags of each log entry (different bits used to specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on).
`-x <Start Entry Number>`	Shows only entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Shows only entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), continues to show log entries. The default behavior is to stop.
`-#`	Show confidential logs in clear text.
`<Log File>`	Specifies the log file to read. If you do not specify the log file explicitly, the command opens the `$FWDIR/log/fw.log` log file. You can specify a switched log file.

Date and Time format

Part of timestamp	Format	Example
Date only	`MMM DD, YYYY`	`June 11, 2018`
Time only Note - In this case, the command assumes the current date.	`HH:MM:SS`	`14:20:00`
Date and Time	`MMM DD, YYYY HH:MM:SS`	`June 11, 2018 14:20:00`

Output

Each output line consists of a single log entry, whose fields appear in this format:

Note - The fields that show depends on the connection type.

```
HeaderDateHour ContentVersion HighLevelLogKey Uuid SequenceNum Flags Action
Origin IfDir InterfaceName LogId ...
```

This table describes some of the fields.

Field Header	Description	Example
`HeaderDateHour`	Date and Time	`12Jun2018 12:56:42`
`ContentVersion`	Version	`5`
`HighLevelLogKey`	High Level Log Key	`<max_null>`, or empty
`Uuid`	Log UUID	`(0x5b1f99cb,0x0,0x3403a8c0,0xc0000000)`
`SequenceNum`	Log Sequence Number	`1`
`Flags`	Internal flags that specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on	`428292`
`Action`	Action performed on this connection	■ `accept` ■ `dropreject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl`
`Origin`	Object name of the Security Gateway that generated this log	`MyGW`

Field Header	Description	Example
IfDir	Traffic direction through interface: ■ < - Outbound (sent by a Security Gateway) ■ > - Inbound (received by a Security Gateway)	■ < ■ >
InterfaceName	Name of the Security Gateway interface, on which this traffic was logged If a Security Gateway performed some internal action (for example, log switch), then the log entry shows daemon	■ eth0 ■ daemon ■ N/A
LogId	Log ID	0
Alert	Alert Type	■ alert ■ mail ■ snmp_trap ■ spoof ■ user_alert ■ user_auth
OriginSicName	SIC name of the Security Gateway that generated this log	CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x
inzone	Inbound Security Zone	Local
outzone	Outbound Security Zone	External
service_id	Name of the service used to inspect this connection	ftp

Field Header	Description	Example
src	Object name or IP address of the connection's source computer	MyHost
dst	Object name or IP address of the connection's destination computer	MyFTPServer
proto	Name of the connection's protocol	tcp
sport_svc	Source port of the connection	64933
ProductName	Name of the Check Point product that generated this log	■ VPN-1 & FireWall-1 ■ Application Control ■ FloodGate-1
ProductFamily	Name of the Check Point product family that generated this log	Network

Examples

Example 1 - Show all log entries with both the date and the time for each log entry

```
fw log -l
```

Example 2 - Show all log entries that start after the specified timestamp

```
[Expert@MyGW:0]# fw log -l -s "June 12, 2018 12:33:00"
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x;
fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host Redirect; fg-1_server_out_rule_name: ;
ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x; inzone:
Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid:
4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_
table: TABLE_END; UP_action_table: TABLE_START; ROW_START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc:
ftp; sport_svc: 64933; ProductFamily: Network;

... ... ...

[Expert@MyGW:0]#
```

Example 3 - Show all log entries between the specified timestamps

```
[Expert@MyGW:0]# fw log -l -b "June 12, 2018 12:33:00" 'June 12, 2018 12:34:00'
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x;
fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host Redirect; fg-1_server_out_rule_name: ;
ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x; inzone:
Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid:
4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_
table: TABLE_END; UP_action_table: TABLE_START; ROW_START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc:
ftp; sport_svc: 64933; ProductFamily: Network;

 12Jun2018 12:33:45 5 N/A 1 ctl MyGW > LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x;
description: Contracts; reason: Could not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on
the gateway.; Severity: 2; status: Failed; version: 1.0; failure_impact: Contracts may be out-of-date; update_service: 1; ProductName: Security
Gateway/Management; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 4 - Show all log entries with action "drop"

```
[Expert@MyGW:0]# fw log -l -c drop
 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x; inzone:
Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid:
4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_
table: TABLE_END; UP_action_table: TABLE_START; ROW_START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc:
ftp; sport_svc: 64933; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 5 - Show all log entries with action "drop", show all field headers, and show log flags

```
[Expert@MyGW:0]# fw log -l -q -w -c drop
 HeaderDateHour: 12Jun2018 12:33:39; ContentVersion: 5; HighLevelLogKey: <max_null>; LogUid: ; SequenceNum: 1; Flags: 428292; Action: drop; Origin:
MyGW; IfDir: <; InterfaceName: eth0; Alert: ; LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x; inzone:
Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid:
4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_
table: TABLE_END; UP_action_table: TABLE_START; ROW_START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc:
ftp; sport_svc: 64933; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 6 - Show only log entries from 0 to 10 (counting from the beginning of the log file)

```
[Expert@MyGW:0]# fw log -l -x 0 -y 10
... ...
[Expert@MyGW:0]#
```

fw logswitch

Description

Switches the current active log file:

1. Closes the current active log file
2. Renames the current active log file
3. Creates a new active log file with the default name

Notes:

- By default, this command switches the active Security log file - `$FWDIR/log/fw.log`
- You can specify to switch the active Audit log file - `$FWDIR/log/fw.adtlog`

Syntax

```
fw [-d] logswitch
      [-audit] [<Name of Switched Log>]
      -h <Target> [[+ | -]<Name of Switched Log>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-audit`	Specifies to switch the active Audit log file (`$FWDIR/log/fw.adtlog`). You can use this parameter only on a Management Server.
`-h <Target>`	Specifies the remote computer, on which to switch the log. **Notes:** ■ The local and the remote computers must have established SIC trust. ■ The remote computer can be a Security Gateway, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed computer by its main IP address or Object Name as configured in SmartConsole.

Parameter	Description
<Name of Switched Log>	Specifies the name of the switched log file. **Notes:** ■ If you do not specify this parameter, then a default name is: `<YYYY-MM-DD_HHMMSS>.log` `<YYYY-MM-DD_HHMMSS>.adtlog` For example, *2018-03-26_174455.log* ■ If you specify the name of the switched log file, then the name of the switch log file is: `<Specified_Log_Name>.log` `<Specified_Log_Name>.adtlog` ■ The log switch operation fails if the specified name for the switched log matches the name of an existing log file. ■ The maximal length of the specified name of the switched log file is 230 characters.
+	Specifies to *copy* the active log from the remote computer to the local computer. **Notes:** ■ If you specify the name of the switched log file, you must write it immediately after *this* + (plus) parameter. ■ The command copies the active log from the remote computer and saves it in the `$FWDIR/log/` directory on the local computer. ■ The default name of the saved log file is: `<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log` For example, *MyGW__2018-03-26_174455.log* ■ If you specify the name of the switched log file, then the name of the saved log file is: `<Gateway_Object_Name>__<Specified_Log_Name>.log` ■ When this command copies the log file from the remote computer, it compresses the file.
-	Specifies to *transfer* the active log from the remote computer to the local computer. **Notes:** ■ The command saves the copied active log file in the `$FWDIR/log/` directory on the local computer and then deletes the switched log file on the remote computer. ■ If you specify the name of the switched log file, you must write it immediately after this - (minus) parameter. ■ The default name of the saved log file is: `<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log` For example, *MyGW__2018-03-26_174455.log* ■ If you specify the name of the switched log file, then the name of the saved log file is: `<Gateway_Object_Name>__<Specified_Log_Name>.log` ■ When this command transfers the log file from the remote computer, it compresses the file. ■ As an alternative, you can use the *"fw fetchlogs" on page 525* command.

Compression

When this command transfers the log files from the remote computer, it compresses the file with the `gzip` command (see RFC 1950 to RFC 1952 for details). The algorithm is a variation of LZ77 method. The compression ratio varies with the content of the log file and is difficult to predict. Binary data are not compressed. Text data, such as user names and URLs, are compressed.

Example - Switching the active Security log on a Security Management Server or Security Gateway

```
[Expert@MGMT:0]# fw logswitch
Log file has been switched to: 2018-06-13_182359.log
[Expert@MGMT:0]#
```

Example - Switching the active Audit log on a Security Management Server

```
[Expert@MGMT:0]# fw logswitch -audit
Log file has been switched to: 2018-06-13_185711.adtlog
[Expert@MGMT:0]#
```

Example - Switching the active Security log on a managed Security Gateway and copying the switched log

```
[Expert@MGMT:0]# fw logswitch -h MyGW +
Log file has been switched to: 2018-06-13_185451.log
[Expert@MGMT:0]#
[Expert@MGMT:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81/fw1/log/fw.log
/opt/CPsuite-R81/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81/fw1/log/fw.log
/opt/CPsuite-R81/fw1/log/2018-06-13_185451.log
[Expert@MyGW:0]#
```

fw lslogs

Description

Shows a list of Security log files (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) residing on the local computer or a remote computer.

Syntax

```
fw [-d] lslogs [-f <Name of Log File 1>] [-f <Name of Log File 2>] ... [-f
<Name of Log File N>] [-e] [-r] [-s {name | size | stime | etime}]
[<Target>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File>`	Specifies the name of the log file to show. Need to specify name only. **Notes:** ■ If the log file name is not specified explicitly, the command shows all Security log files (`$FWDIR/log/*.log`). ■ File names may include `*` and `?` as wildcards (for example, `2019-0?-*`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the "`-f`" parameter for each log file name pattern: `-f <Name of Log File 1> -f <Name of Log File 2> ... -f <Name of Log File N>`
`-e`	Shows an extended file list. It includes the following information for each log file: ■ `Size` - The total size of the log file and its related pointer files ■ `Creation Time` - The time the log file was created ■ `Closing Time` - The time the log file was closed ■ `Log File Name` - The file name
`-r`	Reverses the sort order (descending order).
`-s {name | size | stime | etime}`	Specifies the sort order of the log files using one of the following sort options: ■ `name` - The file name ■ `size` - The file size ■ `stime` - The time the log file was created (this is the default option) ■ `etime` - The time the log file was closed

Parameter	Description
<Target>	Specifies the remote Check Point computer, with which this local Check Point computer has established SIC trust. ■ If you run this command on a Security Management Server or Domain Management Server, then *<Target>* is the applicable object's name or main IP address of the Check Point Computer as configured in SmartConsole. ■ If you run this command on a Security Gateway or Cluster Member, then *<Target>* is the main IP address of the applicable object as configured in SmartConsole.

Example 1 - Default output

```
[Expert@HostName:0]# fw lslogs
     Size Log file name
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.log
         9KB 2019-06-16_000000.log
        10KB 2019-06-17_000000.log
         9KB fw.log
[Expert@HostName:0]#
```

Example 2 - Showing all log files

```
[Expert@HostName:0]# fw lslogs -f "*"
     Size Log file name
         9KB fw.adtlog
         9KB fw.log
         9KB 2019-05-29_000000.adtlog
         9KB 2019-05-29_000000.log
         9KB 2019-05-20_000000.adtlog
         9KB 2019-05-20_000000.log
[Expert@HostName:0]#
```

Example 3 - Showing only log files specified by the patterns

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
         9KB 2019-06-14_000000.adtlog
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 4 - Showing only log files specified by the patterns and their extended information

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
         9KB 2019-06-14_000000.adtlog
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 5 - Showing only log files specified by the patterns, sorting by name in reverse order

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' -e -s name -r
     Size Creation Time Closing Time Log file name
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.log
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.adtlog
         9KB 13Jun2018 18:23:59 14Jun2018 0:00:00 2019-06-14_000000.log
         9KB 13Jun2018 0:00:00 14Jun2018 0:00:00 2019-06-14_000000.adtlog
[Expert@HostName:0]#
```

Example 6 - Showing only log files specified by the patterns, from a managed Security Gateway with main IP address 192.168.3.53

```
[Expert@MGMT:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' 192.168.3.53
     Size Log file name
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
         9KB 2019-06-14_000000.log
         9KB 2019-06-14_000000.adtlog
[Expert@MGMT:0]#
```

fw mergefiles

Description

Merges several Security log files (`$FWDIR/log/*.log`) into a single log file.

Merges several Audit log files (`$FWDIR/log/*.adtlog`) into a single log file.

Important:

- Do not merge the *active* Security file `$FWDIR/log/fw.log` with other Security switched log files.
  Switch the active Security file `$FWDIR/log/fw.log` (with the *"fw logswitch" on page 537* command) and only then merge it with other Security switched log files.
- Do not merge the *active* Audit file `$FWDIR/log/fw.adtlog` with other Audit switched log files.
  Switch the active Audit file `$FWDIR/log/fw.adtlog` (with the *"fw logswitch" on page 537* command) and only then merge it with other Audit switched log files.
- This command unifies logs entries with the same Unique-ID (UID). If you rotate the current active log file before all the segments of a specific log arrive, this command merges the records with the same Unique ID from two different files, into one fully detailed record.
- If the size of the final merged log file exceeds 2GB, this command creates a list of merged files, where the size of each merged file size is not more than 2GB.
  The user receives this warning:

  ```
  Warning: The size of the files you have chosen to merge
  is greater than 2GB. The merge will produce two or more
  files.
  ```

  The names of merged files are:
  - *<Name of Merged Log File>*.log
  - *<Name of Merged Log File>*_1.log
  - *<Name of Merged Log File>*_2.log
  - ... ...
  - *<Name of Merged Log File>*_N.log

Syntax

```
fw [-d] mergefiles {-h | -help}
```

```
fw [-d] mergefiles [-r] [-s] [-t <Time Conversion File>] <Name of Log File
1> <Name of Log File 2> ... <Name of Log File N> <Name of Merged Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`{-h | -help}`	Shows the built-in usage.
`-r`	Removes duplicate entries.
`-s`	Sorts the merged file by the **Time** field in log records.
`-t <Time Conversion File>`	Specifies a full path and name of a file that instructs this command how to adjust the times during the merge. This is required if you merge log files from Log Servers configured with different time zones. The file format is: `<IP Address of Log Server #1> <Signed Date Time #1 in Seconds>` `<IP Address of Log Server #2> <Signed Date Time #2 in Seconds>` `... ...` **Notes** ■ You must specify the absolute path and the file name. ■ The name of the time conversion file cannot exceed 230 characters.
`<Name of Log File 1> ... <Name of Log File N>`	Specifies the log files to merge. **Notes:** ■ You must specify the absolute path and the name of the input log files. ■ The name of the input log file cannot exceed 230 characters.
`<Name of Merged Log File>`	Specifies the output merged log file. **Notes:** ■ The name of the merged log file cannot exceed 230 characters. ■ If a file with the specified name already exists, the command stops and asks you to remove the existing file, or to specify another name. ■ The size of the merged log file cannot exceed 2 GB. In such scenario, the command creates several merged log files, each not exceeding the size limit.

Example - Merging Security log files

```
[Expert@HostName:0]# ls -l $FWDIR/*.log
-rw-rw-r-- 1 admin root 189497 Sep  7 00:00 2019-09-07_000000.log
-rw-rw-r-- 1 admin root  14490 Sep  9 09:52 2019-09-09_000000.log
-rw-rw-r-- 1 admin root  30796 Sep 10 10:56 2019-09-10_000000.log
-rw-rw-r-- 1 admin root  24503 Sep 10 13:08 fw.log
[Expert@HostName:0]#
[Expert@HostName:0]# fw mergefiles -s $FWDIR/2019-09-07_000000.log $FWDIR/2019-09-09_000000.log $FWDIR/2019-
09-10_000000.log /var/log/2019-Sep-Merged.log
[Expert@HostName:0]#
[Expert@HostName:0]# ls -l /var/log/2019-Sep-Merged.log*
-rw-rw---- 1 admin root 213688 Sep 10 13:18 /var/log/2019-Sep-Merged.log
-rw-rw---- 1 admin root   8192 Sep 10 13:18 /var/log/2019-Sep-Merged.logLuuidDB
-rw-rw---- 1 admin root     80 Sep 10 13:18 /var/log/2019-Sep-Merged.logaccount_ptr
-rw-rw---- 1 admin root   2264 Sep 10 13:18 /var/log/2019-Sep-Merged.loginitial_ptr
-rw-rw---- 1 admin root   4448 Sep 10 13:18 /var/log/2019-Sep-Merged.logptr
[Expert@HostName:0]#
```

fw repairlog

Description

Check Point Security log file (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) are databases, with special pointer files.

If these log pointer files become corrupted (which causes the inability to read the log file), this command can rebuild them.

Log File Type	Log File Location	Log Pointer Files
Security log	`$FWDIR/log/*.log`	`*.logptr` `*.logaccount_ptr` `*.loginitial_ptr` `*.logLuuidDB`
Audit log	`$FWDIR/log/*.adtlog`	`*.adtlogptr` `*.adtlogaccount_ptr` `*.adtloginitial_ptr` `*.adtlogLuuidDB`

Syntax

```
fw [-d] repairlog [-u] <Name of Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Specifies to rebuild the unification chains in the log file.
<Name of Log File>	The name of the log file to repair.

Example - Repairing the Audit log file

```
fw repairlog -u 2019-06-17_000000.adtlog
```

fw sam

Description

Manages the Suspicious Activity Monitoring (SAM) rules. You can use the SAM rules to block connections to and from IP addresses without the need to change or reinstall the Security Policy. For more information, see sk112061.

You can create the Suspicious Activity Rules in two ways:

- In SmartConsole from Monitoring Results
- In CLI with the `fw sam` command

Notes:

- VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam_policy" on page 553* and *"sam_alert" on page 635* commands.
- SAM rules consume some CPU resources on Security Gateway.

  > **Best Practice** - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.
- Logs for enforced SAM rules (configured with the `fw sam` command) are stored in the `$FWDIR/log/sam.dat` file.
  By design, the file is purged when the number of stored entries reaches 100,000.
  This data log file contains the records in one of these formats:

`<type>,<actions>,<expire>,<ipaddr>`
`<type>,<actions>,<expire>,<src>,<dst>,<dport>,<ip_p>`

- SAM Requests are stored on the Security Gateway in the kernel table `sam_requests`.
- IP Addresses that are blocked by SAM rules, are stored on the Security Gateway in the kernel table `sam_blocked_ips`.

Note - To configure SAM Server settings for a Security Gateway or Cluster:

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server.
2. From the left navigation panel, click Gateways & Servers.
3. Open the Security Gateway or Cluster object.
4. From the left tree, click **Other > SAM**.
5. Configure the settings.
6. Click **OK**.
7. Install the Access Control Policy on this Security Gateway or Cluster object.

Syntax

- **To add or cancel a SAM rule according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM Server>] [-f
<Security Gateway>] [-t <Timeout>] [-l <Log Type>] [-C] [-e <key=val>]+
[-r] -{n|i|I|j|J} <Criteria>
```

- **To delete all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM Server>] [-f
<Security Gateway>] -D
```

- **To monitor all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM Server>] [-f
<Security Gateway>] [-r] -M -{i|j|n|b|q} all
```

- **To monitor SAM rules according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM Server>] [-f
<Security Gateway>] [-r] -M -{i|j|n|b|q} <Criteria>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-v`	Enables verbose mode. In this mode, the command writes one message to *stderr* for each Security Gateway, on which the command is enforced. These messages show whether the command was successful or not.
`-s <SAM Server>`	Specifies the IP address (in the X.X.X.X format) or resolvable HostName of the Security Gateway that enforces the command. The default is `localhost`.
`-S <SIC Name of SAM Server>`	Specifies the SIC name for the SAM server to be contacted. It is expected that the SAM server has this SIC name, otherwise the connection fails.  **Notes:** ■ If you do not explicitly specify the SIC name, the connection continues without SIC names comparison. ■ For more information about enabling SIC, refer to the OPSEC API Specification. ■ On VSX Gateway, run the *fw vsx showncs -vs <VSID>* command to show the SIC name for the applicable Virtual System.

Parameter	Description
`-f <Security Gateway>`	Specifies the Security Gateway, on which to enforce the action. `<Security Gateway>` can be one of these: ■ *All* - Default. Specifies to enforce the action on all managed Security Gateways, where SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *localhost* - Specifies to enforce the action on this local Check Point computer (on which the `fw sam` command is executed). You can use this syntax only on Security Gateway or StandAlone. ■ *Gateways* - Specifies to enforce the action on all objects defined as Security Gateways, on which SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Security Gateway object* - Specifies to enforce the action on this specific Security Gateway object. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Group object* - Specifies to enforce the action on all specific Security Gateways in this Group object.  **Notes:** ■ You can use this syntax only on Security Management Server or Domain Management Server. ■ VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
`-D`	Cancels all inhibit ("`-i`", "`-j`", "`-I`", "`-J`") and notify ("`-n`") parameters.  **Notes:** ■ To "uninhibit" the inhibited connections, run the `fw sam` command with the "`-C`" or "`-D`" parameters. ■ It is also possible to use this command for active SAM requests.
`-C`	Cancels the `fw sam` command to inhibit connections with the specified parameters.  **Notes:** ■ These connections are no longer inhibited (no longer rejected or dropped). ■ The command parameters must match the parameters in the original `fw sam` command, except for the `-t <Timeout>` parameter.
`-t <Timeout>`	Specifies the time period (in seconds), during which the action is enforced. The default is forever, or until you cancel the `fw sam` command.
`-l <Log Type>`	Specifies the type of the log for enforced action: ■ `nolog` - Does not generate Log / Alert at all ■ `short_noalert` - Generates a Log ■ `short_alert` - Generates an Alert ■ `long_noalert` - Generates a Log ■ `long_alert` - Generates an Alert (this is the default)

Parameter	Description
`-e <key=val>+`	Specifies rule information based on the keys and the provided values. Multiple keys are separated by the plus sign (+). Available keys are (each is limited to 100 characters): ■ `name` - Security rule name ■ `comment` - Security rule comment ■ `originator` - Security rule originator's username
`-r`	Specifies not to resolve IP addresses.
`-n`	Specifies to generate a "Notify" long-format log entry.  **Notes:** ■ This parameter generates an alert when connections that match the specified services or IP addresses pass through the Security Gateway. ■ This action does not inhibit / close connections.
`-i`	Inhibits (drops or rejects) new connections with the specified parameters.  **Notes:** ■ Each inhibited connection is logged according to the log type. ■ Matching connections are rejected.
`-I`	Inhibits (drops or rejects) new connections with the specified parameters, and closes all existing connections with the specified parameters.  **Notes:** ■ Matching connections are rejected. ■ Each inhibited connection is logged according to the log type.
`-j`	Inhibits (drops or rejects) new connections with the specified parameters.  **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-J`	Inhibits new connections with the specified parameters, and closes all existing connections with the specified parameters.  **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-b`	Bypasses new connections with the specified parameters.
`-q`	Quarantines new connections with the specified parameters.
`-M`	Monitors the active SAM requests with the specified actions and criteria.
`all`	Gets all active SAM requests. This is used for monitoring purposes only.

Parameter	Description
<Criteria>	Criteria are used to match connections. The criteria and are composed of various combinations of the following parameters: ■ Source IP Address ■ Source Netmask ■ Destination IP Address ■ Destination Netmask ■ Port (see *IANA Service Name and Port Number Registry*) ■ Protocol Number (see *IANA Protocol Numbers*) Possible combinations are (see the explanations below this table): ■ `src <IP>` ■ `dst <IP>` ■ `any <IP>` ■ `subsrc <IP> <Netmask>` ■ `subdst <IP> <Netmask>` ■ `subany <IP> <Netmask>` ■ `srv <Src IP> <Dest IP> <Port> <Protocol>` ■ `subsrv <Src IP> <Src Netmask> <Dest IP> <Dest Netmask> <Port> <Protocol>` ■ `subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>` ■ `subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>` ■ `dstsrv <Dest IP> <Port> <Protocol>` ■ `subdstsrv <Dest IP> <Dest Netmask> <Port> <Protocol>` ■ `srcpr <IP> <Protocol>` ■ `dstpr <IP> <Protocol>` ■ `subsrcpr <IP> <Netmask> <Protocol>` ■ `subdstpr <IP> <Netmask> <Protocol>` ■ `generic <key=val>`

Explanation for the *<Criteria>* syntax

Parameter	Description
`src <IP>`	Matches the Source IP address of the connection.
`dst <IP>`	Matches the Destination IP address of the connection.
`any <IP>`	Matches either the Source IP address or the Destination IP address of the connection.
`subsrc <IP> <Netmask>`	Matches the Source IP address of the connections according to the netmask.
`subdst <IP> <Netmask>`	Matches the Destination IP address of the connections according to the netmask.

Parameter	Description
`subany <IP> <Netmask>`	Matches either the Source IP address or Destination IP address of connections according to the netmask.
`srv <Src IP> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol.
`subsrv <Src IP> <Netmask> <Dest IP> <Netmask> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol. Source and Destination IP addresses are assigned according to the netmask.
`subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, source netmask, destination netmask, Service (port number) and Protocol.
`subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>`	Matches specific Source IP address, Destination IP, destination netmask, Service (port number) and Protocol.
`dstsrv <Dest IP> <Service> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol.
`subdstsrv <Dest IP> <Netmask> <Port> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol. Destination IP address is assigned according to the netmask.
`srcpr <IP> <Protocol>`	Matches the Source IP address and protocol.
`dstpr <IP> <Protocol>`	Matches the Destination IP address and protocol.
`subsrcpr <IP> <Netmask> <Protocol>`	Matches the Source IP address and protocol of connections. Source IP address is assigned according to the netmask.
`subdstpr <IP> <Netmask> <Protocol>`	Matches the Destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.
`generic <key=val>+`	Matches the GTP connections based on the specified keys and provided values. Multiple keys are separated by the plus sign (+). Available keys are: ■ `service=gtp` ■ `imsi` ■ `msisdn` ■ `apn` ■ `tunl_dst` ■ `tunl_dport` ■ `tunl_proto`

fw sam_policy

Description

Manages the Suspicious Activity Policy editor that works with these types of rules:

- Suspicious Activity Monitoring (SAM) rules.

  See sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rules.

- Rate Limiting rules.

  See sk112454: How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 547*
- *"sam_alert" on page 635*

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

>

Syntax for IPv4

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Syntax for IPv6

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`add <options>`	Adds one Rate Limiting rule one at a time. See *"fw sam_policy add" on page 555*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 567*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 569*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 572*.

fw sam_policy add

Description

The "*fw sam_policy add*" and "*fw6 sam_policy add*" commands:

- Add one Suspicious Activity Monitoring (SAM) rule at a time.
- Add one Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>] [-f
<Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule Originator">]
[-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>] [-f
<Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule Originator">]
[-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>] [-f
<Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule Originator">]
[-z "<Zone>"] quota <Quota Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>] [-f
<Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule Originator">]
[-z "<Zone>"] quota <Quota Filter Arguments
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Optional. Specifies that the rule category is `User-defined`. Default rule category is `Auto`.
`-a {d | n | b}`	Mandatory. Specifies the rule action if the traffic matches the rule conditions: ■ `d` - Drop the connection. ■ `n` - Notify (generate a log) about the connection and let it through. ■ `b` - Bypass the connection - let it through without checking it against the policy rules. **Note** - Rules with action set to *Bypass* cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.
`-l {r | a}`	Optional. Specifies which type of log to generate for this rule for all traffic that matches: ■ `-r` - Generate a regular log ■ `-a` - Generate an alert log
`-t <Timeout>`	Optional. Specifies the time period (in seconds), during which the rule will be enforced. Default timeout is indefinite.
`-f <Target>`	Optional. Specifies the target Security Gateways, on which to enforce the Rate Limiting rule. `<Target>` can be one of these: ■ `all` - This is the default option. Specifies that the rule should be enforced on all managed Security Gateways. ■ Name of the Security Gateway or Cluster object - Specifies that the rule should be enforced only on this Security Gateway or Cluster object (the object name must be as defined in the SmartConsole). ■ Name of the Group object - Specifies that the rule should be enforced on all Security Gateways that are members of this Group object (the object name must be as defined in the SmartConsole).

Parameter	Description
`-n "<Rule Name>"`	Optional. Specifies the name (label) for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`
`-c "<Rule Comment>"`	Optional. Specifies the comment for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`
`-o "<Rule Originator>"`	Optional. Specifies the name of the originator for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	Optional. Specifies the name of the Security Zone for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters.
`ip <IP Filter Arguments>`	Mandatory (use this `ip` parameter, or the `quota` parameter). Configures the *Suspicious Activity Monitoring (SAM)* rule. Specifies the IP Filter Arguments for the SAM rule (you must use at least one of these options): `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` See the explanations below.

Parameter	Description
`quota <Quota Filter Arguments>`	Mandatory (use this `quota` parameter, or the `ip` parameter). Configures the *Rate Limiting* rule. Specifies the Quota Filter Arguments for the Rate Limiting rule (see the explanations below): ■ `[flush true]` ■ `[source-negated {true | false}] source <Source>` ■ `[destination-negated {true | false}] destination <Destination>` ■ `[service-negated {true | false}] service <Protocol and Port numbers>` ■ `[<Limit1 Name> <Limit1 Value>] [<Limit2 Name> <Limit2 Value>] ...[<LimitN Name> <LimitN Value>]` ■ `[track <Track>]`  **Important:** ■ The Quota rules are not applied immediately to the Security Gateway. They are only registered in the Suspicious Activity Monitoring (SAM) policy database. To apply all the rules from the SAM policy database immediately, add "`flush true`" in the `fw samp add` command syntax. ■ Explanation: For new connections rate (and for any rate limiting in general), when a rule's limit is violated, the Security Gateway also drops all packets that match the rule. The Security Gateway computes new connection rates on a per-second basis. At the start of the 1-second timer, the Security Gateway allows all packets, including packets for existing connections. If, at some point, during that 1 second period, there are too many new connections, then the Security Gateway blocks all remaining packets for the remainder of that 1-second interval. At the start of the next 1-second interval, the counters are reset, and the process starts over - the Security Gateway allows packets to pass again up to the point, where the rule's limit is violated.

Explanation for the *IP Filter Arguments* syntax for Suspicious Activity Monitoring (SAM) rules

Argument	Description
`-C`	Specifies that open connections should be closed.
`-s <Source IP>`	Specifies the Source IP address.
`-m <Source Mask>`	Specifies the Source subnet mask (in dotted decimal format - x.y.z.w).
`-d <Destination IP>`	Specifies the Destination IP address.
`-M <Destination Mask>`	Specifies the Destination subnet mask (in dotted decimal format - x.y.z.w).
`-p <Port>`	Specifies the port number (see *IANA Service Name and Port Number Registry*).
`-r <Protocol>`	Specifies the protocol number (see *IANA Protocol Numbers*).

Explanation for the *Quota Filter Arguments* syntax for Rate Limiting rules

Argument	Description
`flush true`	Specifies to compile and load the quota rule to the SecureXL immediately.
`[source-negated {true | false}] source <Source>`	Specifies the source type and its value: ■ `any` The rule is applied to packets sent from all sources. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent from: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:....:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent from: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the source IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the source IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `source-negated false` ■ The `source-negated true` processes all source types, *except* the specified type.

Argument	Description
`[destination-negated {true | false}] destination <Destination>`	Specifies the destination type and its value: ■ `any` The rule is applied to packets sent to all destinations. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent to: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent to: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the destination IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the destination IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `destination-negated false` ■ The `destination-negated true` will process all destination types except the specified type

Argument	Description
`[service-negated {true | false}] service <Protocol and Port numbers>`	Specifies the Protocol number (see *IANA Protocol Numbers*) and Port number (see *IANA Service Name and Port Number Registry*): ■ `<Protocol>` IP protocol number in the range 1-255 ■ `<Protocol Start>-<Protocol End>` Range of IP protocol numbers ■ `<Protocol>/<Port>` IP protocol number in the range 1-255 and TCP/UDP port number in the range 1-65535 ■ `<Protocol>/<Port Start>-<Port End>` IP protocol number and range of TCP/UDP port numbers from 1 to 65535 **Notes:** ■ Default is: `service-negated false` ■ The `service-negated true` will process all traffic except the traffic with the specified protocols and ports

Argument	Description
`[<Limit 1 Name> <Limit 1 Value>] [<Limit 2 Name> <Limit 2 Value>] ... [<Limit N Name> <Limit N Value>]`	Specifies quota limits and their values. **Note** - Separate multiple quota limits with spaces. ■ `concurrent-conns <Value>` Specifies the maximal number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximal ratio of the *concurrent-conns* value to the total number of active connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `pkt-rate <Value>` Specifies the maximum number of packets per second that match this rule. ■ `pkt-rate-ratio <Value>` Specifies the maximal ratio of the *pkt-rate* value to the rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `byte-rate <Value>` Specifies the maximal total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximal ratio of the *byte-rate* value to the bytes per second rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `new-conn-rate <Value>` Specifies the maximal number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximal ratio of the *new-conn-rate* value to the rate of all connections per second through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`).
`[track <Track>]`	Specifies the tracking option: ■ `source` Counts connections, packets, and bytes for specific source IP address, and not cumulatively for this rule. ■ `source-service` Counts connections, packets, and bytes for specific source IP address, and for specific IP protocol and destination port, and not cumulatively for this rule.

Examples

Example 1 - Rate Limiting rule with a range

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

Explanations:

- This rule drops packets for all connections (`-a d`) that exceed the quota set by this rule, including packets for existing connections.
- This rule logs packets (`-l r`) that exceed the quota set by this rule.
- This rule will expire in 3600 seconds (`-t 3600`).
- This rule limits the rate of creation of new connections to 5 connections per second (`new-conn-rate 5`) for any traffic (`service any`) from the source IP addresses in the range 172.16.7.11 - 172.16.7.13 (`source range:172.16.7.11-172.16.7.13`).

  Note - The limit of the total number of log entries per second is configured with the *fwaccel dos config set -n <rate>* command.
- This rule will be compiled and loaded on the SecureXL, together with other rules in the Suspicious Activity Monitoring (SAM) policy database immediately, because this rule includes the "`flush true`" parameter.

Example 2 - Rate Limiting rule with a service specification

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

Explanations:

- This rule logs and lets through all packets (`-a n`) that exceed the quota set by this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all packets except (`service-negated true`) the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53 (`service 1,50-51,6/443,17/53`).
- This rule applies to all packets from source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule does not let any traffic through (`byte-rate 0`) except the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 3 - Rate Limiting rule with ASN

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the Autonomous System number 64500 (`asn:AS64500`).
- This rule applies to packets from source IPv6 addresses FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`).
- This rule applies to all traffic (`service any`).
- This rule does not let any traffic through (`pkt-rate 0`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 4 - Rate Limiting rule with whitelist

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

Explanations:

- This rule bypasses (`-a b`) all packets that match this rule.

  Note - The Access Control Policy and other types of security policy rules still apply.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the source IP addresses in the range 172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`).
- This rule applies to packets sent to TCP port 80 (`service 6/80`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 5 - Rate Limiting rule with tracking

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not log any packets (the `-l r` parameter is not specified).
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all traffic (`service any`).
- This rule applies to all sources except (`source-negated true`) the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule limits the maximal number of concurrent active connections to 655/65536=~1% (`concurrent-conns-ratio 655`) for any traffic (`service any`) except (`service-negated true`) the connections from the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule counts connections, packets, and bytes for traffic only from sources that match this rule, and not cumulatively for this rule.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

fw sam_policy batch

Description

The "*fw sam_policy batch*" and "*fw6 sam_policy batch*" commands:

- Add and delete many Suspicious Activity Monitoring (SAM) rules at a time.
- Add and delete many Rate Limiting rules at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Procedure

1. **Start the batch mode**

   - For IPv4, run:

     ```
     fw sam_policy batch << EOF
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy batch << EOF
     ```

2. **Enter the applicable commands**

   - Enter one "`add`" or "`del`" command on each line, on as many lines as necessary.

     Start each line with only "`add`" or "`del`" parameter (not with "`fw samp`").

- Use the same set of parameters and values as described in these commands:
  - *"fw sam_policy add" on page 555*
  - *"fw sam_policy del" on page 569*
- Terminate each line with a Return (ASCII 10 - Line Feed) character (press Enter).

3. **End the batch mode**

   Type `EOF` and press Enter.

Example of a Rate Limiting rule for IPv4

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota service any source
range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

Description

The "*fw sam_policy del*" and "*fw6 sam_policy del*" commands:

- Delete one configured Suspicious Activity Monitoring (SAM) rule at a time.
- Delete one configured Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy del '<Rule UID>'
```

Syntax for IPv6

```
fw6 [-d] sam_policy del '<Rule UID>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`'<Rule UID>'`	Specifies the UID of the rule you wish to delete.  **Important:** ■ The quote marks and angle brackets (`'<...>'`) are mandatory. ■ To see the Rule UID, run the *"fw sam_policy get" on page 572* command.

Procedure

1. **List all the existing rules in the Suspicious Activity Monitoring policy database**

   List all the existing rules in the Suspicious Activity Monitoring policy database.

   - For IPv4, run:

     ```
     fw sam_policy get
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy get
     ```

   The rules show in this format:

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=... originator=
   ... src_ip_addr=... req_tpe=...
   ```

   Example for IPv4:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all
   timeout=300 action=notify log=log name=Test\ Rule comment=Notify\
   about\ traffic\ from\ 1.1.1.1 originator=John\ Doe src_ip_
   addr=1.1.1.1 req_tpe=ip
   ```

2. **Delete a rule from the list by its UID**

   - For IPv4, run:

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - For IPv6, run:

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   Example for IPv4:

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **Add the flush-only rule**

   - For IPv4, run:

     ```
     fw samp add -t 2 quota flush true
     ```

   - For IPv6, run:

     ```
     fw6 samp add -t 2 quota flush true
     ```

   Explanation:

   The "`fw samp del`" and "`fw6 samp del`" commands only remove a rule from the persistent database. The Security Gateway continues to enforce the deleted rule until the next time you compiled and load a policy. To force the rule deletion immediately, you must enter a flush-only rule right after the "`fw samp del`" and "`fw6 samp del`" command. This flush-only rule immediately deletes the rule you specified in the previous step, and times out in 2 seconds.

   > **Best Practice** - Specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

fw sam_policy get

Description

The "*fw sam_policy get*" and "*fw6 sam_policy get*" commands:

- Show all the configured Suspicious Activity Monitoring (SAM) rules.
- Show all the configured Rate Limiting rules.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t <Type> [+{-v
'<Value>'}] [-n]]
```

Syntax for IPv6

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t <Type> [+{-v
'<Value>'}] [-n]]
```

Parameters

Note - All these parameters are optional.

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Controls how to print the rules: ■ In the default format (without "`-l`"), the output shows each rule on a separate line. ■ In the list format (with "`-l`"), the output shows each parameter of a rule on a separate line. ■ See *"fw sam_policy add" on page 555*.
`-u '<Rule UID>'`	Prints the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets ('<...>') are mandatory.
`-k '<Key>'`	Prints the rules with the specified predicate key. The quote marks are mandatory.
`-t <Type>`	Prints the rules with the specified predicate type. For Rate Limiting rules, you must always use "`-t in`".
`+{-v '<Value>'}`	Prints the rules with the specified predicate values. The quote marks are mandatory.
`-n`	Negates the condition specified by these predicate parameters: ■ `-k` ■ `-t` ■ `+-v`

Examples

Example 1 - Output in the default format

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify log=log
name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe src_ip_addr=1.1.1.1
req_tpe=ip
```

Example 2 - Output in the list format

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

Example 3 - Printing a rule by its Rule UID

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify log=log
name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe src_ip_addr=1.1.1.1
req_tpe=ip
```

Example 4 - Printing rules that match the specified filters

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13
new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source
cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ concurrent-conns-
ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite action=drop
service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655 track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop log=log
service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite action=bypass
source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite action=notify
log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite action=bypass
source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite action=notify
log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite action=drop
service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655 track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite action=notify
log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop log=log
service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite action=bypass
source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite action=drop
service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655 track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite action=notify
log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop log=log
service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite action=drop
service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655 track=source req_type=quota
[Expert@HostName:0]#
```

fwm

Description

Performs various management operations and shows various management information.

Notes:

- For debug instructions, see the description of the `fwm` process in sk97638.
- On a Multi-Domain Server, you must run these commands in the context of the applicable Domain Management Server.

Syntax

```
fwm [-d]
      dbload <options>
      exportcert <options>
      fetchfile <options>
      fingerprint <options>
      getpcap <options>
      ikecrypt <options>
      load [<options>]
      logexport <options>
      mds <options>
      printcert <options>
      sic_reset
      snmp_trap <options>
      unload [<options>]
      ver [<options>]
      verify <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`dbload <options>`	Downloads the user database and network objects information to the specified targets See *"fwm dbload" on page 578*.
`exportcert <options>`	Export a SIC certificate of the specified object to file. See *"fwm exportcert" on page 579*.

Parameter	Description
`fetchfile <options>`	Fetches a specified OPSEC configuration file from the specified source computer. See *"fwm fetchfile" on page 580*.
`fingerprint <options>`	Shows the Check Point fingerprint. See *"fwm fingerprint" on page 581*.
`getpcap <options>`	Fetches the IPS packet capture data from the specified Security Gateway. See *"fwm getpcap" on page 583*.
`ikecrypt <options>`	Encrypts a secret with a key. See *"fwm ikecrypt" on page 584*.
`load <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 622* command to load a policy to a managed Security Gateway. See *"fwm load" on page 585*.
`logexport <options>`	Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file. See *"fwm logexport" on page 586*.
`mds <options>`	Shows information and performs various operations on Multi-Domain Server. See *"fwm mds" on page 591*.
`printcert <options>`	Shows a SIC certificate's details. See *"fwm printcert" on page 592*.
`sic_reset`	Resets SIC on the Management Server. See *"fwm sic_reset" on page 596*.
`snmp_trap <options>`	Sends an SNMP Trap to the specified host. See *"fwm snmp_trap" on page 597*.
`unload <options>`	Unloads the policy from the specified managed Security Gateways. See *"fwm unload" on page 599*.
`ver <options>`	Shows the Check Point version of the Management Server. See *"fwm ver" on page 602*.
`verify <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 622* command to verify a policy. See *"fwm verify" on page 603*.

fwm dbload

Description

Downloads the user database and network objects information to the specified Security Gateways.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] dbload
      -a
      -c <Configuration File>
      <GW1> <GW2> ... <GWN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-a`	Executes commands on all targets specified in the default system configuration file - `$FWDIR/conf/sys.conf`. Note - You must manually create this file.
`-c <Configuration File>`	Specifies the OPSEC configuration file to use. Note - You must manually create this file.
`<GW1> <GW2> ... <GWN>`	Executes commands on the specified Security Gateways.  **Notes:** ■ Enter the main IP address or Name of the Security Gateway object as configured in SmartConsole. ■ If you do not explicitly specify the Security Gateway, the database is downloaded to `localhost`.

fwm exportcert

Description

Export a SIC certificate of the specified managed object to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] exportcert -obj <Name of Object> -cert <Name of CA> -file <Output File> [-withroot] [-pem]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Name of Object>	Specifies the name of the managed object, whose certificate you wish to export.
<Name of CA>	Specifies the name of Certificate Authority, whose certificate you wish to export.
<Output File>	Specifies the name of the output file.
`-withroot`	Exports the certificate's root in addition to the certificate's content.
`-pem`	Save the exported information in a text file. Default is to save in a binary file.

fwm fetchfile

Description

Fetches a specified OPSEC configuration file from the specified source computer.

This command supports only the `fwopsec.conf` or `fwopsec.v4x` files.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fetchfile -r <File> [-d <Local Path>] <Source>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-r <File>`	Specifies the relative `fw1` directory. This command supports only these files: ■ `conf/fwopsec.conf` ■ `conf/fwopsec.v4x`
`-d <Local Path>`	Specifies the local directory to save the fetched file.
`<Source>`	Specifies the managed remote source computer, from which to fetch the file. **Note** - The local and the remote source computers must have established SIC trust.

Example

```
[Expert@MGMT:0]# fwm fetchfile -r "conf/fwopsec.conf" -d /tmp 192.168.3.52
Fetching conf/fwopsec.conf from 192.168.3.52...
Done
[Expert@MGMT:0]#
```

fwm fingerprint

Description

Shows the Check Point fingerprint.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fingerprint [-d]
      <IP address of Target> <SSL Port>
      localhost <SSL Port>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The debug options are: ■ `fwm -d` Runs the complete debug of all `fwm` actions. For complete debug instructions, see the description of the `fwm` process in sk97638. ■ `fingerprint -d` Runs the debug only for the fingerprint actions.
<IP address of Target>	Specifies the IP address of a remote managed computer.
<SSL Port>	Specifies the SSL port number. The default is 443.

Example 1 - Showing the fingerprint on the local Management Server

```
[Expert@MGMT:0]# fwm fingerprint localhost 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email Address,CN=192.168.3.51,L=Locality Name
(eg\, city)
#FINGER 11:A6:F7:1F:B9:F5:15:BC:F9:7B:5F:DC:28:FC:33:C5
##
[Expert@MGMT:0]#
```

Example 2 - Showing the fingerprint from a managed Security Gateway

```
[Expert@MGMT:0]# fwm fingerprint 192.168.3.52 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email Address,CN=192.168.3.52,L=Locality Name
(eg\, city)
#FINGER 5C:8E:4D:B9:B4:3A:58:F3:79:18:F1:70:99:8B:5F:2B
##
[Expert@MGMT:0]#
```

fwm getpcap

Description

Fetches the IPS packet capture data from the specified Security Gateway.

This command only works with IPS packet captures stored on the Security Gateway in the `$FWDIR/log/captures_repository/` directory.

This command does not work with other Software Blades, such as Anti-Bot and Anti-Virus that store packet captures in the `$FWDIR/log/blob/` directory on the Security Gateway.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] getpcap -g <Security Gateway> -u '{<Capture UID>}' -p <Local Path>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-g <Security Gateway>`	Specifies the main IP address or Name of Security Gateway object as configured in SmartConsole.
`-u '{<Capture UID>}'`	Specifies the Unique ID of the packet capture file. To see the Unique ID of the packet capture file, open the applicable log file in **SmartConsole > Logs & Monitor > Logs**.
`-p <Local Path>`	Specifies the local path to save the specified packet capture file. If you do not specify the local directory explicitly, the command saves the packet capture file in the current working directory.

Example

```
[Expert@MGMT:0]# fwm getpcap -g 192.168.162.1 -u '{0x4d79dc02,0x10000,0x220da8c0,0x1ffff}' /var/log/
[Expert@MGMT:0]#
```

fwm ikecrypt

Description

Encrypts the password of an Endpoint VPN Client user using IKE. The resulting string must then be stored in the LDAP database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ikecrypt <Key> <Password>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Key>	Specifies the IKE Key as defined in the **LDAP Account Unit** properties window on the **Encryption** tab.
<Password>	Specifies the password for the Endpoint VPN Client user.

Example

```
[Expert@MGMT:0]# fwm ikecrypt MySecretKey MyPassword
OUQJHiNHCj6HJGH8ntnKQ7tg
[Expert@MGMT:0]#
```

fwm load

Description

Loads a policy on a managed Security Gateway.

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 622* command to load a policy on a managed Security Gateway.

fwm logexport

Description

Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm logexport -h
```

```
fwm [-d] logexport [{-d <Delimiter> | -s}] [-t <Table Delimiter>] [-i
<Input File>] [-o <Output File>] [{-f | -e}] [-x <Start Entry Number>] [-y
<End Entry Number>] [-z] [-n] [-p] [-a] [-u <Unification Scheme File>] [-m
{initial | semi | raw}]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-d <Delimiter> | -s`	Specifies the output delimiter between fields of log entries: ■ `-d <Delimiter>` - Uses the specified delimiter. ■ `-s` - Uses the ASCII character #255 (non-breaking space) as the delimiter. **Note** - If you do not specify the delimiter explicitly, the default is a semicolon (`;`).
`-t <Table Delimiter>`	Specifies the output delimiter inside table field. Table field would look like: *ROWx:COL0,ROWx:COL1,ROWx:COL2*, and so on **Note** - If you do not specify the table delimiter explicitly, the default is a comma (`,`).

Parameter	Description
`-i <Input File>`	Specifies the name of the input log file. **Notes:** ■ This command supports only Security log file (`$FWDIR/log/*.log`) and Audit log file (`$FWDIR/log/*.adtlog`) ■ If you do not specify the input log file explicitly, the command processes the active Security log file `$FWDIR/log/fw.log`
`-o <Output File>`	Specifies the name of the output file. **Note** - If you do not specify the output log file explicitly, the command prints its output on the screen.
`-f`	After reaching the end of the currently opened log file, specifies to continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-e`	After reaching the end of the currently opened log file, continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-x <Start Entry Number>`	Starts exporting the log entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Starts exporting the log entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), specifies to continue the export of log entries. The default behavior is to stop.
`-n`	Specifies not to perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.
`-p`	Specifies to not to perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-a`	Exports only Account log entries.
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`

Parameter	Description
`-m {initial | semi | raw}`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command exports one unified log entry for each ID. This is the default. If you also specify the "`-f`" parameter, then the output does not export any updates, but exports only entries that relate to the start of new connections. To export updates as well, use the "`semi`" parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, exports entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. Exports all log entries.

The output of the `fwm logexport` command appears in tabular format.

The first row lists the names of all log fields included in the log entries.

Each of the next rows consists of a single log entry, whose fields are sorted in the same order as the first row.

If a log entry has no information in a specific field, this field remains empty (as indicated by two successive semi-colons "*;;*").

You can control which log fields appear in the output of the command output:

Step	Instructions
1	Create the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# touch $FWDIR/conf/logexport.ini`
2	Edit the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# vi $FWDIR/conf/logexport.ini`
3	To include or exclude the log fields from the output, add these lines in the configuration file: `[Fields_Info]` `included_fields = field1,field2,field3,<REST_OF_FIELDS>,field100` `excluded_fields = field10,field11` Where: ■ You can specify only the `included_fields` parameter, only the `excluded_fields` parameter, or both. ■ The `num` field must always appear first. You cannot manipulate this field. ■ The `<REST_OF_FIELDS>` is an optional reserved token that refers to a list of fields. • If you specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on a list of fields from the `$FWDIR/conf/logexport_default.C` file. • If you do not specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on the input log file.
4	Save the changes in the file and exit the Vi editor.
5	Export the logs: `fwm logexport <options>`

Example 1 - Exporting all log entries

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_name;fg-1_
client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
0;13Jun2018;19:47:54;CXL1_192.168.3.52;control; ;;daemon;inbound;VPN-1 & FireWall-1;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_Server.checkpoint.com.s6t98x;5;18446744073709551615;2;Log file has been switched to:
MyLog.log;Network;;;;;;;;;;;
1;13Jun2018;19:47:54;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;;;;;;;;;;
... ...
35;13Jun2018;19:55:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host Redirect;;;;;;;;;
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>;1;;;
... ...
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the
gateway.;2;Contracts may be out-of-date
... ...
[Expert@MGMT:0]#
```

Example 2 - Exporting only log entries with specified numbers

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log -x 36 -y 47
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_name;fg-1_
client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>;1;;;
37;13Jun2018;19:56:06;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;2;;Network;Default;Default;Host Redirect;;;;;;;;;
... ...
46;13Jun2018;19:56:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host Redirect;;;;;;;;;
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the
gateway.;2;Contracts may be out-of-date
[Expert@MGMT:0]#
```

fwm mds

Description

- Shows the Check Point version of the Multi-Domain Server.
- Rebuilds status tree for Global VPN Communities.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

```
mdsenv
```

- In the context of a Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] mds
      ver
      rebuild_global_communities_status {all | missing}
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`ver`	Shows the Check Point version of the Multi-Domain Server.
`rebuild_global_communities_status`	Rebuilds status tree for Global VPN Communities: ■ `all` - Rebuilds status tree for all Global VPN Communities. ■ `missing` - Rebuild status tree only for Global VPN Communities that do not have status trees.

Example

```
[Expert@MDS:0]# fwm mds ver
This is Check Point Multi-Domain Security Management R81 - Build 11
[Expert@MDS:0]#
```

fwm printcert

Description

Shows a SIC certificate's details.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] printcert
      -obj <Name of Object> [-cert <Certificate Nick Name>] [-verbose]
      -ca <CA Name> [-x509 <Name of File> [-p]] [-verbose]
      -f <Name of Binary Certificate File> [-verbose]
```

Parameters

Item	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-obj <Name of Object>`	Specifies the name of the managed object, for which to show the SIC certificate information.
`-cert <Certificate Nick Name>`	Specifies the certificate nick name.
`-ca <CA Name>`	Specifies the name of the Certificate Authority. **Note** - Check Point CA Name is `internal_ca`.
`-x509 <Name of File>`	Specifies the name of the X.509 file.
`-p`	Specifies to show the SIC certificate as a text file.
`-f <Name of Binary Certificate File>`	Specifies the binary SIC certificate file to show.
`-verbose`	Shows the information in verbose mode.

Examples

Example 1 - Showing the SIC certificate of a Management Server

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca
Subject: O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Apr 8 13:41:00 2018 Local Time
Not Valid After: Fri Jan 1 05:14:07 2038 Local Time
Serial No.: 1
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Key Usage:
        digitalSignature
        keyCertSign
        cRLSign
Basic Constraint:
        is CA
MD5 Fingerprint:
   7B:F9:7B:4C:BD:40:B9:1C:AB:2C:AE:CF:66:2E:E7:06
SHA-1 Fingerprints:
1. A6:43:3A:2B:1A:04:7F:A6:36:A6:2C:78:BF:22:D9:BC:F7:7E:4D:73
2. KEYS HEM GERM PIT ABUT ROVE RAW PA IQ FAWN NUT SLAM
[Expert@MGMT:0]#
```

Example 2 - Showing the SIC certificate of a Management Server in verbose mode

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca -verbose
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: called
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: closing existing database
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] do_links_getver: strncmp failed. Returning -2
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] db_fetchkey: entering
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] PubKey:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Modulus:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ae b3 75 36 64 e4 1a 40 fe c2 ad 2f 9b 83 0b 45 f1 00 04 bc
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 77 77 76 d1 de 8a cf 9f 32 78 8b d4 b1 b4 be db 75 cc c8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c2 6d ff 3e aa fe f1 2b c3 0a b0 a2 a5 e0 a8 ab 45 cd 87 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ac c6 9f a4 a9 ba 30 79 08 fa 59 4c d2 dc 3d 36 ca 17 d7 c1
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] b2 a2 41 f5 89 0f 00 d4 2d f2 55 d2 30 a5 32 c7 46 7a 6b 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 29 0f 53 9f 35 42 91 e5 7d f7 30 6d bc b3 f2 ae f3 f0 ed 88
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c4 d7 7d 0c 2d f6 5f c8 ed 9f 9a 57 54 79 d0 0f 0b 2f 9c 0d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 94 2e f0 f4 66 62 f7 ae 2e f8 8e 90 08 ba 63 85 b6 46 2f b7
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a7 01 29 9a 14 58 a8 ef eb 07 17 4e 95 8b 2f 48 5f d3 18 10
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 00 d5 03 d7 fd 45 45 ca 67 5b 34 be b8 00 ae ea 9a cd 50
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] d6 e7 a2 81 86 78 11 d7 bf 04 9f 8b 43 3f f7 36 5f ed 31 a8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a3 9d 8b 0a de 05 fb 5c 44 2e 29 e3 3e f4 dd 50 01 0f 86 9d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 55 16 a3 4d f8 90 2d 13 c6 c1 28 57 f8 3e 7c 59
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Exponent: 65537 (0x10001)
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52]
X509 Certificate Version 3
refCount: 1
Serial Number: 1
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Apr 8 13:41:00 2018 Local Time
Not valid after: Fri Jan 1 05:14:07 2038 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyCertSign
                cRLSign
        Basic Constraint (Critical):
                is CA

[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] destroy_rand_mutex: destroy
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] cpKeyTaskManager::~cpKeyTaskManager: called.
[Expert@MGMT:0]#
```

Example 3 - Showing the SIC certificate of a managed Cluster object

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244

printing all certificates of CXL_192.168.3.244

defaultCert:
Host Certificate (level 0):
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Jun 3 19:58:19 2018 Local Time
Not Valid After: Sat Jun 3 19:58:19 2023 Local Time
Serial No.: 85021
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Subject Alternate Names:
        IP Address: 192.168.3.244
CRL distribution points:
        http://192.168.3.240:18264/ICA_CRL2.crl
        CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x
Key Usage:
        digitalSignature
        keyEncipherment
Basic Constraint:
        not CA
MD5 Fingerprint:
   B1:15:C7:A8:2A:EE:D1:75:92:9F:C7:B4:B9:BE:42:1B
SHA-1 Fingerprints:
1. BC:7A:D9:E2:CD:29:D1:9E:F0:39:5A:CD:7E:A9:0B:F9:6A:A7:2B:85
2. MIRE SANK DUSK HOOD HURD RIDE TROY QUAD LOVE WOOD GRIT WITH


               *****
[Expert@MGMT:0]#
```

Example 4 - Showing the SIC certificate of a managed Cluster object in verbose mode

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244 -verbose
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: called
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: closing existing database
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] do_links_getver: strncmp failed. Returning -2

printing all certificates of CXL_192.168.3.244

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] db_fetchkey: entering
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 1 certificates
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] PubKey:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Modulus:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] df 35 c3 45 ca 42 16 6e 21 9e 31 af c1 fd 20 0a 3d 5b 6f 5d
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] e0 a2 0c 0e fa fa 5e e5 91 9d 4e 73 77 fa db 86 0b 5e 5d 0c
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] ce af 4a a4 7b 30 ed b0 43 7d d8 93 c5 4b 01 f4 3d b5 d8 f4
... ... ...
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 34 b1 db ac 18 4f 11 bd d2 fb 26 7d 23 74 5c d9 00 a1 58 1e
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 60 7c 83 44 fa 1e 1e 86 fa ad 98 f7 df 24 4a 21
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Exponent: 65537 (0x10001)
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45]
X509 Certificate Version 3
refCount: 1
Serial Number: 85021
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Jun 3 19:58:19 2018 Local Time
Not valid after: Sat Jun 3 19:58:19 2023 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyEncipherment
        Subject Alternate names:
                IP: 192.168.3.244
        Basic Constraint:
                not CA
        CRL distribution Points:
                URI: http://192.168.3.240:18264/ICA_CRL2.crl
                DN: CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x

defaultCert:

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] destroy_rand_mutex: destroy
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] cpKeyTaskManager::~cpKeyTaskManager: called.
                *****
[Expert@MGMT:0]#
```

fwm sic_reset

Description

Resets SIC on the Management Server.

For detailed procedure, see sk65764: How to reset SIC.

Warning:

- **Before you run this command, take a Gaia Snapshot and a full backup of the Management Server.**
  This command resets SIC between the Management Server and all its managed objects.
- **This operation breaks trust in all Internal CA certificates and SIC trust across the managed environment.**
  Therefore, we do not recommend it at all, except for real disaster recovery.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] sic_reset
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.

fwm snmp_trap

Description

Sends an SNMPv1 Trap to the specified host.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On a Multi-Domain Server, the SNMP Trap packet is sent from the IP address of the Leading Interface.

Syntax

```
fwm [-d] snmp_trap [-v <SNMP OID>] [-g <Generic Trap Number>] [-s <Specific
Trap Number>] [-p <Source Port>] [-c <SNMP Community>] <Target>
["<Message>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-v <SNMP OID>`	Specifies an optional SNMP OID to bind with the message.
`-g <Generic Trap Number>`	Specifies the generic trap number. One of these values: ■ 0 - For `coldStart` trap ■ 1 - For `warmStart` trap ■ 2 - For `linkDown` trap ■ 3 - For `linkUp` trap ■ 4 - For `authenticationFailure` trap ■ 5 - For `egpNeighborLoss` trap ■ 6 - For `enterpriseSpecific` trap (this is the default value)
`-s <Specific Trap Number>`	Specifies the unique trap type. Valid only of generic trap value is 6 (for `enterpriseSpecific`). Default value is 0.
`-p <Source Port>`	Specifies the source port, from which to send the SNMP Trap packets.
`-c <SNMP Community>`	Specifies the SNMP community.
`<Target>`	Specifies the managed target host, to which to send the SNMP Trap packets. Enter an IP address of a resolvable hostname.
`"<Message>"`	Specifies the SNMP Trap text message.

Example - Sending an SNMP Trap from a Management Server and capturing the traffic on the Security Gateway

```
[Expert@MGMT:0]# fwm snmp_trap -g 2 -c public 192.168.3.52 "My Trap Message"
[Expert@MGMT:0]#

[Expert@MyGW_192.168.3.52:0]# tcpdump -s 1500 -vvvv -i eth0 udp and host 192.168.3.51
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
22:49:43.891287 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: UDP (17), length: 103)
192.168.3.51.53450 > MyGW_192.168.3.52.snmptrap: [udp sum ok] { SNMPv1 { Trap(58) E:2620.1.1 192.168.3.240
linkDown 1486440 E:2620.1.1.11.0="My Trap Message" } }
Pressed CTRL+C
[Expert@MyGW_192.168.3.52:0]#
```

fwm unload

Description

Unloads the policy from the specified managed Security Gateways or Cluster Members.

Warning:

1. The `fwm unload` command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the specified Security Gateway (Cluster Member).
2. The `fwm unload` command removes all policies from the specified Security Gateway (Cluster Member).
   This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- If it is necessary to remove the current policy, but keep the Security Gateway (Cluster Member) protected, then run the "`comp_init_policy`" command on the Security Gateway (Cluster Member).
- To load the policies on the Security Gateway (Cluster Member), run one of these commands on the Security Gateway (Cluster Member), or reboot:
  - "`fw fetch`"
  - "`cpstart`"

Syntax

```
fwm [-d] unload <GW1> <GW2> ... <GWN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<GW1> <GW2> ... <GWN>	Specifies the managed Security Gateways by their main IP address or Object Name as configured in SmartConsole.

Example

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name: CXL_Policy
Policy install time: Wed Oct 23 18:23:14 2019
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 1
net.ipv6.conf.eth1.forwarding = 1
net.ipv6.conf.eth3.forwarding = 1
net.ipv6.conf.eth2.forwarding = 1
net.ipv6.conf.eth4.forwarding = 1
net.ipv6.conf.eth5.forwarding = 1
net.ipv6.conf.eth0.forwarding = 1
net.ipv6.conf.eth6.forwarding = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.lo.forwarding = 1
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 1
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 1
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 1
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
[Expert@MyGW:0]#


[Expert@MGMT:0]# fwm unload MyGW

Uninstalling Policy From: MyGW

 Security Policy successfully uninstalled from MyGW...

Security Policy uninstall complete.

[Expert@MGMT:0]#
```

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name:
Policy install time:
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth3.forwarding = 0
net.ipv6.conf.eth2.forwarding = 0
net.ipv6.conf.eth4.forwarding = 0
net.ipv6.conf.eth5.forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth6.forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
[Expert@MyGW:0]#
```

fwm ver

Description

Shows the Check Point version of the Security Management Server.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

```
mdsenv
```

- In the context of a Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ver [-f <Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-f <Output File>`	Specifies the name of the output file, in which to save this information.

Example

```
[Expert@MGMT:0]# fwm ver
This is Check Point Security Management Server R81 - Build 11
[Expert@MGMT:0]#
```

fwm verify

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 622* command to verify a policy on a managed Security Gateway.

Description

Verifies the specified policy package without installing it.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] verify <Policy Name>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Policy Name>	Specifies the name of the policy package as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# fwm verify Standard
 Verifier messages:
Error: Rule 1 Hides rule 2 for Services & Applications: any .
[Expert@MGMT:0]#
```

inet_alert

Description

Notifies an Internet Service Provider (ISP) when a company's corporate network is under attack. This command forwards log messages generated by the alert daemon on your Check Point Security Gateway to an external Management Station. This external Management Station is usually located at the ISP site. The ISP can then analyze the alert and react accordingly.

This command uses the Event Logging API (ELA) protocol to send the alerts. The Management Station receiving the alert must be running the ELA Proxy.

If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the external Management Station running the ELA Proxy at the ISP site and the Check Point Security Gateway generating the alert.

Procedure

Step	Instructions
1	Connect with SmartConsole to the applicable Security Management Server or Domain Management Server, which manages the applicable Security Gateway that should forward log messages to an external Management Station.
2	From the top left **Menu**, click **Global properties**.
3	Click on the **[+]** near the **Log and Alert** and click **Alerts**.
4	Clear the **Send user defined alert no. 1 to SmartView Monitor**.
5	Select the next option **Run UserDefined script under the above**.
6	Enter the applicable **inet_alert** syntax (see the *Syntax* section below).
7	Click **OK**.
8	Install the Access Control Policy on the applicable Security Gateway.

Syntax

```
inet_alert -s <IP Address> [-o] [-a <Auth Type>] [-p <Port>] [-f <Token>
<Value>] [-m <Alert Type>]
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Parameters

Parameter	Description
`-s <IP Address>`	The IPv4 address of the ELA Proxy (usually located at the ISP site).
`-o`	Prints the alert log received to `stdout`. Use this option when `inet_alert` is part of a pipe syntax (`<some command> | inet_alert ...`).
`-a <Auth Type>`	Specifies the type of connection to the ELA Proxy. One of these values: ■ `ssl_opsec`-The connection is authenticated and encrypted (this is the default). ■ `auth_opsec`- The connection is authenticated. ■ `clear`- The connection is neither authenticated, nor encrypted.
`-p <Port>`	Specifies the port number on the ELA proxy. Default port is 18187.
`-f <Token> <Value>`	A field to be added to the log, represented by a `<Token> <Value>` pair as follows: ■ `<Token>` - The name of the field to be added to the log. Cannot contain spaces. ■ `<Value>` - The field's value. Cannot contain spaces. This option can be used multiple times to add multiple `<Token> <Value>` pairs to the log.
`-m <Alert Type>`	The alert to be triggered at the ISP site. This alert overrides the alert specified in the log message generated by the alert daemon. The response to the alert is handled according to the actions specified in the ISP Security Policy: These alerts execute the OS commands: ■ `alert` - Popup alert command ■ `mail` - Mail alert command ■ `snmptrap` - SNMP trap alert command ■ `spoofalert` - Anti-Spoof alert command These NetQuota and ServerQuota alerts execute the OS commands specified in the `$FWDIR/conf/objects.C`: file: `value=clientquotaalert. Parameter=clientquotaalertcmd`

Exist Status

Exit Status	Description
0	Execution was successful.
102	Undetermined error.
103	Unable to allocate memory.
104	Unable to obtain log information from `stdin`
106	Invalid command line arguments.
107	Failed to invoke the OPSEC API.

Example

```
inet_alert -s 10.0.2.4 -a clear -f product cads -m alert
```

This command specifies to perform these actions in the event of an attack:

- Establish a clear connection with the ELA Proxy located at IP address 10.0.2.4
- Send a log message to the specified ELA Proxy. Set the product field of this log message to `cads`
- Trigger the OS command specified in the SmartConsole > **Menu > Global properties > Log and Alert > Popup Alert Command** field.

ldapcmd

Description

This is an LDAP utility that controls these features:

Feature	Description
Cache	LDAP cache operations, such as emptying the cache, as well as providing debug information.
Statistics	LDAP search statistics, such as: ■ All user searches ■ Pending lookups (when two or more lookups are identical) ■ Total lookup time (the total search time for a specific lookup) ■ Cache statistics such as hits and misses These statistics are saved in the `$FWDIR/log/ldap_pid_<Process PID>.stats` file.
Logging	View the alert and warning logs.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcmd [-d <Debug Level>] -p {<Process Name> | all} <Command>
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-p {<Process Name> | all}`	Runs on a specified Check Point process, or all supported Check Point processes.
`<Command>`	One of these commands: ■ `cacheclear {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Clears cache for all objects • `UserCacheObject` - Clears cache for user objects • `TemplateCacheObject` - Clears cache for template objects • `TemplateExtGrpCacheObject` - Clears cache for external template group objects ■ `cachetrace {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Traces cache for all objects • `UserCacheObject` - Traces cache for user objects • `TemplateCacheObject` - Traces cache for template objects • `TemplateExtGrpCacheObject` - Traces cache for external template group objects ■ `log {on | off}` • `on` - Creates LDAP logs • `off` - Does not create LDAP logs ■ `stat {<Print Interval in Sec> | 0}` • `<Print Interval in Sec>` - How frequently to collect the statistics • `0` - Stops collecting the statistics

ldapcompare

Description

This is an LDAP utility that performs compare queries and prints a message whether the result returned a match or not.

This utility opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcompare [-d <Debug Level>] [<Options>] <DN> {<Attribute> <Value> |
<Attribute> <Base64 Value>}
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`<Options>`	See the tables below: ■ Compare options ■ Common options
`<DN>`	Specifies the Distinguished Name.
`<Attribute>`	Specifies the assertion attribute.
`<Value>`	Specifies the assertion value.
`<Base64 Value>`	Specifies the Base64 encoding of the assertion value.

Compare options

Option	Description
`-E [!]<Extension>[=<Extension Parameter>]`	Specifies the compare extensions. **Note** - The exclamation sign "!" indicates criticality. For example: `!dontUseCopy` = Do **not** use Copy
`-M`	Enables the Manage DSA IT control. Use the "`-MM`" option to make it critical.
`-P <LDAP Protocol Version>`	Specifies the LDAP protocol version. Default version is 3.
`-z`	Enables the quiet mode. The command does not print anything. You can use the command return values.

Common options

Option	Description
`-D <Bind DN>`	Specifies the LDAP Server administrator Distinguished Name.

Option	Description
`-e [!]<Extension> [=<Extension Parameter>]`	Specifies the general extensions: **Note** - The exclamation sign "!" indicates criticality. ■ `[!]assert=<Filter>` RFC 4528; an RFC 4515 filter string ■ `[!]authzid=<Authorization ID>` RFC 4370; either "`dn:<DN>`", or "`u:<Username>`" ■ `[!]chaining[=<Resolve Behavior> [/<Continuation Behavior>]]` One of these: • "chainingPreferred" • "chainingRequired" • "referralsPreferred" • "referralsRequired" ■ `[!]manageDSAit` RFC 3296 ■ `[!]noop` ■ `ppolicy` ■ `[!]postread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]preread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]relax` ■ `abandon` SIGINT sends the abandon signal; if critical, does not wait for SIGINT. Not really controls. ■ `cancel` SIGINT sends the cancel signal; if critical, does not wait for SIGINT. Not really controls. ■ `ignore` SIGINT ignores the response; if critical, does not wait for SIGINT. Not really controls.
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname.
`-H <LDAP URI>`	Specifies the LDAP Server Uniform Resource Identifier(s).
`-I`	Specifies to use the SASL Interactive mode.
`-n`	Dry run - shows what would be done, but does not actually do it.
`-N`	Specifies not to use the reverse DNS to canonicalize SASL host name.
`-o <Option>[=<Option Parameter>]`	Specifies the general options: `nettimeout={<Timeout in Sec> | none | max}`
`-O <Properties>`	Specifies the SASL security properties.

Option	Description
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-Q`	Specifies to use the SASL Quiet mode.
`-R <Realm>`	Specifies the SASL realm.
`-U <Authentication Identity>`	Specifies the SASL authentication identity.
`-v`	Runs in verbose mode (prints the diagnostics to *stdout*).
`-V`	Prints version information (use the "`-VV`" option only).
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password (for simple authentication).
`-W`	Specifies to prompt the user for the LDAP Server administrator password.
`-x`	Specifies to use simple authentication.
`-X <Authorization Identity>`	Specifies the SASL authorization identity (either "`dn:<DN>`", or "`u:<Username>`" option).
`-y <File>`	Specifies to read the LDAP Server administrator password from the `<File>`.
`-Y <SASL Mechanism>`	Specifies the SASL mechanism.
`-Z`	Specifies to start the TLS request. Use the "`-ZZ`" option to require successful response.

ldapmemberconvert

Description

This is an LDAP utility that ports from the "`Member`" attribute values in LDAP group entries to the "`MemberOf`" attribute values in LDAP member (User or Template) entries.

This utility converts the LDAP server data to work in either the "`MemberOf`" mode, or "`Both`" mode. The utility searches through all specified group or template entries that hold one or more "`Member`" attribute values and modifies each value. The utility searches through all specified group/template entries and fetches their "`Member`" attribute values.

Each value is the DN of a member entry. The entry identified by this DN is added to the "`MemberOf`" attribute value of the group/template DN at hand. In addition, the utility delete those "`Member`" attribute values from the group/template, unless you run the command in the "`Both`" mode.

When your run the command, it creates a log file `ldapmemberconvert.log` in the current working directory. The command logs all modifications done and errors encountered in that log file.

Important - Back up the LDAP server database *before* you run this conversion utility.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmemberconvert [-d <Debug Level>] -h <LDAP Server> -p <LDAP Server Port>
-D <LDAP Admin DN> -w <LDAP Admin Password> -m <Member Attribute Name> -o
<MemberOf Attribute Name> -c <Member ObjectClass Value> [-B] [-f <File> | -
g <Group DN>] [-L <LDAP Server Timeout>] [-M <Number of Updates>] [-S
<Size>] [-T <LDAP Client Timeout>] [-Z]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.

Parameter	Description
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-m <Member Attribute Name>`	Specifies the LDAP attribute name when fetching and (possibly) deleting a group `Member` attribute value.
`-o <MemberOf Attribute Name>`	Specifies the LDAP attribute name for adding an LDAP "`MemberOf`" attribute value.
`-c <Member ObjectClass Value>`	Specifies the LDAP "`ObjectClass`" attribute value that defines, which type of member to modify. You can specify multiple attribute values with this syntax: `-c <Member Object Class 1> -c <Member Object Class 2> ... -c <Member Object Class N>`
`-B`	Specifies to run in "`Both`" mode.
`-f <File>`	Specifies the file that contains a list of Group DNs separated by a new line: `<Group DN 1>` `<Group DN 2>` `...` `<Group DN N>` Length of each line is limited to 256 characters.
`-g <Group DN>`	Specifies the Group or Template Distinguished Name, on which to perform the conversion. You can specify multiple Group DNs with this syntax: `-g <Group DN 1> -g <Group DN 2> ... -g <Group DN N>`
`-L <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "`never`".
`-M <Number of Updates>`	Specifies the maximal number of simultaneous member LDAP updates. Default is 20.
`-S <Size>`	Specifies the Server side size limit for LDAP operations, in number of entries. Default is "`none`".
`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "`never`".
`-Z`	Specifies to use SSL connection.

Notes

There are two "`GroupMembership`" modes. You must keep these modes consistent:

- `template-to-groups`
- `user-to-groups`

For example, if you apply conversion on LDAP users to include the "`MemberOf`" attributes for their groups, then this conversion has to be applied on LDAP defined templates for their groups.

Troubleshooting

Symptom:

A command fails with an error message stating the connection stopped unexpectedly when you run it with the parameter `-M <Number of Updates>`.

Root Cause:

The LDAP server could not handle that many LDAP requests simultaneously and closed the connection.

Solution:

Run the command again with a lower value for the "`-M`" parameter. The default value should be adequate, but can also cause a connection failure in extreme situations. Continue to reduce the value until the command runs normally. Each time you run the command with the same set of groups, the command continues from where it left off.

Examples

Example 1

A group is defined with the DN "cn=cpGroup,ou=groups,ou=cp,c=us" and these attributes:

```
...
cn=cpGroup
uniquemember="cn=member1,ou=people,ou=cp,c=us"
uniquemember="cn=member2,ou=people,ou=cp,c=us"
...
```

For the two member entries:

```
...
cn=member1
objectclass=fw1Person
...
```

and:

```
...
cn=member2
objectclass=fw1Person
...
```

Run:

```
[Expert@MGMT:0]# ldapconvert -g cn=cpGroup,ou=groups,ou=cp,c=us -h MyLdapServer -d cn=admin -w secret -m uniquemember -o memberof -c fw1Person
```

The result for the group DN is:

```
...
cn=cpGroup
...
```

The result for the two member entries is:

```
...
cn=member1
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

and:

```
...
cn=member2
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

If you run the same command with the "-B" parameter, it produces the same result, but the group entry is not modified.

Example 2

If there is another member attribute value for the same group entry:

```
uniquemember="cn=template1,ou=people, ou=cp,c=us"
```

and the template is:

```
cn=member1
objectclass=fw1Template
```

Then after running the same command, the template entry stays intact, because of the parameter "`-c fw1Person`", but the object class of "`template1`" is "`fw1Template`".

ldapmodify

Description

This is an LDAP utility that imports users to an LDAP server. The input file must be in the LDIF format.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmodify [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Server Port>] [-
D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-a] [-b] [-c] [-F] [-k] [-n]
[-r] [-v] [-T <LDAP Client Timeout>] [-Z] [ -f <Input File> .ldif | <
<Entry>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-a`	Specifies that this is the LDAP "`add`" operation.
`-b`	Specifies to read values from files (for binary attributes).
`-c`	Specifies to ignore errors during continuous operation.
`-F`	Specifies to force changes on all records.
`-k`	Specifies the Kerberos bind.

Parameter	Description
`-K`	Specifies the Kerberos bind, part 1 only.
`-n`	Specifies to print the LDAP "`add`" operations, but do not actually perform them.
`-r`	Specifies to replace values, instead of adding values.
`-v`	Specifies to run in verbose mode.
`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "`never`".
`-Z`	Specifies to use SSL connection.
`-f <Input File>.ldif`	Specifies to read from the `<Input File>.ldif` file. The input file must be in the LDIF format.
`< <Entry>`	Specifies to read the entry from the *stdin*. The "<" character is mandatory part of the syntax. It specifies the input comes from the standard input (from the data you enter on the screen).

ldapsearch

Description

This is an LDAP utility that queries an LDAP directory and returns the results.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapsearch [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Port>] [-D <LDAP
Admin DN>] [-w <LDAP Admin Password>] [-A] [-B] [-b <Base DN>] [-F
<Separator>] [-l <LDAP Server Timeout>] [-s <Scope>] [-S <Sort Attribute>]
[-t] [-T <LDAP Client Timeout>] [-u] [-z <Number of Search Entries>] [-Z]
<Filter> [<Attributes>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-A`	Specifies to retrieve attribute names only, without values.
`-B`	Specifies not to suppress the printing of non-ASCII values.
`-b <Base DN>`	Specifies the Base Distinguished Name (DN) for search.
`-F <Separator>`	Specifies the print separator character between attribute names and their values. The default separator is the equal sign (=).

Parameter	Description
`-l <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "`never`".
`-s <Scope>`	Specifies the search scope. One of these: ■ `base` ■ `one` ■ `sub`
`-S <Sort Attribute>`	Specifies to sort the results by the values of this attribute.
`-t`	Specifies to write values to files in the `/tmp/` directory. Writes each *<attribute>-<value>* pair to a separate file named: `/tmp/ldapsearch-<Attribute>-<Value>` For example, for the `fw1color` attribute with the value `a00188`, the command writes to the file named: `/tmp/ldapsearch-fw1color-a00188`
`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is `never`.
`-u`	Specifies to show user-friendly entry names in the output. For example: shows `cn=Babs Jensen, users, omi` instead of `cn=Babs Jensen, cn=users,cn=omi`
`-z <Number of Search Entries>`	Specifies the maximal number of entries to search on the LDAP Server.
`-Z`	Specifies to use SSL connection.
`<Filter>`	LDAP search filter compliant with RFC-1558. For example: `objectclass=fw1host`
`<Attributes>`	Specifies the list of attributes to retrieve. If you do not specify attributes explicitly, then the command retrieves all attributes.

Example

```
[Expert@MGMT:0]# ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass
```

With this syntax, the command:

1. Connects to the LDAP Server to port 18185.
2. Connects to the LDAP Server with Base DN "`cn=omi`".
3. Queries the LDAP directory for "`fw1host`" objects.
4. For each object found, prints the value of its "`objectclass`" attribute.

mgmt_cli

Description

The `mgmt_cli` tool works directly with the management database on your Management Server.

Syntax on Management Server or Security Gateway running on Gaia OS

```
mgmt_cli <Command Name> <Command Parameters> <Optional Switches>
```

Syntax on SmartConsole computer running on Windows OS 32-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional Switches>
```

Syntax on SmartConsole computer running on Windows OS 64-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles(x86)%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional Switches>
```

Notes

- For a complete list of the `mgmt_cli` options, enter the `mgmt_cli` (`mgmt_cli.exe`) command and press Enter.
- For more information, see the *Check Point Management API Reference*.

migrate

Important - This command is used to migrate the management database from R80.10 and lower versions.
For more information, see the *R81 Installation and Upgrade Guide*.

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/bin/upgrade_tools/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R81/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R81/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R81/log/migrate-2019.06.14_11.21.39.log*

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# ./migrate -h
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate export [-l | -x] [-n] [--
exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full Path>/<Name
of Exported File> &
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate import [-l | -x] [-n] [--
exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full Path>/<Name
of Exported File>.tgz &
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`yes | nohup ./migrate ... &`	This syntax: 1. Sends the "`yes`" input to the interactive "`migrate`" command through the pipeline. 2. The "`nohup`" forces the "`migrate`" command to ignore the hangup signals from the shell. 3. The "`&`" forces the command to run in the background. As a result, when the CLI session closes, the command continues to run in the background. See: ■ sk133312 ■ https://linux.die.net/man/1/bash ■ https://linux.die.net/man/1/nohup
`export`	Exports the management database and applicable Check Point configuration.
`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.

Parameter	Description
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory.  **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory.  **Important:** ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-n`	Runs silently (non-interactive mode) and uses the default options for each setting.  **Important:** ■ If you export a management database in this mode and the specified name of the exported file matches the name of an existing file, the command overwrites the existing file without prompting. ■ If you import a management database in this mode, the "`migrate import`" command runs the "`cpstop`" command automatically.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.
`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
/<Full Path>/	Absolute path to the exported database file. This path must exist.
<Name of Exported File>	■ During the export operation, specifies the name of the output file. The command automatically adds the `*.tgz` extension. ■ During the import operation, specifies the name of the exported file. You must manually enter the `*.tgz` extension in the end.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# ./migrate export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R81/migrate-2019.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R81/log/migrate-2019.06.14_11.21.39.log' for
further details
[Expert@MGMT:0]#
```

migrate_server

Important - This command is used to migrate the management database from R80.20.M1, R80.20, R80.20.M2, R80.30, and higher versions.
For more information, see the *R81 Installation and Upgrade Guide*.

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/scripts/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate_server` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R81/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R81/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R81/log/migrate-2019.06.14_11.21.39.log*

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server -h
```

- To run the Pre-Upgrade Verifier:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server verify -v R81 [-skip_upgrade_tools_
check]
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R81 [-skip_upgrade_tools_
check] [-l | -x] [--include-uepm-msi-files] [--exclude-uepm-postgres-
db] /<Full Path>/<Name of Exported File>
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server import -v R81 [-skip_upgrade_tools_
check] [-l | -x] [-change_ips_file /<Full Path>/<Name of JSON
File>.json] [--include-uepm-msi-files] [--exclude-uepm-postgres-db]
/<Full Path>/<Name of Exported File>.tgz
```

- To import the Domain Management Server database and configuration on a Security Management Server:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server migrate_import_domain -v R81 [-skip_
upgrade_tools_check] [-l | -x] [--include-uepm-msi-files] [--exclude-
uepm-postgres-db] /<Full Path>/<Name of Exported File>.tgz
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`export`	Exports the management database and applicable Check Point configuration.

Parameter	Description
`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server. **Important:** ■ This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands). ■ This note applies to a Multi-Domain Security Management environment, if at least one of the servers changes its IPv4 address comparing to the source server, from which you exported its database. You must do these steps **before** you start the upgrade and import: 1. You must create a special JSON configuration file with the new IPv4 address (es). Syntax: `[{"name":"<<Name of Server 1 Object in SmartConsole>>","newIpAddress4":"<New IPv4 Address of Server 1>"},` `{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]` Example: `[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},` `{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]` 2. You must call this file: **mdss.json** 3. You must put this file on **all** servers in this directory: **/var/log/**
`migrate_import_domain`	On a Security Management Server, imports the management database and applicable Check Point configuration that were exported from a Domain Management Server. **Important** - This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands).
`verify`	Verifies the management database and applicable Check Point configuration that were exported from another Management Server.
`-v R81`	Specifies the version, to which you plan to migrate / upgrade.
`-skip_upgrade_tools_check`	Does not try to connect to Check Point Cloud to check for a more recent version of the Upgrade Tools. > **Best Practice** - Use this parameter on the Management Server that is **not** connected to the Internet.

Parameter	Description
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory.  **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory.  **Important:** ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-change_ips_file /<Full Path>/<Name of JSON File>.json`	 **Important:** ■ This parameter exists only in these builds of the Upgrade Tools: • Upgrade Tools for R80.40 - build 994000406 and lower • Upgrade Tools for R81 - build 995000519 and lower ■ When a higher build of the Upgrade Tools is installed, you must create the **/var/log/mdss.json** file. Specifies the absolute path to the special JSON configuration file with new IPv4 addresses. This file is mandatory during an upgrade of a Multi-Domain Security Management environment. Even if only one of the servers migrates to a new IP address, all the other servers must get this configuration file for the import process. Syntax: `[{"name":"<<Name of Server 1 Object in SmartConsole>>","newIpAddress4":"<New IPv4 Address of Server 1>"},` `{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]` Example: `[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},` `{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`

Parameter	Description
`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.
/<Full Path>/<Name of Exported File>	Specifies the absolute path to the exported database file. This path must exist. ■ During the export operation, specifies the name of the output file. The command automatically adds the `*.tgz` extension. ■ During the import operation, specifies the name of the exported file. You must manually enter the `*.tgz` extension in the end.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R81/migrate-2019.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate_server export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R81/log/migrate-2019.06.14_11.21.39.log' for
further details
[Expert@MGMT:0]#
```

queryDB_util

Description

Searches in the management database for objects or policy rules.

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 622* command to search in the management database for objects or policy rules according to search parameters.

rs_db_tool

Description

Manages Dynamically Assigned IP address (DAIP) gateways in a DAIP database.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

- **To add an entry to the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation add -name <Object Name> -ip
<IPv4 Address> -ip6 <Pv6 Address> -TTL <Time-To-Live>
```

- **To fetch a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation fetch -name <Object Name>
```

- **To delete a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation delete -name <Object Name>
```

- **To list all entries in the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation list
```

- **To synchronize the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation sync
```

Note - You must run this command from the Expert mode.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself.  **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-name <Object Name>`	Specifies the name of the DAIP object.
`-ip <IPv4 Address>`	Specifies the IPv4 address of the DAIP object
`-ip6 <IPv6 Address>`	Specifies the IPv6 address of the DAIP object.
`-TTL <Time-To-Live>`	Specifies the relative time interval (in seconds), during which the entry is valid.

sam_alert

Description

For SAM v1, this utility executes Suspicious Activity Monitoring (SAM) actions according to the information received from the standard input.

For SAM v2, this utility executes Suspicious Activity Monitoring (SAM) actions with User Defined Alerts mechanism.

Important:

- You must run this command on the Management Server.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Notes:

- VSX Gateways and VSX Cluster Members do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam" on page 547* and *"fw sam_policy" on page 553* commands.

SAM v1 syntax

Syntax for SAM v1

```
sam_alert [-v] [-o] [-s <SAM Server>] [-t <Time>] [-f <Security Gateway>]
[-C] {-n|-i|-I} {-src|-dst|-any|-srv}
```

Parameters for SAM v1

Parameter	Description
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-o`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-s <SAM Server>`	Specifies the SAM Server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation.  **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.

Parameter	Description
`-C`	Cancels the specified operation.
`-n`	Specifies to notify every time a connection, which matches the specified criteria, passes through the Security Gateway.
`-i`	Inhibits (drops or rejects) connections that match the specified criteria.
`-I`	Inhibits (drops or rejects) connections that match the specified criteria and closes all existing connections that match the specified criteria.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

SAM v2 syntax

Syntax for SAM v2

```
sam_alert -v2 [-v] [-O] [-S <SAM Server>] [-t <Time>] [-f <Security
Gateway>] [-n <Name>] [-c "<Comment">] [-o <Originator>] [-l {r | a}] -a
{d | r| n | b | q | i} [-C] {-ip |-eth} {-src|-dst|-any|-srv}
```

Parameters for SAM v2

Parameter	Description
`-v2`	Specifies to use SAM v2.
`-v`	Enables the verbose mode for the `fw sam` command.
`-O`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-S <SAM Server>`	the SAM server to be contacted. Default is localhost
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation.  **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-n <Name>`	Specifies the name for the SAM rule. Default is empty.
`-c "<Comment>"`	Specifies the comment for the SAM rule. Default is empty. You must enclose the text in the double quotes or single quotes.
`-o <Originator>`	Specifies the originator for the SAM rule. Default is "`sam_alert`".
`-l {r | a}`	Specifies the log type for connections that match the specified criteria: ■ `r` - Regular ■ `a` - Alert Default is `None`.

Parameter	Description
`-a {d | r| n | b | q | i}`	Specifies the action to apply on connections that match the specified criteria: ■ `d` - Drop ■ `r` - Reject ■ `n` - Notify ■ `b` - Bypass ■ `q` - Quarantine ■ `i` - Inspect
`-C`	Specifies to close all existing connections that match the criteria.
`-ip`	Specifies to use IP addresses as criteria parameters.
`-eth`	Specifies to use MAC addresses as criteria parameters.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

Example

See sk110873: How to configure Security Gateway to detect and prevent port scan.

stattest

Description

Check Point AMON client to query SNMP OIDs.

You can use this command as an alternative to the standard SNMP commands for debug purposes - to make sure the applicable SNMP OIDs provide the requested information.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

- **To query a Regular OID:**

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>
```

  These are specified in the SNMP MIB files.

  For Check Point MIB files, see sk90470.

- **To query a Statistical OID:**

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t <Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

  Statistical OIDs take some time to "initialize".

  For example, to calculate an average, it is necessary to collect enough samples.

  Check Point statistical OIDs are registered in the `$CPDIR/conf/statistical_oid.conf` file.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h <Host>`	Specifies the remote Check Point host to query by its IP address or resolvable hostname.
`-p <Port>`	Specifies the port number, on which the AMON server listens. Default port is 18192.

Parameter	Description
`-x <Proxy Server>`	Specifies the Proxy Server by its IP address or resolvable hostname.  **Note** - Use only when you query a remote host.
`-l <Polling Interval>`	Specifies the time in seconds between queries.  **Note** - Use only when you query a Statistical OID.
`-r <Polling Duration>`	Specifies the time in seconds, during which to run consecutive queries.  **Note** - Use only when you query a Statistical OID.
`-v <VSID>`	On a VSX Gateway, specifies the context of a Virtual Device to query.
`-t <Timeout>`	Specifies the session timeout in milliseconds.
`<Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>`	Specifies the Regular OIDs to query.  **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.
`<Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>`	Specifies the Statistical OIDs to query.  **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.

Example - Query a Regular OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

```
[Expert@HostName]# stattest get 1.3.6.1.4.1.2620.1.6.7.4.2
```

Example - Query a Statistical OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

Information is collected with intervals of 5 seconds during 5 seconds

```
[Expert@HostName]# stattest get -l 5 -r 5 1.3.6.1.4.1.2620.1.6.7.2.3
```

threshold_config

Description

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts.

You can use these thresholds to monitor many system components automatically without requesting information from each object or device.

You configure these SNMP Monitoring Thresholds only on the Security Management Server, Multi-Domain Server, or Domain Management Server.

During policy installation, the managed a Security Gateway and Clusters receive and apply these thresholds as part of their policy.

For more information, see sk90860: How to configure SNMP on Gaia OS.

Procedure

Step	Instructions
1	Connect to the command line on the Management Server.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, switch to the context of the applicable Domain Management Server: `[Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>`
4	Go to the Threshold Engine Configuration menu: `[Expert@HostName:0]# threshold_config`
5	Select the applicable options and configure the applicable settings (see the **Threshold Engine Configuration Options** table below). `Threshold Engine Configuration Options:` `----------` `(1) Show policy name` `(2) Set policy name` `(3) Save policy` `(4) Save policy to file` `(5) Load policy from file` `(6) Configure global alert settings` `(7) Configure alert destinations` `(8) View thresholds overview` `(9) Configure thresholds` `(e) Exit (m) Main Menu` `Enter your choice (1-9) :`

Step	Instructions
6	Exit from the Threshold Engine Configuration menu.
7	Stop the CPD daemon: `[Expert@HostName:0]# cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"` See *"cpwd_admin stop" on page 509*.
8	Start the CPD daemon: `[Expert@HostName:0]# cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"` See *"cpwd_admin start" on page 506*.
9	Wait for 10-20 seconds.
10	Verify that CPD daemon started successfully: `[Expert@HostName:0]# cpwd_admin list | egrep "STAT|CPD"` See *"cpwd_admin list" on page 503*.
11	In SmartConsole, install the Access Control Policy on Security Gateways and Clusters.

Threshold Engine Configuration Options

Menu item	Description
`(1) Show policy name`	Shows the name of the current configured threshold policy.
`(2) Set policy name`	Configures the name for the threshold policy. If you do not specify it explicitly, then the default name is "`Default Profile`".
`(3) Save policy`	Saves the changes in the current threshold policy.
`(4) Save policy to file`	Exports the configured threshold policy to a file. If you do not specify the path explicitly, the file is saved in the current working directory.
`(5) Load policy from file`	Imports a threshold policy from a file. If you do not specify the path explicitly, the file is imported from the current working directory.
`(6) Configure global alert settings`	Configures global settings: ■ How frequently alerts are sent (configured delay must be greater than 30 seconds) ■ How many alerts are sent

Menu item	Description
(7) Configure alert destinations	Configures the SNMP Network Management System (NMS), to which the managed Security Gateways and Cluster Members send their SNMP alerts. `Configure Alert Destinations Options:` `----------` `(1) View alert destinations` `(2) Add SNMP NMS` `(3) Remove SNMP NMS` `(4) Edit SNMP NMS`
(8) View thresholds overview	Shows a list of all available thresholds and their current settings. These include: ■ Name ■ Category (see the next option "(9)") ■ State (disabled or enabled) ■ Threshold (threshold point, if applicable) ■ Description
(9) Configure thresholds	Shows the list of threshold categories to configure. `Thresholds Categories` `----------` `(1) Hardware` `(2) High Availability` `(3) Local Logging Mode Status` `(4) Log Server Connectivity` `(5) Networking` `(6) Resources` See the **Thresholds Categories** table below.

Thresholds Categories

Category	Sub-Categories
(1) Hardware	`Hardware Thresholds:` `----------` `(1) RAID volume state` `(2) RAID disk state` `(3) RAID disk flags` `(4) Temperature sensor reading` `(5) Fan speed sensor reading` `(6) Voltage sensor reading`
(2) High Availability	`High Availability Thresholds:` `----------` `(1) Cluster member state changed` `(2) Cluster block state` `(3) Cluster state` `(4) Cluster problem status` `(5) Cluster interface status`

Category	Sub-Categories
(3) Local Logging Mode Status	Local Logging Mode Status Thresholds: ---------- (1) Local Logging Mode
(4) Log Server Connectivity	Log Server Connectivity Thresholds: ---------- (1) Connection with log server (2) Connection with all log servers
(5) Networking	Networking Thresholds: ---------- (1) Interface Admin Status (2) Interface removed (3) Interface Operational Link Status (4) New connections rate (5) Concurrent connections rate (6) Bytes Throughput (7) Accepted Packet Rate (8) Drop caused by excessive traffic
(6) Resources	Resources Thresholds: ---------- (1) Swap Memory Utilization (2) Real Memory Utilization (3) Partition free space (4) Core Utilization (5) Core interrupts rate

Notes:

- If you run the `threshold_config` command *locally* on a Security Gateway or Cluster Members to configure the SNMP Monitoring Thresholds, then each policy installation erases these *local* SNMP threshold settings and reverts them to the *global* SNMP threshold settings configured on the Management Server that manages this Security Gateway or Cluster.
- On a Security Gateway and Cluster Members, you can save the local Threshold Engine Configuration settings to a file and load it locally later.
- The Threshold Engine Configuration is stored in the `$FWDIR/conf/thresholds.conf` file.
- In a Multi-Domain Security Management environment:
  - You can configure the SNMP thresholds in the context of Multi-Domain Server (MDS) and in the context of each individual Domain Management Server.
  - Thresholds that you configure in the context of the Multi-Domain Server are for the Multi-Domain Server only.
  - Thresholds that you configure in the context of a Domain Management Server are for that Domain Management Server and its managed Security Gateway and Clusters.
  - If an SNMP threshold applies both to the Multi-Domain Server and a Domain Management Server, then configure the SNMP threshold both in the context of the Multi-Domain Server and in the context of the Domain Management Server.
    However, in this scenario you can only get alerts from the Multi-Domain Server, if the monitored object exceeds the threshold.
    Example:
    If you configure the CPU threshold, then when the monitored value exceeds the configured threshold, it applies to both the Multi-Domain Server and the Domain Management Server. However, only the Multi-Domain Server generates SNMP alerts.

CHECK POINT MOBILE ACCESS

Remote work is the new norm. Efforts to slow the spread of COVID-19 accelerated the transition of employees working from home and accessing corporate resources securely through various VPN (Virtual Private Network) technologies. In a recent Gartner CFO survey [1], 74% of companies said they intend to shift employees to work from home permanently.

Check Point Mobile Access is the safe and easy solution to securely connect to corporate applications over the Internet with your Smartphone, tablet or personal computer (PC). Mobile Access allows remote and mobile workers to simply and securely connect to email, calendar, contacts and corporate applications. Because it's fully integrated into the Check Point network security suite, administrators can easily set policy and monitor remote user's use of corporate assets.

Simple and Secure Corporate Access from Mobile Devices

FLEXIBLE

Easy access for mobile workers – secure connectivity for smartphones, tablets, PCs and laptops

SECURE

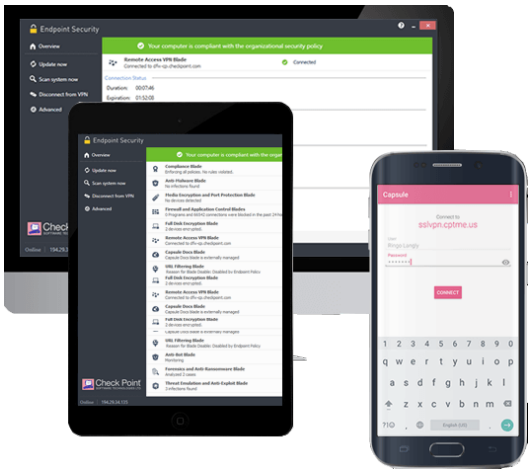
Communicate securely with proven encryption technology, and multi-factor authentication

UNIFIED

Deploy and manage on your existing security gateways from one unified console

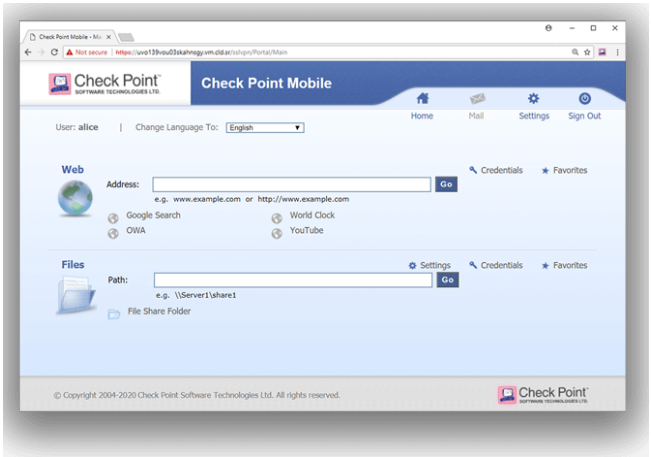
Full Layer-3 VPN Technology using a Client

IPsec VPNs authenticate and encrypt every communication session. Layer-3 VPN technology is highly scalable and allows flexible any-to-any connectivity.



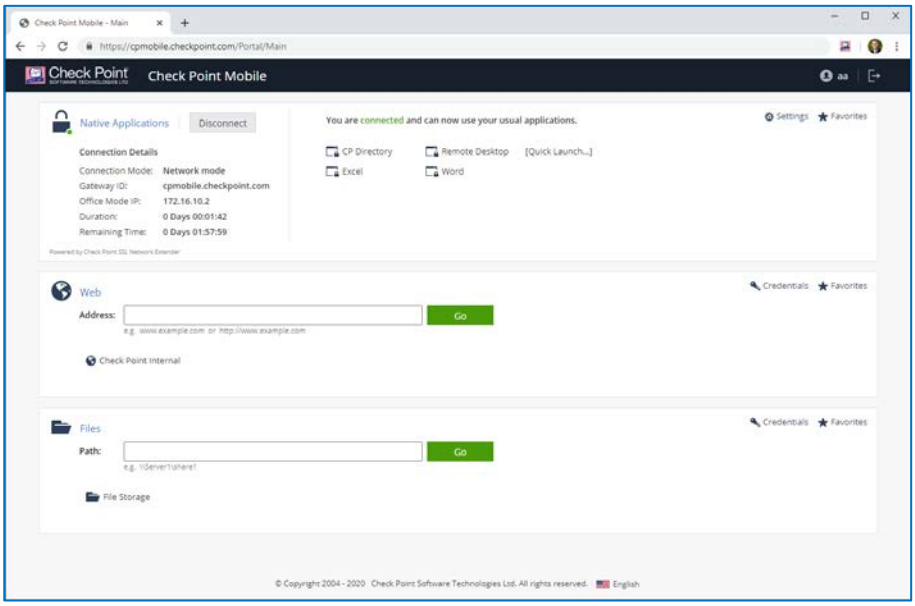
Encrypted SSL/TLS VPN using a Browser

Encrypt communications from unmanaged mobile devices. Both web-based and network-level access through SSL/TLS encryption is delivered through a browser.



SPOTLIGHT ON THE WEB PORTAL

The Web Portal is best for connecting securely to corporate resources from a web browser. Through an integrated web portal, users can access native corporate applications including web-based resources, shared file and email. Administrators can customize the design of the web portal to match their corporate brand identity. Mobile Access offers secure SSL/TLS VPN transport, strong multi-factor authentication and Role-based Access Control (RBAC).



Connect from Everywhere - Web, Mobile and Desktop

DynamicID™ Direct SMS Authentication
Mobile Access can be configured to send a One-Time Password (OTP) to an end-user device such as a mobile phone via an SMS message. SMS two-factor authentication provides an extra level of security while eliminating the difficulties associated with managing hardware tokens.

Compliance Scanner
An endpoint compliance scanner ensures that connecting endpoints are compliant with corporate policy. Out-of-compliance users are offered links to self-remediation resources. Enforce your corporate compliance policy for Windows, macOS and Linux endpoints.

SSL Network Extender (SNX, an On-demand Client)
Best for secure connectivity to corporate resources using non- web-based applications via an on-demand, dissolvable client. The SSL Network Extender (SNX) is used for remote users who need access to network (non-web-based) applications. SSL Network Extender is downloaded automatically from the SSL VPN portal to the endpoint machines, so that client software does not have to be pre-installed and configured on users' PCs and laptops. SNX delivers full network connectivity for IP-based applications including a Layer-3 tunnel to connect to your corporate resources. It supports IP-based applications, including ICMP, TCP, and UDP, without requiring complex configuration to support each application. SNX Application Mode works without requiring administrative privileges and establishes a VPN tunnel for the specified applications.

Secure Workspace
End-users can utilize the Check Point virtual desktop that enables data protection during user sessions and enables cache wiping after the sessions have ended. Secure Workspace protects all session-specific data accumulated on the client side and creates a secure virtual environment insulated from the host. Browser and application caches, files, etc. are encrypted and then deleted when session ends.

SPOTLIGHT ON CLIENTS

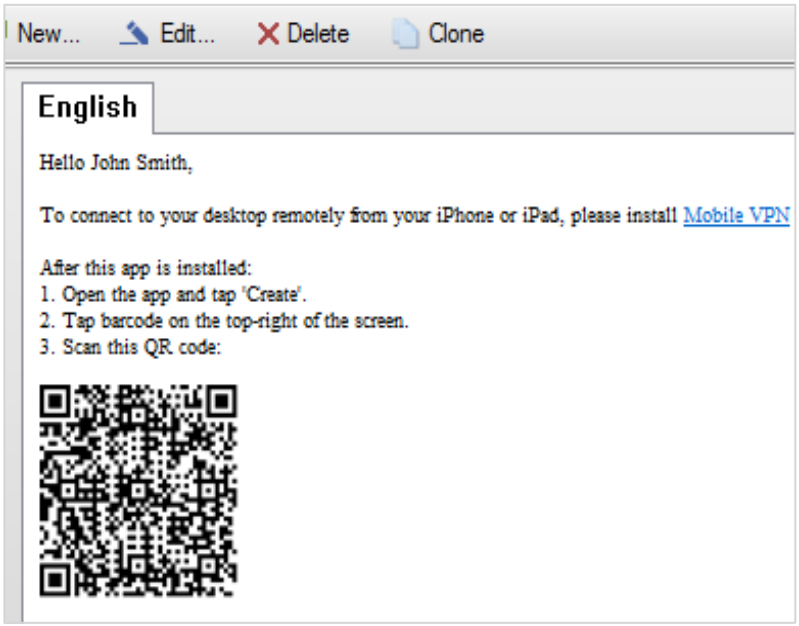
Check Point Capsule VPN (for Windows 10, 8.1)
Securely Access all your corporate resources from your device through a Virtual Private Network (VPN) tunnel. As you launch business applications such as RDP, VoIP or any other app on your mobile device, all transmitted data to corporate is encrypted, without any additional actions required by you.

Check Point Capsule Connect and Capsule VPN (for iOS and Android)
Check Point Connect for iOS and Capsule VPN for Android are simple client-to-site VPN clients available on mobile devices. Simply set up the site and connections to assets protected by the site gateway are secured by an IPsec or SSL VPN.

Check Point Capsule Workspace (for iOS and Android)
Check Point Capsule Workspace is a mobile security container on iOS and Android devices that creates an isolated corporate workspace on personal devices, making it simple to secure corporate data and assets both inside and outside the corporate network. Check Point Capsule Workspace protects and manages enterprise apps and data without needing to manage Mobile Device Management (MDM) profiles. So no matter which team is responsible for supporting smartphones and tablets, they'll value how Capsule Workspace secures mobile environments with ease – including BYOD.

Capsule Workspace is easy to deploy and manage, helping to reduce the time, effort, and cost of keeping mobile devices and data secure. Once deployed, it creates an AES256-bit encrypted container for enterprise apps and data that puts you in control of the sensitive enterprise information you need to protect. It never touches the personal apps, media, or content, on a device which helps improve end user adoption, even on personally-owned devices. Users will also appreciate the native experience and one-touch access Capsule Workspace provides to the critical enterprise apps they need to stay in touch on the go. It supports Microsoft Exchange Server and Office 365 email, calendar, and contacts, and includes secure enterprise instant messaging and document access.

Rapid and Flexible Deployment
With SmartConsole, companies can email users at their leisure with information on how to download the Mobile client directly to users' smartphones. Multiple ways to distribute notice of a Mobile client are available as well as choosing what Mobile client will be available for users using customized emails.



Endpoint VPN Clients (for Windows and macOS)
Mobile Access is part of our larger remote access solution. For additional endpoint protection, install our endpoint VPN client with or without the full Endpoint Security suite. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint system compliance scanning and encryption of all transmitted data. The VPN client has the ability to transparently establish a VPN tunnel upon demand when accessing corporate resources. The connection is re-established when roaming between networks and automatically tears down the VPN tunnel when the device is connected to the local corporate network.

CHECK POINT SECURITY MANAGEMENT

CHECK POINT SECURITY MANAGEMENT

The future of security management

Product Benefits

- Keep pace with dynamic network changes
- Reduce operational overhead
- Better align security with business goals
- Anticipate & prevent the next attack

Product Features

- Single console for all aspects of security
- Unified policy for managing entire infrastructure
- Unparalleled policy granularity & segmentation
- R80.10 API enables security self-service and automated workflows
- Concurrent administration & segregation of duties
- Integrated threat management
- Scalable, extensible architecture

INSIGHTS

Today, managing security can be a complex endeavor. The growing complexity of networks, business innovation requirements, and rapid delivery of services and applications require a new approach to managing security. Traditional security management approaches of multiple point products, manual change processes, monolithic policies and data siloes no longer work. Security needs to be agile, efficient and anticipate the latest threats.

SOLUTION

Check Point R80.10 Security Management sets the standard for reliability and ease-of-use in security management. From policies and operations to people and technology, its future-proof design anticipates your security needs. It consolidates all aspects of your security environment seamlessly so you can deploy the strongest protections across your organization effectively and efficiently – without impeding business innovation.

BUILT UPON A SCALABLE, EXTENSIBLE ARCHITECTURE

UNIFIED CONSOLE, UNIFIED POLICY

With R80.10, access control and threat prevention management for all enforcement points are fully unified under the same console, removing the need to move between multiple interfaces. Unified management for both physical and virtual networks, on-premise or cloud enforcement points, ensures security consistency and full visibility into traffic across the network.

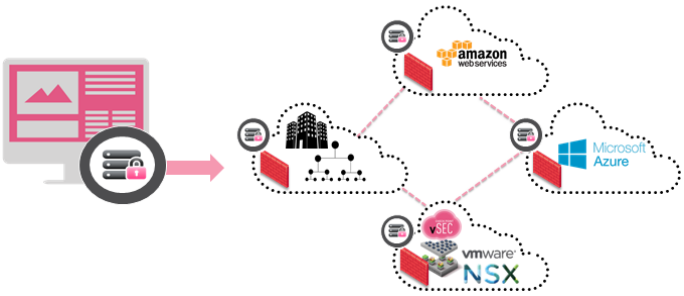


Figure 1: One single policy for your entire infrastructure

A single policy for users, data, applications and networks allows unparalleled granularity control, speeds administration and reduces policy change backlogs.

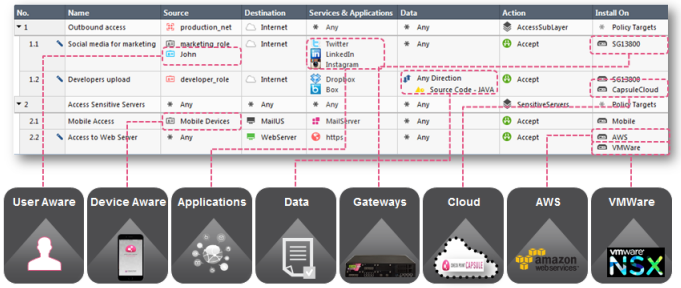


Figure 2: Unified policy with unparalleled granularity

NEXT GENERATION POLICY

Today's virtual cloud environments enable extreme agility where applications, services and servers are automatically provisioned without human interaction. Security installed on the perimeter simply cannot keep up. Check Point's next generation policy makes it extremely easy to segment policy into manageable sections. These sub-policies can be aligned to your network or business function. Each sub-policy can be delegated, automated or deployed independently. Workload can be distributed across teams, freeing key security personnel for strategic tasks.

EFFICIENT OPERATIONS

With too much work and too little staff, security teams need to work smarter. Automation and granular delegation are key to helping alleviate operational overhead. With the R80.10 API, security teams can automate any task or create web portals for security self-service.

Other efficiency elements include features built into the management interface to anticipate the daily needs of an administrator, providing him security intelligence to make better policy decisions. Concurrent administration now allows multiple administrators to work simultaneously on the same policy without conflict.

FULLY INTEGRATED THREAT MANAGEMENT

With R80.10, Threat Management is fully integrated, with logging, monitoring, event correlation and reporting in one place. A visual dashboard provides full visibility into security across the network, helping you monitor the status of your enforcement points and stay alert to potential threats.

Figure 3: Visual, comprehensive view of your environment

This fully customizable dashboard allows you to focus only on what matters to you. You get a comprehensive view of your security posture, and can quickly drill down into incident or log details with a few clicks. Reports are easily tailored to for your stakeholders and accessible from any web browser.

SCALABILITY AND EXTENSIBILITY

The R80.10 platform was built to scale to the most complex and dynamic environments. With our R80.10 API, it is easy to connect security to IT processes and systems across your network, paving the way for you to automate security change control and provisioning across your infrastructure.

SECURITY MANAGEMENT SUITE

The Check Point Security Management suite consists of the following modules:

POLICY MANAGEMENT	
Policy Management	Unified network policy management for Check Point gateways and software blades.
Multi-Domain Management	Central management of many distinct security policies across multiple domains, allowing administrators to consolidate hardware.
Management Portal	Browser-based security management access for groups, such as technical support teams or auditors, to view policies, gateway status and user administration.
OPERATIONS MANAGEMENT	
Compliance	Validates policy and configuration changes in real-time, against a library of 300+ security best practices and industry standards.
Provisioning	Centralizes Check Point device provisioning. Using profiles, security administrators can automate device configuration and easily roll out changes to multiple, geographically distributed devices via a central console. Also enables quick deployment of new devices.
Workflow	Automates policy change management to centrally manage editing, review, approval and auditing of policy changes.
User Directory	Centralizes user management, enabling gateways to use LDAP-based information stores, eliminating risks associated with manually maintaining and synchronizing redundant data stores.
THREAT MANAGEMENT	
SmartEvent and Reporter	Centralizes security event correlation for Check Point enforcement points. Minimizes time spent analyzing data, isolating and prioritizing the real security threats. Centralizes reporting on network, security and user activity and consolidates data into concise pre-defined or custom-built reports.
Monitoring	Centrally monitors Check Point devices. Alerts security team to changes in gateway, end point, remote user and security activity. Presents a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events.

R80.10 Upgrade Path	Versions
Security Management servers supported	R75.40, R75.45, R75.46, R76.47, R75.40 VS, R76, R77, R77.10, R77.20, R77.30, R80

CONTACT US
Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

CHECK POINT™

Quantum
Security Gateway

QUANTUM 6600 SECURITY GATEWAY

Quantum Security Gateway™ Advantage		
Uncompromising Security	Security at Hyperscale	Unified Security

Check Point Quantum 6600 Next Generation Firewalls enables enterprises to deploy the industry's leading threat prevention capabilities at all points of their infrastructure, scaling security almost infinitely according to their changing business needs. It also dramatically accelerates the efficiency of their security operations. This enables enterprises to prevent and block even the most advanced attacks, before they can disrupt business.

Always Protected against Gen V Attacks

Highest caliber prevention with unified security

Security at Hyperscale

On-demand expansion with hyperscalability

Efficient Operations

Cut operation management time by up to 80%

PERFORMANCE HIGHLIGHTS

Gen II Security Firewall	Gen III Security NGFW [1]	Gen V Security Advanced Threat Prevention [2]
18 Gbps	6.2 Gbps	3.7 Gbps

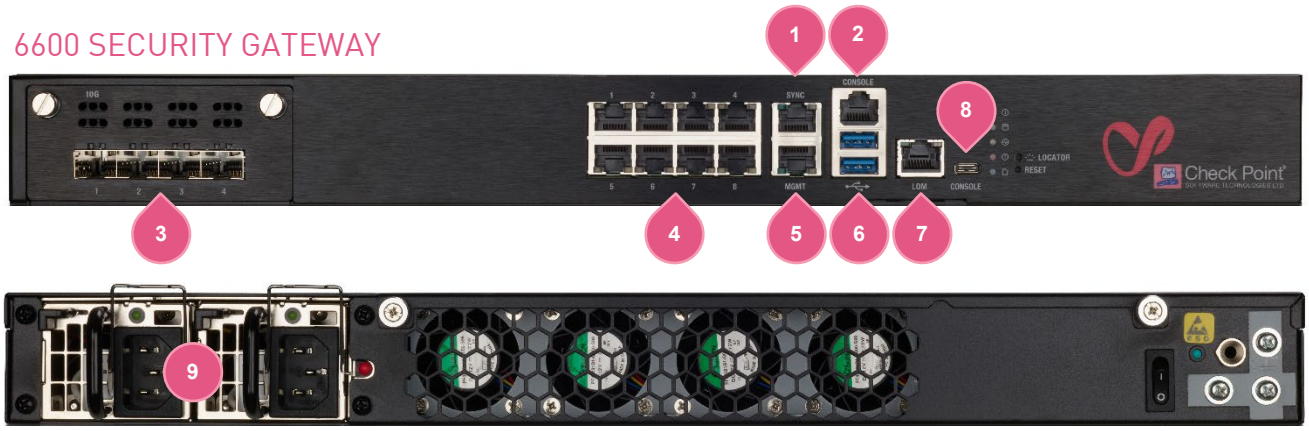
Performance measured with enterprise testing conditions. Additional performance details on page 3. 1: Includes Firewall, Application Control, and IPS. 2: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection.

CHECK POINT™

Quantum
Security Gateway

SPOTLIGHT

6600 SECURITY GATEWAY



1.	Sync 10/100/1000 Base-T port	6.	2x USB 3.0 ports
2.	RJ45 console port	7.	Lights-out Management port
3.	1 network expansion slot	8.	USB Type-C console port
4.	8x 10/100/1000 Base-T ports	9.	Redundant hot-swap power supplies
5.	Management 10/100/1000 Base-T port		

Prevent Known and Zero-day Threats

Check Point SandBlast Threat Emulation is an evasion-resistant sandbox that provides zero-day protection from advanced and unknown threats. SandBlast Threat Extraction (CDR) ensures quick delivery of safe email and web content to users.

	NGFW	NGTP	SNBT
Firewall, VPN, Mobile Access	✔	✔	✔
Content Awareness	✔	✔	✔
Application Control	✔	✔	✔
Intrusion Prevention System	✔	✔	✔
URL Filtering		✔	✔
Antivirus and Anti-Bot		✔	✔
Threat Emulation (sandboxing)			✔
Threat Extraction (CDR)			✔

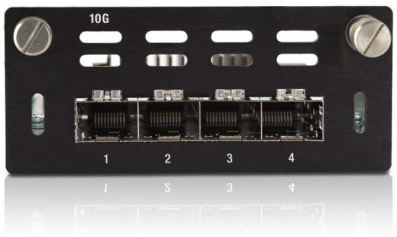
Next Generation Firewall, Next Generation Threat Prevention and SandBlast packages

All-inclusive Security Solutions

Check Point 6600 security gateways include all security technologies in the SandBlast software package for one year. Purchase a renewal for NGFW, NGTP or SandBlast (SNBT) for subsequent years as you like.

High Performance Options

Purchase the affordable Plus package and get a base system plus 4x 10GbE SFP+ ports with transceivers, 2x AC power supplies, Lights-out Management and 16 GB of memory for high connection capacity.



Remote Management and Monitoring

A Lights-Out-Management (LOM) card provides out-of-band management to remotely diagnose, start, restart and manage the appliance from a remote location.

ENTERPRISE-GRADE PLATFORM

	1 GbE (copper)	1 GbE (fiber)	10 GbE	Memory	Redundant Power	LOM
Base model	10	0	0	8 GB	○	○
Plus model	10	0	4	16 GB	●	●
Max capacity	18	4	4	32 GB	●	●

○ optional accessory

CHECK POINT™

Quantum
Security Gateway

SPECIFICATIONS

Performance

Enterprise Test Conditions

Threat Prevention[1] (Gbps)	3.7
NGFW[2] (Gbps)	6.2
IPS (Gbps)	10.14
Firewall (Gbps)	18

RFC 3511, 2544, 2647, 1242 Peformance (Lab)

Firewall 1518B UDP (Gbps)	32
VPN AES-128 (Gbps)	4.9
Connections/sec	116,000
Concurrent connections[3]	2/4/8M

1: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled. 2: Includes Firewall, Application Control and IPS with logging enabled. 3: Performance measured with default/Plus/maximum memory.

Additional Features

Highlights

- 1x CPUs, 6x physical cores
- 1x 240 GB SSD storage
- 1 AC or DC power supply (2x in Plus)
- 8, 16 and 32 GB memory options
- Lights-Out-Management (included in Plus)
- Virtual Systems (Base/Plus/max mem): 10/20/20

Network Expansion Slot Options (1 of 1 slots open)

- 8x 10/100/1000Base-T RJ45 port card, up to 18 ports
- 4x 1000Base-F SFP port card, up to 4 ports
- 4x 10GBase-F SFP+ port card, up to 4 ports

Content Security

First Time Prevention Capabilities

- CPU-level, OS-level and static file analysis
- File disarm and reconstruction via Threat Extraction
- Average emulation time for unknown files that require full sandbox evaluation is under 100 seconds
- Maximal file size for Emulation is 100 MB
- Emulation OS Support: Windows XP, 7, 8.1, 10

Applications

- Use 8,500+ pre-defined or customize your own applications
- Accept, prevent, schedule, and apply traffic-shaping

Data Loss Prevention

- Classify 700+ pre-defined data types
- End user and data owner incident handling

Content Security (continued)

Dynamic User-based Policy

- Integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API
- Enforce consistent policy for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active L2, Active/Passive L2 and L3
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64, NAT46
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply rating: 300W
- AC power input: 100 to 240V (50-60Hz)
- Power consumption avg/max: 84W/122W
- Maximum thermal output: 416 BTU/hr.

Dimensions

- Enclosure: 1RU
- Dimensions (WxDxH): 17.2 x 20 x 1.73 in.(438 x 508 x 44mm)
- Weight (Base/Plus): 16.5/17.4 lbs. (7.5/7.9 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5 to 95%
- Storage: –20° to 70°C, humidity 5 to 95%

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, WEEE, REACH[1], ISO14001[1]

[1]. factory certificate

ORDERING QUANTUM 6600 SECURITY GATEWAYS

BASE CONFIGURATION [1]	SKU
6600 Security Gateway Base Configuration, includes 10x 1GbE copper ports, 8 GB RAM, 1 SSD, 1 AC PSU, telescopic rails, SandBlast (SNBT) Security Subscription Package for 1 Year.	CPAP-SG6600-SNBT
6600 Security Gateway Plus Configuration, includes 10x 1GbE copper ports, 4x 10GbE SFP+ ports, 4x SFP+ SR transceivers, 16 GB RAM, 1 SSD, 2x AC PSU, Lights-out Management, telescopic rails, SandBlast (SNBT) Security Subscription Package for 1 Year.	CPAP-SG6600-PLUS-SNBT

The Base and Plus packages include 2 trial virtual systems (VS). These are not additive or counted when adding additional VS licenses.

1. Renewal NGFW, NGTP and SandBlast (SNBT) packages are available in the online product catalog.

Accessories

INTERFACE CARDS AND TRANSCEIVERS	
8 Port 10/100/1000 Base-T RJ45 interface card	CPAC-8-1C-C
4 Port 1000Base-F SFP interface card; requires additional 1000Base SFP transceivers	CPAC-4-1F-C
SFP transceiver module for 1G fiber ports - long range (1000Base-LX)	CPAC-TR-1LX-C
SFP transceiver module for 1G fiber ports - short range (1000Base-SX)	CPAC-TR-1SX-C
SFP transceiver to 1000 Base-T RJ45 (Copper)	CPAC-TR-1T-C
4 Port 10GBase-F SFP+ interface card	CPAC-4-10F-C
SFP+ transceiver module for 10G fiber ports - for links up to 40km (10GBASE-ER)	CPAC-TR-10ER-C
SFP+ transceiver module for 10G fiber ports - long range up to 10km (10GBase-LR)	CPAC-TR-10LR-C
SFP+ transceiver module for 10G fiber ports - short range (10GBase-SR)	CPAC-TR-10SR-C
SFP+ transceiver 10GBASE-T RJ45 (Copper) - for links up to 30m over CAT6a/CAT7	CPAC-TR-10T-C
4 Port 1GE copper Bypass (Fail-Open) Network interface card (10/100/1000 Base-T)	CPAC-4-1C-BP-C
2 Port 10GE Short-range Fiber Bypass (Fail-Open) Network interface card (10GBase-SR)	CPAC-2-10FSR-BP-C

MEMORY	SKU
Memory upgrade kit from 8GB to 16GB for 6600 appliance	CPAC-RAM8GB-6600
Memory upgrade kit from 8GB to 32GB for 6600 appliance	CPAC-RAM24GB-6600
Memory upgrade kit from 16GB to 32GB for 6600 appliance	CPAC-RAM16GB-6600

SPARES AND MISCELLANEOUS	SKU
Additional/Replacement AC Power Supply for 6600, 6700, 6900 appliances	CPAC-PSU-AC-6600/6700/6900
Additional/Replacement DC Power Supply for 6600, 6700, 6900 appliances	CPAC-PSU-DC-6600/6700/6900
Lights Out Management module	CPAC-NLOM-C
Slide rails for 6000 and 7000 Security Appliances (22" - 32")	CPAC-RAILS-6000/7000
Telescopic slide rails for 6000 and 7000 Security Appliances (24" - 36")	CPAC-RAILS-EXT-6000/7000

Ministério da Economia
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins previstos na Lei nº 8.666, de 1993, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**05.250.796/0001-54**	DUNS®:	**91*****45**
Razão Social:	**NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**		
Nome Fantasia:	**NETWORK SECURE**		
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**24/11/2022**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Demais**		

Ocorrências e Impedimentos

Ocorrência:	**Nada Consta**
Impedimento de Licitar:	**Nada Consta**

Níveis cadastrados:

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**30/07/2022**
FGTS		Validade:	**26/02/2022**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**05/08/2022**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**25/03/2022**
Receita Municipal	Validade:	**24/03/2022**

VI - Qualificação Econômico-Financeira

Validade: **30/04/2022**

Esta declaração é uma simples consulta e não tem efeito legal

CPF: 648.711.503-72 Nome: JOSE MURILO CIRINO NOGUEIRA JUNIOR
Ass: _____

Ministério da Economia
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Certificado de Registro Cadastral - CRC

(Emissão conforme art. 17 da Instrução Normativa nº 03, de 26 abril de 2018)

CNPJ: **05.250.796/0001-54**

Razão Social: **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**

Atividade Econômica Principal:

4651-6/01 - COMÉRCIO ATACADISTA DE EQUIPAMENTOS DE INFORMÁTICA

Endereço:

AVENIDA PONTES VIEIRA, 2340 - SALAS 510 A 514 - DIONISIO TORRES - Fortaleza / Ceará

Observações:

A veracidade das informações poderá ser verificada no endereço www.comprasgovernamentais.gov.br.

Este certificado não substitui os documentos enumerados nos artigos 28 a 31 da Lei nº 8.666, de 1993.

Ministério da Economia
Secretaria de Governo Digital
Departamento Nacional de Registro Empresarial e Integração
Secretaria do Desenvolvimento Econômico

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
23201712520	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial do Estado do Ceará

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP
CEP2000234531

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		2211	1	ALTERACAO DE ENDERECO DENTRO DO MESMO MUNICIPIO
		2003	1	ALTERACAO DE SOCIO/ADMINISTRADOR
		2001	1	ENTRADA DE SOCIO/ADMINISTRADOR

FORTALEZA
Local

30 Outubro 2020
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
20/150.819-2	CEP2000234531	30/10/2020

Identificação do(s) Assinante(s)	
CPF	Nome
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA

CNPJ(MF) nº 05.250.796/0001-54
Nire/Jucec nº **23.2.0171252-0**

Terceira Alteração e Consolidação do Contrato Social

Pelo presente instrumento particular e na melhor forma de direito os abaixo qualificados:
JOSE MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 99010123694 SSP/CE e do CPF/MF sob nº 648.711.503-72, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, na Av. Coronel Miguel Dias, 1010 – Torre A - Apto 1301 – Bairro: Guararapes - CEP: 60810-160;
TATIANA RIBEIRO LEITE, brasileira, solteira, nascida em 29/06/1977, empresaria, portadora da Carteira de Identidade n° 93002319934 SSPDC/CE e do CPF(MF) n° 691.833.093-49, residente e domiciliada na cidade de Fortaleza, estado do Ceará na Rua Franklin Bezerra, 212 – Bairro: Mondubim – CEP: 60.762-260; e
ALARICO ISAIAS DE SOUSA GUIMARAES, brasileiro, casado em regime de comunhão parcial de bens, nascido em 23/04/1980, empresário, portador da Carteira de Identidade n° 96002206506 SSPDS/CE e do CPF(MF) n° 620.143.313-91, residente e domiciliado na cidade de Fortaleza, estado do Ceará na Av. Paisagística, 06 - Apto 407 - Bairro: Itaperi - CEP: 60.743-065.

Únicos sócios da sociedade limitada denominada "**NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**.", estabelecida na cidade de Fortaleza, estado do Ceará, na Rua Capitão Melo, 3373 - Bairro: Joaquim Távora – CEP: 60.120-220, inscrita no CNPJ(MF) 05.250.796/0001-54, registrada na Junta Comercial do Estado do Ceará sob nire n° 23.2.0171252-0, decidem, de comum acordo, alterar e consolidar seu Contrato Social, e o fazem mediante as cláusulas a seguir, em conformidade com o Código Civil Brasileiro:

Primeira – A sociedade resolve alterar o endereço de sua sede social, passando a estabelecer-se na Av. Pontes Vieira, 2340 – Salas 510 a 514 – Bairro: Dionísio Torres – CEP: 60135-238 – Fortaleza – Ceará.

Segunda – Ingressa na sociedade **YURE LEOPOLDO SABINO DE FREITAS**, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 559056187 SSP/SP e do CPF/MF sob nº 525.285.023-20, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, na Rua Barbara de Souza Costa, 100 – CS 08 - Bairro: Lagoa Redonda - CEP: 60831-083, através da transferência de R$10.526,00 (dez mil e quinhentos e vinte e seis reais), representado por 10.526 (dez mil e quinhentas e vinte e seis) quotas de capital de valor unitário R$1,00 (um real) pelo sócio **JOSE MURILO CIRINO NOGUEIRA JUNIOR,** acima qualificado, dando as partes mutuamente, plena geral e irretratável quitação.

Terceira – Após a alteração acima o capital Social da sociedade no valor de R$421.052,00 (quatrocentos e vinte e um mil e cinquenta e dois reais), dividido em 421.052 (quatrocentas e vinte e uma mil e cinquenta e duas) quotas de capital de valor unitário R$1,00 (um real), já

totalmente integralizado em moeda corrente nacional, fica distribuído entre os sócios da seguinte forma:

Sócios	Nº quotas	Valor(R$)	Part(%)
JOSE MURILO CIRINO NOGUEIRA JUNIOR	389.474	389.474,00	92,50
ALARICO ISAIAS DE SOUSA GUIMARAES	10.526	10.526,00	2,50
TATIANA RIBEIRO LEITE	10.526	10.526,00	2,50
YURE LEOPOLDO SABINO DE FREITAS	10.526	10.526,00	2,50
Total do Capital	421.052	421.052,00	100,00

§ 1º **-** Cada quota é indivisível e confere a seu titular o direito a um voto nas deliberações sociais.

§ 2º – A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integralização do capital social.

§ 3º - Na forma do art. 997, inciso VIII, da Lei 10.406/02, os sócios não respondem subsidiariamente pelas obrigações sociais.

Quarta – Os sócios resolvem consolidar o texto do contrato social que passa a vigorar com a seguinte redação:

Contrato Social Consolidado

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ(MF) nº 05.250.796/0001-54
Nire/Jucec nº 23.2.0171252-0

JOSE MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 99010123694 SSP/CE e do CPF/MF sob nº 648.711.503-72, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, à Rua Vicente Linhares, 985 - Apt. 2102 – Bairro: Aldeota - CEP: 60135-270;
TATIANA RIBEIRO LEITE, brasileira, solteira, nascida em 29/06/1977, empresaria, portadora da Carteira de Identidade n° 93002319934 SSPDC/CE e do CPF(MF) n° 691.833.093-49, residente e domiciliada na cidade de Fortaleza, estado do Ceará na Rua Franklin Bezerra, 212 – Bairro: Mondubim – CEP: 60.762-260;
ALARICO ISAIAS DE SOUSA GUIMARAES, brasileiro, casado em regime de comunhão parcial de bens, nascido em 23/04/1980, empresário, portador da Carteira de Identidade n° 96002206506 SSPDS/CE e do CPF(MF) n° 620.143.313-91, residente e domiciliado na cidade de Fortaleza, estado do Ceará na Av. Paisagística, 06 - Apto 407 - Bairro: Itaperi - CEP: 60.743-065; e
YURE LEOPOLDO SABINO DE FREITAS, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 559056187 SSP/SP e do CPF/MF sob

nº 525.285.023-20, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, na Rua Barbara de Souza Costa, 100 – CS 08 - Bairro: Lagoa Redonda - CEP: 60831-083.

Tem entre si, justos e contratados, uma sociedade empresária Limitada, a qual é regida em conformidade com as seguintes clausulas e condições:

Cláusula Primeira – Denominação Social

A sociedade gira sob o nome empresarial de **" NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA"**., adotando por nome de fantasia a expressão "**NETWORK SECURE**".

Cláusula Segunda - Sede e Filiais

A sede e domicílio fiscal da sociedade é na Cidade de Fortaleza, estado do Ceará, na Rua Capitão Melo, 3373 - Bairro: Joaquim Tavora – CEP: 60.120-220.

§ Único - A sociedade não possui filiais, podendo quando servir aos seus interesses, abrir escritórios, representações, sucursais ou outras filiais neste estado ou em qualquer parte do território nacional e no Exterior, destacando para estas uma parte do capital social da matriz.

Clausula Terceira – Objetivo Social

A sociedade tem por objetivo as seguintes atividades:

a) Comercio atacadista de equipamentos de informatica – CNAE 4651-6/01;
b) Locação de equipamentos de computadores e perifericos – CNAE 7733-1/00;
c) Desenvolvimento e licenciamento de programas de computador customizaveis – CNAE 6202-3/00;
d) Suporte tecnico, manutenção e outros serviços em tecnologia da informação – CNAE 6209-1/00;
e) Reparação e Manutenção de computadores e de equipamentos perifericos – CNAE 9511-8/00;
f) Consultoria em Tecnologia da informação – CNAE 6204-0/00;
g) Consultoria em gestão empresarial – CNAE 7020-4/00; e
h) Treinamento em informatica – CNAE 8599-6/03.

Cláusula Quarta – Duração e Inicio das Atividades

A sociedade iniciou suas atividades em 20/08/2002 e sua duração será por tempo indeterminado.

Clausula Quinta – Capital Social

O capital Social da sociedade é de R$421.052,00 (quatrocentos e vinte e um mil e cinquenta e dois reais), dividido em 421.052 (quatrocentas e vinte e uma mil e cinquenta e duas) quotas de

capital de valor unitário R$1,00 (um real), já totalmente integralizado em moeda corrente nacional, distribuídos da seguinte forma:

Sócios	Nº quotas	Valor(R$)	Part(%)
JOSE MURILO CIRINO NOGUEIRA JUNIOR	389.474	389.474,00	92,50
ALARICO ISAIAS DE SOUSA GUIMARAES	10.526	10.526,00	2,50
TATIANA RIBEIRO LEITE	10.526	10.526,00	2,50
YURE LEOPOLDO SABINO DE FREITAS	10.526	10.526,00	2,50
Total do Capital	421.052	421.052,00	100,00

§ 1º **-** Cada quota é indivisível e confere a seu titular o direito a um voto nas deliberações sociais.

§ 2º – A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integralização do capital social.

§ 3º - Na forma do art. 997, inciso VIII, da Lei 10.406/02, os sócios não respondem subsidiariamente pelas obrigações sociais.

Clausula Sexta – Administração

A Administração e o uso da denominação social da sociedade são exercidos pelo sócio **JOSE MURILO CIRINO NOGUEIRA JUNIOR**, já qualificado anteriormente, com os poderes e atribuições de Administrador, que assinará e representará a sociedade, ativa e passivamente, seja como autor ou réu, em juízo ou fora dele e perante terceiros e qualquer repartição pública, ou quaisquer autoridades federais, estaduais ou municipais, bem como, autarquias, sociedade de economia mista e para-estatais.

§ 1º - Os sócios poderão receber "pro-labore" em valores e periodicidade fixada de comum acordo entre eles no início de cada exercício social.

§ 2º - É vedado ao administrador fazer uso da firma na prestação de garantia, fiança, aval ou qualquer outro título de favor, em negócios estranhos ao objeto social.

§ 3º - A sociedade poderá nomear procuradores para, especificando no instrumento de procuração os poderes e o prazo de vigência do mandato.

Clausula Sétima – Deliberações Sociais

Nos termos do disposto no artigo 1076 – Incisos I e II da Lei 10.406/02, o presente contrato poderá ser alterado, inclusive, para transformação do tipo societário, assim como, da ocorrência dos eventos de cisão, fusão ou incorporação com outras sociedades ou em outras sociedades pela vontade de sócios que representem, no mínimo, 75% (setenta e cinco por cento) das quotas de capital da sociedade.

§ Único - No caso de exclusão de sócio que esteja colocando em risco os interesses da sociedade, a alteração do Contrato Social poderá ser realizada por sócios que representem mais de 50% (cinqüenta por cento) do Capital Social.

Clausula Oitava – Prestação de Contas

Nos quatro primeiros meses seguintes ao término de cada exercício social, os sócios deliberarão sobre as contas do exercício e designarão ou substituirão administrador(es) quando for o caso.

Clausula Nona – Transferências de quotas

Nenhum quotista poderá ceder, transferir, alienar ou onerar, a qualquer titulo, suas quotas antes de ofertá-las aos demais quotistas, que terão preferência para aquisição das mesmas por seu respectivo valor, determinado de acordo com o último balanço patrimonial, na proporção do capital que cada um possua. A avaliação das cotas poderá ser feita por critérios baseados em valor de mercado, obtido pela avaliação de especialista indicado pelos demais quotistas, ficando o ônus da contratação às custas do quotistas que deseje ceder, transferir, alienar ou onerar, a qualquer título, suas cotas.

§ 1° - Qualquer quotista que pretender ceder, transferir, alienar ou onerar, a qualquer titulo, suas quotas deverá comunicar sua intenção aos demais sócios, por escrito, com aviso prévio de 30 (trinta) dias, contendo todas as condições da oferta.

§ 2° – Decorrido os 30 (trinta) dias, se algum quotista não exercer a opção a ele assegurada de acordo com o presente, as quotas que ele poderia ter comprado serão oferecidas aos quotistas remanescentes, que terão 5 (cinco) dias, a partir da data da respectiva comunicação, para exercer a opção ou renunciar a mesma.

§ 3° – Cumpridos os prazos e condições fixadas acima, as quotas remanescentes poderão ser alienadas a terceiros interessados, nas mesmas condições de oferta citada no parágrafo primeiro. Na eventualidade da alienação não se concluir e se o ofertante desejar dispor das quotas em condições diferentes daquelas originariamente informadas, o procedimento indicado nos parágrafos anteriores deverá ser novamente observado, e assim sucessivamente até que todas as quotas sejam vendidas, cedidas ou transferidas, em conformidade com a intenção do titular.

§ 4° – Toda e qualquer venda, cessão, oneração ou transferência de quotas que for realizada sem a observância ao disposto nesta clausula será considerada nula de pleno direito e sem qualquer efeito.

Clausula Décima – Dissolução da sociedade

Ocorrendo qualquer situação que implique na dissolução da sociedade, será permitido ao sócio remanescente admitir novo(s) sócio(s) para dar continuidade à mesma.

§ 1° – Os haveres do sócio retirante, morto, invalido, excluído serão apurados com base no ultimo balanço patrimonial levantado pela sociedade, anterior a data da retirada, morte, invalidez ou exclusão e será pago a quem de direito, em até 12 (doze) prestações mensais, iguais e consecutivas atualizadas pelo índice oficial que reflita a variação da inflação.

§ 2º - No caso de falecimento até que se ultime, no processo de inventário, a partilha dos bens deixados pelo de cujus, incumbirá ao inventariante, para todos os efeitos legais, a representação ativa e passiva dos interessados perante a sociedade. Os herdeiros, através de seu inventariante ou representante legal, poderão retirar-se da sociedade.

§ 3º - A retirada, morte, invalidez ou exclusão do sócio, não o exime, ou a seus herdeiros, da responsabilidade pelas obrigações sociais anteriores, até dois anos depois de averbada a resolução da sociedade.

Clausula Décima Primeira – Exercício Social

O exercício social terminará em 31 de dezembro de cada ano, quando será levantado o balanço patrimonial correspondente, bem como, preparadas as demais demonstrações contábeis/financeiras exigidas por lei. Os lucros e/ou prejuízos apurados poderão ser distribuídos proporcionalmente ou desproporcionalmente a participação dos sócios no capital social, não se excluindo da distribuição nenhum dos sócios.

§ 1º - No caso de distribuição desproporcional a participação dos sócios no capital social, será necessária a deliberação unanime dos sócios, lavrando-se ata de reunião dos sócios, realizada especialmente para esta finalidade, devendo haver a unanimidade dos sócios.

§ 2º - A sociedade no interesse dos sócios poderá levantar balanços mensalmente ou noutro período, em qualquer data e em razão dos resultados apurados efetuar a distribuição de lucros ou dividendos e/ou de juros sobre o Capital Social.

Clausula Décima Segunda – Declaração de Desimpedimento

O administrador declara, sob as penas da Lei, que não está impedido de exercer a administração da sociedade, por Lei especial, ou em virtude condenação criminal, ou por se encontrar sob os efeitos dela a pena que vede ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra norma de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

Clausula Décima Terceira – Normas Contratuais Omissas

Os casos omissos do presente contrato serão resolvidos pela aplicação dos dispositivos do Código Civil Brasileiro (Lei 10.406/02) e, supletivamente pela Lei das Sociedades Anônimas (Lei 6.404/76) e sem prejuízo de legislações supervenientes e que venham a tratar da matéria.

Clausula Décima Quarta - Foro

As partes, de comum acordo, elegem o Foro da Comarca de Fortaleza, Estado do Ceará, renunciando a qualquer outro, por mais privilegiado que seja, para dirimir qualquer dúvida que possa emergir deste documento.

E, por estarem justos e contratados, assinam o presente Instrumento de Alteração e Consolidação do Contrato Social.

Fortaleza/CE, 12 de fevereiro de 2019.

Sócios:

JOSE MURILO CIRINO NOGUEIRA JUNIOR
SÓCIO ADMINISTRADOR

ALARICO ISAIAS DE SOUSA GUIMARAES
SÓCIO

TATIANA RIBEIRO LEITE
SÓCIO

YURE LEOPOLDO SABINO DE FREITAS
SÓCIO

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
20/150.819-2	CEP2000234531	30/10/2020

Identificação do(s) Assinante(s)	
CPF	Nome
620.143.313-91	ALARICO ISAIAS DE SOUSA GUIMARAES
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR
691.833.093-49	TATIANA RIBEIRO LEITE
525.285.023-20	YURE LEOPOLDO SABINO DE FREITAS

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, de NIRE 2320171252-0 e protocolado sob o número 20/150.819-2 em 05/11/2020, encontra-se registrado na Junta Comercial sob o número 5481638, em 06/11/2020. O ato foi deferido eletrônicamente pelo examinador Jairo Bezerra Lira.

Certifica o registro, a Secretária-Geral, Lenira Cardoso de Alencar Seraine. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (http://portalservicos.jucec.ce.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)	
CPF	Nome
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR

Documento Principal

Assinante(s)	
CPF	Nome
691.833.093-49	TATIANA RIBEIRO LEITE
620.143.313-91	ALARICO ISAIAS DE SOUSA GUIMARAES
525.285.023-20	YURE LEOPOLDO SABINO DE FREITAS
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR

Declaração Documento(s) Anexo(s)

Assinante(s)	
CPF	Nome
313.429.653-53	OLAVO BRASIL MAGALHAES

Fortaleza. Sexta-feira, 06 de Novembro de 2020

Documento assinado eletrônicamente por Jairo Bezerra Lira, Servidor(a) Público(a), em 06/11/2020, às 11:54 conforme horário oficial de Brasília.

A autencidade desse documento pode ser conferida no portal de serviços da jucec informando o número do protocolo 20/150.819-2.

O ato foi deferido e assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
236.117.073-68	LENIRA CARDOSO DE ALENCAR SERAINE

Fortaleza. Sexta-feira, 06 de Novembro de 2020

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
05.250.796/0001-54 **MATRIZ**		**02/08/2002**

NOME EMPRESARIAL
NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
NETWORK SECURE	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
46.51-6-01 - Comércio atacadista de equipamentos de informática (Dispensada *)

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
46.15-0-00 - Representantes comerciais e agentes do comércio de eletrodomésticos, móveis e artigos de uso doméstico (Dispensada *)
46.18-4-99 - Outros representantes comerciais e agentes do comércio especializado em produtos não especificados anteriormente (Dispensada *)
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis (Dispensada *)
62.04-0-00 - Consultoria em tecnologia da informação (Dispensada *)
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação (Dispensada *)
70.20-4-00 - Atividades de consultoria em gestão empresarial, exceto consultoria técnica específica (Dispensada *)
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios (Dispensada *)
85.99-6-03 - Treinamento em informática (Dispensada *)
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos (Dispensada *)

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV PONTES VIEIRA	**2340**	**SALAS 510 A 514**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
60.135-238	**DIONISIO TORRES**	**FORTALEZA**	**CE**

ENDEREÇO ELETRÔNICO	TELEFONE
ANDREA@NETWORKSECURE.COM.BR	**(85) 3195-2200**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**03/11/2005**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

(*) *A dispensa de alvarás e licenças é direito do empreendedor que atende aos requisitos constantes na Resolução CGSIM nº 51, de 11 de junho de 2019, ou da legislação própria encaminhada ao CGSIM pelos entes federativos, não tendo a Receita Federal qualquer responsabilidade quanto às atividades dispensadas.*

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **04/01/2022** às **14:24:34** (data e hora de Brasília). Página: **1/1**

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
CNPJ: 05.250.796/0001-54

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 10:29:43 do dia 31/01/2022 <hora e data de Brasília>.
Válida até 30/07/2022.
Código de controle da certidão: **21EE.D3D4.A352.5597**
Qualquer rasura ou emenda invalidará este documento.

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 05.250.796/0001-54
Razão Social: NETWORK SECURE SEGURANCA DA INFORM LTDA
Endereço: R CAPITAO MELO 3373 / JOAQUIM TAVORA / FORTALEZA / CE / 60120-220

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 28/01/2022 a 26/02/2022

Certificação Número: 2022012800590011969857

Informação obtida em 28/01/2022 14:46:23

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA (MATRIZ E FILIAIS)
CNPJ: 05.250.796/0001-54
Certidão nº: 28234382/2021
Expedição: 14/09/2021, às 11:03:44
Validade: 12/03/2022 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **05.250.796/0001-54**, **NÃO CONSTA** do Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base no art. 642-A da Consolidação das Leis do Trabalho, acrescentado pela Lei nº 12.440, de 7 de julho de 2011, e na Resolução Administrativa nº 1470/2011 do Tribunal Superior do Trabalho, de 24 de agosto de 2011.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho e estão atualizados até 2 (dois) dias anteriores à data da sua expedição.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho ou Comissão de Conciliação Prévia.

ESTADO DO CEARÁ
SECRETARIA DA FAZENDA
FICHA DE INSCRIÇÃO DO CONTRIBUINTE

FIC

C.G.F
06.180540-8

RAZÃO SOCIAL
NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

ENDEREÇO COMPLETO
PONTES VIEIRA , 02340
Compl.:SALAS 510 A 514 Bairro:DIONISIO TORRES CEP:60135238
Cidade:FORTALEZA UF:CE Distrito: FORTALEZA

C.N.P.J.	CÓD. ÓRGÃO LOCAL
05.250.796/0001-54	201.1000-1
C.N.A.E. PRINCIPAL	**DESCRIÇÃO UNIDADE AUXILIAR**
4651601 - Comércio atacadista de equipamentos de informática	###########
C.N.A.E. PRINCIPAL(ARRECADAÇÃO/FISCALIZAÇÃO)	**C.G.F. ESTABELECIMENTO VINCULADO**
4651601 - Comércio atacadista de equipamentos de informática	###########
C.N.A.E. SECUNDÁRIO	**REGIME DE RECOLHIMENTO**
6209100	NORMAL
C.N.A.E. SECUNDÁRIO 2	**NATUREZA JURÍDICA**
9511800	3 - SOCIEDADE EMPRESARIA LTDA

EMITIDA VIA INTERNET EM 31/01/2022 ÀS 14:28:54

A autenticidade deste documento deverá ser comprovada via Internet, no endereço http://www.sefaz.ce.gov.br

SECRETARIA MUNICIPAL DAS FINANÇAS - SEFIN
CADASTRO DE PRODUTORES DE BENS E SERVIÇOS - CPBS

COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL

NÚMERO DE INSCRIÇÃO
176407-1

DATA INÍCIO ATIVIDADE NO MUNICÍPIO
20/08/2002

NOME / RAZÃO SOCIAL
NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

CPF/CNPJ
05.250.796/0001-54

NOME DE FANTASIA
NETWORK SECURE

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL / OCUPAÇÃO
465160101 - COMÉRCIO ATACADISTA DE EQUIPAMENTOS DE INFORMÁTICA

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS / OCUPAÇÕES
951180001 - REPARAÇÃO E MANUTENÇÃO DE COMPUTADORES E DE EQUIPAMENTOS PERIFERICOS
859960301 - TREINAMENTO EM INFORMÁTICA
461500001 - REPRESENTANTES COMERCIAIS E AGENTES DO COMÉRCIO DE ELETRODOMÉSTICOS, MÓVEIS E ARTIGOS DE USO DOMÉSTICO
461849901 - OUTROS REPRESENTANTES COMERCIAIS E AGENTES DO COMÉRCIO ESPECIALIZADO EM PRODUTOS NÃO ESPECIFICADOS ANTERIORMENTE
620230001 - DESENVOLVIMENTO DE PROGRAMAS DE COMPUTADOR CUSTOMIZAVEIS
620400001 - CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO
620910001 - SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO
702040001 - ATIVIDADES DE CONSULTORIA EM GESTAO EMPRESARIAL, EXCETO CONSULTORIA TECNICA ESPECIFICA
773310001 - ALUGUEL DE MAQUINAS E EQUIPAMENTOS PARA ESCRITORIO

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - SOCIEDADE EMPRESÁRIA LIMITADA

TIPO DE ESTABELECIMENTO
MATRIZ

LOGRADOURO
AV PONTES VIEIRA, 2340

COMPLEMENTO
SALA 510

BAIRRO
DIONÍSIO TORRES

CEP
60135-238

MUNICÍPIO
FORTALEZA

UF
CE

SITUAÇÃO CADASTRAL
ATIVA

REGIME DE TRIBUTAÇÃO
NORMAL

SUBSTITUTO TRIBUTÁRIO
NÃO

OPTANTE DO SIMEI
NÃO

OPTANTE DO SIMPLES NACIONAL
NÃO

DATA DA OPÇÃO NO SIMPLES / SIMEI

DATA DE CADASTRO NA SEFIN
02/08/2002

EMITIDO VIA INTERNET EM 31/01/2022 ÀS 14:34:54
http://www.sefin.fortaleza.ce.gov.br

GOVERNO DO
ESTADO DO CEARÁ
Procuradoria Geral do Estado

Certidão Negativa de Débitos Estaduais

202201432427

Emitida para os efeitos da Instrução Normativa Nº 13 de 02/03/2001

IDENTIFICAÇÃO DO(A) REQUERENTE
Inscrição Estadual: 061805408
CNPJ / CPF: 05250796000154
RAZÃO SOCIAL: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Ressalvado o direito da Fazenda Estadual de inscrever e cobrar as dívidas que venham a ser apuradas, certifico, para fins de direito, que revendo os registros do Cadastro de Inadimplentes da Fazenda Pública Estadual - CADINE, verificou-se nada existir em nome do(a) requerente acima identificado(a) até a presente data e horário, e, para constar, foi emitida esta certidão.

EMITIDA VIA INTERNET EM 24/01/2022 ÀS 10:28:21
VÁLIDA ATÉ 25/03/2022

A autenticidade deste documento deverá ser comprovada via Internet, no endereço www.sefaz.ce.gov.br

Fortaleza
PREFEITURA
Finanças

SECRETARIA MUNICIPAL DAS FINANÇAS - SEFIN

CERTIDÃO NEGATIVA DE DÉBITOS DE TRIBUTOS MUNICIPAIS

Certidão Nº 2021/293755

CPF/CNPJ: 05.250.796/0001-54

Nome ou Razão Social: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Endereço: AV PONTES VIEIRA 2340 SALA 510 DIONÍSIO TORRES CEP 60135-238

Certificamos, para fins de comprovação perante terceiros, que a pessoa acima identificada, até a presente data, não possui débitos de natureza tributária para com o Município de Fortaleza, ressalvado, porém, à Secretaria Municipal das Finanças, o direito de cobrar e inscrever, a qualquer tempo, quaisquer dividas em seu nome na forma da legislação vigente.

Fortaleza, 24 de Dezembro de 2021 (10:06:02)

Certidão expedida gratuitamente com base no decreto 13.716, de 22 de dezembro de 2015.

A autenticidade desta certidão deverá ser confirmada no endereço eletrônico da Secretaria Municipal das Finanças - SEFIN em www.sefin.fortaleza.ce.gov.br.

Válida até 24/03/2022

Qualquer rasura ou emenda invalidará este documento.

CERTIDÃO EMITIDA VIA INTERNET
http://www.sefin.fortaleza.ce.gov.br

Ministério da Economia
Secretaria de Governo Digital
Departamento Nacional de Registro Empresarial e Integração
Secretaria do Desenvolvimento Econômico

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
23201712520	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial do Estado do Ceará

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

CEE2100110240

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	223			BALANCO

FORTALEZA
Local

17 Maio 2021
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
21/074.135-0	CEE2100110240	17/05/2021

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
003.142.373-64	Ananias Rebouças Brito	17/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR	18/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Balanço Patrimonial

Encerrado em 31 de dezembro de 2020

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

CNPJ: 05.250.796/0001-54
Av. Pontes Vieira, 2340 - Salas 510 a 514 - Bairro: Dionisio Torres
CEP: 60135-238 - Fortaleza - CE

NIRE: 23201712520 - Data: 02/08/2002

Balanço Patrimonial

Empresa: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

Conta	31/12/202(		31/12/201(	
ATIVO	3.798.255,54	D	3.153.349,18	D
ATIVO CIRCULANTE	2.338.290,21	D	1.994.974,22	D
DISPONIVEL	1.430.124,25	D	774.688,14	D
CLIENTES	635.786,00	D	659.659,35	D
OUTROS DEBITOS	234.002,10	D	522.248,87	D
ESTOQUES	38.377,86	D	38.377,86	D
ATIVO NÃO CIRCULANTE	1.459.965,33	D	1.158.374,96	D
IMOBILIZADO	1.459.965,33	D	1.158.374,96	D

2.338.290,21

Continua...

Balanço Patrimonial

Empresa: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

Conta	31/12/2020		31/12/2019	
PASSIVO	3.798.255,54	C	3.153.349,18	C
PASSIVO CIRCULANTE	1.333.239,47	C	1.711.935,42	C
FORNECEDORES	737.542,67	C	787.531,02	C
EMPRESTIMOS E FINANCIAMENTOS	236.175,88	C	368.019,96	C
OBRIGAÇÕES FISCAIS E TRABALHISTAS	286.384,04	C	210.748,60	C
CREDORES DIVERSOS	0,00		196.001,30	C
OUTRAS OBRIGAÇÕES	0,00		3.872,49	C
PROVISÕES	73.136,88	C	145.762,05	C
PASSIVO NÃO CIRCULANTE	9.072,90	C	74.069,29	C
PARCELAMENTOS	3.430,36	C	74.006,63	C
RECEITAS A TRIBUTAR	5.642,54	C	62,66	C
PATRIMÔNIO LIQUIDO	2.455.943,17	C	1.367.344,47	C
CAPITAL SOCIAL INTEGRALIZADO	421.052,00	C	421.052,00	C
LUCROS OU (PREJUIZOS) ACUMULADOS	2.034.891,17	C	946.292,47	C

Fortaleza-CE, 31 de Dezembro de 2020

Ananias Rebouças Brito
CPF/MF: 003.142.373-64
CRC (CE): 020.032/O-6
Contador

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
José Murilo Cirino Nogueira Junior
CPF/MF: 648.711.503-72
Sócio- Administrador

Fim

Demonstração do Resultado do Exercício

Empresa: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002
(1) Estabelecimentos: Todos; Centros de Resultado: Todos

Conta	Descrição	01/01/2020 a 31/12/2020	01/01/2019 a 31/12/2019
(+) 001	RECEITA LIQ. DE VENDAS DE BENS/SERVIÇOS	9.273.926,67	5.453.402,62
001.01	RECEITA BRUTA DE VENDAS DE BENS/SERVIÇOS	10.066.409,54	6.263.792,39
001.02	DEDUÇÕES DA RECEITA	792.482,87	810.389,77
(-) 002	CUSTOS DOS BENS E/OU SERVIÇOS VENDIDOS	(3.881.098,32)	(2.062.097,05)
002.01	CUSTO DAS MERCADORIAS VENDIDAS	(257.237,40)	(83.330,52)
002.03	CUSTOS DOS SERVIÇOS PRESTADOS	(3.623.860,92)	(1.978.766,53)
(=) 003	RESULTADO BRUTO	5.392.828,35	3.391.305,57
(-) 004	DESPESAS/RECEITAS OPERACIONAIS	(2.058.156,16)	(2.189.134,21)
004.02	DESPESAS ADMINISTRATIVAS	(2.467.622,92)	(2.307.291,91)
004.03	DESPESAS TRIBUTARIAS	(23.015,29)	(47.860,80)
004.04	OUTRAS DESPESAS OPERACIONAIS	(81.787,32)	(214.461,17)
004.05	OUTRAS RECEITAS OPERACIONAIS	514.269,37	380.479,67
(=) 005	RESULTADO ANT. DO RESULT FINAN. E TRIB.	3.334.672,19	1.202.171,36
(-) 006	RESULTADO FINANCEIRO	(66.191,09)	(39.538,09)
006.01	DESPESA FINANCEIRA	(86.501,79)	(61.889,48)
006.02	RECEITAS FINANCEIRAS	20.310,70	22.351,39
(=) 007	RESULTADO ANTES DA CSLL	3.268.481,10	1.162.633,27
(-) 008	CONTRIBUIÇÃO SOCIAL SOBRE O LUCRO	261.101,63	56.708,63
008.01	CSLL	261.101,63	56.708,63
(=) 009	RESULTADO ANTES DO IRPJ	3.007.379,47	1.105.924,64
(-) 010	IMPOSTO DE RENDA	684.478,15	155.813,92
010.01	IRPJ	684.478,15	155.813,92
(=) 011	RESULTADO LIQUIDO DE OPER. CONTINUADAS	2.322.901,32	950.110,72
(-) 012	RESULTADO LIQUIDO DE OPE. DESCONTINUADAS	(344.233,97)	(232.555,52)
012.01	OUTRAS DESPESAS	(361.199,91)	(247.949,99)
012.02	OUTRAS RECEITAS	16.965,94	15.394,47
(=) 013	LUCRO/PREJUIZO DO PERÍODO	1.978.667,35	717.555,20

Fortaleza-CE, 31 de Dezembro de 2020

Ananias Rebouças Brito
CPF/MF: 003.142.373-64
CRC (CE): 020.032/O-6
Contador

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
José Murilo Cirino Nogueira Junior
CPF/MF: 648.711.503-72
Sócio- Administrador

Fim

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

DEMONSTRAÇAO DE MUTAÇOES DO PATRIMONIO LIQUIDO
EXERCICIOS FINDOS EM 31.12.2020

DESCRIÇÃO - HISTÓRICO	CAPITAL SOCIAL	RESERVAS				LUCROS OU PREJUÍZOS ACUMULADOS	TOTAL PATRIMÔNIO LÍQUIDO
		RESERVAS DE CAPITAL	RESERVAS DE LUCRO	RESERVAS ESTATUTÁRIA	Reserva de Subvenções		
Saldo Final – 31/12/2018	**421.052,00**		**-**	**-**	**-**	**793.600,57**	**1.214.652,57**
Ajustes de execicios anteriore	-	-	-	-	-	-	-
Aumento de Capital Social	-	-	-	-	-	-	-
Reserva de Capital	-	-	-	-	-	-	-
Reserva de Lucro	-	-	-	-	-	-	-
Reserva Estatutária	-	-	-	-	-	-	-
Reserva de Subvenções	-	-	-	-	-	-	-
Lucro / Prejuizo do Exercício	-	-	-	-	-	717.555,20	717.555,20
Lucros Distribuidos	-	-	-	-	-	(564.863,30)	(564.863,30)
Saldo Final – 31/12/2019	**421.052,00**	**-**	**-**	**-**	**-**	**946.292,47**	**1.367.344,47**
Ajustes de execicios anteriore	-	-	-	-	-	276.110,74	276.110,74
Aumento de Capital Social	-	-	-	-	-	-	-
Reserva de Capital	-	-	-	-	-	-	-
Reserva de Lucro	-	-	-	-	-	-	-
Reserva Estatutária	-	-	-	-	-	-	-
Reserva de Subvenções	-	-	-	-	-	-	-
Lucro / Prejuizo do Exercício	-	-	-	-	-	1.978.667,35	1.978.667,35
Lucros Distribuidos	-	-	-	-	-	(1.166.179,39)	(1.166.179,39)
Saldo Final – 31/12/2020	**421.052,00**	**-**	**-**	**-**	**-**	**2.034.891,17**	**2.455.943,17**

FORTALEZA-CE, 31 de Dezembro de 2020

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O-6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

ANÁLISE PATRIMONIAL
Exercício Findo em 31/12/2020

	2020		2019		
01 - LIQUIDEZ CORRENTE					Indica quanto a Empresa tem de Ativo Circulante para cada R$ 1,00 de Passivo Circulante **Quanto maior melhor.**
ATIVO CIRCULANTE	2.338.290,21	**1,75**	1.994.974,22	**1,17**	
PASSIVO CIRCULANTE	1.333.239,47		1.711.935,42		
02 - LIQUIDEZ SECA					Indica quanto a Empresa tem de Ativo Circulante para cada R$1,00 de Passivo Circulante **Quanto maior melhor.**
ATIVO CIRCULANTE - ESTOQUE	2.299.912,35	**1,73**	1.956.596,36	**1,14**	
PASSIVO CIRCULANTE	1.333.239,47		1.711.935,42		
03 - LIQUIDEZ GERAL					Indica quanto a Empresa tem de Ativo Circulante + Realizável a Longo Prazo para cada R$ 1,00 de dívida total **Quanto maior melhor.**
ATIVO CIRC + REALIZ. A LONGO PRAZO	2.299.912,35	**1,71**	1.956.596,36	**1,10**	
PASSIVO CIRC + EXIG. A LONGO PRAZO	1.342.312,37		1.786.004,71		
04 - LIQUIDEZ IMEDIATA					Indica quanto a Empresa possui de recursos disponíveis em relação ao passivo de curto prazo. **Quanto maior melhor.**
DISPONÍVEL	1.430.124,25	**1,07**	774.688,14	**0,45**	
PASSIVO CIRCULANTE	1.333.239,47		1.711.935,42		
05 - SOLVÊNCIA GERAL					Indica quanto a Empresa tem de Ativo total em relação às suas dívidas de curto e longo prazo. **Quanto maior melhor.**
ATIVO TOTAL	3.798.255,54	**2,83**	3.153.349,18	**1,77**	
PASSIVO CIRC. + EXIG. A LONGO PRAZO	1.342.312,37		1.786.004,71		
06 - PARTICIPAÇÕES DE CAPITAIS DE TERCEIROS					Indica quanto a Empresa utiliza de Capitais de Terceiros para cada real de Capital Próprio. **Quanto menor melhor.**
PASSIVO CIRC + EXIG. A LONGO PRAZO	1.342.312,37	**0,98**	1.786.004,71	**1,47**	
PATRIMÔNIO LÍQUIDO	1.367.344,47		1.214.652,57		
07 - COMPOSIÇÃO DO ENDIVIDAMENTO					Indica a relação das obrigações de curto prazo em relação às obrigações totais **Quanto menor melhor.**
PASSIVO CIRCULANTE	1.333.239,47	**0,99**	1.711.935,42	**0,96**	
PASSIVO CIRC + EXIG.A LONGO PRAZO	1.342.312,37		1.786.004,71		
08 - ENDIVIDAMENTO GERAL	**2020**		**2019**		Indica o endividamento total da empresa. Ou seja, quanto do ativo total está comprometido com dívidas. **Quanto menor melhor.**
PASSIVO CIRC + EXIG.A LONGO PRAZO	1.342.312,37	**0,35**	1.786.004,71	**0,57**	
ATIVO TOTAL	3.798.255,54		3.153.349,18		
09 - IMOBILIZAÇÃO DO CAPITAL PRÓPRIO					Indica quanto a Empresa aplicou no Ativo Permanente para cada R$ 1,00 de Patrimônio Líquido. **Quanto menor melhor.**
ATIVO PERMANENTE	1.459.965,33	**1,07**	1.158.374,96	**0,95**	
PATRIMÔNIO LÍQUIDO	1.367.344,47		1.214.652,57		
10 - RENTABILIDADE DO INVESTIMENTO TOTAL					Indica quanto a Empresa obteve de lucro para cada R$ 1,00 investido no ativo **Quanto maior melhor.**
LUCRO LÍQUIDO	1.978.667,35	**0,52**	717.555,20	**0,23**	
ATIVO TOTAL	3.798.255,54		3.153.349,18		
11 - RENTABILIDADE DO CAPITAL PRÓPRIO					Indica quanto a Empresa obteve de lucro para cada R$ 1,00 real de capital investido. **Quanto maior melhor.**
LUCRO LÍQUIDO	1.978.667,35	**1,45**	717.555,20	**0,59**	
PATRIMÔNIO LÍQUIDO	1.367.344,47		1.214.652,57		
12 - IMOBILIZAÇÃO DO RECURSOS NÃO CORRENTES					Indica quanto de recursos não correntes foi destinado ao Ativo Permanente **Quanto menor melhor.**
ATIVO PERMANENTE	1.459.965,33	**1,06**	1.158.374,96	**0,90**	
PAT.LIQUÍDO + EXIG. A LONGO PRAZO	1.376.417,37		1.288.721,86		
13 - CAPITAL DE GIRO PRÓPRIO					
(+) ATIVO CIRCULANTE	2.338.290,21		1.994.974,22		
(+) REALIZÁVEL A LONGO PRAZO	-		-		
(-) PASSIVO CIRCULANTE	(1.333.239,47)		(1.711.935,42)		
(-) EXIGÍVEL A LONGO PRAZO	(9.072,90)		(74.069,29)		
(=) CAPITAL DE GIRO PRÓPRIO	**995.977,84**		**208.969,51**		

Fortaleza-CE, 31 de Dezembro de 2020.

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O-6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

Demonstração do Fluxo de Caixa - Método Indireto

Empresa: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

	01/01/2020 a 31/12/2020	01/01/2019 a 31/12/2019
Atividades Operacionais		
Lucro Líquido	1.978.667,35	717.555,20
Diminuição em CLIENTES	23.873,35	-
Aumento em CLIENTES	-	(279.783,28)
Aumento em ADIANTAMENTOS A FUNCIONARIOS	(3.251,44)	-
Diminuição em ADIANTAMENTOS A FUNCIONARIOS	-	11.601,19
Diminuição em ADIANTAMENTO A FORNECEDORES	308.029,39	192.929,82
Aumento em IMPOSTOS A RECUPERAR	(16.531,18)	(26.772,83)
Diminuição em DESPESAS ANTECIPADAS	-	574,95
Diminuição em DEVEDORES DIVERSOS	-	13,74
Aumento em DEPRECIAÇÃO ACUMULADA	-	160.199,53
Diminuição em FORNECEDORES NACIONAIS	(49.988,35)	-
Aumento em FORNECEDORES NACIONAIS	-	503.666,69
Aumento em IMPOSTOS E CONTRIBUIÇÕES	83.989,74	56.312,81
Diminuição em OBRIGACOES TRABALHISTAS	(8.354,30)	(5.048,60)
Diminuição em CREDITOS DIVERSOS	(196.001,30)	-
Aumento em CREDITOS DIVERSOS	-	83.265,09
Diminuição em OUTRAS OBRIGAÇÕES	(3.872,49)	-
Aumento em OUTRAS OBRIGAÇÕES	-	3.872,49
Diminuição em PROVISÕES	(17.086,08)	-
Aumento em PROVISÕES	-	48.429,47
Diminuição em IMPOSTOS POR REGIME DE CAIXA	(55.539,09)	-
Aumento em IMPOSTOS POR REGIME DE CAIXA	-	62.512,21
Diminuição em PARCELAMENTOS FEDERAIS	(68.343,84)	-
Aumento em PARCELAMENTOS FEDERAIS	-	69.762,47
Diminuição em PARCELAMENTO ESTADUAL	(4.244,16)	(8.308,85)
Aumento em PARCELAMENTO PREVIDENCIARIO	2.011,73	-
Aumento em RECEITAS A TRIBUTAR	5.579,88	62,66
Caixa Líquido das Atividades Operacionais	**1.978.939,21**	**1.590.844,76**
Atividades Investimento		
Aumento em BENS EM OPERAÇÃO	(301.590,37)	(267.753,64)
Caixa Líquido das Atividades Investimento	**(301.590,37)**	**(267.753,64)**
Atividades Financiamento		
Aumento em FINANCIAMENTOS BANCARIOS	83.780,41	-
Diminuição em FINANCIAMENTOS BANCARIOS	-	(143.188,43)
Diminuição em ARRENDAMENTO MERCANTIL	(215.624,49)	(54.842,01)
Diminuição em PATRIMÔNIO LIQUIDO	(890.068,65)	(564.863,30)

Fim

Demonstração do Fluxo de Caixa - Método Indireto

Empresa: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

	01/01/2020 a 31/12/2020	01/01/2019 a 31/12/2019
Caixa Líquido das Atividades Financiamento	**(1.021.912,73)**	**(762.893,74)**
Variação Líquida de Caixa e Equivalente de Caixa	**655.436,11**	**560.197,38**
Caixa e Equivalente de Caixa no Início do Período	**774.688,14**	**214.490,76**
Caixa e Equivalente de Caixa no Fim do Período	**1.430.124,25**	**774.688,14**

Fortaleza-CE, 31 de Dezembro de 2020

Ananias Rebouças Brito
CPF/MF: 003.142.373-64
CRC (CE): 020.032/O-6
Contador

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
José Murilo Cirino Nogueira Junior
CPF/MF: 648.711.503-72
Sócio- Administrador

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

DEMONSTRAÇÃO DOS RESULTADOS ABRANGENTES
EM 31 DE DEZEMBRO DE 2020

	2020	2019
Sobra / Lucro Líquido do Exercício	1.978.667,35	717.555,20
(+/-) Ganhos ou Perdas de Conversões das Demonstrações Contábeis		
Diferenças cambiais de conversão de operações no exterior		
Diferenças cambiais de conversão de equivalência patrimonial de investidas		
Reclassificação de diferenças de variação cambial quando da perda de influência significativa		
Variação líquida de *hedge* de investimento liquido em operações no exterior		
Ajuste da variação do valor justo de imóveis transferidos do ativo imobilizado para propriedades para investimento		
Parcela efetiva das mudanças no valor justo dos *hedges* de fluxo de caixa		
Variação líquida no valor justo dos *hedges* de fluxo de caixa transferido para resultado		
Variação líquida no valor justo de ativos financeiros disponíveis para venda		
Variação líquida no valor justo e ativos financeiros disponíveis para venda transferidos resultado		
Ganhos atuariais de plano de benefícios definido		
Imposto de renda e contribuição social sobre outros resultados abrangentes		
Outros resultados abrangentes, líquidos de imposto de renda e contribuição social		
Total do Resultado Abrangente do Exercício	1.978.667,35	717.555,20
Participação no Resultado Abrangente	-	-
Controladores		
Não controladores		
Total do Resultado Abrangente do Exercício	1.978.667,35	717.555,20

Fortaleza-CE, 31 de Dezembro de 2020.

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O-6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
CNPJ: 05.250.796/0001-54
NIRE: 23201712520 - Data: 02/08/2002

DEMONSTRAÇÃO DO VALOR ADICIONADO
EM 31 DE DEZEMBRO DE 2020

	2020	2019
1. Receitas	**R$ 9.273.926,67**	**R$ 5.453.402,62**
Vendas de mercadorias, produtos e serviços	**R$ 10.066.409,54**	**R$ 6.263.792,39**
Outras receitas		
Provisão para créditos de liquidação duvidosa	-	-
(-) Deduções da receita (Inclui os valores dos impostos - ICMS, IPI, PIS,COFINS e ISS)	-R$ 792.482,87	-R$ 810.389,77
(-) Devoluções de venda e outras deduções	-	-
2. Insumos adquiridos de terceiros	**R$ 5.706.412,22**	**R$ 3.571.541,74**
Custos dos produtos, das mercadorias e dos serviços vendidos	R$ 3.881.098,32	R$ 2.062.097,05
Materiais, energia, serviços de terceiros e outros	R$ 1.825.313,90	R$ 1.509.444,69
3. Valor adicionado bruto = 1-2	**R$ 3.567.514,45**	**R$ 1.881.860,88**
4. Depreciação e amortização	**R$ -**	**R$ 160.313,46**
5. Valor adicionado líquido produzido pela companhia = 3-4	**R$ 3.567.514,45**	**R$ 1.721.547,42**
6. Valor adicionado recebido em transferência	**R$ 551.546,01**	**R$ 418.225,53**
Resultado de equivalência patrimonial		
Receitas financeiras	R$ 20.310,70	R$ 22.351,39
Outras	R$ 531.235,31	R$ 395.874,14
7. Valor adicionado total a distribuir = 5+6	**R$ 4.119.060,46**	**R$ 2.139.772,95**
8. Distribuição do valor adicionado = 7	**R$ 4.119.060,46**	**R$ 2.139.772,95**
8.1. Pessoal	**R$ 628.618,93**	**R$ 791.655,23**
8.2. Impostos, taxas e contribuições	**R$ 968.595,07**	**R$ 260.383,35**
8.3 Remuneração de capitais de terceiros	**R$ 543.179,11**	**R$ 370.179,17**
Despesas Financeiras	R$ 86.501,79	R$ 61.889,48
Aluguéis	R$ 95.477,41	R$ 60.339,70
Outras	R$ 361.199,91	R$ 247.949,99
8.4 Remuneração de capitais próprios	**R$ 1.978.667,35**	**R$ 717.555,20**
Dividendos e juros sobre o capital próprio		
Lucros ou Prejuizos retidos	R$ 1.978.667,35	R$ 717.555,20
Participação dos não controladores nos lucros retidos		

Fortaleza-CE, 31 de Dezembro de 2020.

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O-6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

CNPJ: 05.250.796/0001-54

NIRE: 23201712520 - Data: 02/08/2002

NOTAS EXPLICATIVAS

DEMONSTRAÇÕES CONTÁBEIS EM 31/12/2020

CONTEXTO OPERACIONAL

A empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA é uma pessoa jurídica de direito privado, com fins econômicos, com sede em Fortaleza, estado do Ceará, na Av. Pontes Vieira,2340 - Salas 510 a 514 - Bairro: Dionísio Torres - CEP: 60135-238 Estado do Ceará, cuja principal atividadeé a de Comércio atacadista de equipamentos de informática (CNAE 46.51-6-01). Sua com respaldo legal no Código Civil Brasileiro: LEI N o 10.406, DE 10 DE JANEIRO DE 2002.

REGIME TRIBUTÁRIO

A empresa é enquadrada no regime "Lucro Presumido" A prática contábil adotada é pelo regime de caixa.

CADASTRO

A empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA possui os seguintes registros e inscrições:

a) Contrato Social registrado na Junta Comercial do Estado do Ceará sob o nº 5558409 sob despacho em 08/04/2021.
b) Cadastro Nacional de Pessoas Jurídicas sob nº 05.250.796/0001-54.

PRINCIPAIS PRÁTICAS CONTABEIS

As demonstrações contábeis foram preparadas de acordo com as Normas Internacionais de Relatório Financeiro ("IFRS"). Sempre em consonância com as normas internacionais, com atendimentos da Lei 11.638/07 e Lei 11.941/09 e os pronunciamentos emitidos pelo CPC – Comitê de Pronunciamentos Contábeis, aprovados pelo CFC – Conselho Federal de Contabilidade.

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

Os ativos circulantes e não circulantes

a) O caixa e os equivalentes de caixa estão representadas por aplicações de curto prazo, de alta liquidez, que são prontamente conversíveis em numerários.
b) As aplicações financeiras são registradas ao custo, acrescido dos rendimentos auferidos até a data do balanço e não estão destinados à negociação ou disponíveis para venda;
c) O ativo imobilizado está demonstrado ao custo de aquisição;
d) A depreciação do ativo imobilizado foi feita pelo método linear, aplicando-se as taxas usualmente admitidas para os bens em operação durante um turno de 8(oito) horas diárias;
e) Recuperabilidade de ativos: A Empresa analisou o valor contábil líquido dos ativos com o objetivo de identificar eventos ou mudanças nas circunstâncias econômicas, operacionais ou tecnológicas que possam indicar a deterioração, obsolescência ou perda de seu valor recuperável. Com base nas análises efetuadas, não foram identificadas evidências que requeressem ajustes para perda por redução de seu valor de recuperação.
f) Demais ativos circulantes e não circulantes: Os demais circulantes, compreendidos até um ano e não circulantes, compreendidos acima de um ano, estão demonstrados pelos valores de custo, acrescidos ou reduzidos, quando aplicável, dos respectivos **rendimentos ou provisão para perdas;**

Os passivos circulantes e não circulantes

g) Empréstimos e Financiamentos são reconhecidos inicialmente pelo seu valor justo deduzido dos custos de transação que sejam diretamente atribuíveis ao mesmo;
h) Demais Passivos Circulantes e Não Circulantes são demonstrados pelos valores conhecidos ou calculáveis, acrescidos, quando aplicável, dos correspondentes encargos, variações monetárias e/ou cambiais incorridas até a data do balanço.

BALANÇO PATRIMONIAL

O Balanço Patrimonial tem a finalidade de apresentar a posição financeira e patrimonial da sociedade, representando, portanto, uma posição estática. No balanço, as contas serão classificadas segundo os elementos do patrimônio que registrem, e agrupadas de modo a facilitar o conhecimento e a análise da situação financeira da sociedade.

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

CAPITAL SOCIAL

O Capital Social realizado é de 421.052 (quatrocentas e vinte e uma mil e cinquenta e duas) quotas, cada uma com valor nominal de R$1,00 (um real).

DECLARAÇÃO

Essas Notas Explicativas são partes integrantes e indissociáveis das Demonstrações Contábeis elaboradas em 31/12/2020

Fortaleza-CE, 31 de Dezembro de 2020.

ANANIAS REBOUÇAS BRITO
CPF(MF): 003.142.373-64
CRC/CE: 020.032/O6
CONTADOR

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF(MF): 648.711.503-72
SÓCIO ADMINISTRADOR

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
21/074.135-0	CEE2100110240	17/05/2021

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
003.142.373-64	Ananias Rebouças Brito	17/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR	18/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, de CNPJ 05.250.796/0001-54 e protocolado sob o número 21/074.135-0 em 18/05/2021, encontra-se registrado na Junta Comercial sob o número 5575705, em 18/05/2021. O ato foi deferido eletronicamente pelo examinador Felipe Araujo Veras.

Certifica o registro, a Secretária-Geral, Lenira Cardoso de Alencar Seraine. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucec.ce.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR	18/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
003.142.373-64	Ananias Rebouças Brito	17/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR	18/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
003.142.373-64	Ananias Rebouças Brito	17/05/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Documento assinado eletronicamente por Felipe Araujo Veras, Servidor(a) Público(a), em 18/05/2021, às 16:12.

A autencidade desse documento pode ser conferida no portal de serviços da jucec informando o número do protocolo 21/074.135-0.

O ato foi deferido e assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
236.117.073-68	LENIRA CARDOSO DE ALENCAR SERAINE

Fortaleza. terça-feira, 18 de maio de 2021

ESTADO DO CEARÁ

PODER JUDICIÁRIO

COMARCA DE FORTALEZA

CERTIDÃO DE FALÊNCIA, RECUPERAÇÃO JUDICIAL OU EXTRAJUDICIAL (LEI 8.666/93)

(PESSOA JURÍDICA / 1º GRAU / CÍVEL)

CERTIFICA, a requerimento da parte interessada, que consultando nos Sistemas Informatizados do Serviço de Distribuição desta Comarca, em relação ao(s) Polo(s) PASSIVO OU ATIVO, dos processos de Natureza Cível, EM TRÂMITE, verificou NADA CONSTAR, em nome de NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA - DEMAIS, CNPJ n° 05.250.796/0001-54.

CERTIFICA que, esta certidão só é válida por 30 (trinta) dias, a contar da data de sua emissão

O referido é verdade e dou fé.

FORTALEZA

Sexta-feira, 28 de Janeiro de 2022 às 14:36:27

Observações:

a) os dados informados são de responsabilidade do solicitante e devem ser conferidos pelo interessado e/ou destinatário;

b) a autenticidade deste documento poderá ser confirmada conforme informações no rodapé;

c) a consulta inclui as seguintes classes: FALÊNCIA, CONCORDATA, RECUPERAÇÃO JUDICIAL E RECUPERAÇÃO EXTRAJUDICIAL;

d) esta certidão é expedida nos termos da Resolução 13/2019, do Órgão Especial do Tribunal de Justiça do Estado do Ceará.

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins, que a empresa Network Secure Segurança Da Informação LTDA, estabelecida na Av. Pontes Vieira, 2340 - Dionísio Torres, Ed. UNO Medical & Office - Salas 510 à 514 - 5º andar - Fortaleza/CE, CEP: 60135-238, inscrita no CNPJ 05.250.796/0001-54, FORNECEU, INSTALOU, CONFIGUROU, IMPLEMENTOU e presta serviços com as seguintes características:

1. **DADOS DO CLIENTE:**
Razão Social: HAPVIDA ASSISTENCIA MÉDICA LTDA
CNPJ: 63.554.067/0001-98
Endereço: Avenida Heráclito Graça, Nº 406 – 2º andar, Bairro: Centro, CEP: 60.140-060, Fortaleza/CE.

2. **ENTREGAS REALIZADAS**

2.1. FABRICANTE FORTINET

ITEM	DESCRIÇÃO	QTD
1	FORTIGATE FG-3300E	2
2	LICENÇA FORTINET FG-3300E - 36 MESES 24X7 UTM UNIFIED	2
3	FORTINET FG 60F	1
4	LICENÇA FORTINET FG 60F - 12 MESES 24X7 UTM UNIFIED	1
5	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO	16

Serviços de segurança que contemplam FIREWALL, VPN (IPSEC/SSL) IDS/IPS antivírus, antiphishing, antispyware controle de conteúdo web, antispam, QoS, Traffic Shape, WAN Failover, controle de aplicação entre outras funcionalidades possuindo NOC para monitoramento dos equipamentos acima informados desde 2017.

Atestamos ainda, que os compromissos assumidos pela empresa foram e são cumpridos satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Fortaleza, 17 de fevereiro 2020

Bruno Cascão Lima
Gerente de Segurança da Informação
brunol@hapvida.com.br
+55 85 99150-6428 +55 85 3453-7216
www.hapvida.com.br | Matriz: Tecnologia da Informação

PagueMenos

ATESTADO DE CAPACIDADE TÉCNICA

Declaramos para quem possa interessar que a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, inscrita sob o CNPJ nº 05.250.796/0001-54, situada na Rua Capitão Melo, 3373 – Joaquim Távora, CEP: 60.120-220, Fortaleza – CE, **FORNECEU/VENDEU,** em regime *bundle* 8x5 para 5 (cinco) anos, bem como **CONFIGUROU, IMPLEMENTOU** e realizou **TREINAMENTO** para o **EMPREENDIMENTOS PAGUE MENOS S/A.**, inscrita sob o CNPJ nº 06.626.253/0001-51, com sede na rua SENADOR POMPEU, nº 1520, CEP: 60.025-002 - CENTRO, Fortaleza/CE, Telefone:85-3198.3435, dos Equipamentos e licenças do Fabricante FORTINET, para um ambiente de 10 (dez mil) usuários, podendo suportar até 10 (dez mil) usuários, a nível Brasil, alocados em 26 (vinte e seis) Estados do Brasil. Conforme equipamentos abaixo:

- 02 UNID – **FORTIGATE 1000D** (Firewall, Controladora WLAN e Software de Gerência da WLAN para dispositivos locais e remotos);
- 02 UNID - **FORTIANALYZER 3000E** (Gerenciador Log);
  02 UNID – **FORTIADC 700D** (Controlador de entrega de aplicativos)
- 1.100 UNID - **FORTIGATE 60E** (Firewall, Controladora WLAN e Software de Gerência da WLAN para dispositivos locais e remotos);
- 01 UNID - **FORTIANALYZER 3500E** (Gerenciador Log);
- 01 UNID - **FORTIMANAGER 2000E** (Gerência Centralizada);
- 02 UNID - **FORTIGATE 600D** (Firewall, Controladora WLAN e Software de Gerência da WLAN para dispositivos locais e remotos);
- 02 UNID - **FORTIGATE 100D** (Firewall, Controladora WLAN e Software de Gerência da WLAN para dispositivos locais e remotos);
-

IMPLANTAÇÃO: Instalação, configuração presencial/remota e controle de segurança com alta disponibilidade com as funcionalidades de UTM habilitadas.

SERVIÇOS: Auditoria do SGSI, treinamento, consultoria em infraestrutura de segurança, análise de risco, analise de vulnerabilidade, avaliação em cyber security, Monitoramento e Suporte Técnico; Gerando um total de 1.536 horas nos últimos 4 anos, com cobertura 24x7.

PagueMenos

Declaramos ainda que, o **Sr. Alarico Isaias de Sousa Guimarães**, portador do CPF de nº 620.143.313-91, Gerente do Projeto, acompanhou o cliente, com objetivo de verificar os serviços de: Configuração, Implementação e Treinamento dos equipamentos acima informados.

Atestamos que tem suprido todas as expectativas quanto ao grau de Integridade e regularidade nos serviços prestados, cumprindo corretamente com todas as condições contratuais, não havendo, portanto, nada que venha a desabonar sua conduta.

Fortaleza, 20 de Agosto de 2021.

EMPREENDIMENTOS PAGUE MENOS S/A

Afro Vasconcelos
Diretor de Tecnologia

Afro Jose Campos de Vasconcelos
Diretor de Tecnologia
afro@paguemenos.com.br
85-3198.3421

FACULDADE PERNAMBUCANA DE SAÚDE

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins, que a empresa Network Secure Segurança da Informação LTDA, estabelecida na Av. Pontes Vieira, 2340 - Dionísio Torres, Ed. UNO Medical & Office - Salas 510 à 514 - 5º andar - Fortaleza/CE, CEP: 60135-238, inscrita no CNPJ 05.250.796/0001-54, FORNECEU, INSTALOU, CONFIGUROU, IMPLEMENTOU e presta serviços com as seguintes características:

1. **DADOS DO CLIENTE:**
   Razão Social: ASSOCIACAO EDUCACIONAL DE CIENCIAS DA SAUDE - AECISA
   CNPJ: 05.834.842/0001-62
   Endereço: AVENIDA MARECHAL MASCARENHAS DE MORAIS, Nº 4861 – BAIRRO: IMBIRIBEIRA – RECIFE/PE, TEL.: 81-30357777

2. **ENTREGAS REALIZADAS**

2.1. **FABRICANTE FORTINET**

Serviço Gerenciado de Segurança da Informação, para a segurança de perímetro de rede, com a locação de equipamentos do fabricante FORTINET, listados a seguir, com as funcionalidades de Firewall, VPN - IPSEC/SSL, QoS, Traffic Shape, WAN Failover, DLP, IPS e a prestação de serviços de gestão, suporte e consultoria especializada na solução contratada.

ITEM	DESCRIÇÃO	QTD
1	FORTIGATE FG-600E 3 ANOS	4
2	LICENÇA FORTINET FG-600E - UTM Bundle (NGFW, AV, Web Filtering and Antispam Services).	4
3	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE	4

Atestamos ainda, que os compromissos assumidos pela empresa foram e são cumpridos satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Recife, 17 de fevereiro de 2022.

_____

Marcone Maciel Barros
CPF: 028.976.654-08
Gerente Tecnologia da Informação e Comunicação
barros.marcone@fps.edu.br
(81) 3035.7777 | (81) 3312.7777

Comprovante de Assinatura Eletrônica

contraktor

Datas e horários baseados no fuso horário (GMT -3:00) em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinatura gerado em 17/02/2022 às 17:16:07 (GMT -3:00)

AtestadoCapacidadeTecnica - Fortinet

ID única do documento: #fbf0de95-ecde-4fb0-ae62-75bdf6088df3

Hash do documento original (SHA256): e6b2551e9415be06676dd4917dc808e5991d224c3b74a71c8f31befd350ba6be

Este Log é exclusivo ao documento número #fbf0de95-ecde-4fb0-ae62-75bdf6088df3 e deve ser considerado parte do mesmo, com os efeitos prescritos nos Termos de Uso.

Assinaturas (1)

Marcone Maciel Barros (Gerente de TIC)
Assinou em 17/02/2022 às 17:16:17 (GMT -3:00)

Histórico completo

Data e hora	Evento
17/02/2022 às 17:16:06 (GMT -3:00)	Marcone Maciel Barros solicitou as assinaturas.
17/02/2022 às 17:16:17 (GMT -3:00)	Marcone Maciel Barros (CPF 028.976.654-08; E-mail barros.marcone@fps.edu.br; IP 201.19.203.26), assinou. Autenticidade deste documento poderá ser verificada em https://verificador.contraktor.com.br. Assinatura com validade jurídica conforme MP 2.200-2/01, Art. 10o, §2.
17/02/2022 às 17:16:17 (GMT -3:00)	Documento assinado por todos os participantes.

AO
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
PROCURADORIA GERAL DE JUSTIÇA
COMISSÃO PERMANENTE DE LICITAÇÃO – CPL
REF.: PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ
PROCESSO SEI N.º 2021.015252

DECLARAÇÃO DE DISPENSA DE VISTORIA TÉCNICA,

A empresa Network Secure Segurança da Informação LTDA, inscrita no CNPJ nº 05.250.796/0001-54, sediada na Av. Pontes Vieira, 2340 - Dionísio Torres, UNO - Medical & Office - Sala 510 - 514 - 5º andar - Fortaleza/CE, CEP: 60135-238, telefone (85) 3195-2200, por intermédio de seu representante legal o Sr Yure Leopoldo Sabino De Freitas, portador da Carteira de Identidade nº 559056187 SSP/SP e CPF nº 525.285.023-20, declara que conhece as condições locais para execução do objeto; e que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do trabalho, assume total responsabilidade por este fato e não utilizará deste para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante.

Fortaleza/CE 21 de Fevereiro de 2022.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMÁTICA LTDA
AV: PONTES VIEIRA Nº 2340
DIONÍSIO TORRES SL 510/514
5º ANDAR CEP: 60.135-238
FORTALEZA CEARÁ

YURE LEOPOLDO SABINO DE FREITAS
CPF: 525.285.023-20
DIRETOR COMERCIAL

Ministério da Economia
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Certificado de Registro Cadastral - CRC

(Emissão conforme art. 17 da Instrução Normativa nº 03, de 26 abril de 2018)

CNPJ: **05.250.796/0001-54**

Razão Social: **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**

Atividade Econômica Principal:

4651-6/01 - COMÉRCIO ATACADISTA DE EQUIPAMENTOS DE INFORMÁTICA

Endereço:

AVENIDA PONTES VIEIRA, 2340 - SALAS 510 A 514 - DIONISIO TORRES - Fortaleza / Ceará

Observações:

A veracidade das informações poderá ser verificada no endereço www.comprasgovernamentais.gov.br.

Este certificado não substitui os documentos enumerados nos artigos 28 a 31 da Lei nº 8.666, de 1993.

Ministério da Economia
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Relatório de Credenciamento

Dados do Fornecedor

CNPJ: **05.250.796/0001-54** DUNS®: **914627245**
Razão Social: **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**
Nome Fantasia: **NETWORK SECURE**
Situação do Fornecedor: **Credenciado** Data de Vencimento do Cadastro: **24/11/2022**

Dados do Nível

Situação do Nível: **Cadastrado**

Dados do Fornecedor

Porte da Empresa: **Demais**
Natureza Jurídica: **SOCIEDADE EMPRESÁRIA LIMITADA** MEI: **Não**
Capital Social: **R$ 421.052,00** Data de Abertura da Empresa: **02/08/2002**
CNAE Primário: **4651-6/01 - COMÉRCIO ATACADISTA DE EQUIPAMENTOS DE INFORMÁTICA**

CNAE Secundário 1: **4615-0/00 - REPRESENTANTES COMERCIAIS E AGENTES DO COMÉRCIO**
CNAE Secundário 2: **4618-4/99 - OUTROS REPRESENTANTES COMERCIAIS E AGENTES DO**
CNAE Secundário 3: **6202-3/00 - DESENVOLVIMENTO E LICENCIAMENTO DE PROGRAMAS**
CNAE Secundário 4: **6204-0/00 - CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO**
CNAE Secundário 5: **6209-1/00 - SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS**
CNAE Secundário 6: **7020-4/00 - ATIVIDADES DE CONSULTORIA EM GESTÃO EMPRESARIAL,**
CNAE Secundário 7: **7733-1/00 - ALUGUEL DE MÁQUINAS E EQUIPAMENTOS PARA**
CNAE Secundário 8: **8599-6/03 - TREINAMENTO EM INFORMÁTICA**
CNAE Secundário 9: **9511-8/00 - REPARAÇÃO E MANUTENÇÃO DE COMPUTADORES E DE**

Dados para Contato

CEP: **60.135-238**
Endereço: **AVENIDA PONTES VIEIRA, 2340 - SALAS 510 A 514 - DIONISIO TORRES**
Município / UF: **Fortaleza / Ceará**
Telefone: **(85) 31952200**
E-mail: **ANDREA@NETWORKSECURE.COM.BR**

Relatório de Credenciamento

Dados do Responsável Legal

CPF: **648.711.503-72**
Nome: **JOSE MURILO CIRINO NOGUEIRA JUNIOR**

Dados do Responsável pelo Cadastro

CPF: **648.711.503-72**
Nome: **JOSE MURILO CIRINO NOGUEIRA JUNIOR**
E-mail: **licitacoes@networksecure.com.br**

Relatório de Credenciamento

Sócios / Administradores

Dados do Sócio/Administrador 1

CPF: **648.711.503-72** Participação Societária: **92,50%**
Nome: **JOSE MURILO CIRINO NOGUEIRA JUNIOR**
Número do Documento: **99010123694** Órgão Expedidor: **SSP _ CE**
Data de Expedição: **29/03/1999** Data de Nascimento: **09/07/1981**
Filiação Materna: **ELUZIA PEIXOTO DA SILVA**
Estado Civil: **Casado(a)**

Dados do Cônjuge/Companheiro(a)

Estrangeiro: **Não** CPF: **824.533.063-91**
Nome: **FRANCISCA ANDREA CAMINHA CIRINO**
Carteira de Identidade: **2010002296402** Órgão Expedidor: **SSPDS CE**
Data de Expedição: **17/02/2012**

CEP: **60.810-160**
Endereço: **AVENIDA CORONEL MIGUEL DIAS, 1010 - APTO 1301 - PATRIOLINO**
Município / UF: **Fortaleza / Ceará**
Telefone: **(85) 32249185**
E-mail: **murilo@netorksecure.com.br**

Dados do Sócio/Administrador 2

CPF: **620.143.313-91** Participação Societária: **2,50%**
Nome: **ALARICO ISAIAS DE SOUSA GUIMARAES**
Número do Documento: **96002206506** Órgão Expedidor: **SSPDS CE**
Data de Expedição: **17/03/2014** Data de Nascimento: **23/04/1980**
Filiação Materna: **MARIA AMELIA DE SOUSA GUIMARAES**
Estado Civil: **Casado(a)**

Dados do Cônjuge/Companheiro(a)

Estrangeiro: **Não** CPF: **001.825.713-51**
Nome: **CINTIA SILVA SALAZAR GUIMARAES**
Carteira de Identidade: **97002056669** Órgão Expedidor: **SSP CE**
Data de Expedição: **29/01/1997**

CEP: **60.743-060**
Endereço: **RUA 06, 06 - BL 01 AP 407 - ITAPERI**
Município / UF: **Fortaleza / Ceará**
Telefone: **(85) 92194533**
E-mail: **licitacoes@networksecure.com.br**

Relatório de Credenciamento

Dados do Sócio/Administrador 3

CPF: **691.833.093-49** Participação Societária: **2,50%**
Nome: **TATIANA RIBEIRO LEITE**
Número do Documento: **93002319934** Órgão Expedidor: **SSPDC CE**
Data de Expedição: **29/04/1998** Data de Nascimento: **29/06/1977**
Filiação Materna: **MARIA DE FATIMA RIBEIRO LEITE**
Estado Civil: **Solteiro(a)**
CEP: **04.575-000**
Endereço: **RUA HENRICH HERTEZ, 91 - APTO 81 - CIDADE MONCOES**
Município / UF: **São Paulo / São Paulo**
Telefone: **(85) 32249185**
E-mail: **licitacoes@networksecure.com.br**

Dados do Sócio/Administrador 4

CPF: **525.285.023-20** Participação Societária: **2,50%**
Nome: **YURE LEOPOLDO SABINO DE FREITAS**
Número do Documento: Órgão Expedidor:
Data de Expedição: Data de Nascimento: **06/10/1978**
Filiação Materna: **CLAUDETE SABINO DE FREITAS**
Estado Civil:
CEP: **60.130-271**
Endereço: **RUA EDUARDO BEZERRA, 1200 - APTO 301 - DIONISIO TORRES**
Município / UF: **Fortaleza / Ceará**
Telefone: **(85) 99581335**
E-mail:

Linhas Fornecimento

Materiais

7030 - EQUIPAMENTOS DE ARMAZENAMENTO DE DADOS

Serviços

1260 - Informática - Manutenção/Instalação Sistemas/Periféricos

5398 - Prestação de Serviços de Informática

16918 - Informática - Desenvolvimento / Implantação / Manutenção Re-de de Computador

21652 - Consultoria e Assessoria - Teleinformática

22993 - Informática - Suporte Técnico (Software / Equipamentos)

Ministério da Economia
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins previstos na Lei nº 8.666, de 1993, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**05.250.796/0001-54**	DUNS®:	**914627245**
Razão Social:	**NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**		
Nome Fantasia:	**NETWORK SECURE**		
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**24/11/2022**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Demais**		

Ocorrências e Impedimentos

Ocorrência:	**Nada Consta**
Impedimento de Licitar:	**Nada Consta**
Ocorrências Impeditivas indiretas:	**Nada Consta**
Vínculo com "Serviço Público":	**Nada Consta**

Níveis cadastrados:

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**30/07/2022**
FGTS		Validade:	**26/02/2022**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**05/08/2022**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**25/03/2022**
Receita Municipal	Validade:	**24/03/2022**

VI - Qualificação Econômico-Financeira

Validade: **30/04/2022**

CPF: 856.140.172-91 Nome: EDSON FREDERICO LIMA PAES BARRETO
Ass: _____

TRIBUNAL DE CONTAS DA UNIÃO

Consulta Consolidada de Pessoa Jurídica

Este relatório tem por objetivo apresentar os resultados consolidados de consultas eletrônicas realizadas diretamente nos bancos de dados dos respectivos cadastros. A responsabilidade pela veracidade do resultado da consulta é do Órgão gestor de cada cadastro consultado. A informação relativa à razão social da Pessoa Jurídica é extraída do Cadastro Nacional da Pessoa Jurídica, mantido pela Receita Federal do Brasil.

Consulta realizada em: 21/02/2022 11:40:38

Informações da Pessoa Jurídica:

Razão Social: **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**
CNPJ: **05.250.796/0001-54**

Resultados da Consulta Eletrônica:

Órgão Gestor: **TCU**
Cadastro: **Licitantes Inidôneos**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **CNJ**
Cadastro: **CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **Cadastro Nacional de Empresas Inidôneas e Suspensas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **CNEP - Cadastro Nacional de Empresas Punidas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Obs: A consulta consolidada de pessoa jurídica visa atender aos princípios de simplificação e

racionalização de serviços públicos digitais. Fundamento legal: Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.726, de 8 de outubro de 2018, Decreto nº 8.638 de 15, de janeiro de 2016.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 69.2022.CPL.0772078.2021.015252

Aos Senhores

TADEU AZEVEDO DE MEDEIROS

Diretor de Tecnologia da Informação e Comunicação

C/c

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

NESTE EDIFÍCIO

Assunto: Análise Técnica Proposta e Documentação Técnica no interesse no Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ.

Senhor Diretor e Senhor Chefe,

Cumprimentando-os cordialmente, e no interesse do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ** (doc. 0763629), cujo objeto consiste na *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual*, considerando que qualquer aceitação depende da análise desse Setor competente quanto às especificações técnicas, submeto ao crivo de vossa análise a **Proposta e Planilha de Formação de Preços** (doc. 0772069 e 0772300) e **Documentação de Habilitação pertinentes e afetos à parte técnica** (doc. 0772080) pertencentes à empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54.**

Reitero protestos de elevada estima, colocando-me à disposição para quaisquer esclarecimentos que se façam necessários, quedando-me no aguardo das considerações cabíveis para a continuidade do certame.

Respeitosamente,

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Pregoeiro designado pela PORTARIA N° 229/2022/SUBADM

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 21/02/2022, às 11:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0772078** e o código CRC **1A06CFD8**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - CEP 69000-000 - Manaus - AM - www.mpam.mp.br

PARECER Nº 4.2022.SIET.0775110.2021.015252

OBJETO: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.
ORIGEM: Processo de Compra 2021.015252

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar análise técnica da documentação enviada pela empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA.

2. Análise

O presente parecer se baseia nas disposições do Termo de Referência n. 20.2021.DTIC.0720733.2021.015252, Anexo I ao Edital do certame, SEI 0763629, em seus diversos itens.

A proposta de preço, documento 0772069, informa equipamentos e serviços condizentes com as quantidades e exigências do Termo de Referência. Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo.

Conforme exigência, foram apresentados atestados de capacidade técnica que comprovam, **conjuntamente**, a prestação anterior de serviços de firewall de próxima geração, NGFW, com troughput de 10Gbps, no mínimo. Foram apresentados 03 (três) atestados, disponíveis nas páginas 42, 43, 44 e 45 do documento 0772080, incluindo equipamentos similares e superiores ao objeto deste processo.

3. Conclusão

Após análise dos documentos, com relação à parte técnica, indicamos que a proposta pode ser aceita, dando continuidade aos demais trâmites do processo.

Manaus, 03 de março de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ
Coordenador da Área de Redes

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 03/03/2022, às 09:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Theo Ferreira Pará**, **Agente de Apoio - Manutenção - Suporte Informática**, em 03/03/2022, às 10:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0775110** e o código CRC **4FD398FA**.

DECLARAÇÕES

UASG 925849 - PROCURADORIA GERAL DE JUSTIÇA

Pregão Eletrônico Nº 40052022

CNPJ/CPF	Razão Social/Nome	Porte da Empresa
01.134.191/0007-32	SERVIX INFORMATICA LTDA	Demais (Diferente de ME/EPP)

Data Declarações: 18/02/2022 23:32 **Declaração MEE/EPP:** NÃO **Declaração de Ciência Edital:** SIM
Declaração Fato Superveniente: SIM **Declaração de Menor:** SIM **Declaração Independente de Proposta:** SIM
Declaração de Acessibilidade: SIM **Declaração de Cota de Aprendizagem:** SIM
Declaração de Não Utilização de Trabalho Degradante ou Forçado: SIM

05.250.796/0001-54 NETWORK SECURE SEGURANCA DA INFORMACAO LTDA Demais (Diferente de ME/EPP)

Data Declarações: 20/02/2022 20:27 **Declaração MEE/EPP:** NÃO **Declaração de Ciência Edital:** SIM
Declaração Fato Superveniente: SIM **Declaração de Menor:** SIM **Declaração Independente de Proposta:** SIM
Declaração de Acessibilidade: SIM **Declaração de Cota de Aprendizagem:** SIM
Declaração de Não Utilização de Trabalho Degradante ou Forçado: SIM

23.378.923/0001-87 IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL ME/EPP

Data Declarações: 21/02/2022 09:38 **Declaração MEE/EPP:** SIM **Declaração de Ciência Edital:** SIM
Declaração Fato Superveniente: SIM **Declaração de Menor:** SIM **Declaração Independente de Proposta:** SIM
Declaração de Acessibilidade: SIM **Declaração de Cota de Aprendizagem:** SIM
Declaração de Não Utilização de Trabalho Degradante ou Forçado: SIM

Imprimir o Relatório

Fechar

Pregão Eletrônico

925849.40052022 .23338 .4600 .94191211280

Procuradoria Geral de Justiça

Ata de Realização do Pregão Eletrônico
Nº 04005/2022

Às 10:00 horas do dia 21 de fevereiro de 2022, reuniram-se o Pregoeiro Oficial deste Órgão e respectivos membros da Equipe de Apoio, designados pelo instrumento legal ATO PGJ 188/2021 de 09/07/2021, em atendimento às disposições contidas na Lei nº 10.520 de 17 de julho de 2002 e no Decreto nº 10.024 de 20 de setembro de 2019, referente ao Processo nº 2021.015252, para realizar os procedimentos relativos ao Pregão nº 04005/2022. Modo de disputa: Aberto. Objeto: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.. O Pregoeiro abriu a Sessão Pública em atendimento às disposições contidas no edital, divulgando as propostas recebidas. Abriu-se em seguida a fase de lances para classificação dos licitantes relativamente aos lances ofertados.

Item: 1 - Grupo 1
Descrição: Serviços de gerenciamento de sistemas computacionais
Descrição Complementar: Serviço de Firewall em Alta Disponibilidade.
Tratamento Diferenciado: -
Quantidade: 48
Unidade de fornecimento: UND SERVIÇO TÉCNICO
Valor Estimado: R$ 3.291.872,1600
Situação: Aceito e Habilitado
Intervalo mínimo entre lances: R$ 0,05

Aceito para: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, pelo melhor lance de** R$ 2.150.000,0000 .

Item: 2 - Grupo 1
Descrição: Serviços de gerenciamento de sistemas computacionais
Descrição Complementar: Serviço de Monitoramento da Solução.
Tratamento Diferenciado: -
Quantidade: 48
Unidade de fornecimento: UND SERVIÇO TÉCNICO
Valor Estimado: R$ 2.444.112,0000
Situação: Aceito e Habilitado
Intervalo mínimo entre lances: R$ 0,05

Aceito para: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, pelo melhor lance de** R$ 250.000,0000 .

Item: 3 - Grupo 1
Descrição: Serviços de gerenciamento de sistemas computacionais
Descrição Complementar: Serviço de Migração do Ambiente Atual
Tratamento Diferenciado: -
Quantidade: 1
Unidade de fornecimento: UND SERVIÇO TÉCNICO
Valor Estimado: R$ 30.553,3300
Situação: Aceito e Habilitado
Intervalo mínimo entre lances: R$ 0,05

Aceito para: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, pelo melhor lance de** R$ 112.500,0000 **e com valor negociado a** R$ 30.553,3300 .

Item: 4 - Grupo 1
Descrição: Serviços de Gerenciamento de Sistemas Computacionais
Descrição Complementar: Serviço de Treinamento da Solução.
Tratamento Diferenciado: -
Quantidade: 5
Unidade de fornecimento: UND SERVIÇO TÉCNICO
Valor Estimado: R$ 61.888,3500
Situação: Aceito e Habilitado
Intervalo mínimo entre lances: R$ 0,05

Aceito para: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, pelo melhor lance de** R$ 47.500,0000 .

Relação de Grupos

Grupo 1

Tratamento Diferenciado: -

Aplicabilidade Margem de Preferência: Não

Critério de Valor: R$ 5.828.425,8400
Situação: Aceito e Habilitado com intenção de recurso

Aceito para: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, pelo melhor lance de** R$ 2.560.000,0000 **e com valor negociado a** R$ 2.478.053,3300 .

Itens do grupo:

- 1 - Serviços de gerenciamento de sistemas computacionais

- 2 - Serviços de gerenciamento de sistemas computacionais
- 3 - Serviços de gerenciamento de sistemas computacionais
- 4 - Serviços de Gerenciamento de Sistemas Computacionais

Histórico

Item: 1 - Grupo 1 - Serviços de gerenciamento de sistemas computacionais

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
05.250.796/0001-54	NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	Não	Não	48	R$ 80.810,0000	R$ 3.878.880,0000	20/02/2022 20:27:19
	Descrição Detalhada do Objeto Ofertado: Serviço de Firewall em Alta Disponibilidade – Fabricante Check Point – 2x NGFW - PNs: 2x CP-CPAP-SG66XX-PLUS-INV - 6600 Appliance Plus – Inventory + 2x CP-UPG-CPAP-SG6600-PLUS-SNBT - 6600 Plus appliance with SandBlast subscription package for 1 year + 2x CP-CPSB-SNBT-6600-PLUS-3Y - Next Generation Threat Prevention and Sandblast for additional 3 years for 6600 PLUS Appliance + 2x CP-CPSB-MOB-U - Mobile Access Blade unlimited + Suporte 24x7 e demais serviços conforme especificações técnicas do edital. O prazo de validade da proposta é de 90 (noventa) dias, a contar da data de sua apresentação. **Porte da empresa:** Demais (Diferente de ME/EPP)						
23.378.923/0001-87	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL	Sim	Sim	48	R$ 120.000,0000	R$ 5.760.000,0000	21/02/2022 09:38:06
	Descrição Detalhada do Objeto Ofertado: Serviço de Firewall em Alta Disponibilidade. **Porte da empresa:** ME/EPP						
01.134.191/0007-32	SERVIX INFORMATICA LTDA	Não	Não	48	R$ 144.460,0000	R$ 6.934.080,0000	18/02/2022 23:32:26
	Descrição Detalhada do Objeto Ofertado: Serviço de Firewall em Alta Disponibilidade. **Porte da empresa:** Demais (Diferente de ME/EPP)						

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R$ 6.934.080,0000	01.134.191/0007-32	21/02/2022 10:00:00:520
R$ 5.760.000,0000	23.378.923/0001-87	21/02/2022 10:00:00:520
R$ 3.878.880,0000	05.250.796/0001-54	21/02/2022 10:00:00:520
R$ 6.900.000,0000	01.134.191/0007-32	21/02/2022 10:17:33:797
R$ 5.000.000,0000	23.378.923/0001-87	21/02/2022 10:19:54:557
R$ 6.000.000,0000	01.134.191/0007-32	21/02/2022 10:20:20:153
R$ 5.100.000,0000	01.134.191/0007-32	21/02/2022 10:21:23:327
R$ 3.500.000,0000	05.250.796/0001-54	21/02/2022 10:22:01:357
R$ 4.600.000,0000	01.134.191/0007-32	21/02/2022 10:22:01:977
R$ 4.900.000,0000	23.378.923/0001-87	21/02/2022 10:23:19:587
R$ 4.000.000,0000	01.134.191/0007-32	21/02/2022 10:24:06:843
R$ 3.000.000,0000	05.250.796/0001-54	21/02/2022 10:24:19:653
R$ 4.800.000,0000	23.378.923/0001-87	21/02/2022 10:24:35:323
R$ 3.800.000,0000	01.134.191/0007-32	21/02/2022 10:25:00:193
R$ 3.600.000,0000	01.134.191/0007-32	21/02/2022 10:25:34:817
R$ 2.600.000,0000	05.250.796/0001-54	21/02/2022 10:26:01:637
R$ 3.500.000,0000	01.134.191/0007-32	21/02/2022 10:26:45:870
R$ 4.000.000,0000	23.378.923/0001-87	21/02/2022 10:27:08:130
R$ 3.000.000,0000	23.378.923/0001-87	21/02/2022 10:28:46:610
R$ 3.400.000,0000	01.134.191/0007-32	21/02/2022 10:30:39:140
R$ 2.900.000,0000	23.378.923/0001-87	21/02/2022 10:31:37:580
R$ 3.200.000,0000	01.134.191/0007-32	21/02/2022 10:33:42:153
R$ 3.000.000,0000	01.134.191/0007-32	21/02/2022 10:34:14:733
R$ 2.800.000,0000	23.378.923/0001-87	21/02/2022 10:34:27:187
R$ 2.400.000,0000	05.250.796/0001-54	21/02/2022 10:35:03:400
R$ 2.790.000,0000	23.378.923/0001-87	21/02/2022 10:35:29:113
R$ 2.990.000,0000	01.134.191/0007-32	21/02/2022 10:36:01:693
R$ 2.700.000,0000	23.378.923/0001-87	21/02/2022 10:36:53:573

R$ 2.640.000,0000	23.378.923/0001-87	21/02/2022 10:41:00:237
R$ 2.900.000,0000	01.134.191/0007-32	21/02/2022 10:42:50:533
R$ 2.150.000,0000	05.250.796/0001-54	21/02/2022 10:44:23:077
R$ 2.820.000,0000	01.134.191/0007-32	21/02/2022 10:45:07:647
R$ 2.740.000,0000	01.134.191/0007-32	21/02/2022 10:46:26:973
R$ 2.650.000,0000	01.134.191/0007-32	21/02/2022 10:48:12:920
R$ 2.600.000,0000	23.378.923/0001-87	21/02/2022 10:55:05:647
R$ 2.500.000,0000	23.378.923/0001-87	21/02/2022 10:56:47:043
R$ 2.448.000,0000	23.378.923/0001-87	21/02/2022 10:58:22:627

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Aceite de proposta	07/03/2022 11:36:51	Aceite individual da proposta. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, pelo melhor lance de R$ 2.150.000,0000.
Habilitação de fornecedor	10/03/2022 15:10:29	Habilitação em grupo de propostas. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ/CPF: 05.250.796/0001-54

Para consultar intenção de recurso e demais eventos do item, verificar histórico do Grupo 1.

Item: 2 - Grupo 1 - Serviços de gerenciamento de sistemas computacionais

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.134.191/0007-32	SERVIX INFORMATICA LTDA	Não	Não	48	R$ 8.731,0000	R$ 419.088,0000	18/02/2022 23:32:26
	Descrição Detalhada do Objeto Ofertado: Serviço de Monitoramento da Solução. **Porte da empresa:** Demais (Diferente de ME/EPP)						
23.378.923/0001-87	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL	Sim	Sim	48	R$ 35.000,0000	R$ 1.680.000,0000	21/02/2022 09:38:06
	Descrição Detalhada do Objeto Ofertado: Serviço de Monitoramento da Solução. **Porte da empresa:** ME/EPP						
05.250.796/0001-54	NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	Não	Não	48	R$ 39.050,0000	R$ 1.874.400,0000	20/02/2022 20:27:19
	Descrição Detalhada do Objeto Ofertado: Serviço de Monitoramento da Solução – Fabricante Check Point – PNs: 1x CP-CPSM-NGSM5 - Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year) + 1x CP-CPSB-EVS-COMP-5-3Y - SmartEvent, SmartReporter and Compliance blades for 5 gateways (Smart-1 & open server) 3 year subscription + Suporte 24x7 e demais serviços conforme especificações técnicas do edital. O prazo de validade da proposta é de 90 (noventa) dias, a contar da data de sua apresentação. **Porte da empresa:** Demais (Diferente de ME/EPP)						

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R$ 1.874.400,0000	05.250.796/0001-54	21/02/2022 10:00:00:520
R$ 1.680.000,0000	23.378.923/0001-87	21/02/2022 10:00:00:520
R$ 419.088,0000	01.134.191/0007-32	21/02/2022 10:00:00:520
R$ 1.200.000,0000	05.250.796/0001-54	21/02/2022 10:19:03:757
R$ 1.500.000,0000	23.378.923/0001-87	21/02/2022 10:21:55:410
R$ 900.000,0000	05.250.796/0001-54	21/02/2022 10:25:03:897
R$ 1.400.000,0000	23.378.923/0001-87	21/02/2022 10:25:43:703
R$ 750.000,0000	05.250.796/0001-54	21/02/2022 10:26:18:477
R$ 1.100.000,0000	23.378.923/0001-87	21/02/2022 10:27:53:480
R$ 419.000,0000	01.134.191/0007-32	21/02/2022 10:28:10:743
R$ 1.000.000,0000	23.378.923/0001-87	21/02/2022 10:29:34:840
R$ 990.000,0000	23.378.923/0001-87	21/02/2022 10:32:29:137
R$ 650.000,0000	05.250.796/0001-54	21/02/2022 10:33:58:490
R$ 550.000,0000	05.250.796/0001-54	21/02/2022 10:34:52:603
R$ 418.000,0000	01.134.191/0007-32	21/02/2022 10:38:04:013
R$ 980.000,0000	23.378.923/0001-87	21/02/2022 10:38:19:790

R$ 417.000,0000	01.134.191/0007-32	21/02/2022 10:40:24:860
R$ 416.000,0000	01.134.191/0007-32	21/02/2022 10:42:09:273
R$ 960.000,0000	23.378.923/0001-87	21/02/2022 10:43:22:070
R$ 400.000,0000	01.134.191/0007-32	21/02/2022 10:43:30:307
R$ 320.000,0000	01.134.191/0007-32	21/02/2022 10:45:42:053
R$ 300.000,0000	01.134.191/0007-32	21/02/2022 10:47:55:020
R$ 150.000,0000	01.134.191/0007-32	21/02/2022 10:48:43:380
R$ 140.000,0000	01.134.191/0007-32	21/02/2022 10:49:04:280
R$ 250.000,0000	05.250.796/0001-54	21/02/2022 10:49:24:577
R$ 950.000,0000	23.378.923/0001-87	21/02/2022 10:50:12:930
R$ 940.000,0000	23.378.923/0001-87	21/02/2022 10:51:41:150
R$ 930.000,0000	23.378.923/0001-87	21/02/2022 10:52:49:957
R$ 912.000,0000	23.378.923/0001-87	21/02/2022 10:53:56:847
R$ 720.000,0000	23.378.923/0001-87	21/02/2022 10:59:04:850

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Aceite de proposta	07/03/2022 11:36:51	Aceite individual da proposta. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, pelo melhor lance de R$ 250.000,0000.
Habilitação de fornecedor	10/03/2022 15:10:29	Habilitação em grupo de propostas. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ/CPF: 05.250.796/0001-54

Para consultar intenção de recurso e demais eventos do item, verificar histórico do Grupo 1.

Item: 3 - Grupo 1 - Serviços de gerenciamento de sistemas computacionais

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.134.191/0007-32	SERVIX INFORMATICA LTDA	Não	Não	1	R$ 26.137,0000	R$ 26.137,0000	18/02/2022 23:32:26
	Descrição Detalhada do Objeto Ofertado: Serviço de Migração do Ambiente Atual **Porte da empresa:** Demais (Diferente de ME/EPP)						
23.378.923/0001-87	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL	Sim	Sim	1	R$ 100.000,0000	R$ 100.000,0000	21/02/2022 09:38:06
	Descrição Detalhada do Objeto Ofertado: Serviço de Migração do Ambiente Atual. **Porte da empresa:** ME/EPP						
05.250.796/0001-54	NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	Não	Não	1	R$ 112.500,0000	R$ 112.500,0000	20/02/2022 20:27:19
	Descrição Detalhada do Objeto Ofertado: Serviço de Migração do Ambiente Atual para a nova solução – Fabricante Check Point. Conforme especificações técnicas do edital. O prazo de validade da proposta é de 90 (noventa) dias, a contar da data de sua apresentação. **Porte da empresa:** Demais (Diferente de ME/EPP)						

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R$ 112.500,0000	05.250.796/0001-54	21/02/2022 10:00:00:520
R$ 100.000,0000	23.378.923/0001-87	21/02/2022 10:00:00:520
R$ 26.137,0000	01.134.191/0007-32	21/02/2022 10:00:00:520
R$ 26.000,0000	01.134.191/0007-32	21/02/2022 10:27:55:860
R$ 90.000,0000	23.378.923/0001-87	21/02/2022 10:39:18:310
R$ 70.000,0000	23.378.923/0001-87	21/02/2022 10:45:10:453

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Aceite de proposta	07/03/2022 11:36:51	Aceite individual da proposta. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, pelo melhor lance de R$ 112.500,0000 e com valor negociado a R$

30.553,3300. Motivo: Valor negociado no chat e conforme proposta escrita.

Habilitação de fornecedor	10/03/2022 15:10:29	Habilitação em grupo de propostas. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ/CPF: 05.250.796/0001-54

Para consultar intenção de recurso e demais eventos do item, verificar histórico do Grupo 1.

Item: 4 - Grupo 1 - Serviços de Gerenciamento de Sistemas Computacionais

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
23.378.923/0001-87	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL	Sim	Sim	5	R$ 8.000,0000	R$ 40.000,0000	21/02/2022 09:38:06
	Descrição Detalhada do Objeto Ofertado: Serviço de Treinamento da Solução. **Porte da empresa:** ME/EPP						
05.250.796/0001-54	NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	Não	Não	5	R$ 9.500,0000	R$ 47.500,0000	20/02/2022 20:27:19
	Descrição Detalhada do Objeto Ofertado: Serviço de Treinamento da Solução do Fabricante Check Point. Conforme especificações técnicas do edital. O prazo de validade da proposta é de 90 (noventa) dias, a contar da data de sua apresentação. **Porte da empresa:** Demais (Diferente de ME/EPP)						
01.134.191/0007-32	SERVIX INFORMATICA LTDA	Não	Não	5	R$ 13.405,0000	R$ 67.025,0000	18/02/2022 23:32:26
	Descrição Detalhada do Objeto Ofertado: Serviço de Treinamento da Solução. **Porte da empresa:** Demais (Diferente de ME/EPP)						

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R$ 67.025,0000	01.134.191/0007-32	21/02/2022 10:00:00:520
R$ 47.500,0000	05.250.796/0001-54	21/02/2022 10:00:00:520
R$ 40.000,0000	23.378.923/0001-87	21/02/2022 10:00:00:520
R$ 60.000,0000	01.134.191/0007-32	21/02/2022 10:27:31:793
R$ 39.000,0000	01.134.191/0007-32	21/02/2022 10:43:56:907

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Aceite de proposta	07/03/2022 11:36:51	Aceite individual da proposta. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, pelo melhor lance de R$ 47.500,0000.
Habilitação de fornecedor	10/03/2022 15:10:29	Habilitação em grupo de propostas. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ/CPF: 05.250.796/0001-54

Para consultar intenção de recurso e demais eventos do item, verificar histórico do Grupo 1.

HISTÓRICO DO Grupo 1

Propostas Participaram deste grupo as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Global	Data/Hora Registro
05.250.796/0001-54	NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	Não	Não	-	R$ 5.913.280,0000	20/02/2022 20:27:19
01.134.191/0007-32	SERVIX INFORMATICA LTDA	Não	Não	-	R$ 7.446.330,0000	18/02/2022 23:32:26
23.378.923/0001-87	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL	Sim	Sim	-	R$ 7.580.000,0000	21/02/2022 09:38:06

Eventos do Grupo

Evento	Data	Observações
Encerramento análise de	21/02/2022 10:12:59	Item com análise de propostas finalizada.

propostas		
Abertura	21/02/2022 10:16:01	Item aberto para lances.
Encerramento	21/02/2022 11:01:05	Item encerrado para lances.
Encerramento etapa aberta	21/02/2022 11:01:05	Item com etapa aberta encerrada.
Abertura do prazo - Convocação anexo	21/02/2022 11:22:17	Convocado para envio de anexo o fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54.
Encerramento do prazo - Convocação anexo	21/02/2022 12:31:38	Encerrado o prazo de Convocação de Anexo pelo fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54.
Abertura do prazo - Convocação anexo	07/03/2022 11:53:10	Convocado para envio de anexo o fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54.
Encerramento do prazo - Convocação anexo	07/03/2022 12:04:09	Encerrado o prazo de Convocação de Anexo pelo fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54.
Habilitação de fornecedor	10/03/2022 15:10:30	Habilitação em grupo de propostas. Fornecedor: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - CNPJ/CPF: 05.250.796/0001-54
Registro de intenção de recurso	10/03/2022 15:16:50	Registro de Intenção de Recurso. Fornecedor: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL CNPJ/CPF: 23378923000187. Motivo: Manifestamos intenção de recorrer contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., devido ao não atendimento de re
Aceite de intenção de recurso	10/03/2022 15:50:12	Intenção de recurso aceita. Fornecedor: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ/CPF: 23378923000187.

Intenções de Recurso para o Grupo

CNPJ/CPF	Data/Hora do Recurso	Data/Hora Admissibilidade	Situação
23.378.923/0001-87	10/03/2022 15:16	10/03/2022 15:50	Aceito

Motivo Intenção: Manifestamos intenção de recorrer contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., devido ao não atendimento de requisitos claramente obrigatórios, bem como outros itens que serão devidamente apresentados tempestivamente junto a peça recursal.

Troca de Mensagens

	Data	Mensagem
Sistema	21/02/2022 10:00:00	A sessão pública está aberta. Nesta compra haverá um período para a realização da análise de propostas e após este período os itens serão disponibilizados para o início dos lances. Até 1 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Haverá aviso prévio de abertura dos itens de 1 minutos. Mantenham-se conectados.
Pregoeiro	21/02/2022 10:01:26	Bom dia, Senhores licitantes. Estamos iniciando a sessão pública do pregão eletrônico n.º 4005/2022, promovido pelo Ministério Público do Estado do Amazonas/Procuradoria-Geral de Justiça do Amazonas. Antes de iniciar a fase competitiva, peço a atenção de todos para alguns breves avisos a respeito da presente licitação.
Pregoeiro	21/02/2022 10:01:32	Sejam bem-vindos à sessão pública do pregão eletrônico n.º 4005/2022, cujo objeto é a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.
Pregoeiro	21/02/2022 10:02:01	A licitação será pelo menor por LOTE (ÚNICO).
Pregoeiro	21/02/2022 10:02:05	É importante deixar claro que são de responsabilidade do licitante todas as transações efetuadas em seu nome, especialmente o cadastramento de proposta e o oferecimento de lances, ainda que o acesso ao sistema seja realizado por terceiros.
Pregoeiro	21/02/2022 10:02:10	Na presente licitação será adotado o modo de disputa ABERTO, previsto no art. 32 e parágrafos do decreto n.º 10.024/2019.
Pregoeiro	21/02/2022 10:02:14	O envio de lances, sejam eles intermediários ou destinados a cobrir a melhor oferta, devem respeitar o intervalo mínimo de R$ 0,05 (cinco centavos), de modo que as ofertas em desacordo com este critério não serão processadas pelo sistema.
Pregoeiro	21/02/2022 10:02:22	Conforme disposição contida no art. 26, §2º, do Decreto n.º 10.024/2019, o licitante poderá deixar de apresentar os documentos de habilitação que constem do Sistema de Cadastramento de Fornecedores – Sicaf, cabendo ao interessado em participar do pregão o envio, juntamente com a proposta, dos documentos de habilitação não disponíveis no mencionado cadastro, sendo-lhe vedado o envio posterior de documentação originariamente exigida no edital.

Pregoeiro	21/02/2022 10:02:42	Após a etapa de lances, o pregoeiro poderá realizar diligência, com fundamento no art. 43, §3º, da Lei n.º 8.666/93, destinada a esclarecer ou complementar informações sobre a proposta ajustada ao lance vencedor e/ou documentos de habilitação.
Pregoeiro	21/02/2022 10:02:57	Nos termos do art. 49, inciso V, do Decreto Federal n.º 10.024/19, o fornecedor que não mantiver sua proposta ficará impedido de licitar e contratar com o Estado do Amazonas pelo prazo de até 5 (cinco) anos, razão pela qual os licitantes devem formular seus lances com prudência e responsabilidade.
Pregoeiro	21/02/2022 10:03:01	A exclusão de lance pelo pregoeiro durante a fase competitiva é medida excepcional e somente será promovida quando houver fortes indícios de inexequibilidade do preço.
Pregoeiro	21/02/2022 10:03:26	As eventuais suspensões da sessão pública serão comunicadas pelo pregoeiro no sistema (chat), com indicação da data e horário para a sua retomada, assegurando a todos condições de acompanhar os atos praticados durante a licitação.
Pregoeiro	21/02/2022 10:13:41	Prezados, compatibilizados as especificações e os valores iniciais, informo que em breve estaremos passando à fase de disputa.
Pregoeiro	21/02/2022 10:13:48	Quanto aos lances, relembro que os mesmos podem ser inferiores ao próprio lance, no intuito de permanecer em melhor posição na ordem de classificação.
Pregoeiro	21/02/2022 10:14:38	A melhor proposta para o item 1 figura acima do estimado pela Administração, necessitaremos de preços melhores ou futura negociação;
Sistema	21/02/2022 10:15:00	Etapa de análise de propostas encerrada. A abertura de itens para disputa será iniciada. Mantenham-se conectados.
Sistema	21/02/2022 10:15:01	A abertura do item G1 para lances está agendada para daqui a 1 minuto. Mantenham-se conectados.
Sistema	21/02/2022 10:16:01	O item G1 foi aberto. Solicitamos o envio de lances.
Pregoeiro	21/02/2022 10:16:02	Os demais itens estão dentro do estimado pela Administração, então sugiro os participantes se concentrarem em diminuir os lances especificadamente do item 1.
Pregoeiro	21/02/2022 10:21:38	Necessitamos de um desconto de pelo menos 15% no item 1.
Pregoeiro	21/02/2022 10:27:06	Senhores, o preço para o item 1 já se encontra dentro do estimado.
Pregoeiro	21/02/2022 10:56:26	Alerto para os cuidados necessários quanto à exequibilidade de suas propostas!
Sistema	21/02/2022 11:01:05	O item G1 está encerrado.
Sistema	21/02/2022 11:01:20	A etapa de julgamento de propostas foi iniciada. Acompanhe essa etapa na funcionalidade "Acompanhar Julgamento / Habilitação / Admissibilidade".
Pregoeiro	21/02/2022 11:03:03	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Bom dia Sr. Fornecedor, sua empresa está conectada?
Pregoeiro	21/02/2022 11:06:00	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Antes de convocá-lo para envio da proposta reajustada ao seu último lance, necessitamos negociar. Em razão do disposto no art. 38 do Decreto Federal n.º 10.024/2019 e também na condição 8.30 c/c 9.1 do edital, solicito que verifique a possibilidade de reduzir o valor da sua proposta.
Pregoeiro	21/02/2022 11:06:17	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Ou sua empresa se encontra na sua melhor oferta?
05.250.796/0001-54	21/02/2022 11:08:24	Bom dia, prezado sr. pregoeiro, ja tivemos uma redução considerável na fase de lances. Esse é o nosso melhor valor.
Pregoeiro	21/02/2022 11:10:19	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Compreendo Sr. Fornecedor, todavia existe 1 item da sua proposta acima do meu estimado, de forma que indago qual sua melhor oferta para o item 3?
Pregoeiro	21/02/2022 11:11:36	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Nos termos do subitem 10.2.2. este servidor encontra-se impossibilitado de aceitar preço (global ou unitário) final superior ao preço máximo fixado pela Administração.
Pregoeiro	21/02/2022 11:12:15	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Ademais, sua empresa participou da fase interna de cotação e ofertou preço bem menor ao apresentado no certame. Portanto, questiono qual sua melhor oferta para o item 3?
05.250.796/0001-54	21/02/2022 11:12:22	Solicitamos 5 minutos para que possamos verificar. Por gentileza
05.250.796/0001-54	21/02/2022 11:14:34	Qual seria o valor estimado para o item 3?
Pregoeiro	21/02/2022 11:16:11	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - O maior valor que este Pregoeiro encontra-se limitado consiste em R$ 30.553,33. Sua empresa aceita?
05.250.796/0001-54	21/02/2022 11:17:54	ok, faremos o ajuste conforme o estimado do item 3.
Pregoeiro	21/02/2022 11:18:51	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Obrigado por sua compreensão e aceitação da contraproposta.
Pregoeiro	21/02/2022 11:19:35	Para IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL - Aqueles que tiverem interesse, a estimativa de preços encontra-se disponível no sítio eletrônico desta Instituição, para ampla e irrestrito acesso, no endereço: https://www.mpam.mp.br/servicos/licitacoes/licitacoes-em-andamento/47-licitacoes/pregao-eletronico-em-andamento/15018-pe-4005-2022-cpl-mp-pgj-firewall-de-proxima-geracao-em-alta-disponibilidade
Pregoeiro	21/02/2022 11:19:45	Aqueles que tiverem interesse, a estimativa de preços encontra-se disponível no sítio eletrônico desta Instituição, para ampla e irrestrito acesso, no endereço:

		https://www.mpam.mp.br/servicos/licitacoes/licitacoes-em-andamento/47-licitacoes/pregao-eletronico-em-andamento/15018-pe-4005-2022-cpl-mp-pgj-firewall-de-proxima-geracao-em-alta-disponibilidade
Pregoeiro	21/02/2022 11:20:50	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Feitas tais considerações, promoverei sua convocação para envio da proposta e demais documentos no prazo de 02 horas.
Pregoeiro	21/02/2022 11:21:07	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Caso não seja possível o envio pelo sistema, a empresa, sob sua conta e risco, poderá enviar a proposta, excepcionalmente, para a caixa postal eletrônica institucional licitacao@mpam.mp.br.
Pregoeiro	21/02/2022 11:21:09	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Favor confirmar o recebimento pelos telefones constantes do Edital e, desde que dentro do prazo, sem prejuízo de posterior encaminhamento por meio do sistema, garantindo-se, assim, amplo acesso aos arquivos apresentados.
Pregoeiro	21/02/2022 11:22:09	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Nos termos do Edital: "9.1. O pregoeiro solicitará ao licitante melhor classificado que, no prazo máximo de 02 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados [...]"
Sistema	21/02/2022 11:22:17	Senhor fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, solicito o envio do anexo referente ao grupo G1.
Sistema	21/02/2022 12:31:38	Senhor Pregoeiro, o fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, enviou o anexo para o grupo G1.
Pregoeiro	21/02/2022 12:39:01	Senhores licitantes, informo que será necessário realizar diligência, portanto, com encaminhamento da proposta e demais documentos à análise e manifestação do setor técnico, com fundamento no art. 43, § 3º, da Lei n.º 8.666/93 c/c 10.1.2. do instrumento convocatório.
Pregoeiro	21/02/2022 12:39:11	Logo, decido pela suspensão da presente sessão. A reabertura será comunicada com a antecedência necessária para fins de divulgação do resultado do julgamento da proposta. Agradeço a atenção dispensada, bom dia!
Pregoeiro	04/03/2022 12:02:21	Prezados, informo que o Setor Técnico nos retornou com sua manifestação, de forma que os convoco para segunda-feira, dia 07/03 às 10:30 hrs (Horário local) e 11:30 hrs (Brasília) para continuidade do certame.
Pregoeiro	07/03/2022 11:32:33	Bom dia Srs. Fornecedores, vamos dar continuidade como informado anteriormente.
Pregoeiro	07/03/2022 11:34:49	A proposta fora devidamente encaminhada para o Setor Técnico. Após análise o mesmo nos retornou mediante o PARECER Nº 4.2022.SIET.0775110.2021.015252, com a seguinte conclusão final:
Pregoeiro	07/03/2022 11:35:01	O presente parecer se baseia nas disposições do Termo de Referência n. 20.2021.DTIC.0720733.2021.015252, Anexo I ao Edital do certame, SEI 0763629, em seus diversos itens.
Pregoeiro	07/03/2022 11:35:06	A proposta de preço, documento 0772069, informa equipamentos e serviços condizentes com as quantidades e exigências do Termo de Referência. Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo.
Pregoeiro	07/03/2022 11:35:29	Portanto, decido aceitar a proposta da empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA.
Pregoeiro	07/03/2022 11:37:36	Por sua vez, no que tange a documentação de habilitação, constata-se que a empresa preencheu os requisitos reclamados no Edital.
Pregoeiro	07/03/2022 11:38:13	Com relação a parte técnica, o Setor Requisitante no mesmo documento informado anteriormente, manifestou-se da seguinte forma:
Pregoeiro	07/03/2022 11:38:27	Conforme exigência, foram apresentados atestados de capacidade técnica que comprovam, conjuntamente, a prestação anterior de serviços de firewall de próxima geração, NGFW, com troughput de 10Gbps, no mínimo. Foram apresentados 03 (três) atestados, disponíveis nas páginas 42, 43, 44 e 45 do documento 0772080, ...
Pregoeiro	07/03/2022 11:38:41	... , incluindo equipamentos similares e superiores ao objeto deste processo.
Pregoeiro	07/03/2022 11:41:00	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Senhor Fornecedor, ao realizar as convalidações dos documentos anexados no sistema, constatamos que a maioria permite sua verificação na Internet, como, por exemplo, Contrato Social e Balanco na JUCEA-CE, certidão de falência no TJ-CE. Todavia, os atestados da Hapvida e Pague menos inexiste essa possibilidade.
05.250.796/0001-54	07/03/2022 11:41:45	Bom dia Sr Pregoeiro
Pregoeiro	07/03/2022 11:42:22	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Desta forma, antes de promover sua habilitação no sistema, convoco-o para envio dos originais ou copias autenticadas, nos termos do subitem 11.11.5 c/c 23.7 do Edital.
05.250.796/0001-54	07/03/2022 11:43:50	Certamente Sr Pregoeiro, enviaremos conforme solicitado.
Pregoeiro	07/03/2022 11:43:56	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Portanto, a empresa terá que comprovar ate amanha o envio dos referidos documentos. Para isso, basta enviar o Código de rastreio dos correios ou outro meio de transporte, para o devido acompanhamento, no e-mail licitacao@mpam.mp.br
05.250.796/0001-54	07/03/2022 11:44:25	Podemos anexar no sistema as copias autenticadas?

Pregoeiro	07/03/2022 11:44:32	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Avenida Coronel Teixeira, n. 7995 - Bairro Nova Esperança CEP: 69037-473 - Manaus/AM
Pregoeiro	07/03/2022 11:45:32	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - As copias autenticadas que a empresa pretende anexar temos como convalidar na internet? Se trata de algum cartório digital?
05.250.796/0001-54	07/03/2022 11:46:19	ok, enviaremos os originais. De antemão anexamos as copias autenticadas no portal?
05.250.796/0001-54	07/03/2022 11:46:43	So um instante
Pregoeiro	07/03/2022 11:47:37	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - A empresa poderá enviar para o referido endereço as copias autenticadas sem problemas.
Pregoeiro	07/03/2022 11:48:24	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Se as copias autenticadas possibilitarem a convalidação na internet, basta anexar no sistema que faremos a verificação.
05.250.796/0001-54	07/03/2022 11:50:12	Estamos verificando se as autenticações podem ser validadas online, mas desde ja confirmamos que as mesmas serão enviadas para o endereço informado.
Pregoeiro	07/03/2022 11:50:54	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Salvo engano em João Pessoa existe um cartório digital que possibilita essa confirmação.
Pregoeiro	07/03/2022 11:51:42	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Os demais cartórios possibilitam a confirmação do selo e isto não atende nossas exigências.
Pregoeiro	07/03/2022 11:52:54	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Vamos fazer o seguinte, foi convocar a empresa para juntar as copias autenticadas no sistema. Caso entenda como suficiente, já comunico a decisão.
05.250.796/0001-54	07/03/2022 11:52:54	Sr Pregoeiro, vamos enviar as copias autenticadas mesmo, juntamente com todos os documentos de habilitação solicitados no edital.
Sistema	07/03/2022 11:53:10	Senhor fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, solicito o envio do anexo referente ao grupo G1.
Pregoeiro	07/03/2022 11:53:37	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - *vou convocar
05.250.796/0001-54	07/03/2022 11:54:04	ok
Pregoeiro	07/03/2022 12:01:26	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - A empresa já possui as copias autenticadas?
Sistema	07/03/2022 12:04:09	Senhor Pregoeiro, o fornecedor NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ/CPF: 05.250.796/0001-54, enviou o anexo para o grupo G1.
Pregoeiro	07/03/2022 12:06:34	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Sr. Fornecedor, realmente necessitamos do envio físico das copias autenticadas.
Pregoeiro	07/03/2022 12:07:34	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Favor enviar em atenção do Sr. Edson Barreto, Presidente da CPL do Ministério Publico do Estado do Amazonas, para o endereço informado anteriormente.
05.250.796/0001-54	07/03/2022 12:08:40	Ok Sr Pregoeiro, enviaremos os documentos fisicos.
Pregoeiro	07/03/2022 12:08:45	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Solicitamos, se possível, utilizar do meio de envio mais célere para que possamos encerrar o certame mais breve possível. Não esquecer de nos enviar no e-mail o comprovante ou numero para rastreio.
Pregoeiro	07/03/2022 12:09:17	Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Qualquer duvida, estaremos a disposição por e-mail ou nos telefones constantes do rodapé do Edital.
05.250.796/0001-54	07/03/2022 12:10:45	Sim, ainda hoje serão encaminhados e informado o código para rastreio.
Pregoeiro	07/03/2022 12:10:47	Aos demais, informamos que a manifestação técnica encontra-se disponível no sitio eletrônico desta Instituição, no endereço: https://www.mpam.mp.br/servicos/licitacoes/licitacoes-em-andamento/47-licitacoes/pregao-eletronico-em-andamento/15018-pe-4005-2022-cpl-mp-pgj-firewall-de-proxima-geracao-em-alta-disponibilidade
Pregoeiro	07/03/2022 12:11:26	Outrossim, decido suspender a presente sessão, aguardando o envio dos documentos solicitados. Informaremos com antecedência a futura reabertura.
Pregoeiro	07/03/2022 12:11:43	Grato pela atenção dispensada.
Pregoeiro	08/03/2022 13:06:29	Senhores informo que a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA nos encaminhou devidamente o código de rastreio, ficaremos no aguardo da chegada da documentação para prosseguimento do certame.
Pregoeiro	09/03/2022 13:01:02	Prezados Fornecedores, informo que recebemos devidamente os documentos solicitados. Desta forma, comunico a reabertura amanhã (10/03/2022) às 14 hrs (Horário Local) e 15 hrs (Brasília).
Pregoeiro	10/03/2022 15:00:41	Boa tarde Srs. Licitantes, como informado daremos continuidade ao certame.
Pregoeiro	10/03/2022 15:04:12	Considerando devidamente o recebimento dos documentos solicitados, concluo que a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54 comprovou atender às exigências editalícias.
Pregoeiro	10/03/2022 15:04:23	Nessa etapa, verificou-se a autenticidade das certidões negativa de débitos mediante SICAF, bem como da ausência de distribuição de feitos de falência ou recuperação judicial, junto à Justiça Estadual de domicílio da licitante melhor classificada. Da mesma

		sorte procedeu-se com os demais documentos de habilitação da interessada que permitiam a convalidação.
Pregoeiro	10/03/2022 15:04:37	Passo seguinte, verificou-se as condições da licitante quanto à ausência de sanções pela Administração Pública, no SICAF do Comprasnet, bem como na Relação de Empresas com Sanção Administrativa em Vigor, do TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS – TCE, na Relação de Licitantes Inidôneos do TRIBUNAL DE CONTAS DA UNIÃO – TCU.
Pregoeiro	10/03/2022 15:04:39	Igualmente, na Lista de Empresas Suspensas/Impedidas da COMISSÃO GERAL DE LICITAÇÃO DO ESTADO DO AMAZONAS – CGL, no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), da CONTROLADORIA GERAL DA UNIÃO – CGU, no Cadastro Nacional de Condenações Civis por Ato de Improbidade Administrativa (CNCIA) do CONSELHO NACIONAL DE JUSTIÇA – CNJ.
Pregoeiro	10/03/2022 15:04:43	Ademais, diligenciou-se à Relação de pessoas jurídicas impedidas de contratar com a Administração Pública da SEFAZ-AM, NÃO sendo constatados registros que indicassem restrições à contratação.
Pregoeiro	10/03/2022 15:04:45	Oportunamente, registre-se que com o objetivo de atender aos princípios de simplificação e racionalização de serviços públicos digitais, presentes nas Leis n.ºs 12.965/14 e 13.460/18; e no Decreto nº 8.638/2016, o Tribunal de Contas da União passou a disponibilizar ferramenta que permite a consulta consolidada de pessoas jurídicas que reúne, em um só lugar.
Pregoeiro	10/03/2022 15:04:48	Logo, em relatório único, contendo as Licitantes Inidôneos do TCU, CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade do CNJ; Cadastro Nacional de Empresas Inidôneas e Suspensas e CNEP - Cadastro Nacional de Empresas Punidas ambos do Portal da Transparência.
Pregoeiro	10/03/2022 15:05:01	Assim, este Pregoeiro promoveu a juntada da Consulta Consolidada de Pessoa Jurídica e SICAF da empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54 nos autos do procedimento interno desta Instituição, bem como no sítio eletrônico desta Instituição.
Pregoeiro	10/03/2022 15:05:05	Aqueles que tiverem interesse, o SICAF e a Consulta Consolidada de Pessoa Jurídica encontram-se disponível no endereço: https://www.mpam.mp.br/servicos/licitacoes/licitacoes-em-andamento/47-licitacoes/pregao-eletronico-em-andamento/15018-pe-4005-2022-cpl-mp-pgj-firewall-de-proxima-geracao-em-alta-disponibilidade
Pregoeiro	10/03/2022 15:08:49	Concluída a análise dos documentos de habilitação conforme item 11 do instrumento convocatório e, estando todos conforme e de acordo com a previsões editalícias, este Pregoeiro decide HABILITAR a empresa em foco.
Pregoeiro	10/03/2022 15:09:54	Sendo assim, promoverei sua habilitação no sistema, momento no qual será aberto o prazo de 30 (trinta) minutos para registro de eventual intenção recursal.
Pregoeiro	10/03/2022 15:09:59	Na hipótese de alguma empresa manifestar interesse recursal, será realizado o exame de admissibilidade da intenção. Caso o pregoeiro aceite a intenção, será aberto o prazo de 3 (três) dias corridos para apresentação das razões recursais no sistema, seguido de igual prazo para as contrarrazões.
Pregoeiro	10/03/2022 15:10:07	Se o pregoeiro julgar procedente o recurso, será realizado o retorno do pregão para a fase de julgamento, retificando-se os atos inquinados de irregularidades/ilegalidades, repetindo-se as fases subsequentes.
Pregoeiro	10/03/2022 15:10:11	Outrossim, solicito prudência e bom senso nos Senhores, caso queiram fazer uso desta prerrogativa dos recursos, a fim de evitarmos recursos meramente protelatórios.
Pregoeiro	10/03/2022 15:10:18	Desde já, gostaria de agradecer a todos pela participação neste pregão. Até a próxima.
Sistema	10/03/2022 15:10:30	Srs. Fornecedores, está aberto o prazo para registro de intenção de recursos para os itens/grupos na situação de ´aceito e habilitado´ ou ´cancelado no julgamento´.
Pregoeiro	10/03/2022 15:10:41	Foi informado o prazo final para registro de intenção de recursos: 10/03/2022 às 15:40:00.
Pregoeiro	10/03/2022 15:42:50	Senhores, tivemos a apresentação de recurso. Este Pregoeiro fará a devida aceitação e concessão dos prazos de 3 dias corridos para envio das razões, mais 3 dias para contrarrazões e 5 dias úteis para decisão deste Pregoeiro.
Pregoeiro	10/03/2022 15:45:53	Portanto, a empresa terá até dia 14/03/2022 às 23h59min para enviar as razões e até o dia 17/03/2022 às 23h59min para contrarrazões e até o dia 24/03/2022 para decisão deste Pregoeiro.
Pregoeiro	10/03/2022 15:48:23	Solicito que a empresa apresente as razões diretamente no Sistema Comprasnet e envie cópia em função da formatação para o e-mail desta Comissão (licitacao@mpam.mp.br).
Pregoeiro	10/03/2022 15:49:09	Oportunamente, informo que as razões serão disponibilizadas para acompanhamento dos interessados no sítio oficial desta Instituição: https://www.mpam.mp.br/servicos/licitacoes/licitacoes-em-andamento/47-licitacoes/pregao-eletronico-em-andamento/15018-pe-4005-2022-cpl-mp-pgj-firewall-de-proxima-geracao-em-alta-disponibilidade
Pregoeiro	10/03/2022 15:50:43	Portanto, declaro encerrada a presente sessão.

Eventos do Pregão

Evento	Data/Hora	Observações
Alteração equipe	14/02/2022 09:11:17	
Abertura da sessão	21/02/2022 10:00:00	Abertura da sessão pública

pública		
Encerramento da análise de propostas	21/02/2022 10:15:00	Etapa de análise de propostas encerrada.
Julgamento de propostas	21/02/2022 11:01:20	Início da etapa de julgamento de propostas
Abertura do prazo	10/03/2022 15:10:30	Abertura de prazo para intenção de recurso
Fechamento do prazo	10/03/2022 15:10:41	Fechamento de prazo para registro de intenção de recurso: 10/03/2022 às 15:40:00.

Data limite para registro de recurso: 14/03/2022.
Data limite para registro de contrarrazão: 17/03/2022.
Data limite para registro de decisão: 24/03/2022.

Após encerramento da Sessão Pública, os licitantes melhores classificados foram declarados vencedores dos respectivos itens. Foi divulgado o resultado da Sessão Pública e foi concedido o prazo recursal conforme preconiza o artigo 45, do Decreto 10.024 de 20 de setembro de 2019. Nada mais havendo a declarar, foi encerrada a sessão às 15:51 horas do dia 10 de março de 2022, cuja ata foi lavrada e assinada pelo Pregoeiro e Equipe de Apoio.

EDSON FREDERICO LIMA PAES BARRETO
Pregoeiro Oficial

MAURICIO ARAUJO MEDEIROS
Equipe de Apoio

IURY FECHINE RAMOS
Equipe de Apoio

THIAGO NORONHA DAMASCENO OLIVEIRA
Equipe de Apoio

Imprimir o Relatório

Voltar

PREGÃO ELETRÔNICO

Procuradoria Geral de Justiça

Pregão Eletrônico Nº 04005/2022

RESULTADO POR FORNECEDOR

05.250.796/0001-54 - NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Item	Descrição	Unidade de Fornecimento	Quantidade	Critério de Valor (*)	Valor Unitário	Valor Global
	Grupo 1	-	-	R$ 5.828.425,8400	-	R$ 2.478.053,3300

Marca:
Descrição Detalhada do Objeto Ofertado:

Total do Fornecedor: R$ 2.478.053,3300

Valor Global da Ata: R$ 2.478.053,3300

(*) É necessário detalhar o item para saber qual o critério de valor que é utilizado: Estimado ou Referência ou Máximo Aceitável.

Imprimir o Relatório

Voltar

Pregão Eletrônico

- **Visualização de Propostas**

UASG: 925849 - PROCURADORIA GERAL DE JUSTIÇA
Pregão nº: **40052022**
Modo de Disputa: Aberto

Menu Voltar

Fornecedor assinalado com (*) teve sua proposta desclassificada para o item.
Na coluna "Declaração", os fornecedores que estão assinalados com 'SIM', declaram que estão cientes e concordam com as condições contidas no edital e seus anexos, bem como de que cumprem plenamente os requisitos de habilitação definidos no edital.

Grupo 1 **Critério de Valor:** R$ 5.828.425,8400

Tratamento Diferenciado: -

Aplicabilidade Margem de Preferência: Não

Intervalo mínimo entre lances: -

Fornecedor	Proposta (R$)	Melhor Lance (R$)	Data Melhor Lance	Valor (R$) Negociado	Situação da Proposta	Anexo	Declaração
05.250.796/0001-54 - NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	5.913.280,0000	2.560.000,0000	21/02/2022 10:49:24:577	2.478.053,3300	Aceito e Habilitado	Consultar	SIM

Porte da Empresa: Demais (Diferente de ME/EPP) **Declaração ME/EPP:** NÃO

Declaração de Inexistência de fato superveniente: SIM **Declaração de Menor:** SIM **Declaração independente de proposta:** SIM

Declaração de Não Utilização de Trabalho Degradante ou Forçado: SIM **Declaração de Acessibilidade:** SIM

Declaração de Cota de Aprendizagem: SIM

Consultar Itens do Grupo

Fornecedor	Proposta (R$)	Melhor Lance (R$)	Data Melhor Lance	Valor (R$) Negociado	Situação da Proposta	Anexo	Declaração
01.134.191/0007-32 - SERVIX INFORMATICA LTDA	7.446.330,0000	2.855.000,0000	21/02/2022 10:49:04:280	-		Consultar	SIM

Porte da Empresa: Demais (Diferente de ME/EPP) **Declaração ME/EPP:** NÃO

Declaração de Inexistência de fato superveniente: SIM **Declaração de Menor:** SIM **Declaração independente de proposta:** SIM

Declaração de Não Utilização de Trabalho Degradante ou Forçado: SIM **Declaração de Acessibilidade:** SIM

Declaração de Cota de Aprendizagem: SIM

Consultar Itens do Grupo

Fornecedor	Proposta (R$)	Melhor Lance (R$)	Data Melhor Lance	Valor (R$) Negociado	Situação da Proposta	Anexo	Declaração
23.378.923/0001-87 - IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL	7.580.000,0000	3.278.000,0000	21/02/2022 10:59:04:850	-		Consultar	SIM

Porte da Empresa: ME/EPP **Declaração ME/EPP:** SIM

Declaração de Inexistência de fato superveniente: SIM **Declaração de Menor:** SIM **Declaração independente de proposta:** SIM

Declaração de Não Utilização de Trabalho Degradante ou Forçado: SIM **Declaração de Acessibilidade:** SIM

Declaração de Cota de Aprendizagem: SIM

Consultar Itens do Grupo

Para mais informações sobre o porte da empresa, clique **aqui**.

Menu Voltar

Pregão Eletrônico

- **Visualização de Recursos, Contrarrazões e Decisões**

Pregão nº 40052022

Grupo 1 (Visualizar Itens)

Tratamento Diferenciado: -

Aplicabilidade Margem de Preferência: Não

Sessões Públicas: Atual

Sessão Pública nº 1 (Atual)

CNPJ: 23.378.923/0001-87 - Razão Social/Nome: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL

- Intenção de Recurso
- Recurso
- Contrarrazão do Fornecedor: 05.250.796/0001-54 - NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Menu Voltar

Pregão Eletrônico

- **Visualização de Recursos, Contrarrazões e Decisões**

INTENÇÃO DE RECURSO:

Manifestamos intenção de recorrer contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., devido ao não atendimento de requisitos claramente obrigatórios, bem como outros itens que serão devidamente apresentados tempestivamente junto a peça recursal.

Fechar

PREGÃO ELETRÔNICO

- **Visualização de Recursos, Contrarrazões e Decisões**

RECURSO :

Ilustríssimo Senhor Pregoeiro Oficial do Ministério Público do Estado do Amazonas
Senhor EDSON FREDERICO LIMA PAES BARRETO

Assunto: Recurso Administrativo
Referência: Processo SEI n.º 2021.015252
Pregão Eletrônico: 4.005/2022-CPL/MP/PGJ

IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 23.378.923/0001-87, na condição de licitante participante do certame em epígrafe, VEM, respeitosamente, perante Vossa Senhoria, a tempo e modo, interpor o presente RECURSO ADMINISTRATIVO, contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, que deixou de cumprir requisitos obrigatórios, levando o MD Pregoeiro à tomar decisão equivocada de aceitar e habilitar a sua proposta, o que fazemos com fundamento nos termos da Lei Federal nº 10.520/02, subsidiariamente à Lei Federal 8.666/93 e suas alterações, da Constituição Federal, bem como das normas e condições estabelecidas no instrumento convocatório, junto à Cláusula 12ª do edital do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, pelas razões anexas aduzidas.

Pede deferimento.
Fortaleza - CE, 14/03/2022.

Théo Augusto Ramalho Costa
CEO da It Protect

DAS RAZÕES DE RECURSO

EMÉRITO JULGADOR,

Em face às relevantes razões de fato e de direito a seguir aduzidas, as quais anexamos aqui suas justificativas, requeremos, por conseguinte, que seja este recurso recebido, processado e concedido o efeito suspensivo para análise do presente pedido e em caso desse MD Pregoeiro não reconsiderar sua decisão, que seja determinado o encaminhamento do recurso para apreciação do seu Superior Hierárquico, como determina a nossa legislação que regula as licitações públicas.
Permissa vênia, a r. decisão do Ilustríssimo Julgador, que assim se manifestou "este Pregoeiro decide HABILITAR a empresa em foco" (10/03/2022 15:08:49), sendo que a situação correta é "Aceito e Habilitado", resultando no aceite de uma proposta que não atende aos requisitos exigidos, carece que seja revista e reformada, eis que prolatada em desarmonia com a nossa legislação, eivada de vícios e consubstanciada em afronta às regras que gerem o instrumento convocatório, estando ela, a merecer reparos, senão vejamos:

1. DA TEMPESTIVIDADE
O presente recurso é tempestivo na medida em que a intenção de sua interposição foi manifestada e recebida pelo pregoeiro, no dia 10/03/2022, dentro do prazo mínimo concedido de 30 minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.
Esta Recorrente se manifestou dentro do lapso temporal, consignando, registrando da seguinte forma "Manifestamos intenção de recorrer contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., devido ao não atendimento de requisitos claramente obrigatórios, bem como outros itens que serão devidamente apresentados tempestivamente junto a peça recursal."
Entretanto, a despeito da reclamada decisão, vale constar sobre o direito a recurso e seu respectivo prazo, vale aludir que diante de tal decisão é cabível o presente recurso, em garantia aos princípios do devido processo legal, contraditório e ampla defesa, de aplicação indiscutível no feito administrativo.
O instrumento convocatório, inclusive, prevê que, uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias corridos para apresentar as razões. Desta feita, estando registrado junto à Ata a data limite para registro de recurso: 14/03/2022, resta assim, comprovada a sua tempestividade.
2. REQUISITOS RECURSAIS
A legislação, em especial a Lei n. 8.666/1993, Lei n. 10.520/2002 e o Decreto n. 10.024/2019, exigem que o registro da intenção de recurso deve atender aos requisitos de sucumbência, tempestividade, legitimidade, interesse e motivação, não podendo ter seu mérito julgado de antemão. O Tribunal de Contas da União – TCU, já firmou entendimentos de que não cabe ao Pregoeiro rejeitar sumariamente a intenção de recurso apresentada pelos licitantes no decorrer de um pregão eletrônico, cabendo ao agente condutor do certame, tão somente avaliar se os requisitos de admissibilidade recursal estão ou não presentes.
Assim, analisando as premissas, temos:
a) Sucumbência, que é implicou na nossa derrota perante o certame;
b) Tempestividade, ante a intenção de recursos e protocolo desta peça recursal dentro do prazo estabelecido;
c) Legitimidade, verificada por meio da manifestação desta parte interessada na condição de sucumbente;
d) Interesse, baseado na concessão, segundo o qual não é permitido o prosseguimento de processos nos casos que, mesmo acolhendo o pleito de terminada licitante, a decisão administrativa seja inútil ou que não possa ser aproveitada; e
e) Motivação, apurável ante a exposição objetiva do conteúdo da irresignação em relação à decisão proferida.
Assim, de forma clara e suscinta, mas suficiente para o atendimento do exercício do direito de se manifestar em relação à decisão proferida, esse MD Pregoeiro se manifestou no sentido de realizar a "devida aceitação e concessão dos prazos de 3 dias corridos para envio das razões, mais 3 dias para contrarrazões e 5 dias úteis para decisão deste Pregoeiro", solicitando ainda, a título de alerta, "Outrossim, solicito prudência e bom senso nos Senhores, caso

queiram fazer uso desta prerrogativa dos recursos, a fim de evitarmos recursos meramente protelatórios".
Tal admissibilidade ante ao preenchimento dos requisitos e premissas, nos garantiu o direito de manifestar nosso inconformismo por intermédio desta peça recursal.

3. SÍNTESE DOS FATOS
3.1. Dos elementos ensejadores da pretensão de recorrer contra a decisão
O MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, pelo presente edital e por intermédio da PROCURADORIA GERAL DE JUSTIÇA, tornou pública a realização de licitação, na modalidade PREGÃO, na forma ELETRÔNICA, do tipo menor preço por lote, objetivando a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos.
O objeto inclui todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão funcionar perfeitamente, sem vícios, não constar em listas de end-of sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato. Destaca-se, todas as funcionalidades exigidas.
A abertura da Sessão do Pregão foi designada para ser realizada no dia 21 de fevereiro de 2022, às 10:00 horas, no Portal de Compras do Governo Federal – Comprasnet.
A empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA foi vencedora do certame, arrematando lote único pelo preço final de R$ 2.478.052,85, após negociação onde o MD Pregoeiro deixou clara a relação com a vencedora, manifestando claramente, conforme se verifica junto à ata, da seguinte forma: "Pregoeiro 21/02/2022 11:12:15 - Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Ademais, sua empresa participou da fase interna de cotação e ofertou preço bem menor ao apresentado no certame...".
Tal registro se deu na fase de negociação, que pode ser verificada, como dito, junto à ata de realização do pregão eletrônico.
Em seguida, convocou a licitante para envio da proposta e demais documentos no prazo de 02 horas, sempre orientando detalhadamente a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, quanto a correta forma de proceder.
Em seguida, em 07/03/2022, às 11:35:06, o MD Pregoeiro registrou no sistema: "A proposta de preço, documento 0772069, informa equipamentos e serviços condizentes com as quantidades e exigências do Termo de Referência", baseado no PARECER Nº 4.2022.SIET.0775110.2021.015252, que consigna uma conclusão final. Entretanto, um registro chamou a atenção, na sequência do trecho acima: "Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo". SMJ, MD Pregoeiro, a análise minuciosa e qualitativa deve ser realizada primeiramente na fase de análise da proposta e após contratada, na fase de recebimento, ocorre que não estamos na fase de recebimento. Vejamos o que diz o edital quanto ao indispensável atendimento aos requisitos:
"5.7. Como condição para participação no Pregão, a licitante assinalará "sim" ou "não" em campo próprio do Sistema eletrônico Comprasnet, relativo às seguintes declarações:
(...)
c) que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias"
"9.2. Na proposta vencedora a ser enviada posteriormente deverá constar, conforme modelo do Anexo IV:
(...)
c) Especificações claras, completas e minuciosas, com detalhes do objeto ofertado, inclusive marca, modelo, tipo e referência, no que couber, observadas as especificações mínimas e quantitativos contidos neste Edital e anexos"
"9.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante."
Já o Termo de Referência, exige:
"5.1.11 A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente."
Junto a proposta, temos:
"DECLARAÇÕES:
1. Cumpro plenamente os requisitos de credenciamento e habilitação, inclusive o estabelecido no subitem 5.6 (...)"
Pelos trechos acima, resta claro e evidente que o edital exige atendimento à todos os requisitos especificados. Caso este RECORRENTE esteja com entendimento equivocado quanto a isso, esse MPAM pode estar diante de um vício insanável, pois a legislação e a jurisprudência são claras ao permitir somente a exigência dos requisitos mínimos indispensáveis e se, diante de tantos requisitos, a solução a ser aceita não atender a sua totalidade, não faz o menor sentido registrar além do necessário.
Assim, proceder o aceite de uma proposta em condição diferente do estipulado em edital, afronta mortalmente o princípio da vinculação ao instrumento convocatório. O princípio da vinculação ao instrumento convocatório tem como finalidade principal evitar que administradores realizem análise de documentos de habilitação de forma arbitrariamente subjetiva, o que pode viabilizar o direcionamento do contrato em defesa de interesses pessoais ou de terceiros, em total contrariedade com o princípio da isonomia entre os licitantes e demais princípios da administração pública como moralidade, impessoalidade, legalidade e afronta ao interesse público.
O princípio da vinculação ao instrumento convocatório é corolário do princípio da legalidade e da objetividade das determinações habilitatórias. Impõe à Administração e ao licitante a observância das normas estabelecidas no Edital de forma objetiva, mas sempre velando pelo princípio da competitividade.
Assim, não se pode aceitar qualquer oferta que não atenda a plenitude do que está sendo exigido, considerando que, de fato, esse MPAM realmente especificou os requisitos como exigências mínimas a serem atendidas.
Em situação verificada que a proposta ofertada não atende plenamente os requisitos, deveria o MD pregoeiro, assim proceder: "10.6.2. Nas situações da compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos nos subitens acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de 05 (cinco) dias úteis contados da solicitação."
A diligência era o meio de verificar a compatibilidade absoluta e não registrar que "Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo."
Outro ponto chamou a atenção: a dissintonia e contradição consignadas em ata. Em 07/03/2022 às 11:38:27, há o seguinte registro: "Conforme exigência, foram apresentados atestados de capacidade técnica que comprovam,

conjuntamente, a prestação anterior de serviços de firewall de próxima geração, NGFW, com troughput de 10Gbps, no mínimo. Foram apresentados 03 (três)atestados, disponíveis nas páginas 42, 43, 44 e 45 do documento 0772080" e complementando, "... , incluindo equipamentos similares e superiores ao objeto deste processo."

Data vênia, entendemos que a empresa logrou êxito em comprovar sua aptidão técnica. Entretanto, em 07/03/2022 às 11:41:00, consta registro no sentido de que "Senhor Fornecedor, ao realizar as convalidações dos documentos anexados no sistema (...) Todavia, os atestados da Hapvida e Pague menos inexiste essa possibilidade"

Ora, MD Pregoeiro, como primeiro aceita o documento para depois verificar sua validade? Seria esta a sequência correta? Segundo o Decreto n. 10.024/2019, a comprovação de habilitação é prévia, ou seja, antecede a sua aceitação. Ocorre que o que se observa é uma intenção clara de declarar primeiro o aceite da proposta, para em seguida, verificar a sua validade.

Analisando a solução ofertada, é possível verificar que o equipamento apresentado pela empresa Network Secure não atende ao item 5.2.15.10.15 do Termo de Referência. O item menciona as funcionalidades de Firewall, IPS, App Control, Sandbox e Anti-Malware, logo a funcionalidade que tem que ser considerada é a de Threat Prevention e não a de NGFW, e de acordo com a documentação do fabricante CheckPoint este modelo de equipamento tem capacidade de throughput de apenas 3.7 Gbps e não o mínimo solicitado de 5 Gbps. Assim sendo, o valor de NGFW não pode ser considerado para este item pois o próprio fabricante informa que somente compreende as 3 funcionalidades, no caso FW, IPS e App Control, sem considerar as de SandBox e Anti-Malware. Para estas, o valor válido é da funcionalidade de Threat Prevention como já mencionado.

Segundo o que se pode verificar junto ao edital publicado é que para o alcance dos resultados pretendidos esse item é indispensável. Vejamos.

O não atendimento deste item prejudica a proteção avançada demandada pelo órgão conforme solicitado nos itens 5.1.15.6.4, 5.2.15.6.18, 5.2.15.6.22, 5.2.15.6.26, 5.2.15.6.31, 5.2.15.6.32 e, especialmente, os itens 5.2.15.6.34 e 5.2.15.7. Este desacordo com o exigido põe o órgão em uma posição de insegurança e prejuízo sobre o propósito do investimento haja vista que este modelo de equipamento não terá performance e tampouco capacidade de realizar a proteção efetiva que o MPAM demanda.

Ademais, a empresa tinha a possibilidade de ofertar um modelo com capacidade maior para atendimento do item, porém não o fez. Entende-se, então, que esta atitude prejudica a concorrência pois todas as licitantes precisam apresentar proposta que atenda por completo ao edital a fim de elaborar a sua estratégia de produtos, serviços e preços e quando isso não ocorre permite que aquela que não atendeu tenha uma vantagem na proposta de valor para vencer o certame.

3.2. Do propósito do Recurso Administrativo com Pedido de Reconsideração

Todo processo licitatório é revestido do interesse público, que é supremo. A Administração Pública não licita por licitar. Todo procedimento licitatório possui uma justificativa detalhando a sua necessidade, a qual é obtida após estudo interno que identificou tecnicamente as opções existentes e alternativas viáveis, o que permite concluir pelo cenário que melhor atende a sua demanda.

Este é o objetivo principal do certame.

Assim, esta empresa não está somente defendendo seus interesses mas resguardando essa Administração frente à necessidade levantada por esse MPAM.

Diante de tal premissa, caracterizada por interesse mútuo entre esta empresa e os objetivos desse MPAM, nasceu nosso interesse em apresentar elementos suficientes para provocar uma revisão dos atos praticados e garantir que a solução ofertada comprovadamente atende à todos os requisitos mínimos exigidos.

3.3. Da possibilidade de revisão dos atos

O princípio da autotutela estabelece que a Administração Pública possui o poder de controlar os próprios atos, anulando-os quando ilegais ou revogando-os quando inconvenientes ou inoportunos. Assim, a Administração não precisa recorrer ao Poder Judiciário para corrigir os seus atos, podendo fazê-lo diretamente.

Esse princípio possui previsão em súmula do STF "Súmula nº 473: A Administração pode anular seus próprios atos, quando eivados de vícios que os tornam ilegais, porque deles não se originam direitos; ou revoga-los, por motivo de conveniência ou oportunidade, respeitados os direitos adquiridos, e ressalvada, em todos os casos, a apreciação judicial."

Esse princípio possui previsão junto ao art. 53 da Lei 9.784/99: "A Administração deve anular seus próprios atos, quando eivados de vício de legalidade, e pode revogá-los por motivo de conveniência ou oportunidade, respeitados os direitos adquiridos."

3.4. Da preservação do interesse público

Os interesses representados pela Administração Pública, estão previstos no Art. 37 da Constituição Federal Brasileira, e se aplica na atuação do princípio da supremacia do interesse público.

Essa é uma das prerrogativas conferidas a administração pública, porque a mesma atua por conta de tal interesse, ou seja, o legislador na edição de leis ou normas deve orientar-se por esse princípio, levando em conta que a coletividade está em um nível superior ao do particular.

Se na condição de apresentada, esse MPAM representa a coletividade, deve preservar o interesse público. Desta forma, a necessidade que justificou e embasou o processo licitatório deve ser atendido em sua plenitude, sob o risco de afrontar à Constituição Federal.

A única forma de preservar o interesse público é garantir que a necessidade seja atendida. Pela manifestação exarada de que no recebimento será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, entendemos, SMJ, que o procedimento está eivado de vícios e descumprindo os ditames legais e editalícios, não garantindo a preservação do interesse público e colocando em risco os recursos públicos, uma vez que não se sabe se a solução, de fato, atende à totalidade dos requisitos.

Esta questão, inclusive, exige exercício de consciência e risco quanto a continuidade do processo nos termos atuais, uma vez que tal ato certamente será auditado e questionado por órgãos de controle.

3.5. Risco à quebra da isonomia

De acordo com o art. 3º da Lei nº 8666/93, são princípios expressos da licitação: legalidade, impessoalidade, moralidade, publicidade, igualdade, probidade administrativa, vinculação ao instrumento convocatório e julgamento objetivo.

Dentre eles, destaca-se o princípio da igualdade entre os licitantes, onde a Administração Pública deve conduzir a licitação de maneira impessoal, sem prejudicar nenhum licitante. Desde que preencham os requisitos exigidos, todos os que tiverem interesse em participar da disputa devem ser tratados com isonomia.

Celso Antônio Bandeira de Mello conceitua licitação como um certame que as entidades governamentais devem promover e no qual abrem disputa entre os interessados em com elas travar determinadas relações de conteúdo patrimonial, para escolher a proposta mais vantajosa às conveniências públicas. Estriba-se na ideia de competição, a ser travada economicamente entre os que preencham os atributos e aptidões necessários ao bom cumprimento das obrigações que se propõem assumir.

Todos os dispositivos da lei de licitações ou regulamentação de um específico processo licitatório, devem ser interpretados à luz do princípio da isonomia.
Se o edital é supremo e vincula as partes – MPAM e Licitantes – as suas regras devem ser fielmente obedecidas.
Como visto nesta peça recursal, o instrumento convocatório e seus anexos consignaram os requisitos mínimos de admissibilidade técnica de uma proposta e, o ato de aceitar parcialmente, afronta o edital e desrespeita os demais licitantes, uma vez que, se todos soubessem que haveria aceite parcial de requisitos, teriam ofertado equipamento condizente com as exigências e não tão robusto quanto ao que, por exemplo, ofertamos.
A definição do objeto deve ser clara e precisa e decorrendo análise dos edital, resta claro e evidente o que se pretende contratar: uma solução robusta, completa e que atenda a todos os requisitos e nesta diapasão, quanto mais requisitos, mais elevado é o custo dessa solução. Reiteramos: se o edital deixasse claro a possibilidade de ofertar solução que atendesse apenas parte dos requisitos, as soluções ofertadas representariam custos menores para esse MPAM.
3.6. Do risco de desperdício de recursos públicos
Importa registrar a presunção ope legis prevista no parágrafo único do art. 70 da Constituição Federal, que imputa ao gestor público a obrigação de comprovar a boa e regular aplicação dos recursos postos sob sua administração, mediante a apresentação de prestação de contas.
A fixação dos critérios de aceitabilidade da proposta é requisito obrigatório nos editais de licitação. A fixação de requisitos mínimos de habilitação para fins de qualificação técnica, independentemente de técnico-profissional ou técnico-operacional, deve ser estabelecida de maneira razoável, pertinente e compatível com o objeto licitado, sendo definida como resultado de um processo lógico, fundado em razões técnico-científicas, de forma que não restrinja indevidamente a competitividade da licitação.
Acerca desse tema, Marçal Justen Filho leciona o seguinte:
"Vale insistir acerca da inconstitucionalidade de exigências excessivas, no tocante à qualificação técnica. Observe-se que a natureza do requisito é incompatível com a disciplina precisa, minuciosa e exaustiva por parte da Lei. É impossível deixar de remeter à avaliação da Administração a fixação dos requisitos de habilitação técnica. Essa competência discricionária não pode ser utilizada para frustrar a vontade constitucional de garantir o mais amplo acesso de licitantes, tal como já exposto acima. A Administração apenas está autorizada a estabelecer exigências aptas a evidenciar a execução anterior de objeto similar. (...)
(...)
No entanto, o ônus da prova recai sobre a Administração. Ou seja, diante da dúvida, cabe à Administração demonstrar a necessidade da exigência formulada. Não é encargo do particular evidenciar a desnecessidade do requisito imposto pela Administração. Afinal, quem elaborou o ato convocatório foi a Administração. Não seria possível invocar a mera presunção de legitimidade dos atos administrativos para afastar o dever de a Administração explicar o motivo e o conteúdo das escolhas realizadas."
Assim, presume-se que as exigências expostas no edital sejam as mínimas. Logo, se uma proposta é aceita atendendo parte dos requisitos estipulados, entende-se que tais requisitos não eram essenciais, podendo ser entendidos como excessivos, o que pode ter restringido uma ampla participação, competitividade, busca pela proposta mais vantajosa e ainda, desperdício de recursos públicos.
É de indispensável importância que se avalie o risco de admissibilidade nos termos aqui expostos, sob risco de responsabilização dos agentes que deram causa.
4. DO CABIMENTO E DA LEGITIMIDADE
4.1. Da Legitimidade para Recorrer
Preliminarmente, registra-se que a ora Recorrente, como empresa especializada no ramo pertinente ao objeto licitado, detém total e irrestrita capacidade estrutural e tecnológica de oferecer objeto conforme exigido no edital. E, em razão de sua solidificação no mercado público, possui plena capacidade técnica e financeira para oferecer proposta aderente à exigida por esse MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.
4.2. Do Cabimento do Presente Pedido
O Direito de Peticionar no procedimento licitatório tem como fundamento legal na CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988, que dispõe: "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXXIV - são a todos assegurados, independentemente do pagamento de taxas: a) O direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder; (...)."
É dessa garantia constitucional que decorrem as diversas formas de provocação da Administração Pública para o exercício do direito de petição, nesse sentido vejamos as palavras de Di Pietro: "Dentro do direito de petição estão agasalhados inúmeras modalidades de recursos administrativos... É o caso da representação, da reclamação administrativa, do pedido de reconsideração, dos recursos hierárquicos próprios e impróprios da revisão."
Seguindo esse entendimento, Carvalho Filho afirma que: "O direito de petição é um meio de controle administrativo e dá fundamento aos recursos administrativos por que tais recursos nada mais são do que meios de postulação a um órgão administrativo. O instrumento que propicia o exercício desse direito consagrado na CF é o recurso administrativo."
Desta feita, temos que o presente recurso administrativo instrumentaliza o exercício do direito de petição junto ao poder público.
5. DAS RAZÕES PARA REFORMAR A R. DECISÃO
Ilustre Senhor Julgador, data máxima vênia, a Recorrente logrou êxito em demonstrar que a r. decisão ocorreu em um grande equívoco em admitir proposta que não atende a totalidade dos requisitos mínimos exigidos no edital.
Deve-se chamar a atenção dos julgadores ao fato de que a decisão mais acertada é justamente preservar o interesse público, cancelar o aceite, recusar a proposta e convocar as demais licitantes, na ordem de classificação.
Portanto, baseiam-se às razões da Recorrida, nos prejuízos que o MD Pregoeiro poderá proporcionar, face nítida a falta de vinculação ao edital ou respaldo legal, causando assim o afastamento do maior objetivo do edital que é assegurar o atendimento do interesse desse comprador.
Desta forma, a r. decisão não foi nada razoável e nem proporcional ao declarar a licitante NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, como vencedora da disputa, mas condições trazidas nesta peça recursal.
Assim, se faz necessário que essa Administração julgue provido o presente recurso, com observância ao princípio da eficiência, segurança jurídica e do devido processo legal.
6. DOS PEDIDOS
DIANTE DO EXPOSTO, requer-se que seja conhecido o presente recurso e, ao final, julgando provido, com fundamento nas razões precedentemente aduzidas, com efeito SUSPENSIVO para que seja revisto o equívoco e risco de desperdício de recursos públicos e afastamento do interesse público, anulando a decisão em apreço, na parte atacada neste, promovendo a recusa da proposta da licitante NETWORK SECURE SEGURANCA DA INFORMACAO

LTDA e a convocação das demais licitantes, na ordem de classificação.
Outrossim, lastreada nas razões recursais, requer-se que esse MD Pregoeiro reconsidere sua decisão e, na hipótese não esperada de isso não ocorrer, faça este subir, devidamente informado à autoridade superior, em conformidade com o § 4°, do art. 109, da Lei n. º 8.666/93, observando-se ainda o disposto no § 3° do mesmo artigo.
Termo em que,
Pede e espera deferimento.

Fortaleza - CE, 14/03/2022.

Théo Augusto Ramalho Costa
CEO da It Protect

Voltar

Pregão Eletrônico

- **Visualização de Recursos, Contrarrazões e Decisões**

CONTRARRAZÃO :

EXCELENTÍSSIMO SENHOR PREGOEIRO DA COMISSÃO PERMANENTE DE LICITAÇÃO (CPL), DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.

REF.: EDITAL DO PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ.
Processo SEI nº 2021.015252.

Ref.: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, incluindo treinamento e serviço de migração da plataforma atual.

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA. (VENCEDORA), inscrita sob o CNPJ nº 05.250.796/0001-54, já qualificada nos autos do processo licitatório em epígrafe, neste ato conduzida por seu legal representante infra-assinado, vem, respeitosamente, perante a ilustre presença de Vossa Senhoria, dentro do prazo legal, apresentar as presentes

C O N T R A – R A Z Õ E S

ao RECURSO ADMINISTRATIVO interposto pela Empresa, IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, pelos fatos e fundamentos a seguir:

I.- DOS FATOS.

A empresa NETWORK, credenciou-se no procedimento licitatório nº 4.005/2022-CPL/MP/PGJ, o qual objetiva a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme demais especificações contidas no Edital.

Tal certame atendeu às Condições Gerais constantes naquele Edital, pelo critério de julgamento de menor preço, sob regime de empreitada por preço global, ou seja, a obtenção do somatório dos preços unitários que venha a ser mais vantajoso para esse Órgão.

Destarte, após realizados os trâmites regulares e intrínsecos, previstos no Edital, essa Comissão consagrou vencedora a presente Empresa por ordem de menor preço ofertado e por ter cumprido com as disposições do edital PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ.

Nesse contexto, frise-se, a empresa NETWORK foi declarada vencedora com o valor global de R$ 2.478.052,85 (dois milhões, quatrocentos e setenta e oito mil, cinquenta e dois reais e oitenta e cinco centavos).

Todavia, a Empresa IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, inconformada com a legítima vitória da NETWORK, interpôs Recurso Administrativo, ora contrarrazoado, alegando que essa Comissão supostamente a favoreceu por oportunidade da realização de diligência, assim como por a mesma não apresentar uma solução que supostamente não atende aos requisitos técnicos contidos no Edital.

II.- DAS RAZÕES DA MANUTENÇÃO DA DECISÃO DO SR. PREGOEIRO.
II.1 DOS QUESTIONAMENTOS E ATESTADOS:

Data vênia, o Sr. Pregoeiro não feriu o princípio do julgamento objetivo nem sequer os critérios previstos no Edital do PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ, pois o mesmo baseou-se, correta e legalmente, naquilo que foi exigido pelo Edital, não há o que se falar em suposto favorecimento durante a realização do Pregão.

Nesse sentido, esclarece-se que é legal, e com previsão contida em Edital, a possibilidade de o pregoeiro realizar questionamentos/ações que visem a obtenção de informações complementares necessárias a elucidação daquilo que está sendo apresentado.

Senão, veja-se:

4. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO

4.1 omissis

4.2 Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.
(Grifos nossos)

Não deve prosperar, portanto, qualquer falsa afirmação que a empresa NETWORK deixou de apresentar subsídios indispensáveis para a comprovação da sua capacidade na consecução do objeto contratual.

Trata-se de norma geral, aplicável a todas as modalidades licitatórias e a todas as esferas da federação. Há, inclusive, acórdão do E. Superior Tribunal de Justiça que defende que "A promoção de diligência é uma faculdade da Comissão de licitação, constituindo, portanto, medida discricionária do administrador" (REsp. 102.224/SP, 2ª T., rel. Min. CASTRO MEIRA, j. 5.4.2005, DJU 23.5.2005).

Portanto, tanto a habilitação técnica da Empresa NETWORK, com a correta apresentação da documentação, com a realização de diligência, além de possuir a proposta mais vantajosa são chancelas que lhe permitem figurar como vencedora do certame em tela, visto que detém capacidade técnica e preço melhor que todos os demais participantes.

II.1 DA REGULARIDADE TÉCNICA:

Basicamente, o recorrente buscou questionar a decisão exarada pelo nobre Pregoeiro que concedeu vitória à NETWORK, dentre as alegações, há uma série de questionamentos técnicos, motivo pelo qual, por questões de praticidade e de busca de melhor explicação, opta-se por rebater os pontos de acordo com os itens elencados pelo recorrente, algo que se passamos a fazer desde já.

Cada fabricante possui uma elaboração de documentação técnica/datasheets em formato único, levando em consideração fatores pertinentes para seus processos internos de fabricação e desenvolvimento, e até mesmo de nomenclatura.

Na Tabela de Capacidades - ANEXO I TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252 Item 5.2.15.10.15 lemos: "Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps) entre 5 Gbps e 10 Gbps."
No mesmo anexo, Item 5.2.15.10.17 lemos: Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps) que: "Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps) entre 2,5 Gbps e 5 Gbps."
O edital possui itens duplicados, sendo assim pode ser considerado números distintos de throughput, inclusive no item 5.2.15.10.15 fica mais caracterizado uma capacidade de throughput de NGFW, onde apresenta um maior número, além de não detalhar todas as funcionalidades como no item 5.2.15.10.17.
Já no item 5.2.15.10.17 se faz muito mais característico de um throughput de Threat Prevention pela descrição de todas as funcionalidades exigidas, e consequentemente um número menor para todas as funcionalidades habilitadas, onde todos os fabricantes possuem dois números, sendo um maior para capacidade de NGFW, e um menor para capacidade de Threat Prevention, conforme solicitado no certame.
Em relação ao item 5.2.15.10.15, pode-se observar o valor identificado abaixo via datasheet (6600-security-gateway-datasheet), na página 3. Tal documento técnico também pode ser acessado via link: https://www.checkpoint.com/downloads/products/6600-security-gateway-datasheet.pdf

Onde a legenda do índice 2, "2: Includes Firewall, Application Control and IPS with logging enabled."
Foi apontado que o equipamento que ofertamos em nossa proposta, para o parâmetro em questão (Throughput de Firewall), não apresenta esse valor com as funcionalidades de SandBox e Anti-malware ativadas. Então, visando explanar e esclarecer todas as dúvidas acerca da nossa solução ofertada, vamos demonstrar os seguintes pontos:
1. O appliance ofertado que consta em nossa proposta é o 6600 Plus appliance with SandBlast (SG6600-PLUS-SNBT), o que nos leva ao próximo ponto;
2. O SandBlast é um serviço dentro do portfólio do fabricante, que neste caso já está inclusa na solução, fornecendo a funcionalidade de SandBox com proteção de dia zero contra ameaças avançadas e desconhecidas, malwares desconhecidos e ataques direcionados, prevenindo infecções por explorações não descobertas. Logo, tais funcionalidades de anti-malware e SandBox já acompanham e são habilitadas de forma nativa ao nosso item ofertado, e, são levadas em consideração no parâmetro de NGFW de 6,2 Gbps ficando entre a faixa exigida no edital: 5.2.15.10.15 Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps).

Esta informação encontra-se de forma mais detalhada na página 2 do documento técnico, no link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf
3. Logo é possível ver que nosso appliance ofertado obedece e atende aos valores estabelecidos no edital.

Em relação ao item 5.2.15.10.17, pode-se observar o valor identificado abaixo via datasheet (6600-security-gateway-datasheet), na página 3. Tal documento técnico também pode ser acessado via link: https://www.checkpoint.com/downloads/products/6600-security-gateway-datasheet.pdf

Onde a legenda do índice 1, "1: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled."
O nosso valor de 3,7 Gbps fica entre o intervalo de 2,5 e 5,0 Gbps exigido no edital, conforme imagem abaixo.

Logo é possível ver que nosso appliance ofertado obedece e atende aos valores estabelecidos no edital.

Com as demonstrações e esclarecimentos dos itens 5.2.15.10.15 e 5.2.15.10.17, fica comprovado que efetivamente atendemos aos requisitos mínimos de especificação técnica exigidos no edital, incluindo para os subitens a seguir:
• 5.1.15.6.4 (esse item não existe no edital);
• 5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos.
o A comprovação e atendimento deste item pode ser observado na página 176 do arquivo CP_R81_Quantum_SecurityManagement_AdminGuide, da documentação técnica enviada. Ver imagem abaixo.

• 5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.
o Sabe-se que o Theath Prevention é uma blade do Security Management, ver página 176 do arquivo CP_R81_Quantum_SecurityManagement_AdminGuide, da documentação técnica enviada. Conforme imagem abaixo.

o Partindo da definição de spyware que é um tipo de malware, designado para coletar informações dos usuários em computadores infectados. O Threat Prevention é responsável por determinar as políticas de inspeção das conexões em busca de bots e vírus, onde seu componente principal é "The Rule Base", as regras usam o banco de dados de malware e objetos de rede. Dentro do Threat Prevention é possível observar as configurações existentes para antivírus e spyware, e os respectivos protocolos atendidos. Ver imagens abaixo.

o Todas as informações que constam nas imagens acima, podem ser acessadas em documentação oficial do fabricante via link: https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?

topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/138634 . E no link, https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/101653

• 5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.
o A comprovação deste item, encontra-se em documento oficial do fabricante que pode ser acessado via link: https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0723.html/

• 5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
o Para comprovação desse item, ver página 293 e 294 do arquivo CP_R81_Quantum_SecurityManagement_AdminGuide enviado na documentação técnica. Conforme imagem abaixo.

o Tal comprovação pode ser observada via documento oficial do fabricante no link: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101553. Conforme imagem abaixo:

o Ver também página 5 do documento oficial do fabricante, via link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf . Conforme imagem abaixo:

o E, por último, ver também página 30 do documento oficial do fabricante, via link:https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/105675/FILE/CP_R81.10_ThreatPrevention_AdminGuide.pdf. Conforme imagem abaixo:

• 5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos
o A comprovação deste item pode ser observada na imagem abaixo, podendo ser acessada na documentação oficial do fabricante via link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

• 5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt,.pptx), arquivos java (.jar e class), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox.
o A comprovação e atendimento deste item segue na imagem abaixo, tal informação pode ser acessada via documentação oficial do fabricante no link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

• 5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY
o A comprovação deste item, pode ser observada nos documentos oficiais do fabricante nos links abaixo:
https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf;
https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/108955/FILE/CP_SandBlast_Agent_AdminGuide.pdf.

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/101653

III.- DOS PRINCÍPIOS DO MENOR PREÇO, DA RAZOABILIDADE E DA MELHOR VANTAGEM.

A licitação pública tem como finalidade atender um INTERESSE PÚBLICO, de forma que seus critérios devem ser observados por todos os participantes em estado de IGUALDADE, para que seja possível a obtenção da PROPOSTA MAIS VANTAJOSA.

A licitação é um procedimento administrativo disciplinado por lei e por um ato administrativo prévio, que determina critérios objetivos de seleção de uma proposta de contratação economicamente mais atrativa, com observância ao princípio da isonomia, conduzido por um órgão dotado de competência específica.

Ademais, a observância à necessidade basilar de obter a proposta mais vantajosa é expressamente regulado pelo Art. 3º, da Lei nº 8.666/93, haja vista que acaba por conceder tratamento isonômico e, consequentemente, competitividade ao certame, senão veja-se:

Art. 3o A licitação destina-se a garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.
(Grifos nossos)

Portanto, é correto reconhecer que a Empresa NETWORK atende as exigências técnicas constantes do Edital e escolhê-la como a proposta mais vantajosa para esse Órgão evidenciando-se alinhamento com os princípios elencados no artigo acima.

A proposta da NETWORK, que é R$ 718.000,00 (setecentos e dezoito mil reais) mais econômica que a ofertada pela Empresa Recorrente, cuja aceitação daquele Recurso afrontaria o acima transcrito Art. 3º, da Lei nº 8.666/93, onerando injustificadamente esse Órgão.

Afinal, trata-se de ato com fulcro no próprio princípio da finalidade, da eficiência e da razoabilidade, pois acaba por despender menos recursos financeiros pela mesma solução.

A esse propósito, insta trazer à baila a lição do saudoso professor e magistrado Hely Lopes Meirelles, que assim assevera:

(...) todo ato administrativo, de qualquer autoridade ou Poder, para ser legítimo e operante, há que ser praticado em conformidade com a norma legal pertinente (princípio da legalidade), com a moral da instituição (princípio da moralidade), com a destinação pública própria (princípio da finalidade), com a divulgação oficial necessária (princípio da publicidade) e com presteza e rendimento

funcional (princípio da eficiência). Faltando, contrariando ou desviando-se desses princípios básicos, a Administração Pública vicia o ato, expondo-o a anulação por ela mesma ou pelo Poder Judiciário, se requerida pelo interessado. (in Direito Administrativo Brasileiro, 34ª Edição, 2008, Editora Malheiros, São Paulo, pg. 716).
(Grifos nossos)

A conduta do agente responsável pela Licitação mostrou-se absolutamente regular, atendendo aos princípios previstos na lei das licitações, assim como do Edital, ou seja, princípio do menor preço, da razoabilidade e da melhor vantagem.

Tem-se que a Empresa ora recorrente, de maneira temerária e sem fundamentação legal ou doutrinária, paralisa e inviabiliza o regular desenvolvimento do procedimento licitatório em destaque, em total afronta aos bons costumes a celeridade dos atos administrativos a serem praticados por esse Órgão.

Com sabedoria, o ilustre doutrinário Celso A. Bandeira de Mello afirma que "A licitação é o procedimento destinado à seleção da melhor proposta dentre as apresentadas por aqueles que desejam contratar com administração pública".

Como dito anteriormente, o Sr. Pregoeiro atentou aos princípios do instrumento convocatório e do julgamento objetivo, o que significa procurar razões de fato para sustentar sua escolha ou decisão, ou seja, julgamento sustentado no que está previsto em Edital.

IV.- DOS PEDIDOS.

Em face das razões expostas, a presente Empresa, NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA., requer deste Sr. Pregoeiro:

a) NEGUE provimento ao Recurso Administrativo interposto pela Empresa, IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, para manter na íntegra a r. decisão que consagrou vencedora a Empresa, NETWORK, que faz com base nas contrarrazões acima, nos princípios do menor preço, da razoabilidade e da melhor vantagem;

b) Julgar fundamentadas as contrarrazões ora apresentadas, mantendo a declaração de habilitação da Empresa NETWORK no PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ, por satisfazer todos os requisitos previstos no respectivo Edital e nas demais normas atinentes a administração pública.

Termos em que,
Pede e espera Natural Deferimento.

Fortaleza, 17 de março de 2022.

_____
JOSE MURILO CIRINO NOGUEIRA JUNIOR
NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

Fechar

CONTRARAZÕES NETWORK SECURE - PREGÃO ELETRÔNICO Nº 4.005/2022 - MPAM

Izabel Santos <izabel.santos@networksecure.com.br>

Qui, 17/03/2022 22:30

Para: Comissao Permanente de Licitacao <licitacao@mpam.mp.br>

Cc: Murilo Cirino <murilo@networksecure.com.br>; NTS - EMAIL - LICITACOES <licitacoes@networksecure.com.br>; Gledson Constantino <gledson.constantino@networksecure.com.br>; Jessyca Santana <jessyca.santana@networksecure.com.br>

1 anexos (717 KB)

CONTRA-RAZÕES NETWORK PREGÃO ELETRÔNICO Nº 4.005_2022 MPAM.pdf;

AO
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
PROCURADORIA GERAL DE JUSTIÇA

REF.: EDITAL DO PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ.
Processo SEI nº 2021.015252.

A/C SR. PREGOEIRO DA COMISSÃO PERMANENTE DE LICITAÇÃO (CPL)

Prezado Sr,

Somos a NETWORK SECURE SEGURANÇA DA INFORMACAO LTDA, CNPJ 05250796/0001-54 , vimos por meio deste enviar as CONTRARAZÕES ao recurso apresentado pela empresa IT PROTECT. As mesmas foram anexadas ao portal Comprasnet conforme edital, tempestivamente.

Encaminhamos em anexo o documento contendo imagens ilustrativas.

Desde já nos colocamos a disposição.

Contem conosco,

NTÍSSIMO SENHOR PREGOEIRO DA COMISSÃO PERMANENTE DE LICITAÇÃO (CPL), DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.

REF.: EDITAL DO PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ.
Processo SEI nº 2021.015252.

Ref.: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, incluindo treinamento e serviço de migração da plataforma atual.

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA. (VENCEDORA), inscrita sob o CNPJ nº 05.250.796/0001-54, já qualificada nos autos do processo licitatório em epígrafe, neste ato conduzida por seu legal representante infra-assinado, vem, respeitosamente, perante a ilustre presença de Vossa Senhoria, dentro do prazo legal, apresentar as presentes

C O N T R A – R A Z Õ E S

ao RECURSO ADMINISTRATIVO interposto pela Empresa, IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, pelos fatos e fundamentos a seguir:

I.- DOS FATOS.

A empresa NETWORK, credenciou-se no procedimento licitatório nº 4.005/2022-CPL/MP/PGJ, o qual objetiva a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme demais especificações contidas no Edital.

Tal certame atendeu às Condições Gerais constantes naquele Edital, pelo critério de julgamento de menor preço, sob regime de empreitada por preço global, ou seja, a obtenção do somatório dos preços unitários que venha a ser mais vantajoso para esse Órgão.

Destarte, após realizados os trâmites regulares e intrínsecos, previstos no Edital, essa Comissão **consagrou vencedora a presente Empresa por ordem de menor preço ofertado** e por ter cumprido com as disposições do edital PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ.

Nesse contexto, frise-se, a empresa NETWORK foi declarada vencedora com o valor global de R$ 2.478.052,85 (dois milhões, quatrocentos e setenta e oito mil, cinquenta e dois reais e oitenta e cinco centavos).

Todavia, a Empresa IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, inconformada com a legítima vitória da NETWORK, interpôs Recurso Administrativo,

ora contrarrazoado, alegando que essa Comissão supostamente a favoreceu por oportunidade da realização de diligência, assim como por a mesma não apresentar uma solução que supostamente não atende aos requisitos técnicos contidos no Edital.

II.- DAS RAZÕES DA MANUTENÇÃO DA DECISÃO DO SR. PREGOEIRO.
II.1 DOS QUESTIONAMENTOS E ATESTADOS:

Data vênia, o Sr. Pregoeiro não feriu o princípio do julgamento objetivo nem sequer os critérios previstos no Edital do PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ, pois o mesmo baseou-se, correta e legalmente, naquilo que foi exigido pelo Edital, não há o que se falar em suposto favorecimento durante a realização do Pregão.

Nesse sentido, esclarece-se que é legal, e com previsão contida em Edital, a possibilidade de o pregoeiro realizar questionamentos/ações que visem a obtenção de informações complementares necessárias a elucidação daquilo que está sendo apresentado.

Senão, veja-se:

> 4. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO
>
> 4.1 *omissis*
>
> 4.2 **Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE**, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.
>
> (Grifos nossos)

Não deve prosperar, portanto, qualquer falsa afirmação que a empresa NETWORK deixou de apresentar subsídios indispensáveis para a comprovação da sua capacidade na consecução do objeto contratual.

Trata-se de norma geral, aplicável a todas as modalidades licitatórias e a todas as esferas da federação. Há, inclusive, acórdão do E. Superior Tribunal de Justiça que defende que "*A promoção de diligência é uma faculdade da Comissão de licitação, constituindo, portanto, medida discricionária do administrador*" (REsp. 102.224/SP, 2ª T., rel. Min. CASTRO MEIRA, j. 5.4.2005, DJU 23.5.2005).

Portanto, tanto a habilitação técnica da Empresa NETWORK, com a correta apresentação da documentação, com a realização de **diligência,** além de possuir a proposta mais vantajosa são chancelas que lhe permitem figurar como vencedora do certame em tela, visto que **detém capacidade técnica e preço melhor que todos os demais participantes**.

II.1 DA REGULARIDADE TÉCNICA:

Basicamente, o recorrente buscou questionar a decisão exarada pelo nobre Pregoeiro que concedeu vitória à NETWORK, dentre as alegações, há uma série de questionamentos técnicos, motivo pelo qual, por questões de praticidade e de busca de melhor explicação, opta-se por rebater os pontos de acordo com os itens elencados pelo recorrente, algo que se passamos a fazer desde já.

Cada fabricante possui uma elaboração de documentação técnica/datasheets em formato único, levando em consideração fatores pertinentes para seus processos internos de fabricação e desenvolvimento, e até mesmo de nomenclatura.

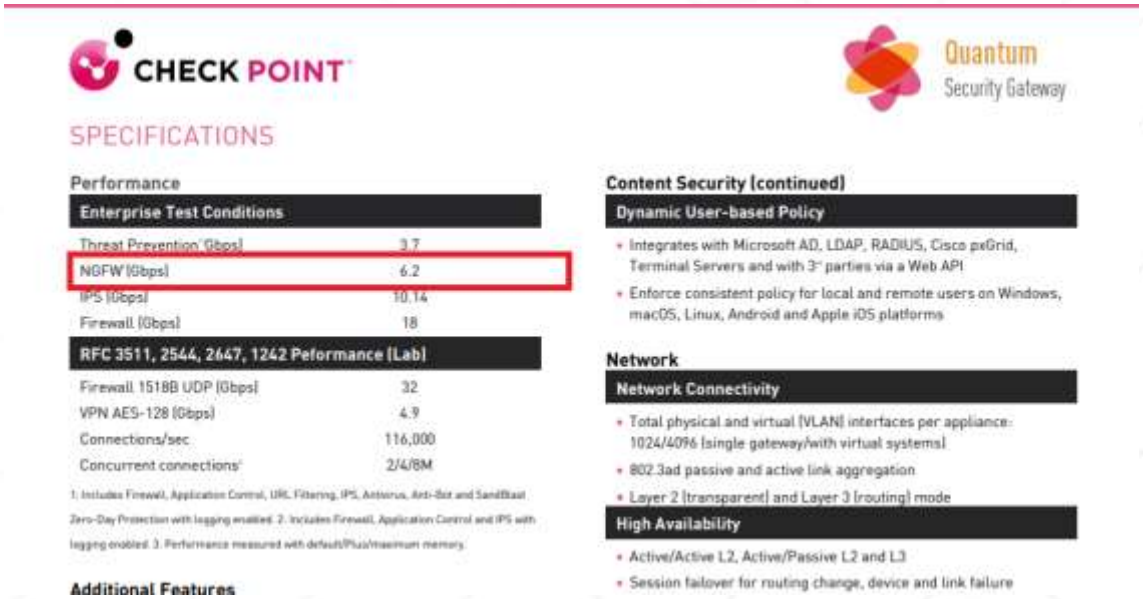
Na Tabela de Capacidades - ANEXO I TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252 Item **5.2.15.10.15** lemos: "Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps) **entre 5 Gbps e 10 Gbps**."

No mesmo anexo, Item **5.2.15.10.17** lemos: Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps) que: "Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps) entre **2,5 Gbps e 5 Gbps."**

O edital possui itens duplicados, sendo assim pode ser considerado números distintos de throughput, inclusive no item **5.2.15.10.15** fica mais caracterizado uma capacidade de throughput de NGFW, onde apresenta um maior número, além de não detalhar todas as funcionalidades como no item **5.2.15.10.17**.

Já no item **5.2.15.10.17** se faz muito mais característico de um throughput de Threat Prevention pela descrição de todas as funcionalidades exigidas, e consequentemente um número menor para todas as funcionalidades habilitadas, onde todos os fabricantes possuem dois números, sendo um maior para capacidade de NGFW, e um menor para capacidade de Threat Prevention, conforme solicitado no certame.

Em relação ao item **5.2.15.10.15,** pode-se observar o valor identificado abaixo via datasheet (6600-security-gateway-datasheet), na página 3. Tal documento técnico também pode ser acessado via link: https://www.checkpoint.com/downloads/products/6600-security-gateway-datasheet.pdf



CHECK POINT

Quantum Security Gateway

SPECIFICATIONS

Performance

Enterprise Test Conditions	
Threat Prevention (Gbps)	3.7
NGFW (Gbps)	6.2
IPS (Gbps)	10.14
Firewall (Gbps)	18
RFC 3511, 2544, 2647, 1242 Performance (Lab)	
Firewall 1518B UDP (Gbps)	32
VPN AES-128 (Gbps)	4.9
Connections/sec	116,000
Concurrent connections	2/4/8M

1. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled. 2. Includes Firewall, Application Control and IPS with logging enabled. 3. Performance measured with default/Plus/maximum memory.

Additional Features

Content Security (continued)

Dynamic User-based Policy

- Integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API
- Enforce consistent policy for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active L2, Active/Passive L2 and L3
- Session failover for routing change, device and link failure

Onde a legenda do índice [2], *"2: Includes Firewall, Application Control and IPS with logging enabled."*

Foi apontado que o equipamento que ofertamos em nossa proposta, para o parâmetro em questão (Throughput de Firewall), não apresenta esse valor com as funcionalidades de SandBox e Anti-malware ativadas. Então, visando explanar e esclarecer todas as dúvidas acerca da nossa solução ofertada, vamos demonstrar os seguintes pontos:

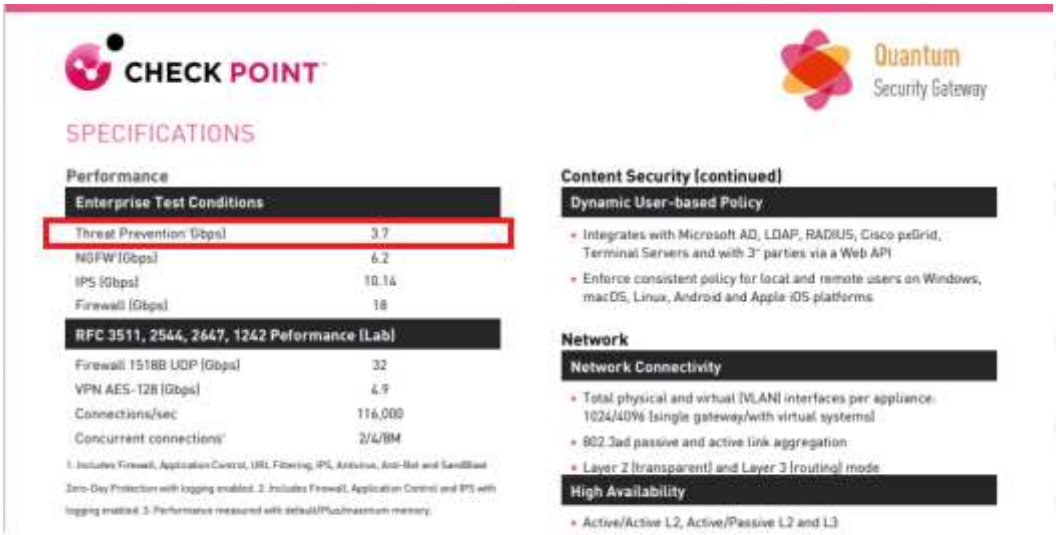
1. O appliance ofertado que consta em nossa proposta é o 6600 Plus appliance with SandBlast (SG6600-PLUS-SNBT), o que nos leva ao próximo ponto;
2. O SandBlast é um serviço dentro do portfólio do fabricante, que neste caso já está inclusa na solução, fornecendo a funcionalidade de SandBox com proteção de dia zero contra ameaças avançadas e desconhecidas, malwares desconhecidos e ataques direcionados, prevenindo infecções por explorações não descobertas. Logo, tais funcionalidades de anti-malware e SandBox já acompanham e são habilitadas de forma nativa ao nosso item ofertado, e, são levadas em consideração no parâmetro de NGFW de **6,2 Gbps** ficando entre a faixa exigida no edital: 5.2.15.10.15 Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps).

5.2.15.10.15	Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps)	05	10

Esta informação encontra-se de forma mais detalhada na página 2 do documento técnico, no link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

3. Logo é possível ver que nosso appliance ofertado obedece e atende aos valores estabelecidos no edital.

Em relação ao item **5.2.15.10.17,** pode-se observar o valor identificado abaixo via datasheet (6600-security-gateway-datasheet), na página 3. Tal documento técnico também pode ser acessado via link: https://www.checkpoint.com/downloads/products/6600-security-gateway-datasheet.pdf



CHECK POINT

Quantum Security Gateway

SPECIFICATIONS

Performance

Enterprise Test Conditions	
Threat Prevention (Gbps)	3.7
NGFW (Gbps)	6.2
IPS (Gbps)	10.14
Firewall (Gbps)	18
RFC 3511, 2544, 2647, 1242 Performance (Lab)	
Firewall 1518B UDP (Gbps)	32
VPN AES-128 (Gbps)	4.9
Connections/sec	116,000
Concurrent connections	2/4/8M

1. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled. 2. Includes Firewall, Application Control and IPS with logging enabled. 3. Performance measured with default/Plus/maximum memory.

Content Security (continued)

Dynamic User-based Policy

- Integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API
- Enforce consistent policy for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active L2, Active/Passive L2 and L3

Onde a legenda do índice [1], *"1: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled."*

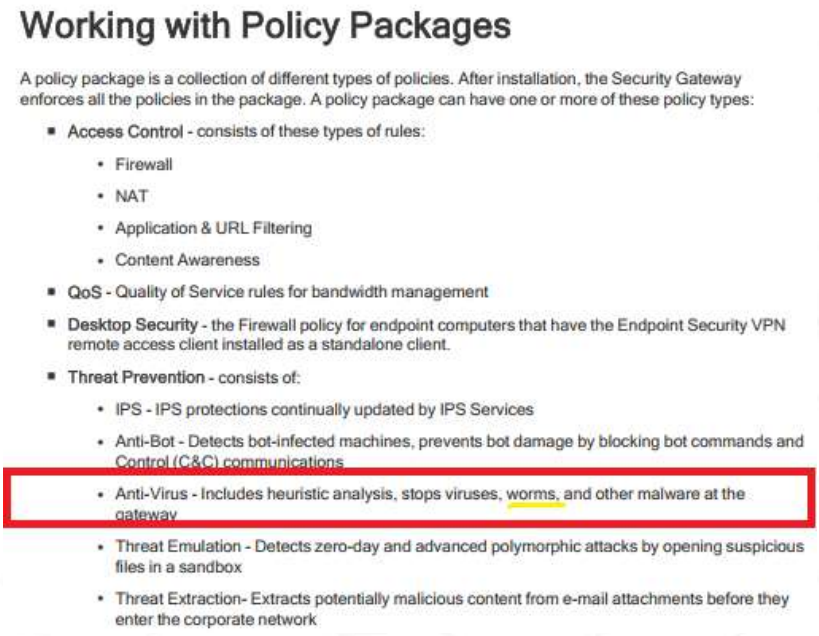
O nosso valor de **3,7 Gbps** fica entre o intervalo de **2,5 e 5,0 Gbps** exigido no edital, conforme imagem abaixo.

5.2.15.10.17	Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivirus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps)	2,5	05

Logo é possível ver que nosso appliance ofertado obedece e atende aos valores estabelecidos no edital.

Com as demonstrações e esclarecimentos dos itens **5.2.15.10.15 e 5.2.15.10.17**, fica comprovado que efetivamente atendemos aos requisitos mínimos de especificação técnica exigidos no edital, incluindo para os subitens a seguir:

- 5.1.15.6.4 (esse item não existe no edital);
- **5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos.**
    - A comprovação e atendimento deste item pode ser observado na página 176 do arquivo **CP_R81_Quantum_SecurityManagement_AdminGuide**, da documentação técnica enviada. Ver imagem abaixo.



Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules:
    - Firewall
    - NAT
    - Application & URL Filtering
    - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
    - IPS - IPS protections continually updated by IPS Services
    - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
    - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
    - Threat Emulation - Detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox
    - Threat Extraction- Extracts potentially malicious content from e-mail attachments before they enter the corporate network

- **5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.**
    - Sabe-se que o Theath Prevention é uma blade do Security Management, ver página 176 do arquivo **CP_R81_Quantum_SecurityManagement_AdminGuide**, da documentação técnica enviada. Conforme imagem abaixo.

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules:
  - Firewall
  - NAT
  - Application & URL Filtering
  - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
  - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
  - Threat Emulation - Detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox
  - Threat Extraction- Extracts potentially malicious content from e-mail attachments before they enter the corporate network

- Partindo da definição de spyware que é um tipo de malware, designado para coletar informações dos usuários em computadores infectados. O Threat Prevention é responsável por determinar as políticas de inspeção das conexões em busca de bots e vírus, onde seu componente principal é "The *Rule Base"*, as regras usam o banco de dados de malware e objetos de rede. Dentro do Threat Prevention é possível observar as configurações existentes para antivírus e spyware, e os respectivos protocolos atendidos. Ver imagens abaixo.

Creating Threat Prevention Rules

In This Section:

Configuring Mail Settings
Configuring IPS Profile Settings
Configuring Anti-Bot Settings
Configuring Anti-Virus Settings
Configuring Threat Emulation Settings
Configuring Threat Extraction Settings
Configuring a Malware DNS Trap
SandBlast Use Cases

- Anti-Virus **UserCheck Settings**:
  - **Prevent** - Select the UserCheck message that opens for a **Prevent** action.
  - **Ask** - Select the UserCheck message that opens for an **Ask** action.
- **Protected Scope**:
  - **Inspect incoming files from**:

    Sends **only incoming** files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:

    - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
    - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
    - **All** - Inspect all incoming files from all interface types.
  - **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.
- The **Protocols** that Anti-Virus scans:
  - **HTTP**
  - **FTP**
  - **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection. This links you to the Mail page of the Profile settings.
- **File Types**:
  - **Process file types known to contain malware**
  - **Process all file types** - Select **Enable deep inspection scanning**, if needed. Remember, it impacts performance.
  - **Process specific file types families**

Protocol

- **Web (HTTP/HTTPS)** - Supported from R80.30 gateways and above. To allow web support, enable HTTPS Inspection. By default, Threat Extraction web support works on these standard ports: HTTP - Port 80, HTTPS - Port 443, HTTPS Proxy - 8080.

  To enable web support on other ports, create a new TCP service. In **General** > **Protocol** select **HTTP**, and in **Match By**, select **Customize** and enter the required port number.

  Notes:

  - After a file is scanned by the Threat Extraction blade, the user receives a message on the action that was done on the file. To customize the message, see sk142852.
  - Threat Extraction web support applies to web downloads, but not web uploads.
- **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection by the Threat Extraction blade. This links you to the Mail page of the Profile settings.

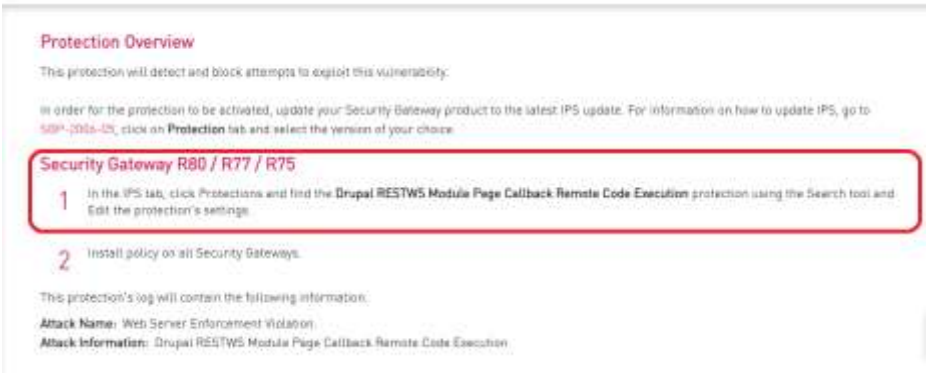
General

General

- **Emulate emails for malicious content (requires Threat Emulation)** - When this option and the Threat Emulation blade are enabled, the Threat Emulation blade scans SMTP traffic.
- **Scan emails for viruses (requires Anti-Virus)** - When this option and the Anti-Virus blade are enabled, the Anti-Virus blade scans SMTP traffic.
- **Extract potentially malicious attachments (requires Threat Extraction)** - When this option and the Threat Extraction blade are enabled, the Threat Extraction blade scans SMTP traffic.

  - Todas as informações que constam nas imagens acima, podem ser acessadas em documentação oficial do fabricante via link: https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/138634 . E no link, https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/101653

- **5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.**
  - A comprovação deste item, encontra-se em documento oficial do fabricante que pode ser acessado via link: https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0723.html/



Protection Overview

This protection will detect and block attempts to exploit this vulnerability.

In order for the protection to be activated, update your Security Gateway product to the latest IPS update. For information on how to update IPS, go to SK#-2016-05, click on **Protection** tab and select the version of your choice.

Security Gateway R80 / R77 / R75

1 In the IPS tab, click Protections and find the **Drupal RESTWS Module Page Callback Remote Code Execution** protection using the Search tool and Edit the protection's settings.

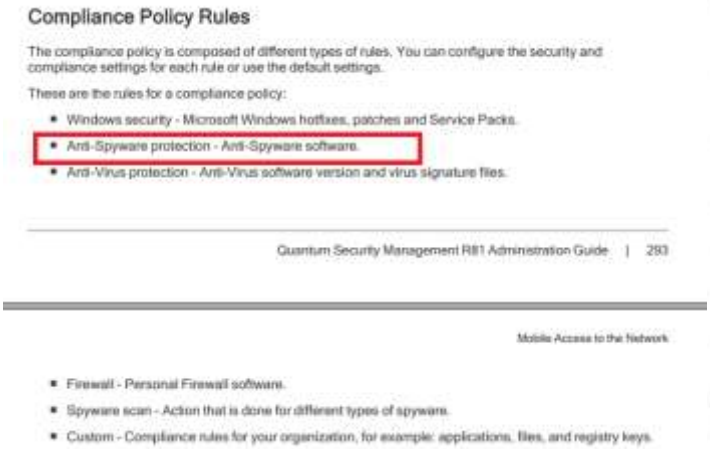
2 Install policy on all Security Gateways.

This protection's log will contain the following information:

Attack Name: Web Server Enforcement Violation

Attack Information: Drupal RESTWS Module Page Callback Remote Code Execution

- **5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.**
  - Para comprovação desse item, ver página 293 e 294 do arquivo **CP_R81_Quantum_SecurityManagement_AdminGuide** enviado na documentação técnica. Conforme imagem abaixo.



Compliance Policy Rules

The compliance policy is composed of different types of rules. You can configure the security and compliance settings for each rule or use the default settings.

These are the rules for a compliance policy:

- Windows security - Microsoft Windows hotfixes, patches and Service Packs.
- Anti-Spyware protection - Anti-Spyware software.
- Anti-Virus protection - Anti-Virus software version and virus signature files.

Quantum Security Management R81 Administration Guide | 293

Mobile Access to the Network

- Firewall - Personal Firewall software.
- Spyware scan - Action that is done for different types of spyware.
- Custom - Compliance rules for your organization, for example: applications, files, and registry keys.

  - Tal comprovação pode ser observada via documento oficial do fabricante no link: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101553. Conforme imagem abaixo:

Check Point Document Threat Extraction Technology

Technical Level

Email Print

Solution ID	sk101553
Technical Level	Basic
Product	Threat Extraction
Version	R77.20 (EOL), R80.10 (EOL), R80.20, R80.30, R80.40, R81, R81.10
OS	Gaia, SecurePlatform 2.6, Crossbeam XOS
Platform / Model	All
Date Created	13-Jul-2014

Solution

Threat Extraction Overview

Threat Extraction is a technology that removes potentially malicious features that are known to be risky from files (macros, embedded objects and more).
This is a new approach for Threat Prevention: instead of determining whether a file is malicious or not, Threat Extraction cleans the file before it enters the organization.
Threat Extraction prevents both known and unknown threats *before* they arrive to the organization, thus providing better protection against zero-day threats.
This approach is considerably quicker than sandboxing the file with Threat Emulation, as has a much lower impact on user experience. Because of different file type support, Threat Extraction should always be used in combination with Threat Emulation.

Plain Text file	txt	mail	Convert to PDF	Bypass
Hypertext Markup Language	html	mail	Convert to PDF	Bypass

To experience this new technology, you may submit files to SandBlast Analysis Page by sending them to threatsit

- Ver também página 5 do documento oficial do fabricante, via link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf . Conforme imagem abaixo:

THREAT EXTRACTION	
File Types	Web downloads and email attachments in the following formats: • Microsoft Word • Microsoft PowerPoint • Microsoft Excel • Adobe PDF • Image files
Extraction Modes	• Clean and keep original file type • Convert to PDF
Extractable Components	Over 15 extractable component types (configurable) including: • Macros and Code • Embedded Objects • Linked Objects • PDF JavaScript Actions • PDF Launch Actions

- E, por último, ver também página 30 do documento oficial do fabricante, via link:https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/105675/FILE/CP_R81.10_ThreatPrevention_AdminGuide.pdf. Conforme imagem abaixo:

Anti-Virus

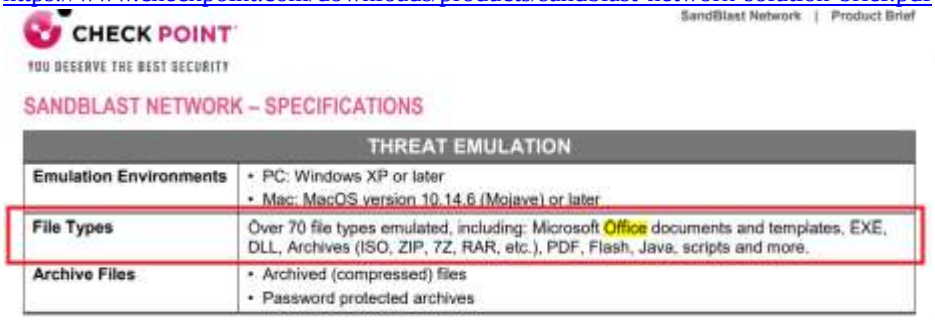
Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans.

The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API (see *"Threat Prevention API" on page 245*).

- **5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos**
  - A comprovação deste item pode ser observada na imagem abaixo, podendo ser acessada na documentação oficial do fabricante via link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

ADDITIONAL PROTECTIONS (included in SandBlast Network licenses)	
General	
SSL Inspection	Included
Identity Awareness	Identity-based policies for users, groups and machines supported through integration with Microsoft Active Directory and Cisco Identity Services Engine
Management	• Single-click policy setup – Supported in R80.40 and above • Threat Extraction for web downloads – R80.30 and above
Supported Protocols	
Threat Emulation	HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP
Threat Extraction	• Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment

- **5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt,.pptx), arquivos java (.jar e class), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox.**
    - A comprovação e atendimento deste item segue na imagem abaixo, tal informação pode ser acessada via documentação oficial do fabricante no link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf



CHECK POINT
YOU DESERVE THE BEST SECURITY

SandBlast Network | Product Brief

SANDBLAST NETWORK – SPECIFICATIONS

THREAT EMULATION	
Emulation Environments	• PC: Windows XP or later • Mac: MacOS version 10.14.6 (Mojave) or later
File Types	Over 70 file types emulated, including: Microsoft Office documents and templates, EXE, DLL, Archives (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts and more.
Archive Files	• Archived (compressed) files • Password protected archives

- **5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY**
    - A comprovação deste item, pode ser observada nos documentos oficiais do fabricante nos links abaixo: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf;

      https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/108955/FILE/CP_SandBlast_Agent_AdminGuide.pdf.

      https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/101653

III.- DOS PRINCÍPIOS DO MENOR PREÇO, DA RAZOABILIDADE E DA MELHOR VANTAGEM.

A licitação pública tem como finalidade atender um INTERESSE PÚBLICO, de forma que seus critérios devem ser observados por todos os participantes em estado de IGUALDADE, para que seja possível a obtenção da PROPOSTA MAIS VANTAJOSA.

A licitação é um procedimento administrativo disciplinado por lei e por um ato administrativo prévio, que determina critérios objetivos de **seleção de uma proposta de contratação economicamente mais atrativa**, com observância ao princípio da isonomia, conduzido por um órgão dotado de competência específica.

Ademais, a observância à necessidade basilar de obter a proposta mais vantajosa é expressamente regulado pelo Art. 3º, da Lei nº 8.666/93, haja vista que acaba por conceder tratamento isonômico e, consequentemente, competitividade ao certame, senão veja-se:

> Art. 3º A licitação destina-se a garantir a observância do princípio constitucional da isonomia, **a seleção da proposta mais vantajosa** para a administração e a promoção do desenvolvimento nacional sustentável e **será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.**
>
> **(Grifos nossos)**

Portanto, é correto **reconhecer que a Empresa NETWORK atende as exigências técnicas constantes do Edital e escolhê-la como a proposta mais vantajosa para esse Órgão evidenciando-se alinhamento com os princípios elencados no artigo acima**.

A proposta da **NETWORK**, que é R$ 718.000,00 (setecentos e dezoito mil reais) mais econômica que a ofertada pela Empresa Recorrente, cuja aceitação daquele Recurso afrontaria o acima transcrito Art. 3º, da Lei nº 8.666/93, **onerando injustificadamente esse Órgão.**

Afinal, trata-se de ato com fulcro **no próprio princípio da finalidade, da eficiência e da razoabilidade**, pois acaba por despender menos recursos financeiros pela mesma solução.

A esse propósito, insta trazer à baila a lição do saudoso professor e magistrado Hely Lopes Meirelles, que assim assevera:

> *(...) todo ato administrativo, de qualquer autoridade ou Poder, para ser legítimo e operante, há que ser praticado em conformidade com a norma legal pertinente (princípio da legalidade***),** *com a moral da instituição (princípio da moralidade),* **com a destinação pública própria (princípio da finalidade),** *com a divulgação oficial necessária (princípio da publicidade) e com presteza e* ***rendimento funcional (princípio da eficiência).*** **Faltando, contrariando ou desviando-se desses princípios básicos, a Administração Pública vicia o ato, expondo-o a anulação por ela mesma ou pelo Poder Judiciário, se requerida pelo interessado**. (*in* Direito Administrativo Brasileiro, 34ª Edição, 2008, Editora Malheiros, São Paulo, pg. 716).
>
> **(Grifos nossos)**

A conduta do agente responsável pela Licitação mostrou-se absolutamente regular, atendendo aos princípios previstos na lei das licitações, assim como do Edital, ou seja, princípio do menor preço, da razoabilidade e da melhor vantagem.

Tem-se que a Empresa ora recorrente, de maneira temerária e sem fundamentação legal ou doutrinária, paralisa e inviabiliza o regular desenvolvimento do procedimento licitatório em destaque, em total afronta aos bons costumes a celeridade dos atos administrativos a serem praticados por esse Órgão.

Com sabedoria, o ilustre doutrinário Celso A. Bandeira de Mello afirma que *"A licitação é o procedimento destinado à seleção da melhor proposta dentre as apresentadas por aqueles que desejam contratar com administração pública".*

Como dito anteriormente, o Sr. Pregoeiro atentou aos princípios do instrumento convocatório e do julgamento objetivo, o que significa procurar razões de fato para sustentar sua escolha ou decisão, ou seja, julgamento sustentado no que está previsto em Edital.

IV.- DOS PEDIDOS.

Em face das razões expostas, a presente Empresa, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, requer deste Sr. Pregoeiro:

a) **NEGUE provimento ao Recurso Administrativo** interposto pela Empresa, IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, para manter na

íntegra a r. decisão que consagrou vencedora a Empresa, NETWORK, que faz com base nas contrarrazões acima, nos princípios do menor preço, da razoabilidade e da melhor vantagem;

b) **Julgar fundamentadas as contrarrazões ora apresentadas**, mantendo a declaração de habilitação da Empresa NETWORK no PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ, por satisfazer todos os requisitos previstos no respectivo Edital e nas demais normas atinentes a administração pública.

Termos em que,
Pede e espera Natural Deferimento.

Fortaleza, 17 de março de 2022.

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

JOSÉ MURILO CIRINO NOGUEIRA JUNIOR
CPF: 648.711.503-72
DIRETOR

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 108.2022.CPL.0782811.2021.015252

Aos Senhores

TADEU AZEVEDO DE MEDEIROS

Diretor de Tecnologia da Informação e Comunicação

C/c

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

NESTE EDIFÍCIO

Assunto: Análise Técnica Recurso Administrativo interposto pela empresa IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI, CNPJ: 23.378.923/0001-87 no interesse no Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ.

Senhor Diretor e Senhor Chefe,

Cumprimentando-os cordialmente, e no interesse do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ** (doc. 0763629), cujo objeto consiste na *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual*, considerando que qualquer manifestação depende da análise desse Setor competente quanto aos apontamentos técnicos levantados, submeto ao crivo de vossa análise o Recurso Administrativo interposto pela pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI, CNPJ: 23.378.923/0001-87** (doc. 0781005), em face da aceitação e habilitação da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54.**

Por oportuno, considerando que a referida petição questiona, em suma, o julgamento (decisão) deste Pregoeiro que se utilizou da manifestação técnica exarada por essa Unidade via **PARECER Nº 4.2022.SIET.0775110.2021.015252**, encaminho os autos para considerações cabíveis.

Ademais, convém destacar que a partir de amanhã iniciará o prazo para apresentação das contrarrazões por parte dos demais licitantes, encerrando-se no próximo dia 17 de março do corrente ano. Lado outro, este Pregoeiro subsidiado pela manifestação desse r. Setor terá o **prazo até o dia 24/03/2022** para emissão da decisão.

Reitero protestos de elevada estima, colocando-me à disposição para quaisquer esclarecimentos que se façam necessários, quedando-me no aguardo das considerações cabíveis para a

continuidade do certame.

Respeitosamente,

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Pregoeiro designado pela PORTARIA N° 229/2022/SUBADM

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 14/03/2022, às 20:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0782811** e o código CRC **91482DCD**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - CEP 69000-000 - Manaus - AM - www.mpam.mp.br

PARECER Nº 9.2022.SIET.0786730.2021.015252

OBJETO: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.
ORIGEM: Processo de Compra 2021.015252

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar análise técnica do recurso interposto pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** (doc. 0781005) e contrarazões da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54** (doc. 0785538), bem como realizar as devidas considerações sobre o questionamento do **PARECER N. 4.2022.SIET.0775110.2021.015252**.

2. Análise

Quanto ao questionamento do parecer anterior, onde se informa que a "análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo" será realizada durante o recebimento do objeto, cabe esclarecer que este é o trâmite previsto para o recebimento, mas não significa que a solução proposta pela empresa vencedora não foi analisada corretamente ou com o devido cuidado. A análise técnica realizada nesta fase do processo de compra, e que culminou na conclusão do parecer n. 4.2022.SIET.0775110.2021.015252, é baseada nas informações prestadas pela vencedora, bem como nas informações disponíveis nos sites dos fabricantes dos equipamentos. Entretanto, uma análise completa, minuciosa e qualitativa, não é possível apenas através de documentações, precisa ser realizada também na prática.

Quanto ao mencioando pela empresa IT PROTECT sobre a solução proposta pela empresa NETWORK SECURE não ter as capacidades técnicas mínimas solicitadas, informamos que durante a análise realizada sobre a documentação do produto, em comparação com as exigências do Termo de Referência deste processo de compra, para elaboração do parecer n. 4.2022.SIET.0775110.2021.015252, apesar de não estar totalmente explícito no texto do parecer, foram conferidos os itens citados, incluindo os *troughputs* mínimos exigidos, sendo concluído que o equipamento atende ao exigido.

Quanto às contrarrazões técnicas apresentadas pela empresa NETWORK SECURE, informamos que a análise descrita pela empresa sobre os itens da documentação técnica do produto é considerada correta. A documentação disponível sobre o produto ofertado indica que o modelo atende aos requisitos mínimos do Termo de Referência deste processo. Não obstante, durante o recebimento todas as exigências serão conferidas e analisadas minuciosamente para posterior emissão do Termo de Recebimento Definitivo.

3. Conclusão

Após análise dos documentos, com relação à parte técnica, mantemos a indicação de que a proposta da empresa vencedora, NETWORK SECURE, pode ser aceita, dando continuidade aos demais trâmites do processo.

Manaus, 21 de março de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ

Coordenador da Área de Redes

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 22/03/2022, às 15:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Theo Ferreira Pará**, **Agente de Apoio - Manutenção - Suporte Informática**, em 22/03/2022, às 15:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0786730** e o código CRC **C924374F**.

DECISÃO Nº 14.2022.CPL.0781007.2021.015252

RAZÕES DE RECURSO APRESENTADA PELA EMPRESA LICITANTE **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87**, NO INTERESSE DO PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ. PRESSUPOSTOS SUBJETIVOS (SUCUMBÊNCIA, LEGITIMIDADE, INTERESSE DE AGIR) ATENDIDOS. PRESSUPOSTOS OBJETIVOS (A EXISTÊNCIA DE UM ATO ADMINISTRATIVO, TEMPESTIVIDADE E FUNDAMENTAÇÃO) ATENDIDOS. MANUTENÇÃO DA DECISÃO DE ACEITAÇÃO E HABILITAÇÃO DA 1.ª COLOCADA.

1. DA DECISÃO

Analisados todos os pressupostos de admissibilidade e os aspectos objetivos dos recursos administrativos dirigidos, este **PREGOEIRO**, com fundamento no artigo 13, § 1.º do ATO PGJ N.º 389/2007, decide:

a) **Conhecer** das oposições formuladas pelas empresas **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL** , CNPJ: 23.378.923/0001-87, no interesse do Pregão Eletrônico n.º 4.003/2022-CPL/MP/PGJ, pelo qual se busca a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;*

b) Após exame das razões recursais formuladas pela empresa susomencionada no ***subitem "a"***, este Pregoeiro apresenta as motivações que culminaram nas decisões outrora prolatadas e, no mérito, **NEGAR PROVIMENTO**, portanto, à manifestação de inconformismo submetida;

c) **Manter a decisão anteriormente prolatada**, quais sejam, **aceitação da proposta** e **habilitação** da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA** , inscrita no CNPJ N.º 05.250.796/0001-54, a fim de dar seguimento ao certame, nos termos art. 17, inciso VII do Decreto nº 10.024/2019; e

d) Envio dos autos à Autoridade Competente, para fins de análise, manutenção da Decisão supra, adjudicação e homologação do certame licitatório em espeque à empresa declarada vencedora, caso assim entenda, com fundamento no artigo 13, IV do Decreto nº 10.024/2019.

2. DO RELATÓRIO

Trata-se de recurso administrativo interposto pela licitante **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL** , CNPJ: 23.378.923/0001-87, no interesse do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, pelo qual se busca a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;*

2.1. Da Manifestação de Intento Recursal

2.1.1. CNPJ: 23.378.923/0001-87 - Razão Social/Nome: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL (doc. 0781002):

No dia 10/03/2022, durante a sessão pública do certame e, epígrafe, a aludida empresa irresignada manifestou-se preliminarmente da seguinte maneira, vejamos:

> **INTENÇÃO DE RECURSO:**
>
> Manifestamos intenção de recorrer contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., devido ao não atendimento de requisitos claramente obrigatórios, bem como outros itens que serão devidamente apresentados tempestivamente junto a peça recursal.

2.2. Das Razões de Recurso

2.2.1. CNPJ: 23.378.923/0001-87 - Razão Social/Nome: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL (doc. 0781005):

Tendo o Pregoeiro verificado a presença dos pressupostos recursais de admissibilidade, resolveu aceitar a manifestação da mencionada licitante, abrindo-se o prazo legal para oferecimento das razões de recurso de 03 (três) dias corridos, logo, com data final até o dia 14/03/2022, 23h59min.

Oportunamente, registre-se que para fins de averiguação da empresa que apresentou as respectivas razões recursais que foram verificados o e-mail institucional, o Setor de Protocolo, bem como, o Sistema Comprasnet, esta última conforme tela extraída devidamente anexada ao presente fólio processual (doc. 0780997).

Assim, no prazo proposto, a empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL**, CNPJ: 23.378.923/0001-87 anexou ao Sistema Comprasnet suas alegações de inconformismo, as quais foram apensadas aos autos (doc. 0781005), arguindo, em suma que houveram possíveis ilegalidades pelo Pregoeiro na condução da fase de lances. Segue, abaixo, em resumo, o pedido da irresignada:

> Ilustríssimo Senhor Pregoeiro Oficial do Ministério Público do Estado do Amazonas
>
> Senhor EDSON FREDERICO LIMA PAES BARRETO
>
> Assunto: Recurso Administrativo Referência: Processo SEI n.º 2021.015252 Pregão Eletrônico: 4.005/2022-CPL/MP/PGJ IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 23.378.923/0001-87, na condição de licitante participante do certame em epígrafe, VEM, respeitosamente, perante Vossa Senhoria, a tempo e modo, interpor o presente RECURSO ADMINISTRATIVO,
>
> contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, que deixou de cumprir requisitos obrigatórios, levando o MD Pregoeiro à tomar decisão equivocada de aceitar e habilitar a sua proposta, o que fazemos com fundamento nos termos da Lei Federal nº 10.520/02, subsidiariamente à Lei Federal 8.666/93 e suas alterações, da Constituição Federal, bem como das normas e condições estabelecidas no instrumento convocatório, junto à Cláusula 12ª do edital do Pregão

Eletrônico n.º 4.005/2022-CPL/MP/PGJ, pelas razões anexas aduzidas.

Pede deferimento.

Fortaleza - CE, 14/03/2022.

Théo Augusto Ramalho Costa CEO da It Protect

DAS RAZÕES DE RECURSO EMÉRITO JULGADOR, Em face às relevantes razões de fato e de direito a seguir aduzidas, as quais anexamos aqui suas justificativas, requeremos, por conseguinte, que seja este recurso recebido, processado e concedido o efeito suspensivo para análise do presente pedido e em caso desse MD Pregoeiro não reconsiderar sua decisão, que seja determinado o encaminhamento do recurso para apreciação do seu Superior Hierárquico, como determina a nossa legislação que regula as licitações públicas. Permissa vênia, a r. decisão do Ilustríssimo Julgador, que assim se manifestou "este Pregoeiro decide HABILITAR a empresa em foco" (10/03/2022 15:08:49), sendo que a situação correta é "Aceito e Habilitado", resultando no aceite de uma proposta que não atende aos requisitos exigidos, carece que seja revista e reformada, eis que prolatada em desarmonia com a nossa legislação, eivada de vícios e consubstanciada em afronta às regras que gerem o instrumento convocatório, estando ela, a merecer reparos, senão vejamos:

1. DA TEMPESTIVIDADE O presente recurso é tempestivo na medida em que a intenção de sua interposição foi manifestada e recebida pelo pregoeiro, no dia 10/03/2022, dentro do prazo mínimo concedido de 30 minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema. Esta Recorrente se manifestou dentro do lapso temporal, consignando, registrando da seguinte forma "Manifestamos intenção de recorrer contra a decisão de habilitar e classificar a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., devido ao não atendimento de requisitos claramente obrigatórios, bem como outros itens que serão devidamente apresentados tempestivamente junto a peça recursal." Entretanto, a despeito da reclamada decisão, vale constar sobre o direito a recurso e seu respectivo prazo, vale aludir que diante de tal decisão é cabível o presente recurso, em garantia aos princípios do devido processo legal, contraditório e ampla defesa, de aplicação indiscutível no feito administrativo. O instrumento convocatório, inclusive, prevê que, uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias corridos para apresentar as razões. Desta feita, estando registrado junto à Ata a data limite para registro de recurso: 14/03/2022, resta assim, comprovada a sua tempestividade.

2. REQUISITOS RECURSAIS A legislação, em especial a Lei n. 8.666/1993, Lei n. 10.520/2002 e o Decreto n. 10.024/2019, exigem que o registro da intenção de recurso deve atender aos requisitos de sucumbência, tempestividade, legitimidade, interesse e motivação, não podendo ter seu mérito julgado de antemão. O Tribunal de Contas da União – TCU, já firmou entendimentos de que não cabe ao Pregoeiro rejeitar sumariamente a intenção de recurso apresentada pelos licitantes no decorrer de um pregão eletrônico, cabendo ao agente condutor do certame, tão somente avaliar se os requisitos de admissibilidade recursal estão ou não presentes. Assim, analisando as premissas, temos: a) Sucumbência, que é implicou na nossa derrota perante o certame; b) Tempestividade, ante a intenção de recursos e protocolo desta peça recursal dentro do prazo estabelecido; c) Legitimidade, verificada por meio da manifestação desta parte interessada na condição de sucumbente; d) Interesse, baseado na concessão, segundo o qual não é permitido o prosseguimento de processos nos casos que, mesmo acolhendo o pleito de terminada licitante, a decisão administrativa seja inútil ou que não possa ser aproveitada; e e) Motivação, apurável ante a exposição objetiva do conteúdo da irresignação em relação à decisão proferida. Assim, de forma clara e suscinta, mas suficiente para o atendimento do exercício do direito de se manifestar em relação à decisão proferida, esse MD Pregoeiro se manifestou no sentido de realizar a "devida aceitação e concessão dos prazos de 3 dias corridos para envio das razões, mais 3 dias para contrarrazões e 5 dias úteis para

decisão deste Pregoeiro", solicitando ainda, a título de alerta, "Outrossim, solicito prudência e bom senso nos Senhores, caso queiram fazer uso desta prerrogativa dos recursos, a fim de evitarmos recursos meramente protelatórios". Tal admissibilidade ante ao preenchimento dos requisitos e premissas, nos garantiu o direito de manifestar nosso inconformismo por intermédio desta peça recursal.

3. SÍNTESE DOS FATOS

3.1. Dos elementos ensejadores da pretensão de recorrer contra a decisão O MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, pelo presente edital e por intermédio da PROCURADORIA GERAL DE JUSTIÇA, tornou pública a realização de licitação, na modalidade PREGÃO, na forma ELETRÔNICA, do tipo menor preço por lote, objetivando a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos. O objeto inclui todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão funcionar perfeitamente, sem vícios, não constar em listas de end-of sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato. Destaca-se, todas as funcionalidades exigidas. A abertura da Sessão do Pregão foi designada para ser realizada no dia 21 de fevereiro de 2022, às 10:00 horas, no Portal de Compras do Governo Federal – Comprasnet. A empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA foi vencedora do certame, arrematando lote único pelo preço final de R$ 2.478.052,85, após negociação onde o MD Pregoeiro deixou clara a relação com a vencedora, manifestando claramente, conforme se verifica junto à ata, da seguinte forma: "Pregoeiro 21/02/2022 11:12:15 - Para NETWORK SECURE SEGURANCA DA INFORMACAO LTDA - Ademais, sua empresa participou da fase interna de cotação e ofertou preço bem menor ao apresentado no certame...". Tal registro se deu na fase de negociação, que pode ser verificada, como dito, junto à ata de realização do pregão eletrônico. Em seguida, convocou a licitante para envio da proposta e demais documentos no prazo de 02 horas, sempre orientando detalhadamente a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, quanto a correta forma de proceder. Em seguida, em 07/03/2022, às 11:35:06, o MD Pregoeiro registrou no sistema: "A proposta de preço, documento 0772069, informa equipamentos e serviços condizentes com as quantidades e exigências do Termo de Referência", baseado no PARECER Nº 4.2022.SIET.0775110.2021.015252, que consigna uma conclusão final. Entretanto, um registro chamou a atenção, na sequência do trecho acima: "Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo". SMJ, MD Pregoeiro, a análise minuciosa e qualitativa deve ser realizada primeiramente na fase de análise da proposta e após contratada, na fase de recebimento, ocorre que não estamos na fase de recebimento. Vejamos o que diz o edital quanto ao indispensável atendimento aos requisitos: "5.7. Como condição para participação no Pregão, a licitante assinalará "sim" ou "não" em campo próprio do Sistema eletrônico Comprasnet, relativo às seguintes declarações: (...) c) que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias" "9.2. Na proposta vencedora a ser enviada posteriormente deverá constar, conforme modelo do Anexo IV: (...) c) Especificações claras, completas e minuciosas, com detalhes do objeto ofertado, inclusive marca, modelo, tipo e referência, no que couber, observadas as especificações mínimas e quantitativos contidos neste Edital e anexos" "9.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante." Já o Termo de Referência, exige: "5.1.11 A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente." Junto a proposta, temos: "DECLARAÇÕES: 1. Cumpro plenamente os requisitos de credenciamento e habilitação,

inclusive o estabelecido no subitem 5.6 (...)" Pelos trechos acima, resta claro e evidente que o edital exige atendimento à todos os requisitos especificados. Caso este RECORRENTE esteja com entendimento equivocado quanto a isso, esse MPAM pode estar diante de um vício insanável, pois a legislação e a jurisprudência são claras ao permitir somente a exigência dos requisitos mínimos indispensáveis e se, diante de tantos requisitos, a solução a ser aceita não atender a sua totalidade, não faz o menor sentido registrar além do necessário. Assim, proceder o aceite de uma proposta em condição diferente do estipulado em edital, afronta mortalmente o princípio da vinculação ao instrumento convocatório. O princípio da vinculação ao instrumento convocatório tem como finalidade principal evitar que administradores realizem análise de documentos de habilitação de forma arbitrariamente subjetiva, o que pode viabilizar o direcionamento do contrato em defesa de interesses pessoais ou de terceiros, em total contrariedade com o princípio da isonomia entre os licitantes e demais princípios da administração pública como moralidade, impessoalidade, legalidade e afronta ao interesse público. O princípio da vinculação ao instrumento convocatório é corolário do princípio da legalidade e da objetividade das determinações habilitatórias. Impõe à Administração e ao licitante a observância das normas estabelecidas no Edital de forma objetiva, mas sempre velando pelo princípio da competitividade. Assim, não se pode aceitar qualquer oferta que não atenda a plenitude do que está sendo exigido, considerando que, de fato, esse MPAM realmente especificou os requisitos como exigências mínimas a serem atendidas. Em situação verificada que a proposta ofertada não atende plenamente os requisitos, deveria o MD pregoeiro, assim proceder: "10.6.2. Nas situações da compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos nos subitens acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de 05 (cinco) dias úteis contados da solicitação." A diligência era o meio de verificar a compatibilidade absoluta e não registrar que "Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo." Outro ponto chamou a atenção: a dissintonia e contradição consignadas em ata. Em 07/03/2022 às 11:38:27, há o seguinte registro: "Conforme exigência, foram apresentados atestados de capacidade técnica que comprovam, conjuntamente, a prestação anterior de serviços de firewall de próxima geração, NGFW, com troughput de 10Gbps, no mínimo. Foram apresentados 03 (três)atestados, disponíveis nas páginas 42, 43, 44 e 45 do documento 0772080" e complementando, "... , incluindo equipamentos similares e superiores ao objeto deste processo." Data vênia, entendemos que a empresa logrou êxito em comprovar sua aptidão técnica. Entretanto, em 07/03/2022 às 11:41:00, consta registro no sentido de que "Senhor Fornecedor, ao realizar as convalidações dos documentos anexados no sistema (...) Todavia, os atestados da Hapvida e Pague menos inexiste essa possibilidade" Ora, MD Pregoeiro, como primeiro aceita o documento para depois verificar sua validade? Seria esta a sequência correta? Segundo o Decreto n. 10.024/2019, a comprovação de habilitação é prévia, ou seja, antecede a sua aceitação. Ocorre que o que se observa é uma intenção clara de declarar primeiro o aceite da proposta, para em seguida, verificar a sua validade. Analisando a solução ofertada, é possível verificar que o equipamento apresentado pela empresa Network Secure não atende ao item 5.2.15.10.15 do Termo de Referência. O item menciona as funcionalidades de Firewall, IPS, App Control, Sandbox e Anti-Malware, logo a funcionalidade que tem que ser considerada é a de Threat Prevention e não a de NGFW, e de acordo com a documentação do fabricante CheckPoint este modelo de equipamento tem capacidade de throughput de apenas 3.7 Gbps e não o mínimo solicitado de 5 Gbps. Assim sendo, o valor de NGFW não pode ser considerado para este item pois o próprio fabricante informa que somente compreende as 3 funcionalidades, no caso FW, IPS e App Control, sem considerar as de SandBox e Anti-Malware. Para estas, o valor válido é da funcionalidade de Threat Prevention como já mencionado. Segundo o que se pode verificar junto ao edital publicado é que para o alcance dos resultados pretendidos esse item é indispensável. Vejamos. O não atendimento deste item prejudica a proteção avançada demandada pelo órgão conforme solicitado nos itens 5.1.15.6.4, 5.2.15.6.18, 5.2.15.6.22, 5.2.15.6.26, 5.2.15.6.31, 5.2.15.6.32 e, especialmente, os itens 5.2.15.6.34 e 5.2.15.7. Este desacordo com o exigido põe o órgão em uma posição de insegurança e prejuízo sobre o propósito do investimento haja vista que este modelo de equipamento

não terá performance e tampouco capacidade de realizar a proteção efetiva que o MPAM demanda. Ademais, a empresa tinha a possibilidade de ofertar um modelo com capacidade maior para atendimento do item, porém não o fez. Entende-se, então, que esta atitude prejudica a concorrência pois todas as licitantes precisam apresentar proposta que atenda por completo ao edital a fim de elaborar a sua estratégia de produtos, serviços e preços e quando isso não ocorre permite que aquela que não atendeu tenha uma vantagem na proposta de valor para vencer o certame.

3.2. Do propósito do Recurso Administrativo com Pedido de Reconsideração Todo processo licitatório é revestido do interesse público, que é supremo. A Administração Pública não licita por licitar. Todo procedimento licitatório possui uma justificativa detalhando a sua necessidade, a qual é obtida após estudo interno que identificou tecnicamente as opções existentes e alternativas viáveis, o que permite concluir pelo cenário que melhor atende a sua demanda. Este é o objetivo principal do certame. Assim, esta empresa não está somente defendendo seus interesses mas resguardando essa Administração frente à necessidade levantada por esse MPAM. Diante de tal premissa, caracterizada por interesse mútuo entre esta empresa e os objetivos desse MPAM, nasceu nosso interesse em apresentar elementos suficientes para provocar uma revisão dos atos praticados e garantir que a solução ofertada comprovadamente atende à todos os requisitos mínimos exigidos.

3.3. Da possibilidade de revisão dos atos O princípio da autotutela estabelece que a Administração Pública possui o poder de controlar os próprios atos, anulando-os quando ilegais ou revogando-os quando inconvenientes ou inoportunos. Assim, a Administração não precisa recorrer ao Poder Judiciário para corrigir os seus atos, podendo fazê-lo diretamente. Esse princípio possui previsão em súmula do STF "Súmula nº 473: A Administração pode anular seus próprios atos, quando eivados de vícios que os tornam ilegais, porque deles não se originam direitos; ou revoga-los, por motivo de conveniência ou oportunidade, respeitados os direitos adquiridos, e ressalvada, em todos os casos, a apreciação judicial." Esse princípio possui previsão junto ao art. 53 da Lei 9.784/99: "A Administração deve anular seus próprios atos, quando eivados de vício de legalidade, e pode revogá-los por motivo de conveniência ou oportunidade, respeitados os direitos adquiridos."

3.4. Da preservação do interesse público Os interesses representados pela Administração Pública, estão previstos no Art. 37 da Constituição Federal Brasileira, e se aplica na atuação do princípio da supremacia do interesse público. Essa é uma das prerrogativas conferidas a administração pública, porque a mesma atua por conta de tal interesse, ou seja, o legislador na edição de leis ou normas deve orientar-se por esse princípio, levando em conta que a coletividade está em um nível superior ao do particular. Se na condição de apresentada, esse MPAM representa a coletividade, deve preservar o interesse público. Desta forma, a necessidade que justificou e embasou o processo licitatório deve ser atendido em sua plenitude, sob o risco de afrontar à Constituição Federal. A única forma de preservar o interesse público é garantir que a necessidade seja atendida. Pela manifestação exarada de que no recebimento será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, entendemos, SMJ, que o procedimento está eivado de vícios e descumprindo os ditames legais e editalícios, não garantindo a preservação do interesse público e colocando em risco os recursos públicos, uma vez que não se sabe se a solução, de fato, atende à totalidade dos requisitos. Esta questão, inclusive, exige exercício de consciência e risco quanto a continuidade do processo nos termos atuais, uma vez que tal ato certamente será auditado e questionado por órgãos de controle.

3.5. Risco à quebra da isonomia De acordo com o art. 3º da Lei nº 8666/93, são princípios expressos da licitação: legalidade, impessoalidade, moralidade, publicidade, igualdade, probidade administrativa, vinculação ao instrumento convocatório e julgamento objetivo. Dentre eles, destaca-se o princípio da igualdade entre os licitantes, onde a Administração Pública deve conduzir a licitação de maneira impessoal, sem prejudicar nenhum licitante. Desde que preencham os requisitos exigidos, todos os que tiverem interesse em

participar da disputa devem ser tratados com isonomia. Celso Antônio Bandeira de Mello conceitua licitação como um certame que as entidades governamentais devem promover e no qual abrem disputa entre os interessados em com elas travar determinadas relações de conteúdo patrimonial, para escolher a proposta mais vantajosa às conveniências públicas. Estriba-se na ideia de competição, a ser travada economicamente entre os que preencham os atributos e aptidões necessários ao bom cumprimento das obrigações que se propõem assumir. Todos os dispositivos da lei de licitações ou regulamentação de um específico processo licitatório, devem ser interpretados à luz do princípio da isonomia. Se o edital é supremo e vincula as partes – MPAM e Licitantes – as suas regras devem ser fielmente obedecidas. Como visto nesta peça recursal, o instrumento convocatório e seus anexos consignaram os requisitos mínimos de admissibilidade técnica de uma proposta e, o ato de aceitar parcialmente, afronta o edital e desrespeita os demais licitantes, uma vez que, se todos soubessem que haveria aceite parcial de requisitos, teriam ofertado equipamento condizente com as exigências e não tão robusto quanto ao que, por exemplo, ofertamos. A definição do objeto deve ser clara e precisa e decorrendo análise dos edital, resta claro e evidente o que se pretende contratar: uma solução robusta, completa e que atenda a todos os requisitos e nesta diapasão, quanto mais requisitos, mais elevado é o custo dessa solução. Reiteramos: se o edital deixasse claro a possibilidade de ofertar solução que atendesse apenas parte dos requisitos, as soluções ofertadas representariam custos menores para esse MPAM.

3.6. Do risco de desperdício de recursos públicos Importa registrar a presunção ope legis prevista no parágrafo único do art. 70 da Constituição Federal, que imputa ao gestor público a obrigação de comprovar a boa e regular aplicação dos recursos postos sob sua administração, mediante a apresentação de prestação de contas. A fixação dos critérios de aceitabilidade da proposta é requisito obrigatório nos editais de licitação. A fixação de requisitos mínimos de habilitação para fins de qualificação técnica, independentemente de técnico-profissional ou técnico-operacional, deve ser estabelecida de maneira razoável, pertinente e compatível com o objeto licitado, sendo definida como resultado de um processo lógico, fundado em razões técnico-científicas, de forma que não restrinja indevidamente a competitividade da licitação. Acerca desse tema, Marçal Justen Filho leciona o seguinte: “Vale insistir acerca da inconstitucionalidade de exigências excessivas, no tocante à qualificação técnica. Observe-se que a natureza do requisito é incompatível com a disciplina precisa, minuciosa e exaustiva por parte da Lei. É impossível deixar de remeter à avaliação da Administração a fixação dos requisitos de habilitação técnica. Essa competência discricionária não pode ser utilizada para frustrar a vontade constitucional de garantir o mais amplo acesso de licitantes, tal como já exposto acima. A Administração apenas está autorizada a estabelecer exigências aptas a evidenciar a execução anterior de objeto similar. (...) (...) No entanto, o ônus da prova recai sobre a Administração. Ou seja, diante da dúvida, cabe à Administração demonstrar a necessidade da exigência formulada. Não é encargo do particular evidenciar a desnecessidade do requisito imposto pela Administração. Afinal, quem elaborou o ato convocatório foi a Administração. Não seria possível invocar a mera presunção de legitimidade dos atos administrativos para afastar o dever de a Administração explicar o motivo e o conteúdo das escolhas realizadas.” Assim, presume-se que as exigências expostas no edital sejam as mínimas. Logo, se uma proposta é aceita atendendo parte dos requisitos estipulados, entende-se que tais requisitos não eram essenciais, podendo ser entendidos como excessivos, o que pode ter restringido uma ampla participação, competitividade, busca pela proposta mais vantajosa e ainda, desperdício de recursos públicos. É de indispensável importância que se avalie o risco de admissibilidade nos termos aqui expostos, sob risco de responsabilização dos agentes que deram causa.

4. DO CABIMENTO E DA LEGITIMIDADE

4.1. Da Legitimidade para Recorrer Preliminarmente, registra-se que a ora Recorrente, como empresa especializada no ramo pertinente ao objeto licitado, detém total e irrestrita capacidade estrutural e tecnológica de oferecer objeto conforme exigido no edital. E, em razão de sua solidificação no mercado público, possui plena capacidade técnica e

financeira para oferecer proposta aderente à exigida por esse MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.

4.2. Do Cabimento do Presente Pedido O Direito de Peticionar no procedimento licitatório tem como fundamento legal na CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988, que dispõe: "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXXIV - são a todos assegurados, independentemente do pagamento de taxas: a) O direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder; (...)." É dessa garantia constitucional que decorrem as diversas formas de provocação da Administração Pública para o exercício do direito de petição, nesse sentido vejamos as palavras de Di Pietro: "Dentro do direito de petição estão agasalhados inúmeras modalidades de recursos administrativos... É o caso da representação, da reclamação administrativa, do pedido de reconsideração, dos recursos hierárquicos próprios e impróprios da revisão." Seguindo esse entendimento, Carvalho Filho afirma que: "O direito de petição é um meio de controle administrativo e dá fundamento aos recursos administrativos por que tais recursos nada mais são do que meios de postulação a um órgão administrativo. O instrumento que propicia o exercício desse direito consagrado na CF é o recurso administrativo." Desta feita, temos que o presente recurso administrativo instrumentaliza o exercício do direito de petição junto ao poder público.

5. DAS RAZÕES PARA REFORMAR A R. DECISÃO

Ilustre Senhor Julgador, data máxima vênia, a Recorrente logrou êxito em demonstrar que a r. decisão ocorreu em um grande equívoco em admitir proposta que não atende a totalidade dos requisitos mínimos exigidos no edital. Deve-se chamar a atenção dos julgadores ao fato de que a decisão mais acertada é justamente preservar o interesse público, cancelar o aceite, recusar a proposta e convocar as demais licitantes, na ordem de classificação. Portanto, baseiam-se às razões da Recorrida, nos prejuízos que o MD Pregoeiro poderá proporcionar, face nítida a falta de vinculação ao edital ou respaldo legal, causando assim o afastamento do maior objetivo do edital que é assegurar o atendimento do interesse desse comprador. Desta forma, a r. decisão não foi nada razoável e nem proporcional ao declarar a licitante NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, como vencedora da disputa, mas condições trazidas nesta peça recursal. Assim, se faz necessário que essa Administração julgue provido o presente recurso, com observância ao princípio da eficiência, segurança jurídica e do devido processo legal.

6. DOS PEDIDOS

DIANTE DO EXPOSTO, requer-se que seja conhecido o presente recurso e, ao final, julgando provido, com fundamento nas razões precedentemente aduzidas, com efeito SUSPENSIVO para que seja revisto o equívoco e risco de desperdício de recursos públicos e afastamento do interesse público, anulando a decisão em apreço, na parte atacada neste, promovendo a recusa da proposta da licitante NETWORK SECURE SEGURANCA DA INFORMACAO LTDA e a convocação das demais licitantes, na ordem de classificação. Outrossim, lastreada nas razões recursais, requer-se que esse MD Pregoeiro reconsidere sua decisão e, na hipótese não esperada de isso não ocorrer, faça este subir, devidamente informado à autoridade superior, em conformidade com o § 4°, do art. 109, da Lei n. º 8.666/93, observando-se ainda o disposto no § 3° do mesmo artigo.

Termo em que,

Pede e espera deferimento.

Fortaleza - CE, 14/03/2022.

Théo Augusto Ramalho Costa CEO da It Protect

2.3. Das Contrarrazões

Do mesmo modo, a teor do § 3º, do art. 109, da Lei n.° 8.666/93, combinado com o inciso XVIII, do artigo 4.°, da Lei n.° 10.520/2002, o prazo de **3 (três) dias corridos**, tendo a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.** , inscrita sob o CNPJ nº 05.250.796/0001-54, apresentado Requerimento de Contrarrazões (doc. 0785538), via e-mail institucional datado de 17.03.2022 (doc. 0788251) e juntado no Sistema Comprasnet (doc. 0788241), com o seguinte teor:

NTÍSSIMO SENHOR PREGOEIRO DA COMISSÃO PERMANENTE DE LICITAÇÃO (CPL), DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS.

REF.: EDITAL DO PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ. Processo SEI nº 2021.015252.

Ref.: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, incluindo treinamento e serviço de migração da plataforma atual.

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA. (VENCEDORA), inscrita sob o CNPJ nº 05.250.796/0001-54, já qualificada nos autos do processo licitatório em epígrafe, neste ato conduzida por seu legal representante infra-assinado, vem, respeitosamente, perante a ilustre presença de Vossa Senhoria, dentro do prazo legal, apresentar as presentes

C O N T R A – R A Z Õ E S

ao RECURSO ADMINISTRATIVO interposto pela Empresa, IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, pelos fatos e fundamentos a seguir:

I.- DOS FATOS.

A empresa NETWORK, credenciou-se no procedimento licitatório nº 4.005/2022- CPL/MP/PGJ, o qual objetiva a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme demais especificações contidas no Edital.

Tal certame atendeu às Condições Gerais constantes naquele Edital, pelo critério de julgamento de menor preço, sob regime de empreitada por preço global, ou seja, a obtenção do somatório dos preços unitários que venha a ser mais vantajoso para esse Órgão.

Destarte, após realizados os trâmites regulares e intrínsecos, previstos no Edital, essa Comissão **consagrou vencedora a presente Empresa por ordem de menor preço ofertado** e por ter cumprido com as disposições do edital PREGÃO ELETRÔNICO Nº 4.005/2022- CPL/MP/PGJ.

Nesse contexto, frise-se, a empresa NETWORK foi declarada vencedora com o valor global de R$ 2.478.052,85 (dois milhões, quatrocentos e setenta e oito mil, cinquenta e dois reais e oitenta e cinco centavos). Todavia, a Empresa IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, inconformada com a legítima vitória da NETWORK, interpôs Recurso Administrativo, ora contrarrazoado, alegando que essa Comissão supostamente a favoreceu por oportunidade da realização de diligência, assim como por a mesma não apresentar uma solução que supostamente não atende aos requisitos

técnicos contidos no Edital.

II.- DAS RAZÕES DA MANUTENÇÃO DA DECISÃO DO SR. PREGOEIRO.

II.1 DOS QUESTIONAMENTOS E ATESTADOS:

Data vênia, o Sr. Pregoeiro não feriu o princípio do julgamento objetivo nem sequer os critérios previstos no Edital do PREGÃO ELETRÔNICO Nº 4.005/2022-CPL/MP/PGJ, pois o mesmo baseou-se, correta e legalmente, naquilo que foi exigido pelo Edital, não há o que se falar em suposto favorecimento durante a realização do Pregão.

Nesse sentido, esclarece-se que é legal, e com previsão contida em Edital, a possibilidade de o pregoeiro realizar questionamentos/ações que visem a obtenção de informações complementares necessárias a elucidação daquilo que está sendo apresentado.

Senão, veja-se:

4. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO

4.1 omissis

4.2 ***Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE****, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis. (Grifos nossos)*

Não deve prosperar, portanto, qualquer falsa afirmação que a empresa NETWORK deixou de apresentar subsídios indispensáveis para a comprovação da sua capacidade na consecução do objeto contratual.

Trata-se de norma geral, aplicável a todas as modalidades licitatórias e a todas as esferas da federação. Há, inclusive, acórdão do E. Superior Tribunal de Justiça que defende que "A promoção de diligência é uma faculdade da Comissão de licitação, constituindo, portanto, medida discricionária do administrador" (REsp. 102.224/SP, 2ª T., rel. Min. CASTRO MEIRA, j. 5.4.2005, DJU 23.5.2005).

Portanto, tanto a habilitação técnica da Empresa NETWORK, com a correta apresentação da documentação, com a realização de **diligência**, além de possuir a proposta mais vantajosa são chancelas que lhe permitem figurar como vencedora do certame em tela, visto que **detém capacidade técnica e preço melhor que todos os demais participantes.**

II.1 DA REGULARIDADE TÉCNICA:

Basicamente, o recorrente buscou questionar a decisão exarada pelo nobre Pregoeiro que concedeu vitória à NETWORK, dentre as alegações, há uma série de questionamentos técnicos, motivo pelo qual, por questões de praticidade e de busca de melhor explicação, opta-se por rebater os pontos de acordo com os itens elencados pelo recorrente, algo que se passamos a fazer desde já.

Cada fabricante possui uma elaboração de documentação técnica/datasheets em formato único, levando em consideração fatores pertinentes para seus processos internos de fabricação e desenvolvimento, e até mesmo de nomenclatura.

Na Tabela de Capacidades - ANEXO I TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252 Item 5.2.15.10.15 lemos: "Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps) entre 5 Gbps e 10 Gbps."

No mesmo anexo, Item 5.2.15.10.17 lemos: Throughput com as

funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps) que: “Throughput com as funcionalidades de Firewall, controle de Aplicação, Filtro URL, IPS, Antivírus, Anti-Bot e controle de ameaças avançadas habilitadas (em Gbps) entre 2,5 Gbps e 5 Gbps.”

O edital possui itens duplicados, sendo assim pode ser considerado números distintos de throughput, inclusive no item 5.2.15.10.15 fica mais caracterizado uma capacidade de throughput de NGFW, onde apresenta um maior número, além de não detalhar todas as funcionalidades como no item 5.2.15.10.17.

Já no item 5.2.15.10.17 se faz muito mais característico de um throughput de Threat Prevention pela descrição de todas as funcionalidades exigidas, e consequentemente um número menor para todas as funcionalidades habilitadas, onde todos os fabricantes possuem dois números, sendo um maior para capacidade de NGFW, e um menor para capacidade de Threat Prevention, conforme solicitado no certame.

Em relação ao item 5.2.15.10.15, pode-se observar o valor identificado abaixo via datasheet (6600-security-gateway-datasheet), na página 3. Tal documento técnico também pode ser acessado via link: https://www.checkpoint.com/downloads/products/6600-security-gatewaydatasheet.pdf

Onde a legenda do índice 2 , “2: Includes Firewall, Application Control and IPS with logging enabled.”

Foi apontado que o equipamento que ofertamos em nossa proposta, para o parâmetro em questão (Throughput de Firewall), não apresenta esse valor com as funcionalidades de SandBox e Anti-malware ativadas. Então, visando explanar e esclarecer todas as dúvidas acerca da nossa solução ofertada, vamos demonstrar os seguintes pontos:

1. O appliance ofertado que consta em nossa proposta é o 6600 Plus appliance with SandBlast (SG6600-PLUS-SNBT), o que nos leva ao próximo ponto;

2. O SandBlast é um serviço dentro do portfólio do fabricante, que neste caso já está inclusa na solução, fornecendo a funcionalidade de SandBox com proteção de dia zero contra ameaças avançadas e desconhecidas, malwares desconhecidos e ataques direcionados, prevenindo infecções por explorações não descobertas. Logo, tais funcionalidades de anti-malware e SandBox já acompanham e são habilitadas de forma nativa ao nosso item ofertado, e, são levadas em consideração no parâmetro de NGFW de 6,2 Gbps ficando entre a faixa exigida no edital: 5.2.15.10.15 Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps).

Esta informação encontra-se de forma mais detalhada na página 2 do documento técnico, no link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf 3. Logo é possível ver que nosso appliance ofertado obedece e atende aos valores estabelecidos no edital.

Em relação ao item 5.2.15.10.17, pode-se observar o valor identificado abaixo via datasheet (6600-security-gateway-datasheet), na página 3. Tal documento técnico também pode ser acessado via link: https://www.checkpoint.com/downloads/products/6600-security-gatewaydatasheet.pdf

Onde a legenda do índice 1 , “1: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled.”

O nosso valor de 3,7 Gbps fica entre o intervalo de 2,5 e 5,0 Gbps exigido no edital, conforme imagem abaixo.

Logo é possível ver que nosso appliance ofertado obedece e atende aos valores estabelecidos no edital.

Com as demonstrações e esclarecimentos dos itens 5.2.15.10.15 e 5.2.15.10.17, fica comprovado que efetivamente atendemos aos requisitos mínimos de especificação técnica exigidos no edital, incluindo para os subitens a seguir:

• 5.1.15.6.4 (esse item não existe no edital);

• 5.2.15.6.18 Bloquear ataques efetuados por worms conhecidos. o A comprovação e atendimento deste item pode ser observado na página 176 do arquivo CP_R81_Quantum_SecurityManagement_AdminGuide, da documentação técnica enviada. Ver imagem abaixo.

• 5.2.15.6.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.

o Sabe-se que o Theath Prevention é uma blade do Security Management, ver página 176 do arquivo CP_R81_Quantum_SecurityManagement_AdminGuide, da documentação técnica enviada. Conforme imagem abaixo.

o Partindo da definição de spyware que é um tipo de malware, designado para coletar informações dos usuários em computadores infectados. O Threat Prevention é responsável por determinar as políticas de inspeção das conexões em busca de bots e vírus, onde seu componente principal é “The Rule Base”, as regras usam o banco de dados de malware e objetos de rede. Dentro do Threat Prevention é possível observar as configurações existentes para antivírus e spyware, e os respectivos protocolos atendidos. Ver imagens abaixo

o Todas as informações que constam nas imagens acima, podem ser acessadas em documentação oficial do fabricante via link: https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/138634 . E no link, https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/101653

• 5.2.15.6.26 A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações de callbacks.

o A comprovação deste item, encontra-se em documento oficial do fabricante que pode ser acessado via link: https://www.checkpoint.com/defense/advisories/public/2016/cpai2016-0723.html/

5.2.15.6.31 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

o Para comprovação desse item, ver página 293 e 294 do arquivo CP_R81_Quantum_SecurityManagement_AdminGuide enviado na documentação técnica. Conforme imagem abaixo.

Tal comprovação pode ser observada via documento oficial do fabricante no link: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101553. Conforme imagem abaixo:

Ver também página 5 do documento oficial do fabricante, via link: https://www.checkpoint.com/downloads/products/sandblast-network-

solution-brief.pdf . Conforme imagem abaixo:

o E, por último, ver também página 30 do documento oficial do fabricante, via link:https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/105675/FILE/CP_R81.10_ThreatPrevention_AdminGuide.pdf. Conforme imagem abaixo:

• 5.2.15.6.32 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos

o A comprovação deste item pode ser observada na imagem abaixo, podendo ser acessada na documentação oficial do fabricante via link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

5.2.15.6.34 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt,.pptx), arquivos java (.jar e class), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox.

o A comprovação e atendimento deste item segue na imagem abaixo, tal informação pode ser acessada via documentação oficial do fabricante no link: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf •

5.2.15.7 PREVENÇÃO DE AMEAÇAS 0-DAY

o A comprovação deste item, pode ser observada nos documentos oficiais do fabricante nos links abaixo: https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf;
https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/108955/FILE/CP_SandBlast_Agent_AdminGuide.pdf.
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/101653

III.- DOS PRINCÍPIOS DO MENOR PREÇO, DA RAZOABILIDADE E DA MELHOR VANTAGEM.

A licitação pública tem como finalidade atender um INTERESSE PÚBLICO, de forma que seus critérios devem ser observados por todos os participantes em estado de IGUALDADE, para que seja possível a obtenção da PROPOSTA MAIS VANTAJOSA.

A licitação é um procedimento administrativo disciplinado por lei e por um ato administrativo prévio, que determina critérios objetivos de seleção de uma proposta de contratação economicamente mais atrativa, com observância ao princípio da isonomia, conduzido por um órgão dotado de competência específica.

Ademais, a observância à necessidade basilar de obter a proposta mais vantajosa é expressamente regulado pelo Art. 3º, da Lei nº 8.666/93, haja vista que acaba por conceder tratamento isonômico e, consequentemente, competitividade ao certame, senão veja-se:

Art. 3o A licitação destina-se a garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos. (Grifos nossos)

Portanto, é correto reconhecer que a Empresa NETWORK atende as exigências técnicas constantes do Edital e escolhê-la como a proposta

mais vantajosa para esse Órgão evidenciando-se alinhamento com os princípios elencados no artigo acima.

A proposta da NETWORK, que é R$ 718.000,00 (setecentos e dezoito mil reais) mais econômica que a ofertada pela Empresa Recorrente, cuja aceitação daquele Recurso afrontaria o acima transcrito Art. 3º, da Lei nº 8.666/93, onerando injustificadamente esse Órgão.

Afinal, trata-se de ato com fulcro no próprio princípio da finalidade, da eficiência e da razoabilidade, pois acaba por despender menos recursos financeiros pela mesma solução.

A esse propósito, insta trazer à baila a lição do saudoso professor e magistrado Hely Lopes Meirelles, que assim assevera:

(...) todo ato administrativo, de qualquer autoridade ou Poder, para ser legítimo e operante, há que ser praticado em conformidade com a norma legal pertinente (princípio da legalidade), com a moral da instituição (princípio da moralidade), com a destinação pública própria (princípio da finalidade), com a divulgação oficial necessária (princípio da publicidade) e com presteza e rendimento funcional (princípio da eficiência). Faltando, contrariando ou desviando-se desses princípios básicos, a Administração Pública vicia o ato, expondo-o a anulação por ela mesma ou pelo Poder Judiciário, se requerida pelo interessado. (in Direito Administrativo Brasileiro, 34ª Edição, 2008, Editora Malheiros, São Paulo, pg. 716). (Grifos nossos)

A conduta do agente responsável pela Licitação mostrou-se absolutamente regular, atendendo aos princípios previstos na lei das licitações, assim como do Edital, ou seja, princípio do menor preço, da razoabilidade e da melhor vantagem.

Tem-se que a Empresa ora recorrente, de maneira temerária e sem fundamentação legal ou doutrinária, paralisa e inviabiliza o regular desenvolvimento do procedimento licitatório em destaque, em total afronta aos bons costumes a celeridade dos atos administrativos a serem praticados por esse Órgão.

Com sabedoria, o ilustre doutrinário Celso A. Bandeira de Mello afirma que "A licitação é o procedimento destinado à seleção da melhor proposta dentre as apresentadas por aqueles que desejam contratar com administração pública". Como dito anteriormente, o Sr. Pregoeiro atentou aos princípios do instrumento convocatório e do julgamento objetivo, o que significa procurar razões de fato para sustentar sua escolha ou decisão, ou seja, julgamento sustentado no que está previsto em Edital.

IV.- DOS PEDIDOS.

Em face das razões expostas, a presente Empresa, NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA., requer deste Sr. Pregoeiro:

a) NEGUE provimento ao Recurso Administrativo interposto pela Empresa, IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI, para manter na íntegra a r. decisão que consagrou vencedora a Empresa, NETWORK, que faz com base nas contrarrazões acima, nos princípios do menor preço, da razoabilidade e da melhor vantagem;

b) Julgar fundamentadas as contrarrazões ora apresentadas, mantendo a declaração de habilitação da Empresa NETWORK no PREGÃO ELETRÔNICO Nº 4.005/2022- CPL/MP/PGJ, por satisfazer todos os requisitos previstos no respectivo Edital e nas demais normas atinentes a administração pública.

Termos em que, Pede e espera Natural Deferimento.

Enfatiza-se que tanto as intenções recursais quanto às razões e contrarrazões propriamente ditas, em prol da transparência dos atos administrativos, foram devidamente disponibilizados, para acesso amplo e irrestrito, no sítio eletrônico desta Instituição no endereço <**https://www.mpam.mp.br/servicos/licitacoes/licitacoes-em-andamento/47-licitacoes/pregao-eletronico-em-andamento/15018-pe-4005-2022-cpl-mp-pgj-firewall-de-proxima-geracao-em-alta-disponibilidade**>.

É o que, em síntese, cabe relatar.

3. DAS RAZÕES DE DECIDIR

Vale ressaltar, em caráter preliminar, que o Pregoeiro conduziu o certame sob os parâmetros dos princípios e regras legais que disciplinam o procedimento licitatório, estabelecidos quer na **Lei n.º 8.666/1993,** Lei de Licitações e Contratos Administrativos, quer na **Lei n.º 10.520/2002**, Lei do Pregão, quer no **Decreto n.º 10.024/2019**, que regulamenta o pregão, na forma eletrônica.

Nesse sentido, lembremos que o dever administrativo de adotar critérios claros, objetivos e legais durante a análise das documentações dos concorrentes em uma licitação decorre da obrigação da Administração Pública manter plena transparência de seus atos, a fim de definir qual a licitante reúne condições de qualificação técnica, jurídica, fiscal e econômica indispensáveis à garantia do cumprimento de seus deveres, sem desviar-se da observância necessária do princípio da igualdade entre os licitantes, estimulando o caráter competitivo da licitação, constante no artigo 3.º da Lei n.º 8.666/93, abaixo disposto:

> "*A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da* ***legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório****, do julgamento objetivo e dos que lhes são correlatos." (g.n.)*

Dentre esses princípios, no caso em foco, destaca-se o da ***vinculação ao instrumento convocatório,*** a um, porque esse primado serviu de lastro para toda a construção do inconformismo da licitante vencida; e, a duas, porque corresponde exatamente ao fundamento primeiro das providências adotadas pelo Pregoeiro do certame. Portanto, esse será o norte para as ponderações e conclusões expostas no presente *decisum*, a seguir delineado por fornecedor interessado.

Assim, passamos à análise de mérito.

3.1. Considerações Recurso interposto pela empresa IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87

Oportunamente, há que se destacar que a empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** se insurge quanto à possível desclassificação indevida praticada por este subscrevente na condução do certame.

Inicialmente, informo que no andamento do referido certame, mais especificamente na fase de aceitação de propostas, as mesmas foram devidamente submetidas ao Setor Requisitante, no caso concreto, ao Setor de Infraestrutura e Telecomunicação - SIET. Por sua vez, quanto da análise da proposta e documentos técnicos da empresa, o aludido setor se manifestou da seguinte forma:

PARECER Nº 4.2022.SIET.0775110.2021.015252

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar análise técnica da documentação enviada pela empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA.

2. Análise

O presente parecer se baseia nas disposições do Termo de Referência n. 20.2021.DTIC.0720733.2021.015252, Anexo I ao Edital do certame, SEI 0763629, em seus diversos itens.

A proposta de preço, documento 0772069, informa equipamentos e serviços condizentes com as quantidades e exigências do Termo de Referência. Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo.

Conforme exigência, foram apresentados atestados de capacidade técnica que comprovam, **conjuntamente**, a prestação anterior de serviços de firewall de próxima geração, NGFW, com troughput de 10Gbps, no mínimo. Foram apresentados 03 (três) atestados, disponíveis nas páginas 42, 43, 44 e 45 do documento 0772080, incluindo equipamentos similares e superiores ao objeto deste processo.

3. Conclusão

Após análise dos documentos, com relação à parte técnica, indicamos que a proposta pode ser aceita, dando continuidade aos demais trâmites do processo.

Manaus, 03 de março de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ
Coordenador da Área de Redes

Dessa forma, com base na referida manifestação técnica, este Pregoeiro decidiu classificar e aceitar a proposta da empresa em foco.

Outrossim, considerando que o presente Recurso é de caráter eminentemente técnico, submetemos novamente às ponderações da Recorrente à Assessoria de Segurança Institucional/MPAM, mediante o **MEMORANDO Nº 69.2022.CPL.0772078.2021.015252**. Desta feita, aquele Setor se pronunciou através do **PARECER Nº 9.2022.SIET.0786730.2021.015252**, com a seguinte conclusão:

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar análise técnica do recurso interposto pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** (doc. 0781005) e contrarazões da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54** (doc. 0785538), bem como realizar as devidas considerações sobre o questionamento do **PARECER N. 4.2022.SIET.0775110.2021.015252**.

2. Análise

Quanto ao questionamento do parecer anterior, onde se informa que a "análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo" será realizada durante o recebimento do objeto, cabe esclarecer que este é o trâmite previsto para o recebimento, mas não significa que a solução proposta pela empresa vencedora não foi analisada corretamente ou com o devido cuidado. A análise técnica realizada nesta fase do processo de compra, e que culminou na conclusão do parecer n. 4.2022.SIET.0775110.2021.015252, é baseada nas informações prestadas pela vencedora, bem como nas informações disponíveis nos sites dos fabricantes dos equipamentos. Entretanto, uma análise completa, minuciosa e qualitativa, não é possível apenas através de documentações, precisa ser realizada também na prática.

Quanto ao mencioando pela empresa IT PROTECT sobre a solução proposta pela empresa NETWORK SECURE não ter as capacidades técnicas mínimas solicitadas, informamos que durante a análise realizada sobre a documentação do produto, em comparação com as exigências do Termo de Referência deste processo de compra, para elaboração do parecer n. 4.2022.SIET.0775110.2021.015252, apesar de não estar totalmente explícito no texto do parecer, foram conferidos os itens citados, incluindo os *troughputs* mínimos exigidos, sendo concluído que o equipamento atende ao exigido.

Quanto às contrarrazões técnicas apresentadas pela empresa NETWORK SECURE, informamos que a análise descrita pela empresa sobre os itens da documentação técnica do produto é considerada correta. A documentação disponível sobre o produto ofertado indica que o modelo atende aos requisitos mínimos do Termo de Referência deste processo. Não obstante, durante o recebimento todas as exigências serão conferidas e analisadas minuciosamente para posterior emissão do Termo de Recebimento Definitivo.

3. Conclusão

Após análise dos documentos, com relação à parte técnica, mantemos a indicação de que a proposta da empresa vencedora, NETWORK SECURE, pode ser aceita, dando continuidade aos demais trâmites do processo.

Manaus, 21 de março de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ
Coordenador da Área de Redes

Ao cotejar os motivos fundantes expostos nas Razões do Recurso (doc. 0781005), observa-se não haver sido trazida qualquer razão jurídica diferenciada ou nova que pudesse ensejar a retificação do entendimento deste Pregoeiro, motivo porquanto se aplica ao caso o princípio da hermenêutica jurídica ***"ubi eadem ratio, ibi eadem legis dispositio",*** que consagra o entendimento no sentido de que "*onde existe a mesma razão fundamental, prevalece a mesma regra de Direito*".

Por esses motivos, não havendo sido juntados, para efeito de análise do pedido de recurso administrativo, elementos jurídicos que ensejassem a alteração da *ratio decidendi* que culminou na desclassificação da empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87,** mantém-se a decisão por seus próprios fundamentos.

Nesse desiderato, esvaída de qualquer lastro fático e/ou jurídico as razões de irresignação, passo a consequente e necessária conclusão quanto ao presente.

4. DA CONCLUSÃO

Portanto, com lastro nas razões expostas, sobretudo na manifestação técnica do Setor de Infraestrutura e Telecomunicações (PARECER Nº 9.2022.SIET. 0786730.2021.015252), por entender que os requisitos e princípios que permeiam os atos da Administração Pública foram devidamente observados por este **PREGOEIRO** quando da análise da proposta e, afastadas as razões apresentadas no ***item 1, "a"***, este subscrevente decide pela **MANUTENÇÃO** do posicionamento inicial e, por conseguinte, **aceitação da proposta** e **habilitação** da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ N.º 05.250.796/0001-54, a fim de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019.

Desta feita, os autos devem ser submetidos à análise e manifestação do ilustre **Ordenador de Despesas**, a fim de que, caso assim entenda, mantenha a decisão proferida por este Pregoeiro, segundo inteligência do § 4.º, do art. 109, da Lei n.° 8.666/93, combinado com o artigo 4°, incisos XXI e XXII da Lei n.° 10.520/2002 e artigo 13, IV do Decreto nº 10.024/2019, e proceda, se entender cabível, à manutenção da *decisum* e adjudicação e homologação do objeto do certame à **empresa vencedora (NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ N.º 05.250.796/0001-54, no valor global de **R$ 2.478.052,85 - doc. 0772069**).

É a decisão.

Manaus, 23 de março de 2022.

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Pregoeiro designado pela PORTARIA N° 167/2022/SUBADM

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 23/03/2022, às 12:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0781007** e o código CRC **A94F6168**.

RELATÓRIO DE LICITAÇÃO Nº 6.2022.CPL.0777809.2021.015252

Excelentíssimo Senhor Subprocurador-Geral de Justiça,

O Pregoeiro, **EDSON FREDERICO LIMA PAES BARRETO**, designado por força da PORTARIA N° 229/2022/SUBADM, datada de 11.02.2022, doc. 0772159, vem APRESENTAR e SUBMETER à vossa apreciação relatório circunstanciado do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ** (doc. 0763629), do tipo menor preço GLOBAL, concernente ao **Processo SEI n.º 2021.015252**, o qual teve por objeto a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.*

1. DA EVOLUÇÃO DOS AUTOS

A evolução dos autos ocorreu conforme descrição e datas do documento **Histórico do Processo 2021.015252**, disponível no Sistema SEI, em Consultar Andamento.

2. DA PUBLICIDADE

Os Avisos da Licitação foram publicados no *Comprasnet* no dia 07/02/2022, com divulgação prevista para o dia 08/02/2022 (doc. 0765236), no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas – DOMPE, Edição n.º 2306 de 04/02/2022 (doc. 0763623), no matutino local "Jornal do Commercio", Edição n.º 43.475, de 05 a 07/02/2022 (doc. 0777812) e no sítio institucional do MP/AM, www.mpam.mp.br.

3. DA SESSÃO PÚBLICA

3.1. Do Credenciamento – As licitantes credenciaram-se na Secretaria de Logística e Tecnologia de Informação – SLTI, do Ministério do Planejamento, Orçamente e Gestão, através das regras do sistema *Comprasnet*, site www.comprasgovernamentais.gov.br.

3.2. Da Proposta – As propostas foram enviadas pelos licitantes através da internet desde 08/02/2022 até a data e hora marcada para a abertura da sessão, a saber, dia 21/02/2022, às 10h. (horário de Brasília).

Iniciada a sessão, as propostas foram preliminarmente analisadas conforme prescrição do item 11 do Edital, compatibilizando-as com as especificações contidas no **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252** e no **QUADRO - RESUMO DO PROCESSO DE COMPRA Nº 345.2021.SCOMS.0731246.2021.015252.**

O Pregoeiro advertiu os participantes para que observassem com cautela as disposições concernentes às convocações emitidas e aos prazos previstos para implementação das providências por ele requeridas.

Foi informado, também, que o Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ seria realizado conforme os ditames do Decreto Federal nº 10.024, de 20 de setembro de 2019.

Nessa etapa, ainda, recomendou-se aos interessados que considerassem atentamente, quando da oferta dos lances, as condições de fornecimento dos materiais e/ou prestação dos serviços reclamados, uma vez que aquelas deveriam ser rigorosamente cumpridas quando da execução, com destaque aos prazos estabelecidos, sob pena de incorrer-se em infração administrativa.

Nessa etapa, alertou-se, ainda, a observação dos requisitos formais da proposta.

3.3. Da Fase de Lances – Aberta a disputa, os interessados tiveram a oportunidade de propor, em lances, condições mais favoráveis que as primeiras, o que ocorreu de fato.

3.4. Da Aceitação – Logo em seguida, o Pregoeiro convocou para apresentação a proposta da licitante mais bem colocada na ordem de classificação dos lances, conforme subitem 10.1 do instrumento convocatório.

Ato seguinte, devidamente recebida a proposta da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54 e os documentos de habilitação, os memos foram devidamente juntados aos autos e submetidos ao crivo do i. Setor de Infraestrutura e Telecomunicação - SIET, nos termos do **MEMORANDO Nº 69.2022.CPL.0772078.2021.015252.**

Ato seguinte, no dia 03/03/2022, recebemos resposta do **Setor de Infraestrutura e Telecomunicação - SIET**, no sentido de **aceitação** da proposta e preenchimento dos requisitos técnicos de habilitação da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54, consoante se conclui pelo **PARECER Nº 4.2022.SIET.0775110.2021.015252.**

Daí, por atender aos prazos fixados e, também, a todos os aspectos formais reclamados pela Administração, inclusive figurando abaixo do valor estimado pela Administração quando comparado ao **QUADRO - RESUMO DO PROCESSO DE COMPRA Nº 345.2021.SCOMS.0731246.2021.015252** e **NOTA DE AUTORIZAÇÃO DE DESPESAS/ADJUDICAÇÃO - NAD Nº 375.2021.DOF - ORÇAMENTO.0744829.2021.015252**, fora devidamente **aceita** pelo Pregoeiro a Proposta Final da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54, documento SEI n.º 0772069, no valor global de **R$ 2.478.052,85** ***(dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos),*** conforme registrado na **ATA DE REALIZAÇÃO** (doc. 0777805) do certame em cotejo.

Oportunamente, registre-se que ocorreu uma divergência no documento Resultado por Fornecedor (doc. 0777806) e o constante na Proposta Final (doc. 0772069), visto que a empresa necessitou

adequar sua proposta em função da dízima periódica, todavia, consiste numa falha meramente formal deste Pregoeiro deixar de lançar no sistema no campo de valor negociado, valendo-se o valor registrado na proposta escrita, sendo este o valor a ser levado em consideração para a contratação, conforme cosnta na Minuta de Despacho de Homologação (doc. 0777810).

Nesse ponto, permita-me abrir um parêntese para esclarecer que este Pregoeiro deixou de exigir a comprovação de exequibilidade, considerando que as 3 (três) primeiras propostas, permaneceram abaixo de R$ 3,3 milhões, conforme Ordem de Classificação (doc. 0777807), o que demonstra, salvo melhor juízo, que o valor orçado e estimado pela Administração via **QUADRO - RESUMO DO PROCESSO DE COMPRA Nº 345.2021.SCOMS.0731246.2021.015252** figura bem superior ao praticado realmente no mercado.

Outrossim, no decorrer da sessão pública observou-se uma ampla DIFERENÇA na comparação das propostas iniciais inseridas no Comprasnet *versus* o valor final do melhor lance, conforme se extrai na Ata da Sessão detalhado abaixo, vejamos:

1. **Fornecedor:** 05.250.796/0001-54 - NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, **Proposta Inicial:** R$ 3.878.880,00; Proposta após os lances: R$ 2.478.052,85;
2. **Fornecedor:** 01.134.191/0007-32 - SERVIX INFORMATICA LTDA. **Proposta Inicial:** R$ 6.934.080,0000; **Proposta após os lances:** R$ 2.855.000,00;
3. **Fornecedor:** 23.378.923/0001-87 - IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL. **Proposta Inicial:** R$ 5.760.000,00; **Proposta após os lances:** R$ 3.278.000,00;

Desta forma, fazendo-se a média dos melhores lances inseridos no Sistema Comprasnet de todas as participantes, vide Ata da Sessão (doc. 0615260), obtemos o **valor médio de R$ 2.870.350,95** ***(dois milhões, oitocentos e setenta mil trezentos e cinquenta reais e noventa e cinco centavos)***. Portanto, concluímos que o valor de R$ 2.478.052,85 *(dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos)* da empresa melhor classificada (**NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54) é perfeitamente plausível e com numerários aproximados, caracterizando-se como uma política de vendas comuns das empresas dos ramos. Ademais, aplicando-se por analogia os percentuais de inexequibilidade das obras e serviços (previsto no art. 47, § 1.º, "b" da Lei n.º 8.666/93), obtemos um **valor como exequível mínimo** de **R$ 2.099.245,67** *(dois milhões, noventa e nove mil duzentos e quarenta e cinco reais e sessenta e sete centavos)*, logo, o valor proposto pela empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54 **mantém-se** dentro do parâmetro ora apresentado.

3.5. Da Habilitação

Na sequência, este subscrevente examinou a documentação de habilitação das licitantes, enviadas no mesmo momento da cadastro da proposta, seguindo-se a orientação do subitem 6.1. do Edital.

Recebidos os documentos, procedeu-se à fase de julgamento das condições de habilitação, utilizando-se, inclusive, das informações do **Sistema de Cadastro de Fornecedores – SICAF** da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54, dentre eles, CRC - Comprasnet, Relatório Nível I - Credenciamento e SICAF - Comprasnet (doc. 0772288);

Nessa etapa, verificou-se a autenticidade das certidões negativa de débitos mediante SICAF, bem como da de ausência de distribuição de feitos de falência ou recuperação judicial, junto à Justiça Estadual de domicílio da licitante (doc. 0772080, pág. 41). Da mesma sorte procedeu-se com os demais documentos de habilitação das interessadas que permitiam a convalidação eletrônica, conforme consta dos autos.

Os documentos de habilitação (doc. 0614966) interpostos gozavam da possibilidade, em sua grande maioria, com exceção dos Atestados da Hapvida e Pague Menos (doc. 0772080, pág. 42 e 43-44, respectivamente) de convalidação eletrônica via internet, razão pela qual o Pregoeiro convocou a empresa para envio dos originais e/ou cópias autenticadas, tendo a mesma devidamente atendido no prazo fixado.

Passo seguinte, verificou-se as condições das licitantes quanto à ausência de sanções pela Administração Pública, no SICAF do *Comprasnet*, bem como na Relação de Empresas com Sanção Administrativa em Vigor, do **TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS – TCE** , na Relação de Licitantes Inidôneos do **TRIBUNAL DE CONTAS DA UNIÃO – TCU,** na Lista de Empresas Suspensas/Impedidas da **COMISSÃO GERAL DE LICITAÇÃO DO ESTADO DO AMAZONAS – CGL**, no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), da **CONTROLADORIA GERAL DA UNIÃO – CGU**, no Cadastro Nacional de Condenações Civis por Ato de Improbidade Administrativa (CNCIA) do **CONSELHO NACIONAL DE JUSTIÇA – CNJ** e na Relação de pessoas jurídicas impedidas de contratar com a Administração Pública da **SEFAZ-AM**, não sendo constatados registros que indicassem restrições à contratação.

Oportunamente, registre-se que com o objetivo de atender aos princípios de simplificação e racionalização de serviços públicos digitais, presentes nas Leis n.ºs 12.965/14 e 13.460/18; e no Decreto nº 8.638/2016, o **Tribunal de Contas da União** passou a disponibilizar ferramenta que permite a consulta consolidada de pessoas jurídicas que reúne, em um só lugar – e em relatório único, contendo as Licitantes Inidôneos do TCU, CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade do CNJ; Cadastro Nacional de Empresas Inidôneas e Suspensas e CNEP - Cadastro Nacional de Empresas Punidas ambos do Portal da Transparência. Assim, este subscrevente promoveu a juntada da Consulta Consolidada de Pessoa Jurídica da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54 (doc. 0772291);

Concluída a análise dos documentos de habilitação conforme item 11 do instrumento convocatório e, estando todos conforme e de acordo com a previsão editalícia, o Pregoeiro decidiu **HABILITAR** a empresa em foco.

4. DA MANIFESTAÇÃO DE INTENÇÃO DE RECURSO

Logo após, concedeu-se o prazo de **30 (trinta) minutos** para registro de intenção de recurso por parte das demais licitantes, ocasião em que o representante da empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87**, **manifestou intenção recursal (doc. 0781002)**, conforme se extrai da **ATA DE REALIZAÇÃO** (doc. 0777805).

5. DA DECISÃO DO RECURSO

Deste modo, apresentanda as contrarrazões no prazo fixado e afastadas as razões recursais da licitante recorrente, decidiu este subscrevente manter a decisão outrora prolatada, pelas razões expostas na **DECISÃO Nº 14.2022.CPL.0781007.2021.015252**, no sentido de **MANTER as**

decisões anteriormente prolatadas, quais sejam, de plena **aceitação** da proposta ofertada, bem como da habilitação da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54**,** a fim de dar seguimento ao certame, nos termos art. 17, inciso VII, do Decreto nº 10.024/2019.

6. DA ECONOMICIDADE

Destaque-se que o valor estimado para a contratação de que trata o objeto do certame, excluindo os grupos/itens fracassados ou desertos foi de **R$ 5.828.425,84** *(cinco milhões, oitocentos e vinte e oito mil quatrocentos e vinte e cinco reais e oitenta e quatro centavos)*, sendo que o valor total da adjudicação decorrente do êxito da licitação em comento foi de **R$ 2.478.052,85** *(dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos),* consoante **RESULTADO POR FORNECEDOR** (doc. 0777808). Logo, a realização deste Pregão significou uma **economia de R$ 3.350.372,99** *(três milhões, trezentos e cinquenta mil trezentos e setenta e dois reais e noventa e nove centavos)*, aos cofres públicos, ou seja, uma **redução de aproximadamente 57,48%** do valor estimado pela Administração.

É o Relatório.

Manaus, 23 de março de 2022.

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Pregoeiro designado pela PORTARIA N° 229/2022/SUBADM

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 23/03/2022, às 12:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0777809** e o código CRC **0F7D60D8**.

MINUTA Nº DESPACHO DE ADJUDICAÇÃO E HOMOLOGAÇÃO

PROCESSO SEI N.º 2021.015252

Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ

H O M O L O G A Ç Ã O

CONSIDERANDO a solicitação inicial constante do **OFÍCIO Nº 108.2021.DTIC.0692180.2021.015252**, bem como o teor do último **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;**

CONSIDERANDO o disposto na Lei, na Ata da Sessão Pública de realização do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ** e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 21/02 a 23/03/2022, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;*

CONSIDERANDO o **RELATÓRIO DE LICITAÇÃO Nº 6.2022.CPL. 0777809.2021.015252**, no qual demonstra que a realização deste Pregão significou uma **economia de R$ 3.350.372,99 *(três milhões, trezentos e cinquenta mil trezentos e setenta e dois reais e noventa e nove centavos)***, aos cofres públicos, ou seja, uma **redução de aproximadamente 57,48%** do valor estimado pela Administração.

CONSIDERANDO o teor da Lei Federal n.º 10.520, de 17.07.2002, do Ato PGJ n.º 322 e 389/2007, do Decreto Federal n.º 10.024/19 e Decreto Estadual n.º 24.818/2005, de 27/01/2005;

CONSIDERANDO a manifestação de intenção recursal formulada pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** , no prazo e condições de que trata o art. 4.º, incisos XVIII e XX, da Lei Federal n.º 10.520/2002;

CONSIDERANDO o exposto na **DECISÃO Nº 14.2022.CPL.0781007.2021.015252**, em que o Pregoeiro **CONHECEU** da oposição formulada e, no mérito, **NEGOU PROVIMENTO**, portanto, à manifestação de inconformismo submetida e, ao final, deliberou pela **MANUTENÇÃO** do posicionamento inicial e, por conseguinte, aceitação da proposta ofertada e habilitação da empresa licitante **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA** , inscrita no CNPJ nº 05.250.796/0001-54, a fim

de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019.

CONSIDERANDO, por derradeiro, o **DESPACHO/DECISÃO N.º ___.2022.SUBADM.** que acatou/refutou as razões da deliberação retromencionada;

R E S O L V E:

I – **ADJUDICAR** o objeto do certame à empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54, no **valor global** de **R$ 2.478.052,85** ***(dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos)***;

II – **HOMOLOGAR** o resultado do procedimento licitatório, referente ao **PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ**, em consonância com a ata de realização do cotejo e demais documentações complementares;

III – À **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, para as providências cabíveis;

IV – Após, à **DIRETORIA DE ORÇAMENTO E FINANÇAS**, para prosseguimento do feito.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DO SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), XX de março de 2022.

GÉBER MAFRA ROCHA

Subprocurador-Geral de Justiça para Assuntos Administrativos

Ordenador de Despesas

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 23/03/2022, às 12:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0777810** e o código CRC **D785A508**.

DESPACHO Nº 26.2022.CPL.0777811.2021.015252

OBJETO: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual.

CONSIDERANDO a realização do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ, iniciado no dia 21 de fevereiro e encerrado no dia 23 de março do corrente ano;

CONSIDERANDO que, dentre os requisitos de validade, o resultado do certame necessita da adjudicação e homologação pelo(a) Ordenador(a) de Despesas desta Procuradoria-Geral de Justiça, nos termos da Lei Federal n.º 10.520, de 17.07.2002, do Ato PGJ n.º 389/2007, Decreto Federal n.º 10.024/2019, e do Decreto Estadual n.º 24.818/2005, face à apresentação de recursos administrativos contra decisão deste Pregoeiro;

CONSIDERANDO a manifestação de intenção recursal formulada pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87**, no prazo e condições de que trata o art. 4.º, incisos XVIII e XX, da Lei Federal n.º 10.520/2002;

CONSIDERANDO o exposto na **DECISÃO Nº 14.2022.CPL.0781007.2021.015252**, em que o Pregoeiro **conheceu das irresignações apresentada pela empresa IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** . Lado outro após exame das razões recursais formuladas pela recorrente susomencionada, este Pregoeiro decidiu, no mérito, **NEGAR PROVIMENTO**, portanto, às manifestações de inconformismo submetidas e, ao final, pela **MANUTENÇÃO** do posicionamento inicial e, por conseguinte, aceitação da proposta ofertada e habilitação da empresa licitante **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA** , inscrita no CNPJ nº 05.250.796/0001-54, a fim de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019.

Encaminhem-se os autos do Procedimento Interno em epígrafe ao Exmo. Sr. Dr. **SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** , para fins de análise, adjudicação e homologação do certame licitatório em espeque à empresa declarada vencedora, caso assim entenda.

Manaus, 23 de março de 2022.

Edson Frederico Lima Paes Barreto

Presidente da Comissão Permanente de Licitação

Ato PGJ n.º 185/2021 - DOMPE, Ed. 2169, de 09.07.2021

Pregoeiro designado pela PORTARIA N° 229/2022/SUBADM

Matrícula n.º 001.042-1A

Documento assinado eletronicamente por **Edson Frederico Lima Paes Barreto**, **Presidente da Comissão Permanente de Licitação - CPL**, em 23/03/2022, às 12:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0777811** e o código CRC **0BDE1CFC**.

DECISÃO Nº 2.2022.01AJ-SUBADM.0789171.2021.015252

Autos nº 2021.0015252

Assunto: Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.

Retornam, mais uma vez, os autos iniciados pelo Ofício 108 (0692180), emanado da Diretoria de Tecnologia da Informação e Comunicação - DTIC, solicitando Contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, descritos e qualificados conforme as especificações e as condições constantes no Edital e seus anexos.

O Edital do Pregão Eletrônico nº 4.005/2022-CPL/2021-CPL/MP/PGJ foi devidamente publicado(1762689, 0765636, 0763623 0777812), tendo o certame sido iniciado em 01/09/2021, às 10h (horário de Brasília/DF), tendo como objeto a "*contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual., descritos e qualificados conforme as especificações e as condições constantes deste Edital e seus anexos.*". **A licitação teve como critério de julgamento o menor preço por lote único.**

A vencedora do certame foi a empresa NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA, que arrematou o único lote pelo valor de R$ 2.478.052,85 (Dois milhões, quatrocentos e setenta e oito reais, cinquenta e dois reais e oitenta e cinco centavos).

A empresa, IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 23.378.923/0001-87 apresentou **recurso administrativo** sustentando em suas razões (0788241) que o senhor pregoeiro teria habilitado empresa cuja proposta não atenderia aos requisitos do edital, eis que não atenderia o item 5.2.15.10.15 do Termo de Referência

Em síntese, a empresa vencedora não poderia ter tido sua proposta aceita, pois os documentos apresentados não permitiram análise qualitativa própria da fase de habilitação, de modo que pelo menos, seria necessária a realização de diligência para suprir a falha, o que não ocorreu.

Em síntese, na Decisão 14 (0781007), após a análise de todos os pressupostos de admissibilidade e das razões recursais, o pregoeiro, com fundamento no artigo 13, §1º, do Ato PGJ n.º 389/2007, decidiu:

a) **Conhecer** das oposições formuladas pelas empresas **IT PROTECT SERVICOS DE CONSULTORIA EM**

INFORMATICA EIREL, CNPJ: 23.378.923/0001-87, no interesse do Pregão Eletrônico n.º 4.003/2022-CPL/MP/PGJ, pelo qual se busca a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;*

b) Após exame das razões recursais formuladas pela empresa susomencionada no ***subitem "a"***, este Pregoeiro apresenta as motivações que culminaram nas decisões outrora prolatadas e, no mérito, **NEGAR PROVIMENTO**, portanto, à manifestação de inconformismo submetida;

c) **Manter a decisão anteriormente prolatada**, quais sejam, **aceitação da proposta** e **habilitação** da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ N.º 05.250.796/0001-54, a fim de dar seguimento ao certame, nos termos art. 17, inciso VII do Decreto nº 10.024/2019; e

d) Envio dos autos à Autoridade Competente, para fins de análise, manutenção da Decisão supra, adjudicação e homologação do certame licitatório em espeque à empresa declarada vencedora, caso assim entenda, com fundamento no artigo 13, IV do Decreto nº 10.024/2019.

Vieram os autos à SUBADM para nova análise das razões recursais.

Em suma, **o ponto fulcral trazido nas razões recursais fora o suposto não atendimento aos requisitos do edital da proposta trazida pela empresa** NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA, que arrematou o único lote pelo valor de R$ 2.478.052,85 (Dois milhões, quatrocentos e setenta e oito reais, cinquenta e dois reais e oitenta e cinco centavos), a qual sagrou-se vitoriosa no certame.

Nada obstante, constato que, por ocasião do julgamento da proposta, como bem observou o senhor pregoeiro em suas razões de decidir, em se tratando de objeto que por sua natureza deveria obedecer critérios técnicos de informática, fora requisitada manifestação dos setores de Tecnologia da Informação do Ministério Público que assim opinaram:

(Parecer 4 0775110)

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar análise técnica da documentação enviada pela empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA.

2. Análise

O presente parecer se baseia nas disposições do Termo de Referência n. 20.2021.DTIC.0720733.2021.015252, Anexo I ao Edital do certame, SEI 0763629, em seus diversos itens.

A proposta de preço, documento 0772069, informa equipamentos e serviços condizentes com as quantidades e exigências do Termo de Referência. Em tempo oportuno, durante o recebimento, será feita análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo.

Conforme exigência, foram apresentados atestados de capacidade técnica que comprovam, **conjuntamente**, a prestação anterior de serviços de firewall de próxima geração, NGFW, com troughput de 10Gbps, no mínimo. Foram apresentados 03 (três) atestados, disponíveis nas páginas 42, 43, 44 e 45 do documento 0772080, incluindo equipamentos similares e superiores ao objeto deste processo.

3. Conclusão

Após análise dos documentos, com relação à parte técnica, indicamos que a proposta pode ser aceita, dando continuidade aos demais trâmites do processo.

Manaus, 03 de março de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ

Coordenador da Área de Redes

(Parecer 9 0786730)

1. Relatório

Trata-se de pedido da Comissão Permanente de Licitação - CPL para realizar análise técnica do recurso interposto pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** (doc. 0781005) e contrarazões da empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, CNPJ: 05.250.796/0001-54** (doc. 0785538), bem como realizar as devidas considerações sobre o questionamento do **PARECER N. 4.2022.SIET.0775110.2021.015252**.

2. Análise

Quanto ao questionamento do parecer anterior, onde se informa que a "análise minuciosa e qualitativa da solução, para todos os itens do objeto, de acordo com todas as exigências do Termo" será realizada durante o recebimento do objeto, cabe esclarecer que este é o trâmite previsto para o recebimento, mas não significa que a solução proposta pela empresa vencedora não foi analisada corretamente ou com o devido cuidado. A análise técnica realizada nesta fase do processo de compra, e que culminou na conclusão do parecer n. 4.2022.SIET.0775110.2021.015252, é baseada nas informações prestadas pela vencedora, bem como nas informações disponíveis nos sites dos fabricantes dos equipamentos. Entretanto, uma análise completa, minuciosa e qualitativa, não é possível apenas através de documentações, precisa ser realizada também na prática.

Quanto ao mencioando pela empresa IT PROTECT sobre a solução proposta pela empresa NETWORK SECURE não ter as capacidades técnicas mínimas solicitadas, informamos que durante a análise realizada sobre a documentação do produto, em comparação com as exigências do Termo de Referência deste processo de compra, para elaboração do parecer n. 4.2022.SIET.0775110.2021.015252, apesar de não estar totalmente explícito no texto do parecer, foram conferidos os itens citados, incluindo os *troughputs* mínimos exigidos, sendo concluído que o equipamento atende ao exigido.

Quanto às contrarrazões técnicas apresentadas pela empresa NETWORK SECURE, informamos que a análise descrita pela empresa sobre os itens da documentação técnica do produto é considerada correta. A documentação disponível sobre o produto ofertado indica que o modelo atende aos requisitos mínimos do Termo de Referência deste processo. Não obstante, durante o recebimento todas as exigências serão conferidas e analisadas minuciosamente para posterior emissão do Termo de Recebimento Definitivo.

3. Conclusão

Após análise dos documentos, com relação à parte técnica, mantemos a indicação de que a proposta da empresa vencedora, NETWORK SECURE, pode ser aceita, dando continuidade aos demais trâmites do processo.

Manaus, 21 de março de 2022.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

THEO FERREIRA PARÁ

Coordenador da Área de Redes

Desta feita, esclareceu-se que a proposta vencedora fora, com efeito, analisada de forma qualitativa, sendo tal verificação baseada na confrontação das informações prestadas pela empresa vencedora em sua proposta com pesquisa de mercado acerca dos componentes objeto da proposição, constatando-se, como se viu, pela compatibilidade mínima desses objetos com o que se visa adquirir no edital, inexistindo mácula no procedimento que ensejasse na inabilitação pretendida, sendo de direito a homologação do certame para a empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, tal qual

adequadamente procedeu o senhor pregoeiro.

Quanto à pretendida determinação de diligência para viabilizar a análise da proposta aviada pela empresa NETWORK, é de se ressaltar que isto, longe de ser uma obrigação, é uma faculdade do pregoeiro de modo que sequer fora necessário ordená-la para estudo da proposta pela comissão licitante, pois, como se viu, de pronto fora apresentado parecer pelo representante da área de TI do Ministério Público, a atestar a compatibilidade da proposta com o instrumento convocatório da licitação.

Nesse sentido: *É facultada à Comissão ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar originariamente da proposta* (art. 43, §3º, da Lei nº 8.666/93).

Com essas considerações, nos termos do artigo 109, §4.º, da Lei n.º 8.666/93 c/c art. 4°, XXI e XXII da Lei n.° 10.520/2002 e art. 13, IV do Decreto nº 10.024/2019, **NEGO PROVIMENTO ao recurso administrativo interposto por IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87,** mantendo em todos os seus termos a decisão inicialmente proferida pelo pregoeiro do certame.

À Comissão Permanente de Licitação - CPL para as providências subsequentes.

GABINETE DO SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), 24 de março de 2022.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 24/03/2022, às 14:08, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0789171** e o código CRC **4E1C4D52**.

DESPACHO Nº 73.2022.01AJ-SUBADM.0789286.2021.015252

PROCESSO SEI N.º 2021.015252

Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ

H O M O L O G A Ç Ã O

CONSIDERANDO a solicitação inicial constante do **OFÍCIO Nº 108.2021.DTIC.0692180.2021.015252**, bem como o teor do último **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;**

CONSIDERANDO o disposto na Lei, na Ata da Sessão Pública de realização do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ** e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 21/02 a 23/03/2022, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;*

CONSIDERANDO o **RELATÓRIO DE LICITAÇÃO Nº 6.2022.CPL. 0777809.2021.015252**, no qual demonstra que a realização deste Pregão significou uma **economia de R$ 3.350.372,99 *(três milhões, trezentos e cinquenta mil trezentos e setenta e dois reais e noventa e nove centavos)***, aos cofres públicos, ou seja, uma **redução de aproximadamente 57,48%** do valor estimado pela Administração.

CONSIDERANDO o teor da Lei Federal n.º 10.520, de 17.07.2002, do Ato PGJ n.º 322 e 389/2007, do Decreto Federal n.º 10.024/19 e Decreto Estadual n.º 24.818/2005, de 27/01/2005;

CONSIDERANDO a manifestação de intenção recursal formulada pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** , no prazo e condições de que trata o art. 4.º, incisos XVIII e XX, da Lei Federal n.º 10.520/2002;

CONSIDERANDO o exposto na **DECISÃO Nº 14.2022.CPL.0781007.2021.015252**, em que o Pregoeiro **CONHECEU** da oposição formulada e, no mérito, **NEGOU PROVIMENTO**, portanto, à manifestação de inconformismo submetida e, ao final, deliberou pela **MANUTENÇÃO** do posicionamento inicial e, por conseguinte, aceitação da proposta ofertada e habilitação da empresa licitante **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA** , inscrita no CNPJ nº 05.250.796/0001-54, a fim

de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019.

CONSIDERANDO, por derradeiro, o **DESPACHO/DECISÃO N.º ___.2022.SUBADM.** que acatou/refutou as razões da deliberação retromencionada;

R E S O L V E:

I – **ADJUDICAR** o objeto do certame à empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54, no **valor global** de **R$ 2.478.052,85** ***(dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos)****;*

II – **HOMOLOGAR** o resultado do procedimento licitatório, referente ao **PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ**, em consonância com a ata de realização do cotejo e demais documentações complementares;

III – À **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, para as providências cabíveis;

IV – Após, à **DIRETORIA DE ORÇAMENTO E FINANÇAS**, para prosseguimento do feito.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DO SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), 24 de março de 2022.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ordenador de Despesas

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 24/03/2022, às 14:08, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0789286** e o código CRC **85B41561**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DESPACHO Nº 75.2022.01AJ-SUBADM.0790316.2021.015252

PROCESSO SEI N.º 2021.015252

Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ

H O M O L O G A Ç Ã O

CONSIDERANDO a solicitação inicial constante do **OFÍCIO Nº 108.2021.DTIC.0692180.2021.015252**, bem como o teor do último **TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;**

CONSIDERANDO o disposto na Lei, na Ata da Sessão Pública de realização do **Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ** e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 21/02 a 23/03/2022, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a *contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;*

CONSIDERANDO o **RELATÓRIO DE LICITAÇÃO Nº 6.2022.CPL. 0777809.2021.015252**, no qual demonstra que a realização deste Pregão significou uma **economia de R$ 3.350.372,99 *(três milhões, trezentos e cinquenta mil trezentos e setenta e dois reais e noventa e nove centavos)***, aos cofres públicos, ou seja, uma **redução de aproximadamente 57,48%** do valor estimado pela Administração.

CONSIDERANDO o teor da Lei Federal n.º 10.520, de 17.07.2002, do Ato PGJ n.º 322 e 389/2007, do Decreto Federal n.º 10.024/19 e Decreto Estadual n.º 24.818/2005, de 27/01/2005;

CONSIDERANDO a manifestação de intenção recursal formulada pela empresa **IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87** , no prazo e condições de que trata o art. 4.º, incisos XVIII e XX, da Lei Federal n.º 10.520/2002;

CONSIDERANDO o exposto na **DECISÃO Nº 14.2022.CPL.0781007.2021.015252**, em que o Pregoeiro **CONHECEU** da oposição formulada e, no mérito, **NEGOU PROVIMENTO**, portanto, à manifestação de inconformismo submetida e, ao final, deliberou pela **MANUTENÇÃO** do posicionamento inicial e, por conseguinte, aceitação da proposta ofertada e habilitação da empresa licitante **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA** , inscrita no CNPJ nº 05.250.796/0001-54, a fim de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019.

CONSIDERANDO, por derradeiro, o **DECISÃO Nº 2.2022.01AJ-SUBADM.0789171.2021.015252.** que refutou as razões da deliberação retromencionada;

R E S O L V E:

I – **ADJUDICAR** o objeto do certame à empresa **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**, inscrita no CNPJ nº 05.250.796/0001-54, no **valor global** de **R$ 2.478.052,85** ***(dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos)****;*

II – **HOMOLOGAR** o resultado do procedimento licitatório, referente ao **PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ**, em consonância com a ata de realização do cotejo e demais documentações complementares;

III – À **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, para as providências cabíveis;

IV – Após, à **DIRETORIA DE ORÇAMENTO E FINANÇAS**, para prosseguimento do feito.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DO SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), 25 de março de 2022.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ordenador de Despesas

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 25/03/2022, às 13:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0790316** e o código CRC **6E9C8FD7**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

CERTIDÃO Nº 1.2022.01AJ-SUBADM.0790333.2021.015252

Certifico, na presente data, que, por conter erro material o qual não pôde ser corrigido via operação própria no sistema SEI, elaborou-se, em substituição ao despacho 73, o despacho 75, este livre de equívocos de digitação e/ou ortografia.

O referido é verdade e dou fé.

Manaus, 25 de março de 2022.

JULIA FERREIRA SARDINHA
Agente Técnico Jurídico - SUBADM

Documento assinado eletronicamente por **Júlia Ferreira Sardinha**, **Assessor(a) Jurídico(a)**, em 25/03/2022, às 14:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0790333** e o código CRC **4065707E**.

CONSIDERANDO a manifestação de intenção recursal formulada pela empresa DESKGRAPHICS REALIZE TECNOLOGIA LTDA., CNPJ N.º 10.537.193/0001-78, no prazo e condições de que trata o art. 4.º, incisos XVIII e XX, da Lei Federal n.º 10.520/2002;

CONSIDERANDO o exposto na DECISÃO Nº 11.2022.CPL.0777511.2020.019936, em que o Pregoeiro CONHECEU da oposição formulada e, no mérito, NEGOU PROVIMENTO, portanto, à manifestação de inconformismo submetida e, ao final, deliberou pela MANUTENÇÃO do posicionamento inicial e, por conseguinte, aceitação da proposta ofertada e habilitação da empresa licitante MAPDATA TECNOLOGIA, INFORMÁTICA E COMÉRCIO LTDA., inscrita no CNPJ nº 66.582.784/0001-11, a fim de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019;

CONSIDERANDO, por derradeiro, a DECISÃO Nº 3.2022.01AJ-SUBADM.0789787.2020.019936, em que se refutou as razões da deliberação retromencionada,

RESOLVE:

I – ADJUDICAR o objeto do certame à empresa MAPDATA TECNOLOGIA, INFORMÁTICA E COMÉRCIO LTDA., inscrita no CNPJ nº 66.582.784/0001-11, no valor global de R$ 99.535,20 (noventa e nove mil quinhentos e trinta e cinco reais e vinte centavos);

II – HOMOLOGAR o resultado do procedimento licitatório, referente ao PREGÃO ELETRÔNICO N.º 4.002/2022-CPL/MP/PGJ, em consonância com a ata de realização do cotejo e demais documentações complementares;

III – À COMISSÃO PERMANENTE DE LICITAÇÃO – CPL, para as providências cabíveis;

IV – Após, à DIRETORIA DE ORÇAMENTO E FINANÇAS, para prosseguimento do feito.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DO SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), 25 de março de 2022.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ordenador de Despesas

DESPACHO DE HOMOLOGAÇÃO Nº 75.2022.01AJ-SUBADM.0790316.2021.015252

PROCESSO SEI N.º 2021.015252
Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ

HOMOLOGAÇÃO

CONSIDERANDO a solicitação inicial constante do OFÍCIO Nº 108.2021.DTIC.0692180.2021.015252, bem como o teor do último TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252;

CONSIDERANDO o disposto na Lei, na Ata da Sessão Pública de realização do Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 21/02 a 23/03/2022, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a contratação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual;

CONSIDERANDO o RELATÓRIO DE LICITAÇÃO Nº 6.2022.CPL.0777809.2021.015252, no qual demonstra que a realização deste Pregão significou uma economia de R$ 3.350.372,99 (três milhões, trezentos e cinquenta mil trezentos e setenta e dois reais e noventa e nove centavos), aos cofres públicos, ou seja, uma redução de aproximadamente 57,48% do valor estimado pela Administração;

CONSIDERANDO o teor da Lei Federal n.º 10.520, de 17.07.2002, do Ato PGJ n.º 322 e 389/2007, do Decreto Federal n.º 10.024/19 e Decreto Estadual n.º 24.818/2005, de 27/01/2005;

CONSIDERANDO a manifestação de intenção recursal formulada pela empresa IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIREL, CNPJ: 23.378.923/0001-87, no prazo e condições de que trata o art. 4.º, incisos XVIII e XX, da Lei Federal n.º 10.520/2002;

CONSIDERANDO o exposto na DECISÃO Nº 14.2022.CPL.0781007.2021.015252, em que o Pregoeiro CONHECEU da oposição formulada e, no mérito, NEGOU PROVIMENTO, portanto, à manifestação de inconformismo submetida e, ao final, deliberou pela MANUTENÇÃO do posicionamento inicial e, por conseguinte, aceitação da proposta ofertada e habilitação da empresa licitante NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, inscrita no CNPJ nº 05.250.796/0001-54, a fim de dar seguimento ao certame, nos termos do art. 17, inciso VII, do Decreto n.º 10.024/2019;

CONSIDERANDO, por derradeiro, o DECISÃO Nº 2.2022.01AJ-SUBADM.0789171.2021.015252. que refutou as razões da deliberação retromencionada;

RESOLVE:

I – ADJUDICAR o objeto do certame à empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, inscrita no CNPJ nº 05.250.796/0001-54, no valor global de R$ 2.478.052,85 (dois milhões, quatrocentos e setenta e oito mil cinquenta e dois reais e oitenta e cinco centavos);

II – HOMOLOGAR o resultado do procedimento licitatório, referente ao PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ, em consonância com a ata de realização do cotejo e demais documentações complementares;

III – À COMISSÃO PERMANENTE DE LICITAÇÃO – CPL, para as providências cabíveis;

IV – Após, à DIRETORIA DE ORÇAMENTO E FINANÇAS, para prosseguimento do feito.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DO SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), 25 de março de 2022.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ordenador de Despesas

ATOS DA PROMOTORIA DE JUSTIÇA

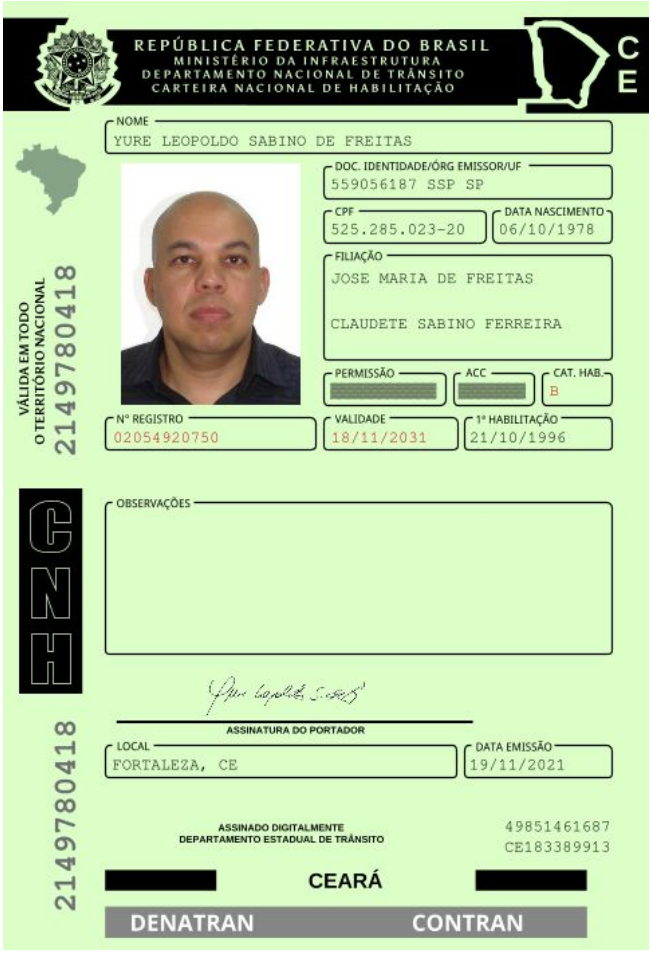
EXTRATO DE PROMOTORIA

Extrato da Portaria n.º 0005/2022/54PJ
Instauração de Procedimento Administrativo

Processo n.º: 09.2022.00000138-1

CNH Digital

Departamento Nacional de Trânsito



QR-CODE

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua validade poderá ser confirmada por meio do programa Assinador Serpro.

As orientações para instalar o Assinador Serpro e realizar a validação do documento digital estão disponíveis em:
< http://www.serpro.gov.br/assinador-digital >, opção Validar Assinatura.

SERPRO / DENATRAN

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
05.250.796/0001-54 **MATRIZ**		**02/08/2002**

NOME EMPRESARIAL
NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
NETWORK SECURE	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
46.51-6-01 - Comércio atacadista de equipamentos de informática (Dispensada *)

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
46.15-0-00 - Representantes comerciais e agentes do comércio de eletrodomésticos, móveis e artigos de uso doméstico (Dispensada *)
46.18-4-99 - Outros representantes comerciais e agentes do comércio especializado em produtos não especificados anteriormente (Dispensada *)
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis (Dispensada *)
62.04-0-00 - Consultoria em tecnologia da informação (Dispensada *)
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação (Dispensada *)
70.20-4-00 - Atividades de consultoria em gestão empresarial, exceto consultoria técnica específica (Dispensada *)
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios (Dispensada *)
85.99-6-03 - Treinamento em informática (Dispensada *)
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos (Dispensada *)

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV PONTES VIEIRA	**2340**	**SALAS 510 A 514**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
60.135-238	**DIONISIO TORRES**	**FORTALEZA**	**CE**

ENDEREÇO ELETRÔNICO	TELEFONE
ANDREA@NETWORKSECURE.COM.BR	**(85) 3195-2200**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**03/11/2005**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

(*) *A dispensa de alvarás e licenças é direito do empreendedor que atende aos requisitos constantes na Resolução CGSIM nº 51, de 11 de junho de 2019, ou da legislação própria encaminhada ao CGSIM pelos entes federativos, não tendo a Receita Federal qualquer responsabilidade quanto às atividades dispensadas.*

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **17/03/2022** às **10:00:55** (data e hora de Brasília). Página: **1/1**

TIM S.A.
Av.Tristão Gonçalves,1461/1477
Centro - Fortaleza - CE
CNPJ: 02.421.421/0008-98 - I.E.: 62877542
CNPJ da Matriz: 02.421.421/0001-11

R$ 85,99

VENCIMENTO
20/12/2021

EMISSÃO: 02/12/2021
POSTAGEM: 10/12/2021
FATURA: 4611619788

YURE LEOPOLDO SABINO DE FREITAS
RUA GENERAL TERTULIANO POTIGUARA, 158, APTO 701
ALDEOTA
60135-280 - FORTALEZA - CE

CLIENTE: 1.77270378
CPF/CNPJ: 52528502320
ACESSO: 85 99958-1335
DÉBITO AUTOMÁTICO: 00000009133585930017

IMPORTANTE PARA YURE

Consta nessa fatura a cobrança de um novo serviço: TIM Banca Virtual Premium Jornais para o número 85999581335. Consta nessa fatura a cobrança de um novo serviço: TIM Segurança Digital Premium para o número 85999581335.

RESUMO DA SUA CONTA DE 01/NOV A 30/NOV

Serviços TIM S.A.	VALOR
TIM Black C Light 3 0	**R$ 85,99**

VEJA ABAIXO O RESUMO DA SUA CONTA PARA O NÚMERO: 85 99958-1335

MENSALIDADES

Vantagens que seu plano oferece	FRANQUIA	CONSUMO	QUANTIDADE	N° DIAS	PERIODO	VALOR
TIM Black C Light 3 0 (117/PÓS/SMP)	-	-	1	30	01/11 a 30/11	**105,99**
Desconto TIM Black C Light 3 0	-	-	3/12	30	01/11 a 30/11	−20,00
Subtotal						85,99
20GB de Internet	20GB	5,28GB	1	30	01/11 a 30/11	Incluído
Minutos Locais e DDD com 41	Ilimitado	1008m48s	1	30	01/11 a 30/11	Incluído
TIM Music	-	-	1	30	01/11 a 30/11	Incluído
TIM Segurança Digital Premium	-	-	1	30	01/11 a 30/11	Incluído
Audiobooks by Ubook	-	-	1	30	01/11 a 30/11	Incluído
TIM Banca Virtual Premium Jornais	-	-	1	30	01/11 a 30/11	Incluído
					Total de Mensalidades	**85,99**

MAIS DETALHES DA SUA CONTA

Você pode ver sua conta detalhada sempre que desejar, com toda a comodidade e segurança, no App Meu TIM. Para acessá-la, visite www.appmeutim.com.br do seu celular TIM. Central de Atendimento: 1056

IMPOSTO TIM S.A.	ALÍQUOTA	BASE DE CÁLCULO	VALOR	FUST:	R$ 0,32
ICMS	30%	R$ 48,91	R$ 14,67	FUNTTEL:	R$ 0,16
PIS/COFINS - Serviços Telecom	3,65%				
PIS/COFINS - Serviços Não Telecom	9,25%				
ISS		R$ 13,63	R$ 0,33		

Em atendimento à Lei 12.741/2012
As contribuições ao FUST [1%] e FUNTTEL [0,5%] não são repassadas às tarifas

Informações Complementares – Plano(s) e Serviços de Valor Adicionado (SVA)

Incluídos no(s) Plano(s)

Franquia(s)	R$ 60,29
SVA	R$ 45,70
Desconto(s) Franquia(s)	R$ −11,38
Desconto(s) SVA	R$ −8,62

Para sua comodidade e praticidade, cadastre sua conta agora mesmo em débito automático. Acesse o site ou app Meu TIM para ativação e mais informações: meutim.com.br

NOME DO CLIENTE
YURE LEOPOLDO SABINO DE FREITAS

AUTENTICAÇÃO MECÂNICA

IDENTIFICAÇÃO DE DÉBITO AUTOMÁTICO	MÊS DE REFERÊNCIA	DATA DE EMISSÃO	DATA DE VENCIMENTO	VALOR
00000009133585930017	DEZ/2021	02/12/2021	**20/12/2021**	**R$ 85,99**

84660000000 - 0 | 85990109011 - 7 | 00461161978 - 6 | 80133585930 - 3

PAGUE COM PIX

Nº de Identificação do documento: 4611619788

Ministério da Economia
Secretaria de Governo Digital
Departamento Nacional de Registro Empresarial e Integração
Secretaria do Desenvolvimento Econômico

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
23201712520	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial do Estado do Ceará

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP
CEP2000234531

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		2211	1	ALTERACAO DE ENDERECO DENTRO DO MESMO MUNICIPIO
		2003	1	ALTERACAO DE SOCIO/ADMINISTRADOR
		2001	1	ENTRADA DE SOCIO/ADMINISTRADOR

FORTALEZA
Local

30 Outubro 2020
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
20/150.819-2	CEP2000234531	30/10/2020

Identificação do(s) Assinante(s)	
CPF	Nome
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA

CNPJ(MF) nº 05.250.796/0001-54
Nire/Jucec nº **23.2.0171252-0**

Terceira Alteração e Consolidação do Contrato Social

Pelo presente instrumento particular e na melhor forma de direito os abaixo qualificados:
JOSE MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 99010123694 SSP/CE e do CPF/MF sob nº 648.711.503-72, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, na Av. Coronel Miguel Dias, 1010 – Torre A - Apto 1301 – Bairro: Guararapes - CEP: 60810-160;
TATIANA RIBEIRO LEITE, brasileira, solteira, nascida em 29/06/1977, empresaria, portadora da Carteira de Identidade n° 93002319934 SSPDC/CE e do CPF(MF) n° 691.833.093-49, residente e domiciliada na cidade de Fortaleza, estado do Ceará na Rua Franklin Bezerra, 212 – Bairro: Mondubim – CEP: 60.762-260; e
ALARICO ISAIAS DE SOUSA GUIMARAES, brasileiro, casado em regime de comunhão parcial de bens, nascido em 23/04/1980, empresário, portador da Carteira de Identidade n° 96002206506 SSPDS/CE e do CPF(MF) n° 620.143.313-91, residente e domiciliado na cidade de Fortaleza, estado do Ceará na Av. Paisagística, 06 - Apto 407 - Bairro: Itaperi - CEP: 60.743-065.

Únicos sócios da sociedade limitada denominada "**NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**.", estabelecida na cidade de Fortaleza, estado do Ceará, na Rua Capitão Melo, 3373 - Bairro: Joaquim Távora – CEP: 60.120-220, inscrita no CNPJ(MF) 05.250.796/0001-54, registrada na Junta Comercial do Estado do Ceará sob nire n° 23.2.0171252-0, decidem, de comum acordo, alterar e consolidar seu Contrato Social, e o fazem mediante as cláusulas a seguir, em conformidade com o Código Civil Brasileiro:

Primeira – A sociedade resolve alterar o endereço de sua sede social, passando a estabelecer-se na Av. Pontes Vieira, 2340 – Salas 510 a 514 – Bairro: Dionísio Torres – CEP: 60135-238 – Fortaleza – Ceará.

Segunda – Ingressa na sociedade **YURE LEOPOLDO SABINO DE FREITAS**, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 559056187 SSP/SP e do CPF/MF sob nº 525.285.023-20, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, na Rua Barbara de Souza Costa, 100 – CS 08 - Bairro: Lagoa Redonda - CEP: 60831-083, através da transferência de R$10.526,00 (dez mil e quinhentos e vinte e seis reais), representado por 10.526 (dez mil e quinhentas e vinte e seis) quotas de capital de valor unitário R$1,00 (um real) pelo sócio **JOSE MURILO CIRINO NOGUEIRA JUNIOR,** acima qualificado, dando as partes mutuamente, plena geral e irretratável quitação.

Terceira – Após a alteração acima o capital Social da sociedade no valor de R$421.052,00 (quatrocentos e vinte e um mil e cinquenta e dois reais), dividido em 421.052 (quatrocentas e vinte e uma mil e cinquenta e duas) quotas de capital de valor unitário R$1,00 (um real), já

totalmente integralizado em moeda corrente nacional, fica distribuído entre os sócios da seguinte forma:

Sócios	Nº quotas	Valor(R$)	Part(%)
JOSE MURILO CIRINO NOGUEIRA JUNIOR	389.474	389.474,00	92,50
ALARICO ISAIAS DE SOUSA GUIMARAES	10.526	10.526,00	2,50
TATIANA RIBEIRO LEITE	10.526	10.526,00	2,50
YURE LEOPOLDO SABINO DE FREITAS	10.526	10.526,00	2,50
Total do Capital	421.052	421.052,00	100,00

§ 1º **-** Cada quota é indivisível e confere a seu titular o direito a um voto nas deliberações sociais.

§ 2º – A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integralização do capital social.

§ 3º - Na forma do art. 997, inciso VIII, da Lei 10.406/02, os sócios não respondem subsidiariamente pelas obrigações sociais.

Quarta – Os sócios resolvem consolidar o texto do contrato social que passa a vigorar com a seguinte redação:

Contrato Social Consolidado

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ(MF) nº 05.250.796/0001-54
Nire/Jucec nº 23.2.0171252-0

JOSE MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 99010123694 SSP/CE e do CPF/MF sob nº 648.711.503-72, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, à Rua Vicente Linhares, 985 - Apt. 2102 – Bairro: Aldeota - CEP: 60135-270;
TATIANA RIBEIRO LEITE, brasileira, solteira, nascida em 29/06/1977, empresaria, portadora da Carteira de Identidade n° 93002319934 SSPDC/CE e do CPF(MF) n° 691.833.093-49, residente e domiciliada na cidade de Fortaleza, estado do Ceará na Rua Franklin Bezerra, 212 – Bairro: Mondubim – CEP: 60.762-260;
ALARICO ISAIAS DE SOUSA GUIMARAES, brasileiro, casado em regime de comunhão parcial de bens, nascido em 23/04/1980, empresário, portador da Carteira de Identidade n° 96002206506 SSPDS/CE e do CPF(MF) n° 620.143.313-91, residente e domiciliado na cidade de Fortaleza, estado do Ceará na Av. Paisagística, 06 - Apto 407 - Bairro: Itaperi - CEP: 60.743-065; e
YURE LEOPOLDO SABINO DE FREITAS, brasileiro, casado em regime de comunhão parcial de bens, empresário, portador da Carteira de Identidade nº 559056187 SSP/SP e do CPF/MF sob

nº 525.285.023-20, residente e domiciliado na cidade de Fortaleza, Estado do Ceará, na Rua Barbara de Souza Costa, 100 – CS 08 - Bairro: Lagoa Redonda - CEP: 60831-083.

Tem entre si, justos e contratados, uma sociedade empresária Limitada, a qual é regida em conformidade com as seguintes clausulas e condições:

Cláusula Primeira – Denominação Social

A sociedade gira sob o nome empresarial de **" NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA"**., adotando por nome de fantasia a expressão "**NETWORK SECURE**".

Cláusula Segunda - Sede e Filiais

A sede e domicílio fiscal da sociedade é na Cidade de Fortaleza, estado do Ceará, na Rua Capitão Melo, 3373 - Bairro: Joaquim Tavora – CEP: 60.120-220.

§ Único - A sociedade não possui filiais, podendo quando servir aos seus interesses, abrir escritórios, representações, sucursais ou outras filiais neste estado ou em qualquer parte do território nacional e no Exterior, destacando para estas uma parte do capital social da matriz.

Clausula Terceira – Objetivo Social

A sociedade tem por objetivo as seguintes atividades:

a) Comercio atacadista de equipamentos de informatica – CNAE 4651-6/01;
b) Locação de equipamentos de computadores e perifericos – CNAE 7733-1/00;
c) Desenvolvimento e licenciamento de programas de computador customizaveis – CNAE 6202-3/00;
d) Suporte tecnico, manutenção e outros serviços em tecnologia da informação – CNAE 6209-1/00;
e) Reparação e Manutenção de computadores e de equipamentos perifericos – CNAE 9511-8/00;
f) Consultoria em Tecnologia da informação – CNAE 6204-0/00;
g) Consultoria em gestão empresarial – CNAE 7020-4/00; e
h) Treinamento em informatica – CNAE 8599-6/03.

Cláusula Quarta – Duração e Inicio das Atividades

A sociedade iniciou suas atividades em 20/08/2002 e sua duração será por tempo indeterminado.

Clausula Quinta – Capital Social

O capital Social da sociedade é de R$421.052,00 (quatrocentos e vinte e um mil e cinquenta e dois reais), dividido em 421.052 (quatrocentas e vinte e uma mil e cinquenta e duas) quotas de

capital de valor unitário R$1,00 (um real), já totalmente integralizado em moeda corrente nacional, distribuídos da seguinte forma:

Sócios	Nº quotas	Valor(R$)	Part(%)
JOSE MURILO CIRINO NOGUEIRA JUNIOR	389.474	389.474,00	92,50
ALARICO ISAIAS DE SOUSA GUIMARAES	10.526	10.526,00	2,50
TATIANA RIBEIRO LEITE	10.526	10.526,00	2,50
YURE LEOPOLDO SABINO DE FREITAS	10.526	10.526,00	2,50
Total do Capital	421.052	421.052,00	100,00

§ 1º **-** Cada quota é indivisível e confere a seu titular o direito a um voto nas deliberações sociais.

§ 2º – A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integralização do capital social.

§ 3º - Na forma do art. 997, inciso VIII, da Lei 10.406/02, os sócios não respondem subsidiariamente pelas obrigações sociais.

Clausula Sexta – Administração

A Administração e o uso da denominação social da sociedade são exercidos pelo sócio **JOSE MURILO CIRINO NOGUEIRA JUNIOR**, já qualificado anteriormente, com os poderes e atribuições de Administrador, que assinará e representará a sociedade, ativa e passivamente, seja como autor ou réu, em juízo ou fora dele e perante terceiros e qualquer repartição pública, ou quaisquer autoridades federais, estaduais ou municipais, bem como, autarquias, sociedade de economia mista e para-estatais.

§ 1º - Os sócios poderão receber "pro-labore" em valores e periodicidade fixada de comum acordo entre eles no início de cada exercício social.

§ 2º - É vedado ao administrador fazer uso da firma na prestação de garantia, fiança, aval ou qualquer outro título de favor, em negócios estranhos ao objeto social.

§ 3º - A sociedade poderá nomear procuradores para, especificando no instrumento de procuração os poderes e o prazo de vigência do mandato.

Clausula Sétima – Deliberações Sociais

Nos termos do disposto no artigo 1076 – Incisos I e II da Lei 10.406/02, o presente contrato poderá ser alterado, inclusive, para transformação do tipo societário, assim como, da ocorrência dos eventos de cisão, fusão ou incorporação com outras sociedades ou em outras sociedades pela vontade de sócios que representem, no mínimo, 75% (setenta e cinco por cento) das quotas de capital da sociedade.

§ Único - No caso de exclusão de sócio que esteja colocando em risco os interesses da sociedade, a alteração do Contrato Social poderá ser realizada por sócios que representem mais de 50% (cinqüenta por cento) do Capital Social.

Clausula Oitava – Prestação de Contas

Nos quatro primeiros meses seguintes ao término de cada exercício social, os sócios deliberarão sobre as contas do exercício e designarão ou substituirão administrador(es) quando for o caso.

Clausula Nona – Transferências de quotas

Nenhum quotista poderá ceder, transferir, alienar ou onerar, a qualquer titulo, suas quotas antes de ofertá-las aos demais quotistas, que terão preferência para aquisição das mesmas por seu respectivo valor, determinado de acordo com o último balanço patrimonial, na proporção do capital que cada um possua. A avaliação das cotas poderá ser feita por critérios baseados em valor de mercado, obtido pela avaliação de especialista indicado pelos demais quotistas, ficando o ônus da contratação às custas do quotistas que deseje ceder, transferir, alienar ou onerar, a qualquer título, suas cotas.

§ 1° - Qualquer quotista que pretender ceder, transferir, alienar ou onerar, a qualquer titulo, suas quotas deverá comunicar sua intenção aos demais sócios, por escrito, com aviso prévio de 30 (trinta) dias, contendo todas as condições da oferta.

§ 2° – Decorrido os 30 (trinta) dias, se algum quotista não exercer a opção a ele assegurada de acordo com o presente, as quotas que ele poderia ter comprado serão oferecidas aos quotistas remanescentes, que terão 5 (cinco) dias, a partir da data da respectiva comunicação, para exercer a opção ou renunciar a mesma.

§ 3° – Cumpridos os prazos e condições fixadas acima, as quotas remanescentes poderão ser alienadas a terceiros interessados, nas mesmas condições de oferta citada no parágrafo primeiro. Na eventualidade da alienação não se concluir e se o ofertante desejar dispor das quotas em condições diferentes daquelas originariamente informadas, o procedimento indicado nos parágrafos anteriores deverá ser novamente observado, e assim sucessivamente até que todas as quotas sejam vendidas, cedidas ou transferidas, em conformidade com a intenção do titular.

§ 4° – Toda e qualquer venda, cessão, oneração ou transferência de quotas que for realizada sem a observância ao disposto nesta clausula será considerada nula de pleno direito e sem qualquer efeito.

Clausula Décima – Dissolução da sociedade

Ocorrendo qualquer situação que implique na dissolução da sociedade, será permitido ao sócio remanescente admitir novo(s) sócio(s) para dar continuidade à mesma.

§ 1° – Os haveres do sócio retirante, morto, invalido, excluído serão apurados com base no ultimo balanço patrimonial levantado pela sociedade, anterior a data da retirada, morte, invalidez ou exclusão e será pago a quem de direito, em até 12 (doze) prestações mensais, iguais e consecutivas atualizadas pelo índice oficial que reflita a variação da inflação.

§ 2º - No caso de falecimento até que se ultime, no processo de inventário, a partilha dos bens deixados pelo de cujus, incumbirá ao inventariante, para todos os efeitos legais, a representação ativa e passiva dos interessados perante a sociedade. Os herdeiros, através de seu inventariante ou representante legal, poderão retirar-se da sociedade.

§ 3º - A retirada, morte, invalidez ou exclusão do sócio, não o exime, ou a seus herdeiros, da responsabilidade pelas obrigações sociais anteriores, até dois anos depois de averbada a resolução da sociedade.

Clausula Décima Primeira – Exercício Social

O exercício social terminará em 31 de dezembro de cada ano, quando será levantado o balanço patrimonial correspondente, bem como, preparadas as demais demonstrações contábeis/financeiras exigidas por lei. Os lucros e/ou prejuízos apurados poderão ser distribuídos proporcionalmente ou desproporcionalmente a participação dos sócios no capital social, não se excluindo da distribuição nenhum dos sócios.

§ 1º - No caso de distribuição desproporcional a participação dos sócios no capital social, será necessária a deliberação unanime dos sócios, lavrando-se ata de reunião dos sócios, realizada especialmente para esta finalidade, devendo haver a unanimidade dos sócios.

§ 2º - A sociedade no interesse dos sócios poderá levantar balanços mensalmente ou noutro período, em qualquer data e em razão dos resultados apurados efetuar a distribuição de lucros ou dividendos e/ou de juros sobre o Capital Social.

Clausula Décima Segunda – Declaração de Desimpedimento

O administrador declara, sob as penas da Lei, que não está impedido de exercer a administração da sociedade, por Lei especial, ou em virtude condenação criminal, ou por se encontrar sob os efeitos dela a pena que vede ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra norma de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

Clausula Décima Terceira – Normas Contratuais Omissas

Os casos omissos do presente contrato serão resolvidos pela aplicação dos dispositivos do Código Civil Brasileiro (Lei 10.406/02) e, supletivamente pela Lei das Sociedades Anônimas (Lei 6.404/76) e sem prejuízo de legislações supervenientes e que venham a tratar da matéria.

Clausula Décima Quarta - Foro

As partes, de comum acordo, elegem o Foro da Comarca de Fortaleza, Estado do Ceará, renunciando a qualquer outro, por mais privilegiado que seja, para dirimir qualquer dúvida que possa emergir deste documento.

E, por estarem justos e contratados, assinam o presente Instrumento de Alteração e Consolidação do Contrato Social.

Fortaleza/CE, 12 de fevereiro de 2019.

Sócios:

JOSE MURILO CIRINO NOGUEIRA JUNIOR
SÓCIO ADMINISTRADOR

ALARICO ISAIAS DE SOUSA GUIMARAES
SÓCIO

TATIANA RIBEIRO LEITE
SÓCIO

YURE LEOPOLDO SABINO DE FREITAS
SÓCIO

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
20/150.819-2	CEP2000234531	30/10/2020

Identificação do(s) Assinante(s)	
CPF	Nome
620.143.313-91	ALARICO ISAIAS DE SOUSA GUIMARAES
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR
691.833.093-49	TATIANA RIBEIRO LEITE
525.285.023-20	YURE LEOPOLDO SABINO DE FREITAS

LENIRA CARDOSO DE ALENCAR SERAINE
SECRETARIA GERAL

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa NETWORK SECURE SEGURANCA DA INFORMACAO LTDA, de NIRE 2320171252-0 e protocolado sob o número 20/150.819-2 em 05/11/2020, encontra-se registrado na Junta Comercial sob o número 5481638, em 06/11/2020. O ato foi deferido eletrônicamente pelo examinador Jairo Bezerra Lira.

Certifica o registro, a Secretária-Geral, Lenira Cardoso de Alencar Seraine. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (http://portalservicos.jucec.ce.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)	
CPF	Nome
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR

Documento Principal

Assinante(s)	
CPF	Nome
691.833.093-49	TATIANA RIBEIRO LEITE
620.143.313-91	ALARICO ISAIAS DE SOUSA GUIMARAES
525.285.023-20	YURE LEOPOLDO SABINO DE FREITAS
648.711.503-72	JOSE MURILO CIRINO NOGUEIRA JUNIOR

Declaração Documento(s) Anexo(s)

Assinante(s)	
CPF	Nome
313.429.653-53	OLAVO BRASIL MAGALHAES

Fortaleza. Sexta-feira, 06 de Novembro de 2020

Documento assinado eletrônicamente por Jairo Bezerra Lira, Servidor(a) Público(a), em 06/11/2020, às 11:54 conforme horário oficial de Brasília.

A autencidade desse documento pode ser conferida no portal de serviços da jucec informando o número do protocolo 20/150.819-2.

O ato foi deferido e assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
236.117.073-68	LENIRA CARDOSO DE ALENCAR SERAINE

Fortaleza. Sexta-feira, 06 de Novembro de 2020

PROCURAÇÃO bastante que faz e assina, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, na forma abaixo:

Saibam quantos este público instrumento virem que, aos 13 (treze) dias do mês de outubro do ano de 2020 (dois mil e vinte), nesta cidade de Fortaleza, Capital do Estado do Ceará, República Federativa do Brasil, na Rua Capitão Melo, nº 3373, bairro Joaquim Távora, onde eu, Gisele Maria Tavares Pordeus de Vasconcelos, escrevente autorizada, vim em diligência, estava o sócio administrador, adiante qualificado, da ora outorgante, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.,** pessoa jurídica de direito privado, que tem o nome de fantasia NETWORK SECURE, com sede nesta Capital, na Rua Capitão Melo, nº 3373, bairro Joaquim Távora, inscrita no CNPJ sob o nº 05.250.796/0001-54, neste ato representada por seu sócio administrador JOSÉ MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado, empresário, nascido no dia 09/07/1981, filho de Jose Murilo Cirino Nogueira e Eluzia Peixoto da Silva, com endereço eletrônico: murilo@networksecure.com.br, residente e domiciliado nesta Capital, na Av. Coronel Miguel Dias, nº 1010, aptº 1301, T-A, bairro Guararapes, portador da CNH nº 1226678851-DETRAN-CE, registro nº 00809571455, emitida no dia 17/12/2015, onde consta a cédula de identidade nº 99010123694-SSP-CE, inscrito no CPF sob o nº 648.711.503-72, o presente reconhecido por mim, pela verificação dos documentos supraexibidos em seus originais, de cuja(s) identidade(s) e capacidade jurídica dou fé. Então pela outorgante NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA., me foi dito, representada como está, que nomeava e constituía seu bastante procurador, **YURE LEOPOLDO SABINO DE FREITAS,** brasileiro, casado, diretor comercial, nascido no dia 06/10/1978, filho de Jose Maria de Freitas e Claudete Sabino Ferreira, com endereço eletrônico: yure.sabino@networksecure.com.br, residente e domiciliado nesta Capital, na Rua Bárbara de Sousa Costa, nº 100, casa 08, bairro Lagoa Redonda, portador da CNH nº 1406940509-DETRAN-CE, registro nº 02054920750, emitida no dia 08/12/2016, onde consta a cédula de identidade nº 559056187-SSP-SP, inscrito no CPF sob o nº 525.285.023-20, a quem confere poderes amplos e ilimitados para praticar todos os atos relativos à contrato em geral, responder a repartições públicas e privadas, licitação, podendo formular ofertas escritas e verbais, negociar preços, assinar documentos de habilitação, atas e instrumentos de compromisso, interpor recursos e renunciar o direito de propô-los, retirar login e senha, preenchendo e assinando todas as formalidades legais para viabilidade do mesmo, praticar todos os demais atos pertinentes ao certame em nome da empresa outorgante, assistir a abertura de propostas, fazer impugnações, reclamações, protestos e recursos, assinar propostas, atas, documentos necessários, fazer novas propostas, rebaixos, descontos, receber em devolução documentos pertencentes a outorgante, assinar contratos, acordar, discordar, desistir de recursos, juntar e retirar documentos, prestar esclarecimentos, informações, assinar requerimentos e petições, podendo tudo requerer e assinar para o bom e fiel cumprimento do presente mandato, o que será dado por bom, firme e valioso e preencher todas as formalidades

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
Fortaleza, CE
16 OUT. 2020
ROBERTO FIUZA MAIA - TABELIÃO
FABRICIO GOULART DE AQUINO - ESC. AUTORIZ.
CLAUDIA CARNEIRO DA SILVA - ESC. AUTORIZ.
CONCEIÇÃO DE MARIA CORREIA MAIA - ESC. SUBST.
MARTHA MARY MOTA RIBEIRO - ESC. AUTORIZ.
SELO DE AUTENTICIDADE
OCRS AUTENTICAÇÃO N. IH 593185

legais, **sendo vedado o substabelecimento. O PRESENTE INSTRUMENTO TEM VALIDADE DE 5 (CINCO) ANOS A CONTAR DESTA DATA. (FEITO SOB MINUTA). OS PODERES AQUI ELENCADOS ESTÃO SUJEITOS À OBSERVÂNCIA DAS RESTRIÇÕES CONTIDAS NO CONTRATO SOCIAL E ADITIVOS DA REFERIDA EMPRESA. O(s) nome(s) e dados do(s) procurador(es) e os elementos relativos ao objeto do presente instrumento foram fornecidos e conferidos pelo(s) outorgante(s), que por eles se responsabiliza(m)**. E como assim o disse, do que dou fé, lavrei este instrumento, que lido e achado conforme, aceita e assina. Eu, (a.) Gisele Maria Tavares Pordeus de Vasconcelos, escrevente autorizada, a lavrei. Eu, Rodrigo de Paula Pessoa Maia, escrevente substituto, a subscrevo. (a.a.) Rodrigo de Paula Pessoa Maia. **JOSÉ MURILO CIRINO NOGUEIRA JUNIOR**. Está conforme o original. Dou fé. Selo nº AAE245133-K2L9, AAE669928-D8I9. Trasladada em seguida. VÁLIDO SOMENTE COM SELO DE AUTENTICIDADE.

Subscrevo e assino

Em testemunho da verdade.

Gisele Maria Tavares Pordeus de Vasconcelos
Escrevente Autorizada

PODER JUDICIÁRIO Estado do Ceará
Selo Tipo 1
REGISTRAL DISTRIBUIÇÃO
Nº AAE669928-D8I9
SELO DIGITAL DE AUTENTICIDADE
Consulte a validade do Selo Digital em selodigital.tjce.jus.br/portal

PODER JUDICIÁRIO Estado do Ceará
Selo Tipo 6
SELO-6
Nº AAE245133-K2L9
SELO DIGITAL DE AUTENTICIDADE
Consulte a validade do Selo Digital em selodigital.tjce.jus.br/portal

CUSTAS E EMOLUMENTOS INCIDENTES

Nº do Atendimento:	100326
Total Emolumentos:	R$ 37,99
Total FERMOJU:	R$ 4,44
Total Selos:	R$ 6,23
Valor Total:	R$ 48,66

Base de Cálculo / Atos com Valor Declarado
Bem/Negócio 1. R$ 0,00

Detalhamento da cobrança / Listagem dos códigos da tabela de emolumentos evolvidos

Códigos: 2003 / 5023

3º OFÍCIO DE NOTAS
Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
Fortaleza - CE.
16 OUT. 2020
ROBERTO FEIJA MAIA - TABELIÃO
FABRICIO GOMART DE ALENCAR - ESC. AUTORIZ.
CLAUDIA CARNEIRO DA SILVA - ESC. AUTORIZ.
CONCEIÇÃO DE MARIA CORRÊA MAIA - ESC. SUBST.
MARIA MARLY MOTA RIBEIRO - ESC. AUTORIZ.

AUTENTICAÇÃO JHYK 03 N. IH 593192

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
CNPJ: 05.250.796/0001-54

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 10:29:43 do dia 31/01/2022 <hora e data de Brasília>.
Válida até 30/07/2022.
Código de controle da certidão: **21EE.D3D4.A352.5597**
Qualquer rasura ou emenda invalidará este documento.

GOVERNO DO
ESTADO DO CEARÁ
Procuradoria Geral do Estado

Certidão Negativa de Débitos Estaduais

202204682246

Emitida para os efeitos da Instrução Normativa Nº 13 de 02/03/2001

IDENTIFICAÇÃO DO(A) REQUERENTE
Inscrição Estadual: 061805408
CNPJ / CPF: 05250796000154
RAZÃO SOCIAL: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Ressalvado o direito da Fazenda Estadual de inscrever e cobrar as dívidas que venham a ser apuradas, certifico, para fins de direito, que revendo os registros do Cadastro de Inadimplentes da Fazenda Pública Estadual - CADINE, verificou-se nada existir em nome do(a) requerente acima identificado(a) até a presente data e horário, e, para constar, foi emitida esta certidão.

EMITIDA VIA INTERNET EM 02/03/2022 ÀS 11:48:24
VÁLIDA ATÉ 01/05/2022

A autenticidade deste documento deverá ser comprovada via Internet, no endereço www.sefaz.ce.gov.br

Fortaleza
PREFEITURA
Finanças

SECRETARIA MUNICIPAL DAS FINANÇAS - SEFIN

CERTIDÃO NEGATIVA DE DÉBITOS DE TRIBUTOS MUNICIPAIS

Certidão Nº 2022/69003

CPF/CNPJ: 05.250.796/0001-54

Nome ou Razão Social: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Endereço: AV PONTES VIEIRA 2340 SALA 510 DIONÍSIO TORRES CEP 60135-238

Certificamos, para fins de comprovação perante terceiros, que a pessoa acima identificada, até a presente data, não possui débitos de natureza tributária para com o Município de Fortaleza, ressalvado, porém, à Secretaria Municipal das Finanças, o direito de cobrar e inscrever, a qualquer tempo, quaisquer dividas em seu nome na forma da legislação vigente.

Fortaleza, 22 de Março de 2022 (09:57:32)

Certidão expedida gratuitamente com base no decreto 13.716, de 22 de dezembro de 2015.

A autenticidade desta certidão deverá ser confirmada no endereço eletrônico da Secretaria Municipal das Finanças - SEFIN em www.sefin.fortaleza.ce.gov.br.

Válida até 20/06/2022

Qualquer rasura ou emenda invalidará este documento.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA (MATRIZ E FILIAIS)
CNPJ: 05.250.796/0001-54
Certidão nº: 7049143/2022
Expedição: 02/03/2022, às 11:43:56
Validade: 29/08/2022 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **05.250.796/0001-54**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.° 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

ESTADO DO CEARÁ

PODER JUDICIÁRIO

COMARCA DE FORTALEZA

CERTIDÃO DE FALÊNCIA, RECUPERAÇÃO JUDICIAL OU EXTRAJUDICIAL (LEI 8.666/93)

(PESSOA JURÍDICA / 1º GRAU / CÍVEL)

CERTIFICA, a requerimento da parte interessada, que consultando nos Sistemas Informatizados do Serviço de Distribuição desta Comarca, em relação ao(s) Polo(s) PASSIVO OU ATIVO, dos processos de Natureza Cível, EM TRÂMITE, verificou NADA CONSTAR, em nome de NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA - DEMAIS, CNPJ n° 05.250.796/0001-54.

CERTIFICA que, esta certidão só é válida por 30 (trinta) dias, a contar da data de sua emissão

O referido é verdade e dou fé.

FORTALEZA

Quinta-feira, 17 de Março de 2022 às 09:04:06

Observações:

a) os dados informados são de responsabilidade do solicitante e devem ser conferidos pelo interessado e/ou destinatário;

b) a autenticidade deste documento poderá ser confirmada conforme informações no rodapé;

c) a consulta inclui as seguintes classes: FALÊNCIA, CONCORDATA, RECUPERAÇÃO JUDICIAL E RECUPERAÇÃO EXTRAJUDICIAL;

d) esta certidão é expedida nos termos da Resolução 13/2019, do Órgão Especial do Tribunal de Justiça do Estado do Ceará.

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 05.250.796/0001-54
Razão Social: NETWORK SECURE SEGURANCA DA INFORM LTDA
Endereço: R CAPITAO MELO 3373 / JOAQUIM TAVORA / FORTALEZA / CE / 60120-220

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 07/03/2022 a 05/04/2022

Certificação Número: 2022030700311014077525

Informação obtida em 07/03/2022 12:47:43

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

CONTRATO ADMINISTRATIVO Nº 003/2022 - MP/PGJ

Termo de Contrato Administrativo que entre si celebram o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, visando à prestação de serviço de solução de firewall de próxima geração.

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, por intermédio de sua **PROCURADORIA-GERAL DE JUSTIÇA**, órgão de sua Administração Superior, com sede na Avenida Coronel Teixeira, 7.995, Nova Esperança, 69.037-473, Manaus/AM, inscrita no CNPJ (MF) sob o n.º 04.153.748/0001-85, doravante denominada **CONTRATANTE**, neste ato representada por neste ato representado por seu Subprocurador-Geral de Justiça para Assuntos Administrativos, o Exmo. Sr. Dr. **GÉBER MAFRA ROCHA**, RG nº 07300891 SSPAM e CPF nº 384.778.582-68, e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA,** com sede na Av. Pontes Vieira, 2340 - salas 510 a 514, CEP nº 60.135-238 - Dionísio Torres - Fortaleza - CE, inscrita no CNPJ (MF) sob o n.º 05.250.796/0001-54, daqui por diante denominada **CONTRATADA**, neste ato representada por seu bastante procurador, Sr. **YURE LEOPOLDO SABINO DE FREITAS**, portador do documento de identidade n.º 559056187 SSP/SP, e inscrito no CPF (MF) sob o n.º 525.285.023-20, tendo em vista o que consta no Processo n.º **2021.015252**, doravante referido por **PROCESSO** e, em consequência do **PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ**, resolvem firmar o presente **TERMO DE CONTRATO ADMINISTRATIVO PARA PRESTAÇÃO DE SERVIÇO DE INFORMÁTICA,** nos termos da Lei n.º 8.666/1993 e mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

O objeto do presente ajuste é a prestação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme as especificações constantes no Termo de Referência nº 20.2021.DTIC.0720733.2021.015252.

CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO:

O objeto deste ajuste compreende a contratação de serviço de firewall de próxima geração em alta disponibilidade, pelo **período de 48 (quarenta e oito) meses**, para instalação na sede do **CONTRATANTE**, compreendendo os serviços de instalação, configuração, migração e ativação de equipamentos de segurança; de sistema de monitoramento dos serviços providos e de treinamento para a equipe do **CONTRATANTE**, pela **CONTRATADA**, conforme condições e especificações detalhadas neste Contrato.

Parágrafo primeiro. Os serviços serão prestados conforme o seguinte quantitativo:

ITEM	DESCRIÇÃO	UND	QTD
01	Serviço de Firewall em Alta Disponibilidade	Meses	48
02	Serviço de Monitoramento da Solução	Meses	48
03	Serviço de Migração do Ambiente Atual	Unidades	01
04	Serviço de Treinamento da Solução	Pessoas	05

Tabela 1 - Descrição e Quantitativo dos Serviços

CLÁUSULA TERCEIRA – DAS CARACTERÍSTICAS TÉCNICAS:

1. ESPECIFICAÇÕES GERAIS PARA TODOS OS ITENS:

1.1. São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos

"possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

1.2. Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de *end-of-sale, end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato; Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

1.3. Todos os casos citados no item anterior serão considerados como funcionamento em Modo de Contingência e deverão ser substituídos sem nenhum custo adicional para a **CONTRATANTE,** seguindo os prazos de substituição estabelecidos no item Acordo de Nível de Serviço (SLA).

1.4. O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia, conforme item 4.10, ou na exposição de ativos a riscos de segurança.

1.5. Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do **CONTRATANTE**.

1.6. A **CONTRATADA** deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

1.7. Os produtos deverão ser entregues acondicionados em embalagens que permitam sua proteção contra impactos, umidade e demais agentes que possam ocasionar danos. A **CONTRATADA** será obrigada ao reparo imediato de qualquer dano eventual de manuseio/transporte .

1.8. Quaisquer recursos materiais que tenham sido instalados nas dependências do **CONTRATANTE** pela **CONTRATADA** durante a execução contratual deverão ser devolvidos, por ocasião do término contratual, devendo a **CONTRATADA** arcar com todos os custos referentes ao envio e transporte desses materiais.

1.9. Após o encerramento do contrato, caso haja a necessidade expressa pelo **CONTRATANTE**, a **CONTRATADA** deverá manter os equipamentos e os softwares de gerenciamento já instalados, pelo prazo máximo de 90 (noventa) dias, não estando obrigada à prestação de serviço e garantia neste período, de modo a garantir a continuidade do negócio do **CONTRATANTE** durante uma eventual transição para os serviços de outra contradada.

1.10. Toda documentação gerada durante a prestação dos serviços, como os fluxos de atendimento de solicitações do Catálogo de Serviço, será de propriedade do **CONTRATANTE**, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do **CONTRATANTE**.

1.11. A **CONTRATADA** deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

1.12. A **CONTRATADA** deverá manter o **CONTRATANTE** atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

2. ITEM 01 - SERVIÇO DE FIREWALL EM ALTA DISPONIBILIDADE:

2.1. O Serviço de Firewall em Alta Disponibilidade refere-se aos Serviços de "Firewall" provido por, pelo menos, 02 (dois) conjuntos de equipamentos idênticos, funcionando em modo ativo-ativo ou ativo-passivo, capazes de regular o tráfego de dados entre as distintas redes do **CONTRATANTE** e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), utilizando tecnologias de Firewalls de próxima geração (NGFW).

2.2. Deverá contemplar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados.

2.3. Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

2.4. O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o

atendimento via e-mail ou sítio Web.

2.5. Os equipamentos instalados para execução dos serviços de segurança deverão ser adequados para montagem em rack padrão de 19 polegadas, incluindo todos os acessórios necessários a serem fornecidos pela **CONTRATADA**.

2.6. Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

2.7. Deverá ser provida, por meio de um *appliance* físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

2.8. Os serviços de instalação e implantação da solução serão de responsabilidade da **CONTRATADA**, que deverá prover todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário, inclusive os demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir a operação de todas as funcionalidades dos serviços especificados.

2.9. Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

2.10. Após a reunião de alinhamento, a **CONTRATADA** deverá entregar um plano de implantação, contemplando todos os itens do Lote, em até 5 (cinco) dias úteis, para análise e aprovação do **CONTRATANTE**.

2.11. O **CONTRATANTE** entregará à **CONTRATADA**, durante a Reunião de Alinhamento de Expectativas, relação nominal de até 5 (cinco) servidores que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados de manutenção. Esses perfis serão criados, removidos e bloqueados a critério do **CONTRATANTE** e configurados pela **CONTRATADA** quando da entrega da solução. Os usuários e perfis poderão ser ajustados a qualquer tempo, durante o período de vigência do contrato, sem ônus para o **CONTRATANTE**.

2.12. O Serviço de Firewall em Alta Disponibilidade deverá ser composto por no mínimo 2 (dois) conjuntos de equipamentos do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades exigidas neste Termo, instaladas nos mesmos *appliances* que compõem a solução, operando em alta disponibilidade.

2.13. Havendo necessidade de número de portas além da capacidade dos equipamentos do tipo *appliance*, para atender ao exigido na Tabela de Capacidades, cláusulas de 5.2.15.10.7 a 5.2.15.10.22 do Termo de Referência, será permitido adicionar um único switch por conjunto de equipamentos, sem que haja perda de desempenho, mantendo a alta disponibilidade da solução e atendendo a todas as exigências deste Termo.

2.14. Para maior segurança e conformidade de garantia, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, GNU/Linux entre outros.

2.15. A solução deve ser capaz de atender às especificações mínimas dos serviços constante no **item 5.2.15 do Termo de Referência Nº 20.2021.DTIC.0720733.2021.015252**, integrante do Edital do **PREGÃO ELETRÔNICO N.º 4.005/2022-CPL/MP/PGJ**, a serem ofertados em uma única plataforma.

3. ITEM 02 - SERVIÇO DE MONITORAMENTO DA SOLUÇÃO:

3.1. Compreende um sistema de monitoramento para coleta de informações da solução de firewall de próxima geração em alta disponibilidade, baseado em dashboards, que permita a criação e personalização de regras de coleta, de filtro, de gráficos e de relatórios, possibilitando a emissão de alertas que serão enviados aos administradores.

3.2. Deverá ser baseado em Dashboard, para fácil visualização.

3.3. Deve ser entregue com regras genéricas criadas pela **CONTRATADA**, como uso de processador, memória, tráfego nas portas, ataques e parâmetros similares.

3.4. O serviço da **CONTRATADA** deve incluir a possibilidade de criação de regras personalizadas solicitadas pelo **CONTRATANTE**.

3.5. Deve possuir acesso WEB (HTTPS).

3.6. Deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

3.7. Deve ter capacidade de emitir alertas via SMS e email, no mínimo, sendo desejável envio de mensagem através dos aplicativos Telegram e Microsoft Teams.

4. ITEM 03 - SERVIÇO DE MIGRAÇÃO DO AMBIENTE ATUAL

4.1. O **CONTRATANTE** possui atualmente uma unidade de NEXT GENERATION FIREWALL, da marca Palo Alto Networks, modelo PA-3020, cujas funcionalidades deverão ser totalmente migradas para a solução

ofertada.

4.2. O **CONTRATANTE** possui atualmente uma unidade de pfSense, que atua hoje como roteador de borda, fechando os links "full-route" BGPs com as operadoras, cujas funcionalidades deverão ser totalmente migradas para a solução ofertada.

4.3. A **CONTRATADA** deverá proceder com a migração total de VPNs, NATs, rotas estáticas, rotas dinâmicas, políticas, QoS, IPS, IDS, dentre outros recursos hoje usados, além de sugerir melhorias/adaptações/boas práticas, quando possível.

4.4. O **CONTRATANTE** possui infraestrutura hiper convergente, e para tanto usa o Acropolis Hypervisor Virtualization and Software - Nutanix. Assim, caso a **CONTRATADA** necessite usar máquinas virtuais (VMs) para a prestação do serviço, tais VMs deverão ser compatíveis com a infraestrutura hiper convergente do **CONTRATANTE**.

4.5. A **CONTRATADA** deverá iniciar o processo de migração com a reunião de alinhamento em até 5 (cinco) dias úteis após a assinatura do contrato.

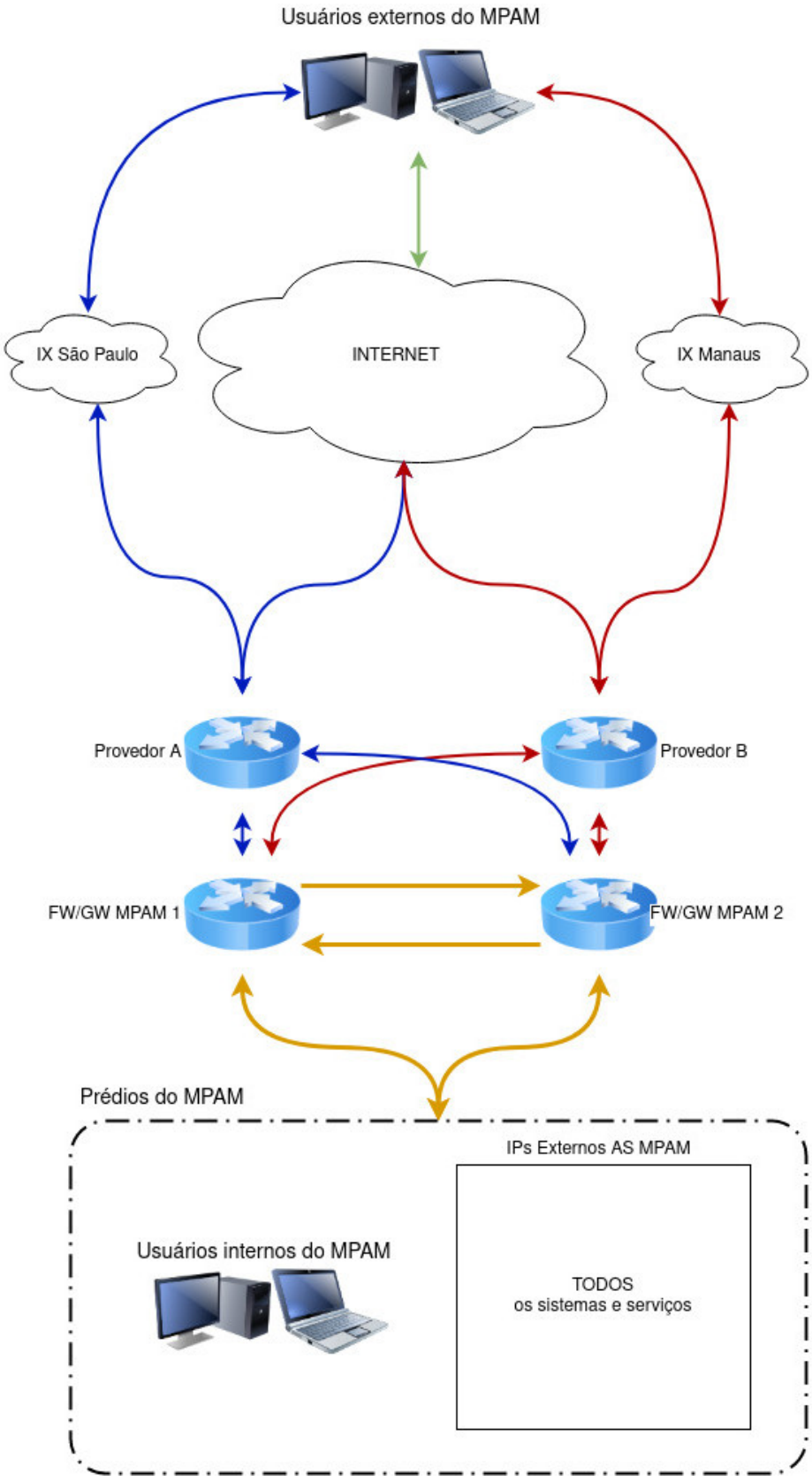
4.6. A **CONTRATADA** deverá finalizar o processo de migração após testes e aprovação pelo **CONTRATANTE** em até 60 (sessenta) dias após o seu início.

4.7. A **CONTRATADA** deverá evitar, durante o processo de migração, interromper os serviços de rede do **CONTRATANTE**, nos horários das 8hs às 18hs, em dias de expediente do **CONTRATANTE**.

4.8. É de responsabilidade da **CONTRATADA** a emissão de relatórios, execução de comandos/scripts e otimizações. Fica a cargo do **CONTRATANTE** fornecer as informações do negócio e tirar quaisquer dúvidas existentes.

4.9. A **CONTRATADA** deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do **CONTRATANTE**, sendo vedada sua cessão, locação ou venda a terceiros.

4.10. A topologia da solução deve seguir conforme imagem a seguir:



5. ITEM 04 - SERVIÇO DE TREINAMENTO DA SOLUÇÃO:

5.1. A **CONTRATADA** deverá transferir o conhecimento das Soluções de Segurança da Informação ofertadas por meio de um treinamento. O treinamento deverá ser ofertado para a quantidade de pessoas especificada no objeto, com duração de pelo menos 4 (quatro) horas por dia, pelo número de dias necessários para perfazer a carga horária total.

5.2. A carga horária total para o treinamento deve ser de, no mínimo, **40 horas**.

5.3. A **CONTRATADA** deverá apresentar um Plano de Capacitação contemplando as ações de treinamento, que será avaliado e aprovado pela **FISCALIZAÇÂO**.

5.4. O conteúdo programático do treinamento deve abranger, minimamente, o mesmo conteúdo ensinado pelo fabricante dos equipamentos, compreendendo as tecnologias envolvidas nos produtos, serviços, softwares e

licenças utilizados para atender aos requisitos das especificações técnicas presentes neste estudo. O treinamento deverá contemplar atividades teóricas e práticas, abordando toda a utilização de funcionalidades básicas e avançadas da solução, bem como atividades de suporte (troubleshooting). Todo o material utilizado deverá ser fonecido em português do Brasil ou inglês.

5.5. O conteúdo programático do treinamento deverá abranger preferencialmente atividades práticas, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo, bem como, em tópicos de interesse da Equipe Técnica do **CONTRATANTE**.

5.6. O treinamento será avaliado por meios próprios e, caso este seja julgado insatisfatório, a **CONTRATADA** deverá prover uma nova turma, com novo instrutor, sem qualquer ônus para o **CONTRATANTE**. Ao final do treinamento serão realizadas avaliações que deverão ser julgadas satisfatórias por pelo menos 80% dos participantes, sendo considerada satisfatórias notas 4 e 5, conforme legenda abaixo:

1 - Péssimo	2 - Ruim	3 - Regular	4 - Bom	5 - Excelente

5.7. A avaliação deve conter pelo menos os seguintes itens para julgamento:

Conteúdo / Programa	Adequação do conteúdo do programa.
	Aplicabilidade do conteúdo à realidade profissional.
	Equilíbrio entre a teoria e a prática.
	Nível de obtenção de novos conhecimentos.
Atuação do Instrutor	Conhecimentos do assunto tratado.
	Didática utilizada.

5.8. A **CONTRATADA** deverá fornecer certificado de participação individual contendo o nome do participante, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.9. Caso o treinamento seja ofertado de forma presencial, o **CONTRATANTE** irá disponibilizar sala de aula e um computador por aluno para realização do treinamento nas dependências do **CONTRATANTE**.

5.10. O treinamento poderá ser efetivado de forma remota. Caso seja utilizada a modalidade remota, a **CONTRATADA** deverá fornecer um laboratório remoto, para que os participantes possam simular os conceitos abordados. Neste caso será utilizada a ferramenta de videoconferência institucional do **CONTRATANTE**.

5.11. Será de responsabilidade da **CONTRATADA** prover todas as despesas relativas a pessoal especializado para ministrar a capacitação e quaisquer outras despesas oriundas, derivadas ou conexas, ambiente virtual de aprendizagem, simuladores e material didático.

5.12. A **CONTRATADA** deverá também fornecer ambiente virtual de emulação dos softwares da solução ou disponibilizar equipamentos para realização dos laboratórios e exercícios práticos, não podendo utilizar-se dos que serão usados na execução dos serviços de segurança. Essa restrição visa não atrasar a implantação dos novos serviços por conta do treinamento.

5.13. Os instrutores designados pela **CONTRATADA** deverão ser profissionais capacitados na solução ofertada e possuírem conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados, com experiência comprovada por meio de certificação oficial, emitida pelo fabricante dos equipamentos que serão utilizados na prestação dos serviços, de engenheiro especialista ou similar.

5.14. A **CONTRATADA** deverá apresentar, com no mínimo 15 (quinze) dias de antecedência para o início do treinamento, a(s) certificação(ões) oficial(is) do(s) instrutor(es) emitida(s) pelo fabricante dos equipamentos a serem utilizados na prestação dos serviços desta contratação.

5.15. A **CONTRATADA** deve permitir a gravação do treinamento, em todo conteúdo ministrado, a ser realizada com recursos do **CONTRATANTE** e com finalidade de uso exclusivamente interno do **CONTRATANTE**, sem possibilidade de divulgação a terceiros, exceto se expressamente permitido pela **CONTRATADA**.

6. SUPORTE TÉCNICO E GERENCIAMENTO DOS SERVIÇOS:

6.1. A **CONTRATADA** deverá disponibilizar ao **CONTRATANTE** um número telefônico único, um endereço de email e um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados. Entende-se por portal, ferramenta de gerência acessível pela internet, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS.

6.2. No atendimento por meio de telefone a **CONTRATADA** fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

6.3. O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências, registros de solicitações e reclamações enviadas pelo MPAM em relação aos serviços prestados.

6.4. Cada chamado deverá conter, no mínimo, as seguintes informações:

6.4.1. Número único do registro/ocorrência - a ser fornecido pela **CONTRATADA**.

6.4.2. Identificação do atendente.

6.4.3. Identificação do solicitante.

6.4.4. Data e hora de abertura do chamado/início da interrupção.

6.4.5. Descrição da ocorrência.

6.4.6. Designação do equipamento, quando for o caso.

6.4.7. Ações corretivas tomadas.

6.4.8. Situação - aberto, solucionado, fechado, em atendimento, improcedente, duplicado e similares.

6.5. O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

6.6. O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da **CONTRATADA**.

6.7. Não deverá haver qualquer limitação para o número de solicitações de reparo.

6.8. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos serviços prestados, ou seja, a **CONTRATADA** deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

7. GARANTIA TÉCNICA:

7.1. A **CONTRATADA** deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, a ser prestado em Manaus, capital do Estado do Amazonas, a contar da emissão dos Termos de Aceite referentes aos itens 01, 02 e 03, sendo considerada a data daquele que for emitido por último.

7.2. A **CONTRATADA** deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual.

7.3. Os produtos devem ser isentos de falhas e vulnerabilidades tais como vírus, malwares e outras pragas digitais, inclusive backdoors.

7.4. A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas ao **CONTRATANTE**.

7.5. Caso sejam detectadas falhas ou bugs nos produtos, a **CONTRATADA** deverá realizar as atualizações necessárias à correção do problema.

7.6. A **CONTRATADA** deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

7.7. A **CONTRATADA** é a única responsável pelos produtos fornecidos ao **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.

7.8. A **CONTRATADA** responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo **CONTRATANTE**, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

7.9. Caso sejam detectados erros ou impropriedades na solução apresentada, caberá à **CONTRATADA** apresentar novas soluções dentro dos prazos e condições estabelecidas no Acordo de Nível de Serviço - SLA, sem prejuízo de aplicação de penalidades previstas.

7.10. Os hardwares e softwares oferecidos não podem constar, durante toda vigência do contrato, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

7.11. A **CONTRATADA** deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas durante todo período de vigência do contrato, sem ônus adicional para o **CONTRATANTE**.

7.12. No que se refere a software, durante a vigência do Contrato, a **CONTRATADA** deverá prover e aplicar toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o **CONTRATANTE**. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

7.12.1. Patches, fixes, correções, updates e service packs.

7.12.2. Novas releases, builds e funcionalidades.

7.12.3. O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito.

7.12.4. O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do contrato.

7.12.5. Se os equipamentos forem descontinuados pelo fabricante, o mesmo deverá ser substituído pelo seu sucedâneo caso deixe de receber as atualizações de assinaturas e de segurança.

7.12.6. A cada nova liberação de versão e release, a **CONTRATADA** deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

7.12.7. A **CONTRATADA** deverá fornecer tais atualizações independentemente de solicitação expressa do **CONTRATANTE**.

7.12.8. A **CONTRATADA** deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato.

7.12.9. As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas para terem vigência, no mínimo, durante o prazo contratual.

8. MANUTENÇÃO PREVENTIVA E CORRETIVA:

8.1. Os serviços de manutenção *on-site*, serão prestados nas dependências do **CONTRATANTE** na cidade de Manaus, no Estado do Amazonas, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo fabricante, credenciada através de declaração do fabricante e com técnicos treinados e certificados nos equipamentos, ou diretamente pelo fabricante dos produtos.

8.2. O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a substituição total ou parcial do produto como peças, partes, componentes e acessórios. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do **CONTRATANTE**, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

8.3. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho.

8.4. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, peças, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso.

8.5. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados para todos os produtos fornecidos.

8.6. A **CONTRATADA** deverá executar a assistência técnica preventiva (conforme SLA) e a corretiva sempre que solicitado pelo **CONTRATANTE** ou quando seu monitoramento indique algum incidente. Sendo que a prestação desses serviços deve ser realizada nas dependências do **CONTRATANTE**, onde se encontrarem instalados esses produtos, somente para os casos em que não seja possível a execução remota.

8.7. O **CONTRATANTE** poderá determinar à **CONTRATADA** a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos, conforme SLA. Para os casos de manutenção corretiva, essas serão solicitadas sempre que a solução apresentar falhas e não haja atendimento por parte da **CONTRATADA**.

8.8. Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, traslado, deslocamento, embalagem, peças, partes, manuais do fabricante e/ou outras despesas oriundas, derivadas ou conexas, serão de inteira responsabilidade da **CONTRATADA**, não devendo gerar qualquer ônus adicional ao **CONTRATANTE**.

8.9. A **CONTRATADA** deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências para subsidiar as análises e decisões administrativas do **CONTRATANTE**.

8.10. O serviço de suporte deverá ser efetuado *on-site* sempre que se fizer necessário ou quando for solicitado pelo **CONTRATANTE**, cobrindo todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o **CONTRATANTE**.

8.11. Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do **CONTRATANTE**, a **CONTRATADA** deverá desinstalar, embalar e transportar

o item defeituoso, instalar item temporário e reinstalar o item reparado, bem como deverá arcar com todos os custos inerentes à operação.

8.12. Quando da detecção de problemas ou inconformidades, a **CONTRATADA** deverá imediatamente abrir um chamado técnico, informar o **CONTRATANTE** e providenciar a sua reparação dentro dos prazos estabelecidos no Acordo de Nível de Serviço (SLA).

8.13. A **CONTRATADA** encaminhará mensagem de e-mail para o **CONTRATANTE**, em endereço a ser disponibilizado para esse fim, informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da **CONTRATADA** e/ou por meio de abertura de chamado a critério da equipe técnica do **CONTRATANTE**, conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

8.14. Todos os custos diretos e indiretos para realização do atendimento presencial (*on-site*) serão de responsabilidade exclusiva da **CONTRATADA**.

8.15. Dentro do mesmo endereço, a ser executada pela **CONTRATADA**, durante a vigência do contrato, a localidade de instalação poderá sofrer até 1 (uma) alteração, sem custos adicionais para o **CONTRATANTE**.

8.16. Para liberação de acesso aos locais de instalação dos ativos integrantes da solução, durante a vigência do contrato, o(s) técnico(s) designado(s) para prestar o atendimento deverá(ão) se apresentar devidamente identificado(s) no ato do atendimento.

8.17. O pedido de atendimento poderá ocorrer por meio de alertas provenientes do sistema de monitoramento ou por meio de solicitação formal efetuada por servidor do **CONTRATANTE**, devidamente credenciado, mediante o registro da demanda e abertura de ordem de serviço.

8.18. Em qualquer modalidade o atendimento deve ser prestado em português e estar disponível vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365).

8.19. A **CONTRATADA** deve possuir equipe técnica de suporte com pelo menos 02 (dois) profissionais capacitados e certificados oficialmente pelo fabricante da solução ofertada, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada, além de comprovação do vínculo profissional dos técnicos com a pretensa licitante, no início da presstação dos serviços. Sempre que houver mudança na equipe técnica da **CONTRATADA**, deve haver comunicação formal ao **CONTRATANTE**, incluindo as comprovações exigidas.

9. ACORDO DE NÍVEL DE SERVIÇO (SLA):

9.1. Os serviços deverão ser prestados de forma ininterrupta, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, observados os parâmetros de qualidade mínimos previstos neste termo.

9.2. A **CONTRATADA** deverá executar a assistência técnica preventiva a cada 2 (dois) meses.

9.3. A **CONTRATADA** deverá executar a assistência técnica corretiva em até 2 (dois) dias úteis após a abertura de chamado ou detecção da falha.

9.4. A realização de assistência técnica preventiva, caso não seja solicitada pelo **CONTRATANTE**, deverá ser comunicada com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do **CONTRATANTE**.

9.5. Em caso de uso de CPU/MEMÓRIA acima de 75%, para o funcionamento em modo ativo/passivo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

9.6. Em caso de uso de CPU/MEMÓRIA acima de 50%, para o funcionamento em modo ativo/ativo, dentro do horário de pico (8hs as 14hs, de segunda a sexta) por pelo menos 3 (três) dias consecutivos, a solução será considerada como operando em Modo de Contingência.

9.7. Qualquer parte da solução que apresente 3 (três) ocorrências de defeitos ou deficiências em um período de 15 (quinze) dias, não implicando na indisponibilidade do serviço do **CONTRATANTE**, a solução será considerada como operando em Modo de Contingência.

9.8. Em caso de comprometimento da alta disponibilidade, a solução será considerada como operando em Modo de Contingência.

9.9. A **CONTRATADA** deverá manter os equipamentos de TI utilizados nas versões mais recentes dos softwares, updates, releases, builds e service packs necessários para o devido funcionamento da solução durante a vigência contratual. Este checkup faz parte da manutenção preventiva.

9.10. Será permitido o funcionamento da solução em Modo de Contingência por um período máximo de 60 dias consecutivos.

9.11. O Modo de Contingência se caracteriza por:

9.11.1. Funcionalidade de alta disponibilidade (redundância) comprometida por falha em qualquer componente de um dos conjuntos da solução que não implique em parada total, mas inviabilize a alta disponibilidade.

9.11.2. Funcionamento acima dos limiares de desempenho, conforme estabelecido nos itens 9.5 e 9.6 acima.

9.11.3. Qualquer componente da solução que se encontre em lista de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante ou fora de garantia.

9.11.4. Operação com funcionalidade ou performance abaixo dos mínimos exigidos neste Termo.

9.12. Excedidos 30 (trinta) dias do prazo máximo estabelecido para o funcionamento em Modo de Contingência, a solução será considerada como em estado de Inoperância Total, ainda que permaneça funcionando em Modo de Contingência, caracterizando a não prestação do serviço contratado.

9.13. O estado de Inoperância Total se caracteriza por caso de falha ou vício que implique na indisponibilidade total ou parcial de qualquer serviço do **CONTRATANTE**.

9.14. O prazo máximo para reestabelecimento do serviço que esteja em estado de Inoperância Total é de 6 (seis) horas, contados da abertura de chamado ou detecção da falha pela **CONTRATADA**.

CLÁUSULA QUARTA – DOS PRAZOS PARA A PRESTAÇÃO DOS SERVIÇOS:

A **CONTRATADA** deverá concluir a implantação, ativação e entrega dos sistemas e equipamentos que compõem os itens 01, 02 e 03, especificados cláusula anterior deste ajuste, **em até 65 (sessenta e cinco) dias corridos**, contados a partir da assinatura do contrato.

Parágrafo primeiro. A **CONTRATADA** deverá, em comum acordo com o **CONTRATANTE**, no prazo máximo de **120 (cento e vinte) dias corridos**, contados a partir da assinatura do contrato, finalizar o treinamento indicado no item 04 da cláusula anterior.

Parágrafo segundo. A **CONTRATADA** poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pela **CONTRATANTE**, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, da lei n. 8.666/93.

Parágrafo terceiro. Antes de findar os prazos fixados nos itens anteriores, a **CONTRATADA** poderá formalizar pedido de sua prorrogação, de forma oficial e fundamentada, cujas razões expostas serão examinadas pelo **CONTRATANTE,** que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato, observado o disposto no artigo 57, 410 da lei n. 8.666/93.

Parágrafo quarto. O prazo da prestação dos serviços deverá contar da assinatura do contrato, prorrogáveis de comum acordo, até o limite estabelecido na Lei n. 8.666/93, e suas alterações.

CLÁUSULA QUINTA – DO RECEBIMENTO:

O recebimento dos serviços será realizado pela **FISCALIZAÇÃO** do **CONTRATANTE**.

Parágrafo primeiro. O recebimento será feito nas seguintes etapas:

1. Será emitido Termo Individual de ACEITE para cada item do Contrato.

2. Será emitido Termo de Recebimento Definitivo para todo o Lote.

Parágrafo segundo. Para fins de aceite, a **CONTRATADA** deverá comunicar formalmente a efetiva disponibilização dos serviços para cada item do Lote:

1. Para a emissão do Termo Individual de ACEITE para o Item 01:

1.1. Será emitido após Período de Funcionamento Experimental de até 15 (quinze) dias, que se iniciará após comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

1.2. Durante Período de Funcionamento Experimental a **FISCALIZAÇÃO** deverá concluir os testes necessários para constatar o funcionamento regular dos serviços disponibilizados.

1.3. A **FISCALIZAÇÃO** realizará avaliação qualitativa das especificações dos equipamentos e funcionalidades que compõem a solução conforme exigências deste Termo.

2. Para a emissão do Termo Individual de ACEITE para o Item 02:

2.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

2.2. A **FISCALIZAÇÃO** realizará testes com as credenciais fornecidas, teste de uso da ferramenta e teste de disponibilidade necessários para constatar o funcionamento regular dos serviços disponibilizados.

3. Para a emissão do Termo Individual de ACEITE para o Item 03:

3.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito, por parte da **CONTRATADA**, incluindo evidencias que demonstrem inequivocadamente que todas os critérios estabelecidos na seção 5.4 deste Termo foram atendidos, atestando a efetiva disponibilização dos serviços.

3.2. A **FISCALIZAÇÃO** realizará avaliação qualitativa das evidências apresentadas considerando a disponibilidade dos serviços do **CONTRATANTE**.

4. Para a emissão do Termo Individual de ACEITE para o Item 04:

4.1. Será emitido em até 15 (quinze) dias após a comunicação por escrito por parte

da **CONTRATADA** atestando a efetiva disponibilização dos serviços.

4.2. A **FISCALIZAÇÃO** observará os critérios estabelecidos na seção 5.5 deste Termo.

Parágrafo terceiro. Somente depois de realizados e aprovados os testes definidos, o **CONTRATANTE**, por meio da **FISCALIZAÇÃO**, emitirá o Termo de Aceite, atestando a conformidade com as especificações neste Contrato, liberando o início de faturamento.

Parágrafo quarto. A contagem do prazo para a efetiva entrega e prestação de cada item de serviço especificado no lote será suspenso quando a **CONTRATADA** comunicar a efetiva disponibilização do serviço, e, se for o caso, será retomado no dia seguinte a partir da emissão de comunicado por escrito do **CONTRATANTE** indicando NÃO ACEITE do serviço em virtude de não conformidade com algum dos requisitos presentes nesse termo de referência.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO:

A execução do objeto deste contrato dar-se-á indiretamente pela **CONTRATADA**, sob o regime de empreitada por preço global.

CLÁUSULA SÉTIMA – DAS GARANTIAS:

Os serviços ora pactuados são garantidos em conformidade com o Código de Proteção e Defesa do Consumidor, Lei n.º 8.078, de 11 de setembro de 1990, artigos 26 e 27, e nos termos do Item 7 da Cláusula Terceira deste Contrato.

CLÁUSULA OITAVA – GESTÃO E DA FISCALIZAÇÃO:

A **CONTRATANTE** nomeará um servidor ou comissão, por meio de ato específico, doravante denominado(a) **FISCALIZAÇÃO**, para gerir e fiscalizar a execução deste contrato, com autoridade para exercer, como representante da **CONTRATANTE**, toda e qualquer ação destinada ao acompanhamento da execução contratual, observando as determinações do artigo 67 da Lei n.º 8.666/93, em especial:

1. Abrir processo de gestão do presente contrato, fazendo constar todos os documentos referentes à fiscalização dos serviços.
2. Gerir, acompanhar e fiscalizar a execução dos serviços, realizando diretamente toda e qualquer comunicação com a **CONTRATADA**, mediante ofício ou outros documentos.
3. Atestar a respectiva nota fiscal/fatura emitida corretamente pela **CONTRATADA**, para a efetivação do pagamento correspondente.
4. Verificar quando da liquidação dos serviços a documentação de regularidade fiscal da **CONTRATADA**.
5. Indicar as ocorrências verificadas, determinando o que for necessário à regularização das faltas observadas.
6. Fixar prazo limite para realização das providências necessárias à regularização de eventuais vícios, defeitos ou incorreções resultantes da execução do presente contrato.
7. Solicitar à **CONTRATADA** e a seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento da avença e anexar aos autos cópia dos documentos que comprovem essas solicitações.
8. **Informar, com a antecedência necessária, o término do ajuste.**
9. Encaminhar à Administração Superior toda e qualquer modificação que se faça necessária e envolva acréscimo ou supressão de despesa e dilatação de prazos, para fins das providências administrativas indispensáveis.
10. Verificar a manutenção das condições de habilitação da **CONTRATADA**, exigindo sua regularização, durante a vigência do contrato.
11. Prestar as informações e os esclarecimentos necessários ao desenvolvimento das tarefas.
12. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições no curso de execução do objeto do contrato, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.
13. Rejeitar, no todo ou em parte, o fornecimento executado em desacordo com o contrato.
14. Comunicar à Administração, de forma imediata, as ocorrências que impliquem possíveis sanções à **CONTRATADA**, bem como as decisões e providências que ultrapassarem sua competência, para a adoção das medidas convenientes.
15. Praticar todos os demais atos e exigências que se fizerem necessários ao fiel cumprimento do presente contrato.

Parágrafo primeiro. A **FISCALIZAÇÃO** será exercida no interesse da **CONTRATANTE** e não exclui nem reduz as responsabilidades contratuais da **CONTRATADA**, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade do poder público ou de seus agentes e prepostos.

Parágrafo segundo. Quaisquer exigências da **FISCALIZAÇÃO** inerentes ao objeto deste contrato deverão ser prontamente atendidas pela **CONTRATADA**, sem qualquer ônus para a **CONTRATANTE**.

Parágrafo terceiro. A **CONTRATADA** deverá manter preposto, aceito pela **CONTRATANTE**, para representá-la administrativamente na execução do contrato, devendo, **no prazo máximo de 10 (dez) dias da assinatura do instrumento,** informar nome, telefone, endereços e outros meios de comunicação entre a **CONTRATANTE** e o preposto responsável pela execução do contrato operacional e financeira.

Parágrafo quarto. As comunicações e notificações feitas pela **CONTRATANTE** à **CONTRATADA**, a serem realizadas sob o âmbito do presente contrato, serão feitas por meio de ofícios, e-mails ou por telefone.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA:

Constituem obrigações da **CONTRATADA**:

1. Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo, observando as prescrições e as recomendações do fabricante/fornecedor, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.
2. Comunicar imediatamente, à **CONTRATANTE**, toda e qualquer irregularidade ou dificuldade que impossibilite a execução dos serviços objeto deste contrato.
3. Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que o **CONTRATANTE** julgar necessário.
4. Manter contato e realizar o planejamento dos serviços com o **CONTRATANTE** de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.
5. Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, o objeto deste ajuste que não atenda às especificações exigidas, em que se verifiquem imperfeições, vícios, defeitos ou incorreções ou rejeitados pela fiscalização.
6. Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pelo **CONTRATANTE** em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste contrato.
7. Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.
8. Acatar as observações feitas pela **FISCALIZAÇÃO** quanto à execução dos serviços.
9. Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.
10. Reparar, corrigir, remover ou substituir, às suas expensas, no todo ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.
11. Seguir as orientações da Lei n. 9.472/97, do Termo de Concessão ou autorização emitido pela ANATEL, e demais disposições regulamentares pertinentes aos serviços a serem prestados.
12. Credenciar junto ao **CONTRATANTE** um representante, denominado preposto, aceito pelo **CONTRATANTE**, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, indicando as formas de contato no mínimo telefone, para comunicação rápida e email para comunicação formal.
13. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação.
14. Implantar a supervisão permanente dos serviços, de modo adequado e de forma a obter uma operação correta e eficaz.
15. Responsabilizar-se por todos os serviços não explícitos nestas especificações, mas necessários à execução dos serviços programados e ao perfeito funcionamento das instalações.
16. Respeitar o sistema de segurança do **CONTRATANTE** e fornecer todas as informações solicitadas por ele.
17. Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.
18. Acatar que o **CONTRATANTE** não aceitará, sob nenhum pretexto, a transferência de responsabilidade da **CONTRATADA** para outras entidades, sejam fabricantes, representantes ou

quaisquer outros.

Parágrafo primeiro. A inadimplência da **CONTRATADA**, com referência aos encargos decorrentes dos serviços constantes deste contrato, não transfere à **CONTRATANTE** a responsabilidade por seu pagamento, nem pode onerar o objeto do contrato ou restringir a manutenção contratada.

Parágrafo segundo. A **CONTRATADA** declara, antecipadamente, aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos, explicações que a **CONTRATANTE** julgar necessário.

Parágrafo terceiro. A inobservância das especificações constantes deste Contrato implicará a não aceitação parcial ou total dos serviços, devendo a **CONTRATADA** refazer as partes recusadas sem direito a indenização.

Parágrafo quarto. Todos os equipamentos fornecidos pela **CONTRATADA**, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área, tais como: ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações).

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE:

Constituem obrigações do **CONTRATANTE**:

1. Fornecer à **CONTRATADA** as informações necessárias à fiel execução do objeto deste Termo.
2. Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA** durante o prazo de vigência deste Contrato.
3. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 8.666/93, o exato cumprimento das cláusulas e condições contratuais.
4. Designar, e informar à **CONTRATADA**, fiscal do contrato e seu substituto, mantendo tais dados atualizados.
5. Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos materiais, de forma a assegurar o perfeito cumprimento do contrato.
6. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção e exigindo as medidas reparadoras devidas.
7. Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este Termo.
8. Fazer uso adequado dos equipamentos fornecidos pela **CONTRATADA**, seguindo as instruções constantes de seus manuais de uso.
9. Efetuar regularmente o pagamento à **CONTRATADA**, conforme nota de empenho e dentro dos critérios estabelecidos neste contrato, quanto aos serviços efetivamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pela **CONTRATANTE**, bem como dos demais documentos exigidos neste termo.

CLÁUSULA DÉCIMA PRIMEIRA – DA VIGÊNCIA DO CONTRATO:

O presente contrato terá vigência de **48 (quarenta e oito) meses**, contados da sua assinatura, conforme art. 57, inciso IV, da Lei n.º 8.666/1993.

Parágrafo primeiro. O prazo acima referido terá início e vencimento em dia de expediente e terá eficácia legal após a publicação de seu extrato na impressa oficial.

CLÁUSULA DÉCIMA SEGUNDA – DO VALOR DO CONTRATO:

O valor global do presente contrato é de **R$ 2.478.052,85 (dois milhões, quatrocentos e setenta e oito mil, cinquenta e dois reais e oitenta e cinco centavos)**, conforme a seguinte tabela:

ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO (B)	VALOR TOTAL
01	Serviço de Firewall em Alta Disponibilidade	Meses	48	R$ 44.791,66	R$ 2.149.999,68
02	Serviço de Monitoramento da Solução	Meses	48	R$ 5.208,33	R$ 249.999,84
03	Serviço de Migração do Ambiente Atual	Unidades	01	R$ 30.553,33	R$ 30.553,33
04	Serviço de Treinamento da Solução	Pessoas	05	R$ 9.500,00	R$ 47.500,00

TOTAL (R$)	**R$ 2.478.052,85**

Parágrafo primeiro. A proposta apresentada pela **CONTRATADA**, datada de 21 de fevereiro de 2022, faz parte deste instrumento contratual como anexo.

Parágrafo segundo. No preço total do contrato já estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, lucro e outros necessários ao cumprimento integral do objeto deste instrumento.

CLÁUSULA DÉCIMA TERCEIRA – DA LIQUIDAÇÃO E DO PAGAMENTO:

O pagamento será efetuado após a efetiva disponibilização dos serviços pela **CONTRATADA** e emissão pelo **CONTRATANTE** do Termo Individual de Aceite para cada item do Lote, mediante depósito na conta corrente da **CONTRATADA**, por meio de ordem bancária, seguindo as seguintes etapas:

1. Para os Itens 01 e 02:

1.1 Mensalmente, a **CONTRATADA** deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

1.2 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada dia de funcionamento da solução em Modo de Contingênica além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

1.3 Desconto de 2% (dois por cento) sobre o valor da parcela mensal contratada, a ser descontado diretamente na fatura do respectivo mês, para cada hora de funcionamento da solução em estado de Inoperância Total além do limite estabelecido na seção 5.9 - Acordo de Nível de Serviço (SLA).

1.4 A data de início de cobrança dos serviços deverá observar a data de emissão do Termo de Aceite, sendo que a primeira fatura corresponderá à prestação de serviços desde a data de emissão do Termo de Aceite, para cada item do Lote, até o último dia do respectivo mês, de forma pro rata.

1.5 As demais faturas deverão abranger o período do primeiro ao último dia do mês.

1.6 Os valores a serem faturados concernentes aos serviços objeto desta contratação estarão sujeitos a descontos nas situações de descumprimento das metas estabelecidas para os indicadores elencados na especificação do serviço, item Acordo de Nível de Serviço (SLA).

1.7 Os descontos aplicados nas faturas mensais não isentam a **CONTRATADA** de quaisquer sanções legais ou das sanções dispostas na seção 12 - SANÇÕES ADMINISTRATIVAS.

1.8 Os descontos aplicados nas faturas mensais, conforme dispostos acima, oriundos do descumprimento dos níveis mínimos de serviço estipulados no item Acordo de Nível de Serviço (SLA), não se configuram como penalidades ou multas.

1.9 No primeiro dia útil do mês subsequente, antes da emissão na nota fiscal, a **CONTRATADA** deverá enviar à **FISCALIZAÇÃO** relatório referente aos períodos, destacando eventuais descontos e as causas da(s) indisponibilidade(s) ocorridas na prestação dos serviços para a devida aprovação.

1.10 As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da **CONTRATADA** no que diz respeito ao atendimento dos níveis de serviços especificados no acordo de nível de serviço, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

2. Para os Itens 03 e 04:

2.1 A **CONTRATADA** deverá apresentar, para fins de liquidação e pagamento, Nota Fiscal ou Fatura relativa aos serviços prestados, devidamente acompanhada das comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF), CNDT e às Fazendas Federal, Estadual e Municipal.

2.2 Os pagamentos relativos aos Itens serão realizados de uma única vez, no mês seguinte a emissão do Termo de Aceite.

Parágrafo primeiro. A nota fiscal e os demais documentos exigidos no edital e neste contrato, para fins de liquidação e pagamento das despesas, deverão ser apresentados no Setor de Protocolo da **CONTRATANTE**, situado na Avenida Coronel Teixeira, n.º 7.995, Nova Esperança, Manaus/AM ou enviados ao e-mail **protocolo@mpam.mp.br.**

Parágrafo segundo. Ao **CONTRATANTE** fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas neste Termo.

Parágrafo terceiro. Nenhum pagamento será efetuado à **CONTRATADA** quando forem constatadas as irregularidades abaixo especificadas, sendo que tais situações não caracterizam inadimplência da **CONTRANTATE** e, por conseguinte, não geram direito à compensação financeira: a) os

serviços/produtos não abrangidos pelo objeto contratual; b) ausência de comprovação da regularidade fiscal e trabalhista da **CONTRATADA**, e c) pendência de liquidação de qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

Parágrafo quarto. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

Parágrafo quinto. O atraso no pagamento decorrente das circunstâncias descritas na obrigação anterior, não exime a **CONTRATADA** de promover o pagamento de impostos e contribuições nas datas regulamentares.

Parágrafo sexto. O documento fiscal será devolvido à **CONTRATADA** caso contenha erros ou em caso de circunstância que impeça a sua liquidação, ficando o pagamento pendente até que seja sanado o problema. Nessa hipótese, o prazo para pagamento se iniciará após a regularização ou reapresentação do documento fiscal, não acarretando qualquer ônus para a **CONTRATANTE**.

Parágrafo sétimo. Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela **CONTRATANTE**, entre a data de vencimento e a do dia do efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, serão calculados por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = i ÷ 365 = (6÷100) ÷ 365 = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

Parágrafo oitavo. Aplica-se a mesma regra disposta no parágrafo anterior, na hipótese de eventual pagamento antecipado, observado o disposto no art. 40, XIV, "d", da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA:

1) **Unidade Gestora:** 03101 - Procuradoria Geral de Justiça**; Unidade Orçamentária**: 03101 - Procuradoria Geral de Justiça; **Programa de Trabalho**: 03.122.0001.2001.0001 - Administração da Unidade; **Fonte**: 0100 - Recursos Ordinários; **Natureza da Despesa**: 33904016 - Locação de Software, tendo sido emitida, pela **CONTRATANTE**, em 31/03/2022, a Nota de Empenho n.º 2022NE0000539, no valor global de **R$** 480.553,24 **(quatrocentos e oitenta mil, quinhentos e cinquenta e três reais e vinte e quatro centavos)**.

2) **Unidade Gestora:** 03101 - Procuradoria Geral de Justiça**; Unidade Orçamentária**: 03101 - Procuradoria Geral de Justiça; **Programa de Trabalho**: 03.122.0001.2001.0001 - Administração da Unidade; **Fonte**: 0100 - Recursos Ordinários; **Natureza da Despesa**: 33904012 - Treinamento e capacitação em TIC, tendo sido emitida, pela **CONTRATANTE**, em 31/03/2022, a Nota de Empenho n.º 2022NE0000540, no valor global de **R$** 47.500,00 **(quarenta e sete mil e quinhentos reais)**.

CLÁUSULA DÉCIMA QUINTA – DA GARANTIA CONTRATUAL:

Nos termos do art. 56 da Lei n º 8.666, de 21/6/1993, para segurança do integral cumprimento do Contrato, a **CONTRATADA** apresentará garantia, no prazo máximo de 10 (dez) dias da assinatura deste contrato, de **5% (cinco por cento)** do valor total do contrato, que corresponde à importância de **R$ 123.902,64 (cento e vinte e três mil, novecentos e dois reais e sessenta e quatro centavos).**

1. Será ainda exigida prestação de garantia adicional de valor igual à diferença entre o valor limite de exequibilidade obtido durante o certame e o valor da proposta vencedora, desde que este seja inferior a 80% (oitenta por cento) da média aritmética calculada, nos termos do § 2º, do artigo 48, da Lei Federal nº 8.666/93.

2. No caso de acréscimo no valor contratual, a licitante vencedora obriga-se a depositar junto ao Ministério Público, na mesma modalidade, o valor referente à diferença da garantia. Mesma providência deverá ser tomada no caso de prorrogação no prazo contratual para adequar o vencimento da garantia ao disposto no subitem abaixo.

3. As garantias prestadas serão liberadas após a assinatura do Termo de Encerramento do contrato, e quando em dinheiro atualizadas monetariamente, conforme dispões o § 4º, do artigo 56 da Lei n. 8.666/93.

Parágrafo primeiro. A garantia prestada deverá formalmente cobrir pagamentos não efetuados pela **CONTRATADA** referentes à:

1. prejuízos advindos do não cumprimento do objeto do contrato;

2. prejuízos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

3. multas punitivas aplicadas pela Administração à **CONTRATADA**; e

4. obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**.

Parágrafo segundo. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no parágrafo primeiro.

Parágrafo terceiro. A garantia em dinheiro deverá ser efetuada em conta caução, devidamente designada para este fim, aberta em instituição financeira oficial e mediante autorização específica da **CONTRATANTE**.

Parágrafo quarto. A garantia deverá ter validade durante a execução do contrato e estender-se-á por mais **3 (três) meses após o término da vigência contratual**. Na hipótese de prorrogação do prazo de vigência contratual, a **CONTRATADA** deverá apresentar prorrogação equivalente de prazo de validade da referida garantia.

Parágrafo quinto. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato, por dia de atraso, observado o máximo de 2% (dois por cento).

Parágrafo sexto. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a retenção dos pagamentos devidos à **CONTRATADA** e/ou a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n.º 8.666, de 1993.

1. O bloqueio efetuado com base neste parágrafo não gera direito a nenhum tipo de compensação financeira à **CONTRATADA**.
2. A **CONTRATADA**, a qualquer tempo, poderá substituir o bloqueio efetuado por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

Parágrafo sétimo. A **CONTRATADA** se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, para o pagamento da multa contratual ou encargos trabalhistas e previdenciários, e ainda, na alteração do valor contratado, para manter o percentual inicial, **no prazo de até 10 (dez) dias**, contados da assinatura do termo aditivo ou a partir da data em que for notificada pela **CONTRATANTE**, a partir do qual se observará o disposto nesta cláusula.

Parágrafo oitavo. A garantia somente será liberada ante a comprovação de que a empresa pagou todos os encargos trabalhistas e previdenciárias decorrentes da contratação, bem como apresentação de toda a documentação solicitada no edital pela **CONTRATANTE**.

Parágrafo nono. Será considerada extinta a garantia:

1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da **CONTRATANTE**, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do contrato;
2. no prazo de três meses após o término da vigência, caso a **CONTRATANTE** não comunique a ocorrência de sinistros.

Parágrafo décimo. A garantia não será extinta, em caso de ocorrência de sinistro ou irregularidade, devidamente comunica à seguradora pela **FISCALIZAÇÃO.**

CLÁUSULA DÉCIMA SEXTA – DO REAJUSTAMENTO:

Os preços propostos não serão reajustados durante todo o período de vigência do contrato.

CLÁUSULA DÉCIMA SÉTIMA – DAS ALTERAÇÕES:

Competem a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei n.º 8.666/1993 e em outras disposições legais pertinentes, realizar, por escrito, por meio de Termo Aditivo, as alterações contratuais que julgarem convenientes.

Parágrafo único. A **CONTRATADA** fica obrigada a aceitar as alterações unilaterais, conforme disposto no art. 65, I, da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA OITAVA – DAS PENALIDADES:

Em caso de inexecução total ou parcial, execução imperfeita, ou qualquer inadimplemento ou infração contratual, a **CONTRATADA**, sem prejuízo das responsabilidades civil e criminal, ficará sujeita às seguintes penalidades:

1. advertência;

2. multas percentuais, nos termos do parágrafo segundo desta cláusula;

3. rescisão administrativa do contrato;

4. suspensão temporária do direito de participar de licitação e impedimento de contratar;

5. declaração de inidoneidade para licitar e contratar.

Parágrafo primeiro. As penas acima referidas serão propostas pela **FISCALIZAÇÃO** e impostas pela autoridade competente, assegurada à **CONTRATADA** a prévia e ampla defesa na via administrativa.

Parágrafo segundo. A Advertência por escrito será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem corno, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do **CONTRATANTE**.

Parágrafo terceiro. Serão aplicadas à **CONTRATADA** as seguintes multas:

I - **2% (dois por cento)** sobre o valor global contratado, a cada reincidência na penalidade de advertência. Na hipótese de reincidência por 5 (cinco) vezes na penalidade de advertência, será considerado descumprimento total da obrigação, punível com as sanções previstas em lei.

II - **2% (dois por cento)** sobre o valor global contratado, por dia de atraso, no caso de descumprimento do tempo máximo, conforme Clásula Quarta - DOS PRAZOS PARA A PRESTAÇÃO DOS SERVIÇOS, limitado a 10 (dez) dias. O atraso superior a 10 (dez) dias será considerado como descumprimento total da obrigação, punível com as sanções previstas em lei.

III - **10% (dez por cento)** sobre o valor global contratado, no caso de, sem justificativa aceita pelo **CONTRATANTE**, o vencedor não retirar a Nota de Empenho, a Autorização de Fornecimento de Materiais/Serviço ou não assinar o contrato deixando, assim, de cumprir os prazos fixados, sem prejuízo das demais sanções previstas.

IV - **até 20% (vinte por cento)** sobre o valor global contratado, nos casos de INEXECUÇÃO PARCIAL do objeto contratado.

V - **até 30% (trinta por cento)** sobre o valor global contratado, nos casos de INEXECUÇÃO TOTAL do objeto contratado.

VI - **até 30% (trinta por cento)** sobre o valor global contratado, na hipótese de rescisão do contrato por culpa da **CONTRATADA**.

Parágrafo quarto. As multas contratuais serão descontadas dos pagamentos a que fizer jus a **CONTRATADA**, podendo ser cobrado judicialmente, quando necessário.

CLÁUSULA DÉCIMA NONA – DA RESCISÃO DO CONTRATO:

A inadimplência das cláusulas e condições estabelecidas neste contrato, por parte da **CONTRATADA**, assegurará à **CONTRATANTE** o direito de rescindir o contrato, mediante notificação através de ofício, entregue diretamente ou por via postal, com prova de recebimento, sem ônus de qualquer espécie para Administração e prejuízo das sanções previstas neste ajuste.

Parágrafo primeiro. Rescisão Unilateral. Ficará o presente contrato rescindido unilateralmente pela **CONTRATANTE**, mediante formalização, assegurado o contraditório e a ampla defesa, nos termos do art. 78, incisos I a XII e XVII, da Lei n.º 8.666/93.

Parágrafo segundo. Rescisão Bilateral. Ficará o presente contrato rescindido por acordo entre as partes, desde que haja conveniência para a Administração, nos casos do art. 78, XIII a XVI, da Lei n.º 8.666/93.

Parágrafo terceiro. Rescisão Judicial. O presente contrato poderá ser rescindido, judicialmente, nos termos da lei.

Parágrafo quarto. A falta dos registros ou documentações, incluindo a ART ou RRT, ou, ainda, constatada a irregularidade, ensejará o rompimento do vínculo contratual, sem prejuízo das multas contratuais, bem como das demais cominações legais.

Parágrafo quinto. Fica vedado, à **CONTRATADA**, sob pena de rescisão contratual, CAUCIONAR ou utilizar o contrato para qualquer operação financeira, sem prévia e expressa anuência da **CONTRATANTE**.

CLÁUSULA VIGÉSIMA – DO VÍNCULO EMPREGATÍCIO:

Os empregados e prepostos da **CONTRATADA** não terão qualquer vínculo empregatício com a **CONTRATANTE**, correndo por conta exclusiva da primeira todas as obrigações decorrentes da legislação trabalhista, previdenciária, fiscal e comercial, as quais se obriga a saldar na época devida.

CLÁUSULA VIGÉSIMA PRIMEIRA – DAS NORMAS APLICÁVEIS:

O presente contrato deverá respeitar as seguintes leis e/ou decretos e resoluções:

1. Lei n.º 8.666/1993 – Licitações e Contratos;
2. Lei n.º 8.078/1990 – Código de Defesa do Consumidor;
3. Lei n.º 10.406/2002 – Código Civil Brasileiro.

Parágrafo único. A **CONTRATADA** declara conhecer todas essas normas e concorda em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

CLÁUSULA VIGÉSIMA SEGUNDA – DO TRATAMENTO DOS DADOS PESSOAIS:

As partes obrigam-se a realizar o tratamento de dados pessoais em obediências as disposições legais vigentes, nos moldes da Lei 13.709/2018 (LGPD), visando dar efetiva proteção aos dados coletados de pessoas naturais que possam identificá-las ou torná-las identificáveis.

1. O consentimento para o tratamento de dados pessoais, citado nesta Cláusula, se dará por meio da assinatura deste contrato.
2. O tratamento de dados pessoais se dará, exclusivamente, para os fins necessários ao cumprimento do objeto deste Contrato sem a possibilidade de tratamento futuro incompatível com a finalidade.
3. O usuário autoriza expressamente que suas informações e dados pessoais sejam compartilhados pela **CONTRATADA** com Autoridades públicas, administrativas e judiciais, que, no exercício de sua competência, exijam informações, mesmo que não haja ordem ou citação executiva ou judicial para esse efeito, para os seguintes fins:

3.1. colaborar na investigação e denunciar fraudes, pirataria, violação de direitos de propriedade intelectual ou qualquer outro ato ilícito, bem como qualquer atividade ou circunstância que possa gerar responsabilidade legal para a **CONTRATADA** e/ou aos seus usuários;

3.2. resguardar um interesse público, a aplicação ou administração da justiça, o reconhecimento, exercício ou defesa de um direito em um processo judicial ou administrativo e/ou a resolução de disputas; e

3.3. cumprir com qualquer lei, regulamento ou disposição legal aplicável, ou algum mandato de autoridade competente devidamente fundamentado e motivado.

CLÁUSULA VIGÉSIMA TERCEIRA – DA PUBLICAÇÃO:

O presente contrato será publicado, sob a forma de extrato, no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, após a sua assinatura, correndo as despesas por conta da **CONTRATANTE**, nos termos do art. 61, parágrafo único, da Lei n.º 8.666/1993 e ATO PGJ N.º 082/2012.

CLÁUSULA VIGÉSIMA QUARTA – DAS DISPOSIÇÕES GERAIS:

A **CONTRATADA**, em cumprimento à Resolução n.º 37/2009 do Conselho Nacional do Ministério Público, declara que não possui sócios, gerentes ou diretores que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas.

Parágrafo único. Os casos omissos neste contrato serão resolvidos pela Administração Superior da **CONTRATANTE**, baseada na legislação vigente.

CLÁUSULA VIGÉSIMA QUINTA – DO FORO CONTRATUAL:

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na justiça estadual, no Foro de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

E por estarem de acordo, foi o presente termo de contrato, depois de lido e anuído, assinado digitalmente pelas partes e por duas testemunhas.

GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ministério Público do Estado do Amazonas

YURE LEOPOLDO SABINO DE FREITAS
Representante Legal
Network Secure Segurança da Informação Ltda

Documento assinado eletronicamente por **Géber Mafra Rocha**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 31/03/2022, às 15:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **YURE LEOPOLDO SABINO DE FREITAS**, **Representante Legal**, em 31/03/2022, às 15:57, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Maikon Antonio Freitas Martins**, **Testemunha**, em 04/04/2022, às 09:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Caroline Ellen Bezerra**, **Testemunha**, em 04/04/2022, às 13:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0790812** e o código CRC **84D3E91D**.

Ministério da Economia
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins previstos na Lei nº 8.666, de 1993, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**05.250.796/0001-54**	DUNS®:	**914627245**
Razão Social:	**NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**		
Nome Fantasia:	**NETWORK SECURE**		
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**24/11/2022**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Demais**		

Ocorrências e Impedimentos

Ocorrência:	**Nada Consta**
Impedimento de Licitar:	**Nada Consta**
Ocorrências Impeditivas indiretas:	**Nada Consta**
Vínculo com "Serviço Público":	**Nada Consta**

Níveis cadastrados:

Documento(s) assinalado(s) com "*" está(ão) com prazo(s) vencido(s).
Fornecedor possui alguma pendência no Nível de Cadastramento indicado. Verifique mais informações sobre pendências nas funcionalidades de consulta.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**23/08/2022**
FGTS		Validade:	**05/04/2022**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**23/08/2022**

IV - Regularidade Fiscal Estadual/Distrital e Municipal (Possui Pendência)

Receita Estadual/Distrital	Validade:	**25/03/2022** (*)
Receita Municipal	Validade:	**24/03/2022** (*)

VI - Qualificação Econômico-Financeira

Validade: **30/04/2022**

CPF: 614.178.822-04 Nome: HELDER NOBREGA RIBEIRO
Ass: _____

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

Nome completo: **NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**

CPF/CNPJ: **05.250.796/0001-54**

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 15:56:13 do dia 31/03/2022, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=INABILITADO:5

Código de controle da certidão: FGQ3310322155613

Atenção: qualquer rasura ou emenda invalidará este documento.

GOVERNO DO ESTADO DO AMAZONAS

ADMINISTRAÇÃO FINANCEIRA INTEGRADA

Nota de Empenho

Unidade Gestora 003101 - PROCURADORIA GERAL DE JUSTICA	**Número Documento** 2022NE0000539	**Data Emissão** 31/03/2022
Gestão 00001 - ADMINISTRACAO DIRETA	**Processo** 000000.015252/2021	**NE Original**
Credor 05250796000154 - NETWORK SECURE SEGURANCA DA INFORMAÇAO LTDA	**Licitação** 8 - Pregão Eletrônico	**Referência** Art. 2°,§ 1º, Lei 10.520/02
Evento 400091 - Empenho de Despesa	**Modalidade** 3 - Global	**Valor** 480.553,24

Unidade Orçamentária	03101	PROCURADORIA GERAL DE JUSTIÇA
Programa Trabalho	03.122.0001.2001.0001	Administraçãc da Unidade
Fonte Recurso	01000000	Recursos Ordinários
Natureza Despesa	33904016	Locação de Software

Município 9999 - Estado
Convênio

Origem do Material 1 - Origem Nacional
Tipo de Empenho 9 - Despesa Normal

Cronograma de Desembolso

Janeiro	0,00	**Fevereiro**	0,00	**Março**	0,00	**Abril**	80.553,32
Maio	49.999,99	**Junho**	49.999,99	**Julho**	49.999,99	**Agosto**	49.999,99
Setembro	49.999,99	**Outubro**	49.999,99	**Novembro**	49.999,99	**Dezembro**	49.999,99

Descrição dos Itens

Unid.	Descrição	Qtde	Preço Unitário	Preço Total
Mês	Valor que se empenha em favor de Network Secure Segurança da Informação Ltda, conforme NAD nº 375.2021.DOF-Orçamento, Pregão Eletrônico nº 4.005/2022-CPL/MP/PGJ, Despacho nº 075.2022.01AJ-SUBADM e demais documentos no SEI nº 2021.015252, , referente a:	9	44,791.6600	403.124,94
	1) Serviço de Firewall em alta disponibilidade;			
Mês	2) Serviço de monitoramento da solução;	9	5,208.3300	46.874,97
Unidade	3) Serviço de migração do ambiente atual;	1	30,553.3300	30.553,33

Observação:
*Valor do contrato em 2022 (09 meses): R$ 480.553,24
*Valor do contrato em 2023 (12 meses): R$ 599.999,88
*Valor do contrato em 2024 (12 meses): R$ 599.999,88
*Valor do contrato em 2025 (12 meses): R$ 599.999,88
*Valor do contrato em 2026 (03 meses): R$ 149.999,97

Géber Mafra Rocha
Subprocurador-Geral de Justiça
Para Assuntos Administrativos

Francisco Edinaldo Lira de Carvalho
Diretor de Orçamento e Finanças

Saldo Anterior:	1.143.462,78	**Valor do Empenho:**	480.553,24	**Valor Disponível**	662.909,54
Data de Entrega:	31/03/2022	**Local de Entrega:**	PGJ AM		
Ordenador de Despesa:	ALBERTO RODRIGUES DO NASCIMENTO JUNIOR	**Usuário Operador da NE :**	REINALDO AMON CAVALCANTI GOMES		

Nota de Empenho

Unidade Gestora 003101 - PROCURADORIA GERAL DE JUSTICA	**Número Documento** 2022NE0000540	**Data Emissão** 31/03/2022
Gestão 00001 - ADMINISTRACAO DIRETA	**Processo** 000000.015252/2021	**NE Original**
Credor 05250796000154 - NETWORK SECURE SEGURANCA DA INFORMAÇAO LTDA	**Licitação** 8 - Pregão Eletrônico	**Referência** Art. 2°,§ 1º, Lei 10.520/02
Evento 400091 - Empenho de Despesa	**Modalidade** 1 - Ordinário	**Valor** 47.500,00

Unidade Orçamentária	03101	PROCURADORIA GERAL DE JUSTIÇA
Programa Trabalho	03.122.0001.2001.0001	Administração da Unidade
Fonte Recurso	01000000	Recursos Ordinários
Natureza Despesa	33904012	Treinamento e capacitação em TIC

Município 9999 - Estado
Convênio

Origem do Material 1 - Origem Nacional
Tipo de Empenho 9 - Despesa Normal

Cronograma de Desembolso

Janeiro	0,00	**Fevereiro**	0,00	**Março**	0,00	**Abril**	47.500,00
Maio	0,00	**Junho**	0,00	**Julho**	0,00	**Agosto**	0,00
Setembro	0,00	**Outubro**	0,00	**Novembro**	0,00	**Dezembro**	0,00

Descrição dos Itens

Unid.	Descrição	Qtde	Preço Unitário	Preço Total
Pessoa	Valor que se empenha em favor de Network Secure Segurança da Informação Ltda, conforme NAD nº 375.2021.DOF-Orçamento, Pregão Eletrônico nº 4.005/2022-CPL/MP/PGJ, Despacho nº 075.2022.01AJ-SUBADM e demais documentos no SEI nº 2021.015252, referente a serviço de treinamento da solução Firewall.	5	9,500.0000	47.500,00

Géber Mafra Rocha
Subprocurador-Geral de Justiça
Para Assuntos Administrativos

Francisco Edinaldo Lira de Carvalho
Diretor de Orçamento e Finanças

Saldo Anterior:	662.909,54	**Valor do Empenho:**	47.500,00	**Valor Disponível**	615.409,54
Data de Entrega:	31/03/2022	**Local de Entrega:**	PGJ AM		
Ordenador de Despesa:	ALBERTO RODRIGUES DO NASCIMENTO JUNIOR	**Usuário Operador da NE :**	REINALDO AMON CAVALCANTI GOMES		

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 241.2022.DCCON.0795891.2021.015252

Manaus, 04 de abril de 2022.

Ao Exmo. Sr. Dr.
GÉBER MAFRA ROCHA
Subprocurador-Geral de Justiça para Assuntos Administrativos
NESTA

Assunto: Solicitação de designação de gestor/fiscal - Contrato Administrativo nº 003/2022 - MP/PGJ.

Senhor Subprocurador-Geral de Justiça para Assuntos Administrativos,

Considerando a celebração do Contrato Administrativo nº 003/2022 - MP/PGJ (0790812), firmado entre este Ministério Público e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, cujo objeto é a prestação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme as especificações constantes no Termo de Referência nº 20.2021.DTIC.0720733.2021.015252, **informo sobre a necessidade de designação de gestor/fiscal para o Contrato em questão.**

Respeitosamente,

Documento assinado eletronicamente por **Caroline Ellen Bezerra**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 04/04/2022, às 13:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0795891** e o código CRC **4E79BD60**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 243.2022.DCCON.0795924.2021.015252

Manaus, 04 de abril de 2022.

À Diretoria de Orçamento e Finanças da PGJ/AM

À Diretoria de Tecnologia de Informação e Comunicação da PGJ/AM

À Chefia do Setor de Infraestrutura e Telecomunicações da PGJ/AM

NESTA

Assunto: Encaminhamento dos autos para a tomada de providências quanto à celebração do **Contrato Administrativo Nº 003/2022 - MP/PGJ.**

Senhores Diretores e Senhor Chefe,

Considerando a celebração do **Contrato Administrativo Nº 003/2022 - MP/PGJ**, encaminho os presentes autos para a tomada de providências afetas a cada setor mencionado no campo dos destinatários.

Informo que, na presente data, esta Divisão de Contratos e Convênios (DCCON) solicitou a publicação do Contrato Administrativo Nº 003/2022 - MP/PGJ no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas (DOMPE/AM), e ainda informou a Subprocuradoria-Geral de Justiça para Assuntos Administrativos (SUBADM) sobre a necessidade de ser designado gestor/fiscal para o Contrato em questão, conforme consta no Memorando 241 (0795891).

Atenciosamente,

Documento assinado eletronicamente por **Caroline Ellen Bezerra**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 04/04/2022, às 13:04, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0795924** e o código CRC **49FD5D30**.

DESPACHO Nº 20.2022.DOF - CONTABILIDADE.0796290.2021.015252

Após análise técnica das condições para registro de contrato no AFI, verifico conformidade mínima, e repasso para o serviço de liquidação e registros, **para escrituração imediata no AFI das NE´s: 2022NE0000539 e 2022NE0000540, em seus SALDOS totais,** pelo **evento 540412** (registro de assinatura de contratos -SERVIÇOS), colocando a informação em **observação da vigência, objeto, fonte de recursos, fiscal do contrato, e número do SEI, e** demais informações, respectivamente, **do CONTRATO ADMINISTRATIVO Nº 003/2022 - MP/PGJ, conforme cada CNPJ e credor abaixo:**

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA., inscrita no CNPJ (MF) sob o n.º 05.250.796/0001-54.

Após o registro e inclusão na planilha de controle de contratos 2022 destes dados acima, ao Diretor da DOF para assinatura das NL´s de registro, e por fim anexá-las neste SEI.

Nesta data assinado eletronicamente,

Att.

Documento assinado eletronicamente por **Clilson Castro Viana**, **Agente Técnico - Contador**, em 04/04/2022, às 15:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0796290** e o código CRC **6389A0D5**.

PORTARIA Nº 311/2022/DRH

A DIVISÃO DE RECURSOS HUMANOS, no uso de suas atribuições, e

CONSIDERANDO que a possibilidade de concessão de Licença Médica, a que fazem jus os servidores deste Ministério Público, encontra amparo legal no art. 65, inciso I, c/c art. 68, todos da Lei nº 1.762, de 14 de novembro de 1986 - Estatuto dos Servidores Públicos Civis do Estado do Amazonas;

CONSIDERANDO a delegação de competência conferida pelo Despacho Nº 585.2018.01AJ-SUBADM.0251007.2018.016174, e

CONSIDERANDO o teor do Processo SEI nº 2022.000497 e Laudo Médico n.º 210644/2022, expedido pela Junta Médica Pericial do Estado,

RESOLVE:

CONCEDER, por 90 (noventa) dias, no período de 10/01/2022 a 09/04/2022, licença para tratamento de saúde ao(à) servidor (a) MILENE DE OLIVEIRA MIRANDA, AGENTE TÉCNICO COMUNICÓLOGO, nos termos do art. 65, inciso I, c/c o art. 68, todos da Lei nº 1.762, de 14 de novembro de 1986 – Estatuto dos Servidores Públicos Civis do Estado do Amazonas.

Publique-se, registre-se, cumpra-se.

DIVISÃO DE RECURSOS HUMANOS, em Manaus, 04 de Abril de 2022.

DMES BRITO DE SOUZA
Chefe da Divisão de Recursos Humanos

REQUERIMENTO Nº 159641/2022

Interessado: Manoel Edson Sevalho de Souza
A DIVISÃO DE RECURSOS HUMANOS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) servidor(a) em epígrafe, relativos ao período aquisitivo 2022, originalmente previstas para o período de 25/04/2022 a 04/05/2022, para fruição no período de 12/09/2022 a 21/09/2022.
Dmes Brito de Souza
CHEFE DA DIVISÃO DE RECURSOS HUMANOS

EXTRATOS DE CONTRATOS E CONVÊNIOS

EXTRATO DE CONTRATO

Processo: 2021.015252
Espécie: Contrato Administrativo n.º 003/2022 - MP/PGJ.
Licitação: Pregão Eletrônico n.º 4.005/2022-CPL/MP/PGJ.
Objeto: Prestação de serviço de solução de firewall de próxima geração em alta disponibilidade, com monitoramento, pelo período de 48 (quarenta e oito) meses, incluindo treinamento e serviço de migração da plataforma atual, conforme as especificações constantes no Termo de Referência nº 20.2021.DTIC.0720733.2021.015252.
Valor: R$ 2.478.052,85
Dotação Orçamentária: 1) Unidade Gestora: 03101 - Procuradoria Geral de Justiça; Unidade Orçamentária: 03101 - Procuradoria Geral de Justiça; Programa de Trabalho: 03.122.0001.2001.0001 - Administração da Unidade; Fonte: 0100 - Recursos Ordinários; Natureza da Despesa: 33904016 - Locação de Software, tendo sido emitida, pela CONTRATANTE, em 31/03/2022, a Nota de Empenho n.º 2022NE0000539, no valor global de R$ 480.553,24 (quatrocentos e oitenta mil, quinhentos e cinquenta e três reais e vinte e quatro centavos). 2) Unidade Gestora: 03101 - Procuradoria Geral de Justiça; Unidade Orçamentária: 03101 - Procuradoria Geral de Justiça; Programa de Trabalho: 03.122.0001.2001.0001 - Administração da Unidade; Fonte: 0100 - Recursos Ordinários; Natureza da Despesa: 33904012 - Treinamento e capacitação em TIC, tendo sido emitida, pela CONTRATANTE, em 31/03/2022, a Nota de Empenho n.º 2022NE0000540, no valor global de R$ 47.500,00 (quarenta e sete mil e quinhentos reais).
Vigência: 48 (quarenta e oito) meses, compreendendo o período de 31 de março de 2022 a 31 de março de 2026.
Contratante: Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça.
Contratada: Network Secure Segurança da Informação Ltda.
Signatários: Exmo. Sr. Géber Mafra Rocha (Subprocurador-Geral de Justiça para Assuntos Administrativos) e Sr. Yure Leopoldo Sabino de Freitas (Representante legal da contratada).
Data: 31.03.2022.

Géber Mafra Rocha
Subprocurador-Geral de Justiça para Assuntos Administrativos

EXTRATO DE CONTRATO

Processo: 2020.019936
Espécie: Contrato Administrativo n.º 004/2022 - MP/PGJ.
Licitação: Pregão Eletrônico n.º 4.002/2022-CPL/MP/PGJ.
Objeto: Aquisição de 2 (duas) licenças de software AutoCAD One (AutoCAD, Architecture, Electrical, MAP 3D, Mechanical, MEP, Plant 3D eRaster Design), Civil 3D, Infraworks, Revit, Navisworks Manage e treinamento, visando suprir as necessidades da Divisão de Engenharia, Arquitetura e Cálculo do Ministério Público do Amazonas (MPAM), nos termos do Edital do PREGÃO ELETRÔNICO N.º 4.002/2022-CPL/MP/PGJ, conforme o Termo de Referência n.º 39.2020.DEAC.0552573.2020.019936.
Valor: R$ 99.535,20
Dotação Orçamentária: 1) Unidade Gestora: 03101 - Procuradoria Geral de Justiça; Unidade Orçamentária: 03101 - Procuradoria Geral de Justiça; Programa de Trabalho: 03.122.0001.2001.0001 - Administração da Unidade; Fonte: 0100 - Recursos Ordinários; Natureza da Despesa: 33904016 - Locação de Software, tendo sido emitida, pela CONTRATANTE, em 30/03/2022, a Nota de Empenho n.º 2022NE0000536, no valor global de R$ 75.055,20 (setenta e cinco mil, cinquenta e cinco reais e vinte centavos). 2) Unidade Gestora: 03101 - Procuradoria Geral de Justiça; Unidade Orçamentária: 03101 - Procuradoria Geral de Justiça; Programa de Trabalho: 03.122.0001.2001.0001 - Administração da Unidade; Fonte: 0100 - Recursos Ordinários; Natureza da Despesa: 33904012 - Treinamento e capacitação em TIC, tendo sido emitida, pela CONTRATANTE, em 30/03/2022, a Nota de Empenho n.º 2022NE0000537, no valor global de R$ 24.480,00 (vinte e quatro mil, quatrocentos e oitenta reais).
Vigência: 36 (trinta e seis) meses, compreendendo o período de 31 de março de 2022 a 31 de março de 2025.
Contratante: Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça.
Contratada: Mapdata - Tecnologia, Informática e Comércio Ltda.
Signatários: Exmo. Sr. Géber Mafra Rocha (Subprocurador-Geral de Justiça para Assuntos Administrativos) e Sra. Débora Cristina Cassim (Representante legal da contratada).
Data: 31.03.2022.

Géber Mafra Rocha
Subprocurador-Geral de Justiça para Assuntos Administrativos

DIVERSOS

EXTRATO Nº PORTARIA Nº 2022/0000019135.01PROM_PIN

O MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, por meio da 1ª Promotoria da Comarca de Parintins, pelo Promotor de Justiça que ao final subscreve, no exercício de suas atribuições, as quais estão dispostas no art. 129, III, da Constituição Federal de 1988, no art. 8, § 1, da Lei nº 7.347/85, no art. 26, I, da Lei nº 8.625/93 e no art. ºº22, da Lei nº 8.429/92;

GOVERNO DO ESTADO DO AMAZONAS

ADMINISTRAÇÃO FINANCEIRA INTEGRADA

Nota de Lançamento

Unidade Gestora 003101 - PROCURADORIA GERAL DE JUSTICA	Data Emissão	Número
Gestão 00001 - ADMINISTRACAO DIRETA	04/04/2022	2022NL0000768

Credor 05250796000154 - NETWORK SECURE SEGURANCA DA INFORMAÇAO LTDA

Tipo de Documento: OUTROS

Natureza da Despesa: 33904016 - Locação de Software

Observação

Registro do Contrato Administrativo nº 003/2022-MP/PGJ, conforme NE 2022NE0000539, contida no processo SEI nº 2021.015252, com vigência para o período de 31.03.2022 A 31.03.2026.

Evento	Inscricão Evento	Classificação	Fonte	Valor
540412			01000000	480.553,24

Francisco Edinaldo Lira de Carvalho
Diretor de Orçamento e Finanças

Ordenador :	Usuário Operador da NL:
ALBERTO RODRIGUES DO NASCIMENTO JUNIOR	MANOEL EDSON SEVALHO DE SOUZA

Nota de Lançamento

Unidade Gestora 003101 - PROCURADORIA GERAL DE JUSTICA	Data Emissão	Número
Gestão 00001 - ADMINISTRACAO DIRETA	04/04/2022	2022NL0000769
Credor 05250796000154 - NETWORK SECURE SEGURANCA DA INFORMAÇAO LTDA		
Tipo de Documento: OUTROS		
Natureza da Despesa: 33904012 - Treinamento e capacitação em TIC		
Observação Registro do Contrato Administrativo nº 003/2022-MP/PGJ, conforme NE 2022NE0000540, contida no processo SEI nº 2021.015252, com vigência para o período de 31.03.2022 A 31.03.2026.		

Evento	Inscricão Evento	Classificação	Fonte	Valor
540412			01000000	47.500,00

Francisco Edinaldo Lira de Carvalho
Diretor de Orçamento e Finanças

Ordenador :	Usuário Operador da NL:
ALBERTO RODRIGUES DO NASCIMENTO JUNIOR	MANOEL EDSON SEVALHO DE SOUZA

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 28.2022.DTIC.0796546.2021.015252

A Sua Excelência o Senhor

Doutor **GEBER MAFRA ROCHA**

Subprocurador-Geral de Justiça para Assuntos Administrativos

Assunto: Indicação de Fiscal e Suplente ao Contrato Administrativo nº 003/2022 - MP/PGJ.

Excelentíssimo Senhor Subprocurador-Geral de Justiça para Assuntos Administrativos,

Honrado em cumprimentar Vossa Excelência, oportunidade que, apresento indicação de Gestor e Fiscal, bem como seus respectivos suplentes, relativo ao Contrato Administrativo nº 003/2022 - MP/PGJ, firmado entre este *Parquet* e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA,** como segue:

1.1. Gestor: Chefe do Setor de Infraestrutura e Telecomunicações;

1.2. Fiscal: Theo Ferreira Pará, Agente de Apoio - Manutenção em Informática;

1.3. Gestor suplente: Diretor de Tecnologia de Informação e Comunicação;

1.4. Fiscal suplente: Hudson Barreiros da Silva, Agente Técnico - Analista de Redes.

Respeitosamente,

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutira e Telecomunicações

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 05/04/2022, às 16:47, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0796546** e o código CRC **BB84C44E**.

PREZADO SEGURADO PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS

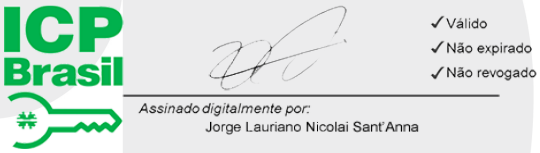
Encaminhamos anexa a **Apólice Digital** da BMG Seguros S.A., documento emitido conforme os mais rígidos critérios de segurança em autenticação e certificação digital existentes no mercado.

BMG SEGUROS S.A.

TÍTULO: APÓLICE SEGURO GARANTIA

Nº Apólice: 01741202200010775006953 1 - ENDOSSO 0000000
Controle Interno: 181202
Data da publicação: Apr 5 2022 4:02PM
Publicado por: Seguradora BMG SEGUROS S.A.
CNPJ 19.486.258/0001-78

Documento eletrônico digitalmente assinado por:



Documento eletrônico assinado digitalmente conforme MP nº 2.200-2/2001, que instituiu a infra-estrutura de Chaves Públicas Brasileiras - ICP - Brasil por: Signatários(as):

JORGE LAURIANO NICOLAI SANT ANNA Nº de Série do Certificado: 3A6BBBDC1887A622 Data e Hora Atual Apr 5 2022 4:02PM

RENATA OLIVER COUTINHO Nº de Série do Certificado: 1AFD06DF8AE26AB6 Data e Hora Atual Apr 5 2022 4:02PM

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe oferece o art. 62 da Constituição, adota a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, com força de lei, que assim dispõe:

Art 1º - Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Após sete dias úteis da emissão deste documento, poderá ser verificado se a apólice ou endosso foi corretamente registrado no site da SUSEP - www.susep.gov.br

Apólice N° 01741202200010775006953 1
Endosso N° 0000000
Proposta Nº 213687

bmg | Seguros

Seguro Garantia

CONSTRUÇÃO, FORNECIMENTO ou PRESTAÇÃO DE SERVIÇOS

A BMG SEGUROS S.A. garante pelo presente instrumento ao Segurado:

PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
INSCRITO NO CNPJ: 04.153.748/0001-85
COM SEDE NA: AVENIDA Coronel Teixeira, 7995 - Compensa
CEP: 69030-480 - Manaus - AM

o fiel cumprimento das obrigações assumidas pelo Tomador:

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
INSCRITO NO CNPJ/MF: 05.250.796/0001-54
COM SEDE NA: AVENIDA Pontes Vieira, 2340 - salas 510 a 514 - Dionisio Torres
CEP: 60135-238 - Fortaleza - CE

até o valor de:

R$ 123.902,64 - CENTO E VINTE E TRÊS MIL E NOVECENTOS E DOIS REAIS E SESSENTA E QUATRO CENTAVOS

Fica ainda declarado que esta APÓLICE é prestada para o seguinte objeto:

O presente contrato de seguro garante a indenização, até o valor da garantia fixado na apólice, pelos prejuízos decorrentes do inadimplemento das obrigações assumidas pelo Tomador no Contrato Número 003/2022 - MP/PGJ, Processo n.o 2021.015252, PREGÃO ELETRÔNICO N.o 4.005/2022-CPL/MP/PGJ

Início de Vigência: 24:00 horas do dia 31/03/2022
Fim de Vigência: 24:00 horas do dia 30/06/2026

Corretor:	Código SUSEP Corretor:
CORE INSURANCE ASSESSORIA E CORRETOR	202022713

Apólice N° 01741202200010775006953 1
Endosso N° 0000000
Proposta Nº 213687
Ramo 0775

bmg | Seguros

Seguro Garantia

CONSTRUÇÃO, FORNECIMENTO ou PRESTAÇÃO DE SERVIÇOS

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Cobertura Trabalhista e Previdenciária
A presente apólice não se vincula a contrato de prestação de serviços com regime de dedicação exclusiva de mão de obra.
A existência deste regime de contratação enseja a nulidade de pleno direito da garantia, não gerando efeitos jurídicos em razão da autonomia de vontade e boa-fé que regem os contratos, nos termos do Código Civil Brasileiro, cabendo ao segurado a recusa imediata da presente apólice.

COBERTURA ADICIONAL I: AÇÕES TRABALHISTAS E PREVIDENCIÁRIAS:

Objeto:

1.1. Esta cobertura adicional tem por objeto garantir exclusivamente ao segurado, até o limite máximo de indenização, o reembolso dos prejuízos comprovadamente sofridos em relação às obrigações de natureza trabalhista e previdenciária de responsabilidade do tomador oriundas do contrato principal, nas quais haja condenação judicial do tomador ao pagamento e o segurado seja condenado subsidiariamente e que os valores tenham sido pagos por este, em decorrência de sentença condenatória transitada em julgado, bem como do trânsito em julgado dos cálculos homologados ou ainda nas hipóteses de acordo entre as partes com prévia anuência da seguradora e consequente homologação do Poder Judiciário.

1.2. No que diz respeito à subsidiariedade, a responsabilidade do segurado será referente à relação trabalhista e/ou previdenciária entre o autor/reclamante da demanda trabalhista e o tomador, oriundas do contrato principal objeto desta garantia, ocorridas dentro do período de vigência da apólice. Consequentemente, a responsabilidade da seguradora será relativa ao período de vigência da apólice e que o débito trabalhista seja decorrente unicamente do lapso temporal garantido.

2. Definições:

Definem-se, para efeito desta cobertura adicional:

2.1. Autor/Reclamante: aquele que propõe na justiça trabalhista uma reclamatória e esta seja oriunda do contrato principal, firmado entre tomador e segurado, o qual é objeto da apólice em questão.

2.2. Limite Máximo de Indenização: valor máximo que a seguradora se responsabilizará perante o segurado em função do pagamento de indenização, por cobertura contratada.

2.3. Obrigações Previdenciárias: são aquelas especificadas pelas Leis nº 8.212/91 e todas as suas alterações posteriores no que couber, bem como em leis esparsas, as quais

Seguro Garantia

CONSTRUÇÃO, FORNECIMENTO ou PRESTAÇÃO DE SERVIÇOS

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

dispõem sobre o recolhimento das contribuições devidas a cada categoria de empregado, observando-se as datas e percentuais.

2.4. Obrigações Trabalhistas: entende-se por obrigações trabalhistas as decorrentes do pagamento da contraprestação devida ao empregado pelo seu labor dispensado ao tomador, bem como de seus encargos, sendo a remuneração a que tem direito e todos seus reflexos, conforme determina a legislação em vigor.

2.5. Responsabilidade Subsidiária: é aquela que recai sobre garantias que somente são exigidas quando a principal é insuficiente, ou seja, inadimplente o real empregador - prestador de serviços, aqui denominado tomador, e esgotadas as tentativas de executá-lo, pode-se exigir do segurado o cumprimento das obrigações do réu/tomador, desde que o segurado tenha participado da relação processual e conste do título executivo judicial.

3. Expectativa, Reclamação e Caracterização do Sinistro:

3.1. Expectativa: quando o segurado receber citação(ões) judicial(ais) para apresentar defesa trabalhista e/ou previdenciária, cujo autor/reclamante reivindique crédito de natureza remuneratória ou direito de responsabilidade do tomador, deverá comunicar à seguradora, tão logo seja citado, enviando cópia(s) da(s) referida(s) citação(ões) e de todo(s) documento(s) juntado(s) aos autos tanto pelo autor/ reclamante como pelo réu/tomador.

3.1.1. Caso ocorra o item 3.1. acima e reste pendente o trânsito em julgado da sentença, o segurado terá seus direitos preservados até decisão definitiva.

3.1.2. Estão cobertas por esta garantia somente as ações trabalhistas distribuídas na Justiça do Trabalho.

3.2. Reclamação: a Expectativa de Sinistro será convertida em Reclamação, mediante comunicação do segurado à seguradora, quando transitada em julgado a ação, com o pagamento dos valores constantes na condenação do segurado.

3.2.1. Para a Reclamação do Sinistro será necessária a apresentação dos seguintes documentos, sem prejuízo do disposto no item 7.2.1. das Condições Gerais:

a) comprovante(s) de pagamento dos valores citados no item 3.2. desta Cobertura Adicional;
b) certidão(ões) de trânsito em julgado das sentenças proferidas e com os valores homologados;
c) acordo devidamente homologado pelo Poder Judiciário, se houver.
d) guias de recolhimento do Fundo de Garantia por Tempo de Serviço – FGTS;
e) guias de recolhimento do INSS dos empregados que trabalharam nos serviços

contratados;
f) documentos comprobatórios de que o autor/reclamante trabalhou para o réu/tomador no contrato principal dentro do período de vigência da apólice.

3.3. A Reclamação de Sinistros amparada pela presente cobertura poderá ser realizada durante o prazo prescricional, nos termos o art. 7º, inciso XXIX da Constituição da República, no que se refere ao Direito do Trabalho.

3.4. A não formalização da Reclamação do Sinistro tornará sem efeito a Expectativa do Sinistro;

3.5. Caracterização: recebida a notificação, devidamente acompanhada dos documentos citados no item 3.2.1, a Seguradora deverá concluir o processo de regulação de sinistro e emitir o relatório final de regulação de sinistro.

4. Acordos:

4.1. Nas hipóteses, e no momento, em que o segurado tenha intenção de realizar acordos nas ações judiciais cobertas por esta cobertura, o mesmo deverá enviar uma memória de cálculo simples das verbas pleiteadas pelo autor, juntamente com uma estimativa do valor a ser acordado.

4.2. A seguradora, após receber os documentos constantes no item 4.1. e fizer sua análise da situação fático-jurídica, enviará ao segurado em até 20 (vinte) dias da data do recebimento, sua aceitação ao valor proposto, ou apresentará um valor máximo alternativo ou ainda, manifestar-se-á se enviará preposto para audiência, cuja data será devidamente comunicada pelo segurado em tempo hábil.

4.3. Acordos decorrentes das reclamatórias trabalhistas e/ou previdenciárias poderão ser realizados, desde que cumpridos os requisitos dos itens 4.1. e 4.2.

5. Indenização:

Caracterizado o sinistro na forma descrita no item 3.5., a seguradora indenizará o segurado, por meio de reembolso, até o limite máximo de indenização estabelecido na apólice.

6. Perda de Direito:

Além das perdas de direito descritas na Cláusula 11 das Condições Gerais, o segurado perderá o direito à indenização na ocorrência de uma ou mais das seguintes hipóteses:

I – Não cumprimento por parte do segurado das exigências descritas na Cláusula 3 desta

Apólice N° 01741202200010775006953 1
Endosso N° 0000000
Proposta Nº 213687
Ramo 0775

Seguro Garantia

CONSTRUÇÃO, FORNECIMENTO ou PRESTAÇÃO DE SERVIÇOS

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

Cobertura Adicional.
II – Quando o segurado deixar de apresentar defesa ou perder prazo para interposição de recurso ou for considerado revel nos termos do artigo 844, parágrafo único da Consolidação de Leis do Trabalho ou confessar.
III – se o segurado firmar acordo sem a prévia anuência da seguradora ou este não for homologado pelo Poder Judiciário.
IV – Nos casos de condenações do tomador e/ou segurado no que se refere a dano moral e/ou dano material, assédio moral ou sexual decorrentes de responsabilidade civil do tomador e/ou do segurado e indenizações por acidente de trabalho.

7. Ratificação:
Ratificam-se integralmente as disposições das Condições Gerais e Especiais que não tenham sido alteradas pela presente Condições Particulares._

Apólice N° 0174120220001077500695 31
Endosso N° 0000000
Proposta Nº 213687
Ramo 0775

bmg | Seguros

Seguro Garantia

CONSTRUÇÃO, FORNECIMENTO ou PRESTAÇÃO DE SERVIÇOS

Demonstrativo de Prêmio

Prêmio Líquido:	2.655,27
Custo de Apólice:	0,00
Adicional de Fracionamento:	0,00
IOF:	0,00
Prêmio Total:	2.655,27

Forma de Pagamento

Forma de Pagamento: À Vista
Número de Prestação: 1

Parcelas	Data Vencimento	Valor das Parcelas
1	14/04/2022	2.655,27

Forma de Cobrança: FICHA DE COMPENSAÇÃO - ITAÚ

Disposições: - Caso a data limite para o pagamento do prêmio à vista ou de qualquer uma de suas parcelas coincida com dia em que não haja expediente bancário, o pagamento poderá ser efetuado no primeiro dia útil em que houver expediente bancário. - A Seguradora encaminhará o documento de cobrança diretamente ao Tomador ou seu representante legal ou, ainda, por expressa solicitação de qualquer um destes, ao corretor de seguros, observada a antecedência mínima de 5 (cinco) dias úteis, em relação à data do respectivo vencimento. - Em caso de parcelamento do prêmio, não será permitida a cobrança de nenhum valor adicional, a título de custo administrativo de fracionamento. Quando houver parcelamento com juros, haverá a possibilidade de antecipar o pagamento de qualquer uma das parcelas, com a consequente redução proporcional dos juros pactuados.

As condições anexas constituem parte integrante e inseparável DESTA APÓLICE para todos os fins de direito. esta Apólice é emitida em 2 (duas) vias de igual teor, sendo uma via do(s) Segurado(s) e outra da Seguradora.

Após sete dias úteis da emissão deste documento, poderá ser verificado se a apólice ou endosso foi corretamente registrado no site da SUSEP - www.susep.gov.br
as condições contratuais deste produto protocolizadas pela sociedade junto à susep poderão ser consultadas no endereço eletrônico www.susep.gov.br, de acordo com o número de processo constante da Apólice/proposta.

SÃO PAULO, 5 DE ABRIL DE 2022.

SUSEP - Superintendência de Seguros Privados - Autarquia Federal responsável pela fiscalização, normatização e controle dos mercados de seguro, previdência complementar aberta, capitalização, resseguro e corretagem de seguros.

Apólice N° 01741202200010775006953 1
Endosso N° 0000000
Proposta Nº 213687
Ramo 0775

bmg | Seguros

Condições Particulares

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

1. Cláusula Normas Anticorrupção

1.1 Fica estabelecido que, especificamente para fins indenizatórios, estarão cobertos pela presente apólice os prejuízos e/ou demais penalidades decorrentes de atos e/ou fatos violadores de normas anticorrupção, perpetrados pelo tomador no âmbito do contrato garantido e que tragam prejuízos ao segurado, e desde que não conte com a comprovada participação do segurado, seus respectivos sócios/acionistas, representantes, titulares ou funcionários.

2. Cláusula Culpa ou Dolo

2.1. Este contrato de seguro garante a indenização, até o valor da garantia fixado na apólice, pelos prejuízos decorrentes de culpa ou dolo do Tomador durante a execução do contrato, não assegurando riscos referentes a indenizações a terceiros, danos ambientais e lucros cessantes, despesas de contenção de sinistro ou despesas de salvamento, bem como não assegura riscos referentes a outros ramos ou modalidades de seguro.

3. Cláusula de Inalienabilidade e Irrevogabilidade

3.1 Acrescenta-se o item 1.4. as Condições Especiais desta apólice conforme abaixo:

1.4 A presente apólice é inalienável e irrevogável até a data prevista como termo final das obrigações assumidas pelo Tomador no Contrato Principal, o que coincide com a data final de vigência da apólice. Esta garantida a devida atualização monetária da apólice, de acordo com os índices previstos no Contrato Principal firmado entre o Tomador e o Segurado.

4. Ratificação

4.1 Ratificam-se integralmente as disposições das Condições Gerais e Especiais que não tenham sido alteradas pela presente Condições Particulares.

Apólice N° 01741202200010775006953 1
Endosso N° 0000000
Proposta Nº 213687
Ramo 0775

bmg | Seguros

Condições Especiais

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

1. Objeto:

1.1. Este contrato de seguro garante a indenização, até o valor da garantia fixado na Apólice, pelos prejuízos decorrentes do inadimplemento das obrigações assumidas pelo Tomador no contrato principal, para construção, fornecimento ou prestação de serviços.

1.2. Encontram-se também garantidos por este contrato de seguro os valores das multas e indenizações devidas à Administração Pública, tendo em vista o disposto na Lei nº 8.666/93.

1.3. Poderá ainda ser contratada, com verba específica independente, a Cobertura Adicional de Ações Trabalhistas e Previdenciárias, conforme descrito no Capítulo III deste Anexo.

2. Definições:

Define-se, para efeito desta modalidade, além das definições constantes do art. 6° da Lei n° 8.666/93 e do art. 2° da Lei n° 8.987/95:

I – Prejuízo: perda pecuniária comprovada, excedente aos valores originários previstos para a execução do objeto do contrato principal, causada pelo inadimplemento do Tomador, excluindo-se qualquer prejuízo decorrente de outro ramo de seguro, tais como responsabilidade civil, lucros cessantes.

3. Vigência:

3.1 A vigência da Apólice será fixada de acordo com as seguintes regras:

I – Coincidindo com o prazo de vigência do contrato administrativo pertinente à execução de obras, serviços e/ou compras;
II – Por períodos renováveis, no caso de concessões e permissões do serviço público.

3.2. As renovações, a que se refere o inciso II do item 3.1., não se presumem, serão precedidas de notificação escrita da Seguradora ao Segurado e ao Tomador, com antecedência de até noventa dias da data do término de vigência da apólice em vigor, declarando seu explícito interesse na manutenção da garantia.

4. Expectativa, Reclamação e Caracterização do Sinistro:

4.1. Expectativa: tão logo realizada a abertura do processo administrativo para apurar possível inadimplência do Tomador, este deverá ser imediatamente notificado pelo Segurado, indicando claramente os itens não cumpridos e concedendo-lhe prazo para regularização da inadimplência apontada, remetendo

cópia da notificação para a Seguradora, com o fito de comunicar e registrar a Expectativa de Sinistro.

4.2. Reclamação: a Expectativa de Sinistro será convertida em Reclamação, mediante comunicação pelo segurado à seguradora, da finalização dos procedimentos administrativos que comprovem o inadimplemento do tomador, data em que restará oficializada a Reclamação do Sinistro.

4.2.1. Para a Reclamação do Sinistro será necessária a apresentação dos seguintes documentos, sem prejuízo do disposto no item 7.2.1. das Condições Gerais:

a) Cópia do contrato principal ou do documento em que constam as obrigações assumidas pelo Tomador, seus anexos e aditivos se houver, devidamente assinados pelo segurado e pelo Tomador;
b) Cópia do processo administrativo que documentou a inadimplência do Tomador;
c) Cópias de atas, notificações, contra notificações, documentos, correspondências, inclusive e- mails, trocados entre o Segurado e o Tomador, relacionados à inadimplência do Tomador;
d) Planilha, relatório e/ou correspondências informando da existência de valores retidos;
e) Planilha, relatório e/ou correspondências informando os valores dos prejuízos sofridos;

4.2.2 A não formalização da Reclamação do Sinistro tornará sem efeito a Expectativa do Sinistro;

4.3 Caracterização: quando a Seguradora tiver recebido todos os documentos listados no item 4.2.1. e, após análise, ficar comprovada a inadimplência do tomador em relação às obrigações cobertas pela Apólice, o sinistro ficará caracterizado, devendo a Seguradora emitir o relatório final de regulação;

5. Acompanhamento e Inspeção de Riscos

5.1. Visando ao acompanhamento dos riscos assumidos, a Seguradora reserva-se o direito de, a qualquer tempo durante a vigência do seguro, solicitar documentação que atualize o status dos riscos, realizar inspeções, vistorias e verificações no local do risco e ou canteiro de obras, por conta própria ou por terceiros nomeados por ela, obrigando-se o Segurado e/ou o Tomador a:

5.1.1. fornecer os esclarecimentos, documentos e provas que lhe forem solicitados, devendo facilitar o desempenho das tarefas da Seguradora;

Condições Especiais

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

5.1.2. acompanhar pessoalmente, ou através de preposto devidamente credenciado, as inspeções realizadas pela Seguradora, que poderá endereçar possíveis recomendações ao Segurado, estipulando prazos para que sejam cumpridas;
5.1.3 implementar as recomendações apresentadas, nos prazos estipulados.

5.2. O Segurado e/ou o Tomador permitirá a entrada da Seguradora no canteiro de obras, por conta própria ou por seus prestadores de serviços devidamente identificados, sempre que esta entenda necessário. Para isso, a Seguradora agendará a visita com antecedência mínima de 48h, aguardando a confirmação da data e horário da vistoria pelo Segurado e/ou Tomador, no prazo máximo de 10 dias.

6. Ratificação:

Ratificam-se integralmente as disposições das Condições Gerais que não tenham sido alteradas pela presente Condição Especial.

Apólice N° 01741202200010775006953 1
Endosso N° 0000000
Proposta Nº 213687
Ramo 0775

bmg | Seguros

Condições Gerais

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

1. OBJETO

1.1. Este contrato de seguro garante o fiel cumprimento das obrigações assumidas pelo Tomador perante o Segurado, conforme os termos da Apólice e até o valor da garantia fixado nesta, e de acordo com a(s) modalidade(s) e/ou cobertura(s) adicional(is) expressamente contratada(s), em razão de participação em licitação, em contrato principal pertinente a obras, serviços, inclusive de publicidade, compras, concessões e permissões no âmbito dos Poderes da União, Estados, do Distrito Federal e dos Municípios, ou, ainda as obrigações assumidas em função de:
I – processos administrativos;
II – processos judiciais, inclusive execuções fiscais;
III – parcelamentos administrativos de créditos fiscais, inscritos ou não, em dívida ativa;
IV – regulamentos administrativos.
1.2. Encontram-se também garantidos por este seguro os valores devidos ao Segurado, tais como multas e indenizações, oriundos do inadimplemento das obrigações assumidas pelo Tomador, previstos em legislação específica, para cada caso.

2. DEFINIÇÕES

Aplicam-se a este seguro, as seguintes definições:

2.1. Apólice: documento, assinado pela Seguradora, que representa formalmente o contrato de Seguro Garantia.
2.2. Condições Gerais: conjunto das cláusulas, comuns a todas as modalidades e/ou coberturas de um plano de seguro, que estabelecem as obrigações e os direitos das partes contratantes.
2.3. Condições Especiais: conjunto das disposições específicas relativas a cada modalidade e/ou cobertura de um plano de seguro, que alteram as disposições estabelecidas nas Condições Gerais.
2.4. Condições Particulares: conjunto de cláusulas que alteram, de alguma forma, as Condições Gerais e/ou Condições Especiais, de acordo com cada Segurado.
2.5. Contrato Principal: todo e qualquer ajuste entre órgãos ou entidades da Administração Pública (segurado) e particulares (tomadores), em que haja um acordo de vontades para a formação de vínculo e a estipulação de obrigações recíprocas, seja qual for a denominação utilizada.
2.6. Endosso: instrumento formal, assinado pela Seguradora, que introduz modificações na apólice de Seguro Garantia, mediante solicitação e anuência expressa das partes.
2.7. Indenização: pagamento dos prejuízos e/ou multas resultantes do inadimplemento das obrigações cobertas pelo seguro.
2.8. Limite Máximo de Garantia: valor máximo que a Seguradora se responsabilizará perante o Segurado em função do pagamento de indenização.

2.9. Prêmio: importância devida pelo Tomador à Seguradora, em função da cobertura do seguro, e que deverá constar da Apólice ou Endosso.
2.10. Processo de Regulação de Sinistro: procedimento pelo qual a Seguradora constatará ou não a procedência da reclamação de sinistro, bem como a apuração dos prejuízos cobertos pela Apólice.
2.11. Proposta de Seguro: instrumento formal de pedido de emissão de Apólice de seguro, firmado nos termos da legislação em vigor.
2.12. Relatório Final de Regulação: documento emitido pela Seguradora no qual se transmite o posicionamento acerca da caracterização ou não do sinistro reclamado, bem como os possíveis valores a serem indenizados.
2.13. Segurado: a Administração Pública ou o Poder Concedente.
2.14. Seguradora: a sociedade de seguros garantidora, nos termos da Apólice, do cumprimento das obrigações assumidas pelo Tomador.
2.15. Seguro Garantia: seguro que garante o fiel cumprimento das obrigações assumidas pelo Tomador perante o Segurado, conforme os termos da Apólice.
2.16. Sinistro: o inadimplemento das obrigações do Tomador cobertas pelo seguro.
2.17. Tomador: devedor das obrigações por ele assumidas perante o Segurado.

3. ACEITAÇÃO

3.1. A contratação/alteração do contrato de seguro somente poderá ser feita mediante proposta assinada pelo proponente, seu representante ou por corretor de seguros habilitado. A proposta escrita deverá conter os elementos essenciais ao exame e aceitação do risco.
3.2. A Seguradora fornecerá, obrigatoriamente, ao proponente, protocolo que identifique a proposta por ela recepcionada, com a indicação da data e da hora de seu recebimento.
3.3. A Seguradora terá o prazo de 15 (quinze) dias para se manifestar sobre a aceitação ou não da proposta, contados da data de seu recebimento, seja para seguros novos ou renovações, bem como para alterações que impliquem modificação do risco.
3.3.1. Caso o proponente do seguro seja pessoa física, a solicitação de documentos complementares, para análise e aceitação do risco, ou da alteração proposta, poderá ser feita apenas uma vez, durante o prazo previsto no item 3.3..
3.3.2. Se o proponente for pessoa jurídica, a solicitação de documentos complementares poderá ocorrer mais de uma vez, durante o prazo previsto no item 3.3., desde que a Seguradora indique os fundamentos do pedido de novos elementos, para avaliação da proposta ou taxação do risco.
3.3.3. No caso de solicitação de documentos complementares, para análise e aceitação do risco, ou da alteração proposta, o prazo de 15 (quinze) dias previsto no item 3.3. ficará suspenso, voltando a correr a partir da data em que se der a entrega da documentação.
3.4. No caso de não aceitação da proposta, a Seguradora comunicará o fato, por

escrito, ao proponente, especificando os motivos da recusa.
3.5. A ausência de manifestação, por escrito, da Seguradora, no prazo acima aludido, caracterizará a aceitação tácita do seguro.
3.6. Caso a aceitação da proposta dependa de contratação ou alteração de resseguro facultativo, o prazo aludido no item 3.3. será suspenso até que o Ressegurador se manifeste formalmente, comunicando a Seguradora, por escrito, ao proponente, tal eventualidade, ressaltando a consequente inexistência de cobertura enquanto perdurar a suspensão.
3.7. A emissão da Apólice ou do Endosso será feita em até 15 (quinze) dias, a partir da data de aceitação da proposta.

4. VALOR DA GARANTIA

4.1. O valor da garantia desta Apólice é o valor máximo nominal por ela garantido.
4.2. Quando efetuadas alterações previamente estabelecidas no contrato principal ou no documento que serviu de base para a aceitação do risco pela Seguradora, o valor da garantia deverá acompanhar tais modificações, devendo a Seguradora emitir o respectivo Endosso.
4.3. Para alterações posteriores efetuadas no contrato principal ou no documento que serviu de base para a aceitação do risco pela Seguradora, em virtude das quais se faça necessária a modificação do valor contratual, o valor da garantia poderá acompanhar tais modificações, desde que solicitado e haja o respectivo aceite pela Seguradora, por meio da emissão de Endosso.

5. PRÊMIO DO SEGURO

5.1. O Tomador é responsável pelo pagamento do prêmio à Seguradora por todo o prazo de vigência da Apólice.
5.2. Fica entendido e acordado que o seguro continuará em vigor mesmo quando o Tomador não houver pagado o prêmio nas datas convencionadas.
5.2.1. Não paga pelo Tomador, na data fixada, qualquer parcela do prêmio devido, poderá a sSguradora recorrer à execução do contrato de contragarantia.
5.3. Em caso de parcelamento do prêmio, não será permitida a cobrança de nenhum valor adicional, a título de custo administrativo de fracionamento, devendo ser garantido ao tomador, quando houver parcelamento com juros, a possibilidade de antecipar o pagamento de qualquer uma das parcelas, com a consequente redução proporcional dos juros pactuados.
5.4. Se a data limite para o pagamento do prêmio a vista ou de qualquer uma de suas parcelas coincidir com dia em que não haja expediente bancário, o pagamento poderá ser efetuado no primeiro dia útil em que houver expediente bancário.
5.5. A Sociedade Seguradora encaminhará o documento de cobrança diretamente ao tomador ou seu representante, observada a antecedência mínima de 05 (cinco) dias úteis, em relação à data do respectivo vencimento.

Condições Gerais

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

6. VIGÊNCIA

6.1. Para as modalidades do Seguro Garantia nas quais haja a vinculação da apólice a um contrato principal, a vigência da apólice será igual ao prazo estabelecido no contrato principal, respeitadas as particularidades previstas nas Condições Especiais de cada modalidade contratada.
6.2. Para as demais modalidades, a vigência da apólice será igual ao prazo informado na mesma, estabelecido de acordo com as disposições previstas nas Condições Especiais da respectiva modalidade.
6.3. Quando efetuadas alterações de prazo previamente estabelecidas no contrato principal ou no documento que serviu de base para a aceitação do risco pela Seguradora, a vigência da apólice acompanhará tais modificações, devendo a Seguradora emitir o respectivo endosso.
6.4. Para alterações posteriores efetuadas no contrato principal ou no documento que serviu de base para a aceitação do risco pela Seguradora, em virtude das quais se faça necessária a modificação da vigência da Apólice, esta poderá acompanhar tais modificações, desde que solicitado e haja o respectivo aceite pela Seguradora, por meio da emissão de Endosso.

7. EXPECTATIVA E CARACTERIZAÇÃO DO SINISTRO

7.1. A Expectativa, Reclamação e Caracterização do Sinistro serão especificadas para cada modalidade nas Condições Especiais, quando couberem.
7.2. A seguradora descreverá nas Condições Especiais os documentos que deverão ser apresentados para efetivação da Reclamação do Sinistro.
7.2.1. Com base em dúvida fundada e justificável, a seguradora poderá solicitar documentação e/ou informação complementar.
7.3. A Reclamação de Sinistros amparados pela presente apólice poderá ser realizada durante o prazo prescricional, nos termos da Cláusula 17 destas Condições Gerais;
7.4. Caso a Seguradora conclua pela não caracterização do sinistro, comunicará formalmente ao segurado, por escrito, sua negativa de indenização, apresentando, conjuntamente, as razões que embasaram sua conclusão, de forma detalhada.

8. INDENIZAÇÃO

8.1. Caracterizado o sinistro, a Seguradora cumprirá a obrigação descrita na apólice, até o limite máximo de garantia da mesma, Segundo uma das formas abaixo, conforme for acordado entre as partes:
I – realizando, por meio de terceiros, o objeto do contrato principal, de forma a lhe dar continuidade, sob a sua integral responsabilidade; e/ou
II – indenizando, mediante pagamento em dinheiro, os prejuízos e/ou multas causados pela inadimplência do tomador, cobertos pela Apólice.
8.2. Do prazo para o cumprimento da obrigação:

8.2.1. O pagamento da indenização ou o início da realização do objeto do contrato principal deverá ocorrer dentro do prazo máximo de 30 (trinta) dias, contados da data de recebimento do último documento solicitado durante o processo de regulação do sinistro.
8.2.2. Na hipótese de solicitação de documentos de que trata o item 7.2.1., o prazo de 30 (trinta) dias será suspenso, reiniciando sua contagem a partir do dia útil subsequente àquele em que forem completamente atendidas as exigências.
8.2.3. No caso de decisão judicial ou decisão arbitral, que suspenda os efeitos de reclamação da Apólice, o prazo de 30 (trinta) dias será suspenso, reiniciando sua contagem a partir do primeiro dia útil subsequente a revogação da decisão.
8.3. Nos casos em que haja vinculação da Apólice a um contrato principal, todos os saldos de créditos do Tomador no contrato principal serão utilizados na amortização do prejuízo e/ou da multa objeto da reclamação do sinistro, sem prejuízo do pagamento da indenização no prazo devido.
8.3.1. Caso o pagamento da indenização já tiver ocorrido quando da conclusão da apuração dos saldos de créditos do Tomador no contrato principal, o Segurado obriga-se a devolver à Seguradora qualquer excesso que lhe tenha sido pago.

9. ATUALIZAÇÃO DE VALORES

9.1. O não pagamento das obrigações pecuniárias da Seguradora, inclusive da indenização nos termos da Cláusula 8 destas Condições Gerais, dentro do prazo para pagamento da respectiva obrigação, acarretará em:
a) atualização monetária, a partir da data de exigibilidade da obrigação, sendo, no caso de indenização, a data de caracterização do sinistro; e
b) incidência de juros moratórios calculados “pro rata temporis”, contados a partir do primeiro dia posterior ao término do prazo fixado.
9.2. O índice utilizado para atualização monetária será o IPCA/IBGE - Índice de Preços ao Consumidor Amplo da Fundação Instituto Brasileiro de Geografia e Estatística - ou índice que vier a substituí-lo, sendo calculado com base na variação positiva apurada entre o último índice publicado antes da data de obrigação de pagamento e aquele publicado imediatamente anterior à data de sua efetiva liquidação.
9.3. Os juros moratórios, contados a partir do primeiro dia posterior ao término do prazo fixado para pagamento da obrigação, serão equivalentes à taxa que estiver em vigor para a mora do pagamento de impostos devidos à Fazenda Nacional.
9.4. O pagamento de valores relativos à atualização monetária e juros de mora será feito independente de qualquer interpelação judicial ou extrajudicial, de uma só vez, juntamente com os demais valores devidos no contrato.

10. SUB-ROGAÇÃO

10.1. Paga a indenização ou iniciado o cumprimento das obrigações inadimplidas pelo

Tomador, a Seguradora sub-rogar-se-á nos direitos e privilégios do Segurado contra o Tomador, ou contra terceiros cujos atos ou fatos tenham dado causa ao sinistro.
10.2. É ineficaz qualquer ato do Segurado que diminua ou extinga, em prejuízo do segurador, os direitos a que se refere este item.

11. PERDA DE DIREITOS

O Segurado perderá o direito à indenização na ocorrência de uma ou mais das seguintes hipóteses:
I – Casos fortuitos ou de força maior, nos termos do Código Civil Brasileiro;
II – Descumprimento das obrigações do Tomador decorrente de atos ou fatos de responsabilidade do Segurado;
III – Alteração das obrigações contratuais garantidas por esta apólice, que tenham sido acordadas entre Segurado e Tomador, sem prévia anuência da Seguradora;
IV – Atos ilícitos dolosos ou por culpa grave equiparável ao dolo praticados pelo Segurado, pelo beneficiário ou pelo representante, de um ou de outro;
V – O Segurado não cumprir integralmente quaisquer obrigações previstas no contrato de seguro;
VI – Se o Segurado ou seu representante legal fizer declarações inexatas ou omitir de má-fé circunstâncias de seu conhecimento que configurem agravação de risco de inadimplência do Tomador ou que possam influenciar na aceitação da proposta;
VII – Se o Segurado agravar intencionalmente o risco.

12. CONCORRÊNCIA DE GARANTIAS

No caso de existirem duas ou mais formas de garantia distintas, cobrindo cada uma delas o objeto deste seguro, em benefício do mesmo Segurado ou beneficiário, a Seguradora responderá, de forma proporcional ao risco assumido, com os demais participantes, relativamente ao prejuízo comum.

13. CONCORRÊNCIA DE APÓLICES

É vedada a utilização de mais de um Seguro Garantia na mesma modalidade para cobrir o objeto deste contrato, salvo no caso de apólices complementares.

14. EXTINÇÃO DA GARANTIA

14.1. A garantia expressa por este seguro extinguir-se-á na ocorrência de um dos seguintes eventos, o que ocorrer primeiro, sem prejuízo do prazo para reclamação do sinistro conforme item 7.3. destas Condições Gerais:
I – quando o objeto do contrato principal garantido pela Apólice for definitivamente

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

realizado mediante termo ou declaração assinada pelo Segurado ou devolução da Apólice;
II – quando o Segurado e a Seguradora assim o acordarem;
III – quando o pagamento da indenização ao Segurado atingir o limite máximo de garantia da Apólice;
IV – quando o contrato principal for extinto, para as modalidades nas quais haja vinculação da Apólice a um contrato principal, ou quando a obrigação garantida for extinta, para os demais casos; ou
V – quando do término de vigência previsto na Apólice, salvo se estabelecido em contrário nas Condições Especiais.
14.2. Quando a garantia da Apólice recair sobre um objeto previsto em contrato, esta garantia somente será liberada ou restituída após a execução do contrato, em consonância com o disposto no parágrafo 4º do artigo 56 da Lei Nº 8.666/1993, e sua extinção se comprovará, além das hipóteses previstas o item 14.1, pelo recebimento do objeto do contrato nos termos do art. 73 da Lei Nº 8.666/93.

15. RESCISÃO CONTRATUAL

15.1. No caso de rescisão total ou parcial do contrato, a qualquer tempo, por iniciativa do Segurado ou da Seguradora e com a concordância recíproca, deverão ser observadas as seguintes disposições:
15.1.1. Na hipótese de rescisão a pedido da sociedade Seguradora, esta reterá do prêmio recebido, além dos emolumentos, a parte proporcional ao tempo decorrido;
15.1.2. Na hipótese de rescisão a pedido do Segurado, a sociedade Seguradora reterá, no máximo, além dos emolumentos, o prêmio calculado de acordo com a seguinte tabela de prazo curto:

Relação a ser aplicada sobre a vigência original para obtenção de prazo em dias	% Do Prêmio	Relação a ser aplicada sobre a vigência original para obtenção de prazo em dias	% Do Prêmio
15/365	13	195/365	73
30/365	20	210/365	75
45/365	27	225/365	78
60/365	30	240/365	80
75/365	37	255/365	83
90/365	40	270/365	85
105/365	46	285/365	88
120/365	50	300/365	90
135/365	56	315/365	93
150/365	60	330/365	95
165/365	66	345/365	98

180/365	70	365/365	100

15.1.2.1. Para prazos não previstos na tabela constante do subitem 15.1.2., deverá ser utilizado percentual correspondente ao prazo imediatamente inferior.

16. CONTROVÉRSIAS

16.1. As controvérsias surgidas na aplicação destas Condições Contratuais poderão ser resolvidas:
I – por arbitragem; ou
II – por medida de caráter judicial.
16.2. No caso de arbitragem, deverá constar, na apólice, a cláusula compromissória de arbitragem, que deverá ser facultativamente aderida pelo Segurado por meio de anuência expressa.
16.2.1. Ao concordar com a aplicação desta cláusula, o Segurado estará se comprometendo a resolver todos os seus litígios com a Seguradora por meio de Juízo Arbitral, cujas sentenças têm o mesmo efeito que as sentenças proferidas pelo Poder Judiciário.
16.2.2. A cláusula de arbitragem é regida pela Lei nº 9307, de 23 de setembro de 1996.

17. PRESCRIÇÃO

Os prazos prescricionais são aqueles determinados pela lei.

18. FORO

As questões judiciais entre seguradora e segurado serão processadas no foro do domicílio deste.

19. DISPOSIÇÕES FINAIS

19.1. A aceitação do seguro estará sujeita à análise do risco.
19.2. As apólices e endossos terão seu início e término de vigência às 24hs das datas para tal fim neles indicadas.
19.3. O registro deste plano na Susep não implica, por parte da Autarquia, incentivo ou recomendação à sua comercialização.
19.4. Após sete dias úteis da emissão deste documento, poderá ser verificado se a apólice ou endosso foi corretamente registrado no site da Susep - www.susep.gov.br.
19.5. A situação cadastral do corretor de seguros pode ser consultada no site www.susep.gov.br, por meio do número de seu registro na Susep, nome completo, CNPJ ou CPF.
19.6. Este seguro é contratado a primeiro risco absoluto.

bmg | Seguros

Condições Gerais

SEGURADO: PROCURADORIA GERAL DE JUSTICA DO ESTADO DO AMAZONAS
TOMADOR: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

19.7. Considera-se como âmbito geográfico das modalidades contratadas todo o território nacional, salvo disposição em contrário nas Condições Especiais e/ou Particulares da Apólice.
19.8. Os eventuais encargos de tradução referentes ao reembolso de despesas efetuadas no exterior ficarão totalmente a cargo da Sociedade Seguradora.