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.

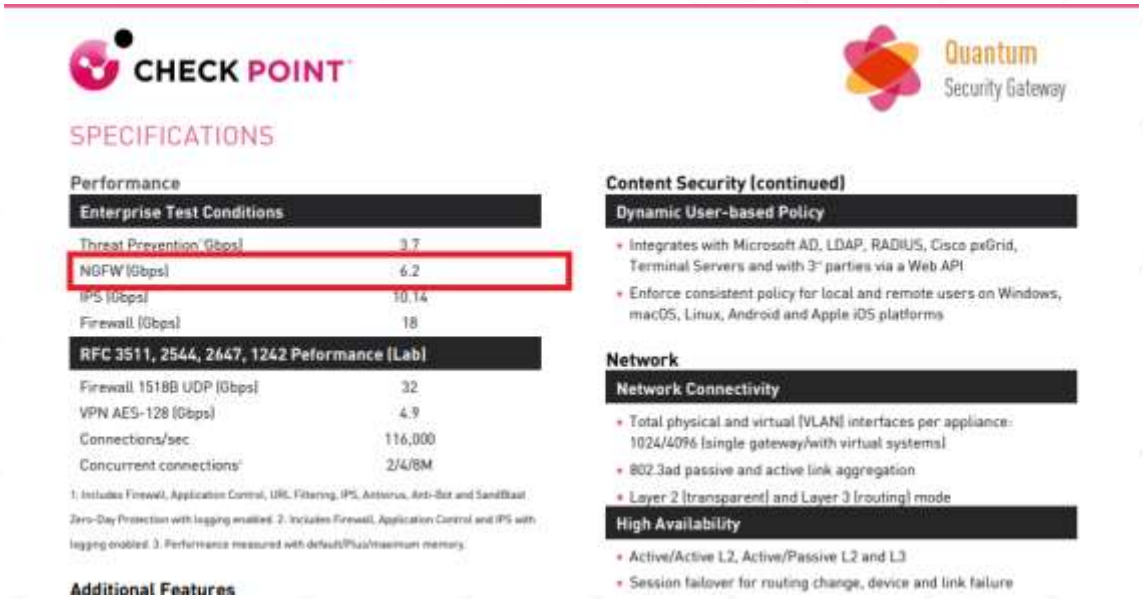
Na Tabela de Capacidades - ANEXO I TERMO DE REFERÊNCIA Nº 20.2021.DTIC.0720733.2021.015252 Item **5.2.15.10.15** lemos: "Throughput de Firewall* com as funcionalidades de FW, IPS, App Control, Sandbox e Anti-malware ativadas (em Gbps) **entre 5 Gbps e 10 Gbps**."

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:

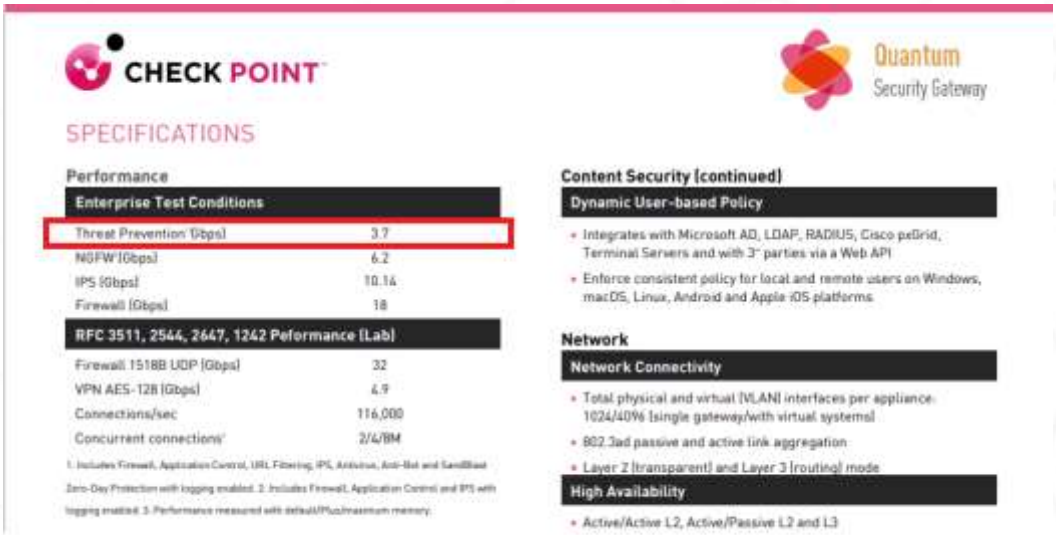
1. O appliance ofertado que consta em nossa proposta é o 6600 Plus appliance with SandBlast (SG6600-PLUS-SNBT), o que nos leva ao próximo ponto;
2. O SandBlast é um serviço dentro do portfólio do fabricante, que neste caso já está inclusa na solução, fornecendo a funcionalidade de SandBox com proteção 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."*

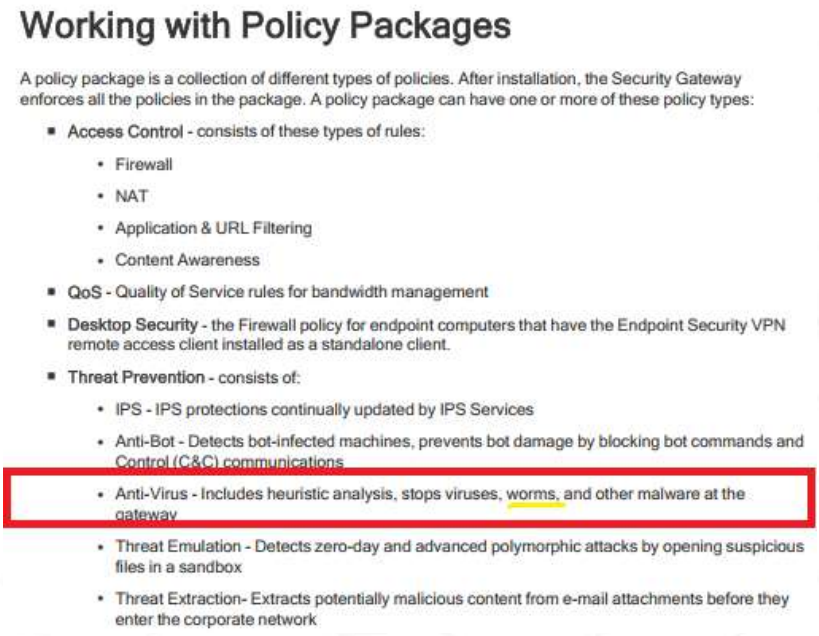
O nosso valor de **3,7 Gbps** fica entre o intervalo de **2,5 e 5,0 Gbps** exigido no edital, conforme imagem abaixo.

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.

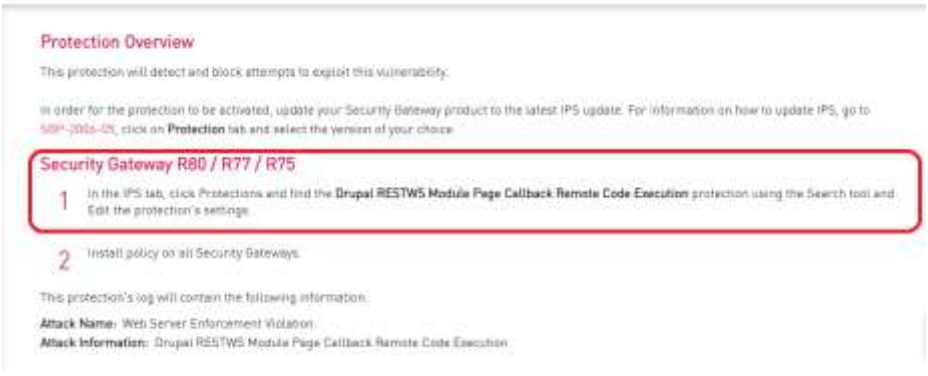
General

General

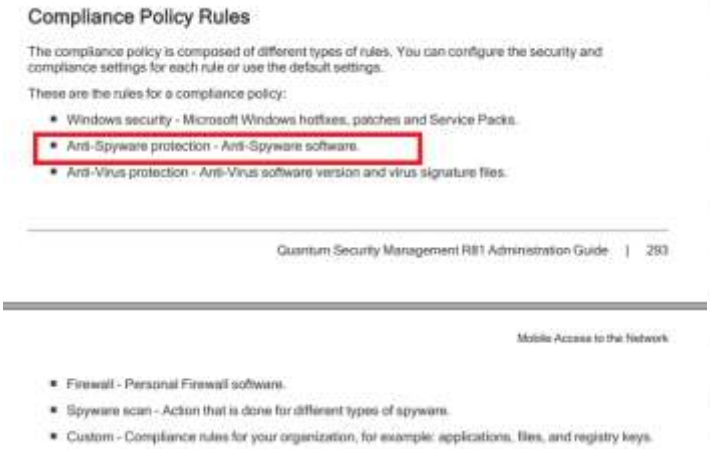
- **Emulate emails for malicious content (requires Threat Emulation)** - When this option and the Threat Emulation blade are enabled, the Threat Emulation blade scans SMTP traffic.
- **Scan emails for viruses (requires Anti-Virus)** - When this option and the Anti-Virus blade are enabled, the Anti-Virus 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/



- **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.



    - 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:

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

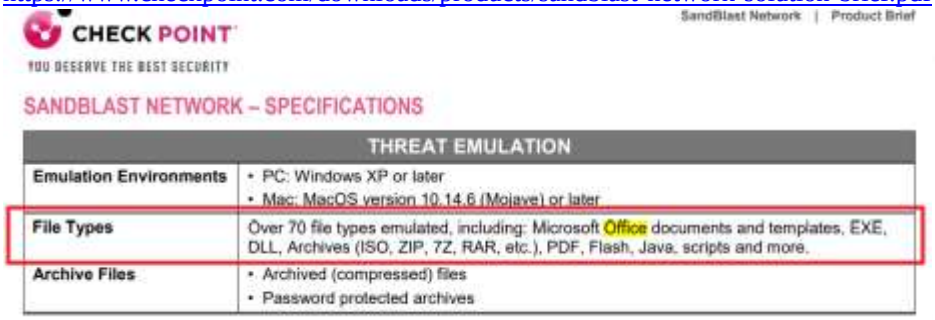
Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans.

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