


| | | |
|--|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD |
| | | TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | | |

1. INTRODUÇÃO

1.1 Por causa da variedade de ataques, qualquer estratégia de segurança cibernética deve ser baseada na combinação de diferentes tipos de proteção. Essas proteções são organizadas em camadas de segurança em que cada uma das camadas visa oferecer uma linha de defesa para diferentes alvos de ataques e tipos de ameaça. A Figura 1 apresenta a topologia física da rede corporativa e os pontos de proteção de perímetro dos Firewalls Corporativo, de DCN e de Usuário, objetos dessa especificação técnica e responsáveis por realizar o monitoramento e controle de todo tráfego externo e interno da rede.

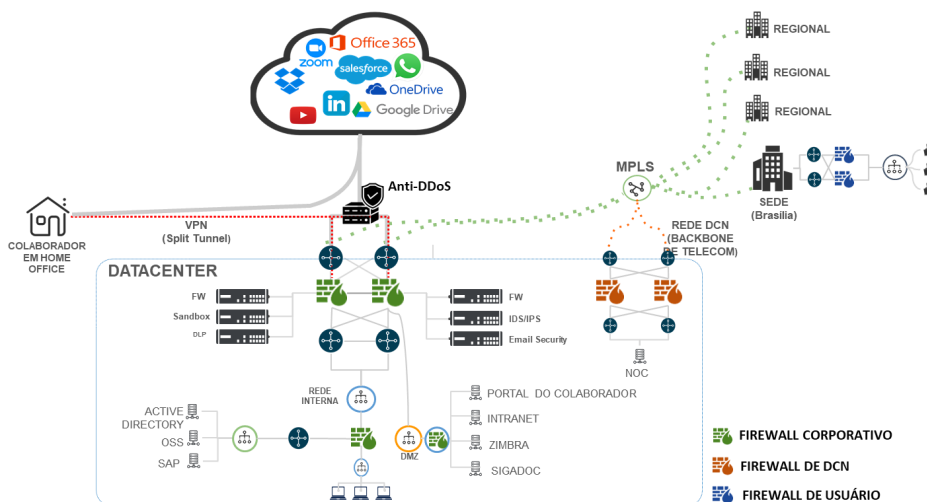



Figura 1: Topologia Física da rede corporativa da Telebras

1.2 A Tabela 1 apresenta o quantitativo estimado dos itens que precisam ser adquiridos para realizar a atualização da planta de Firewalls.

Tabela 1: Quantitativo a ser contratado

| CLUSTER | ITEM | Part Number | DESCRIÇÃO | UNIDADE DE MEDIDA | QTD | VALOR UNIT. | VALOR TOTAL |
|----------------|------|--------------------------------------|--|-------------------|-----|-------------|-------------|
| Cluster Tipo I | 1 | CPAP-SG9700-PLUS-SNBT CPSB-MOB-U* | Cluster de alta disponibilidade Firewall NGFW - Tipo I | Unidade | 1 | R\$ | R\$ |
| | 2 | CPSB-SNBT-9700-PLUS CPCES-CO-PREMIUM | Cluster de alta disponibilidade Firewall NGFW - Tipo I Subscrição (licenças), garantia e suporte anual | Ano | 5 | R\$ | R\$ |
| | 3 | - | Serviços de Instalação, migração e Configuração / Parametrização do Cluster Tipo I | Unidade | 1 | R\$ | R\$ |



| | | | |
|---|--|--|---------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | | DOD TLB-NTE-2023/00681 |
| | | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | | |

| CLUSTER | ITEM | Part Number | DESCRIÇÃO | UNIDADE DE MEDIDA | QTD | VALOR UNIT. | VALOR TOTAL |
|---------------------|------|---|---|-------------------|-----|-------------|-------------|
| Cluster Tipo II | 4 | CPAP-SG9400-PLUS-SNBT | Cluster de alta disponibilidade Firewall NGFW - Tipo II | Unidade | 1 | R\$ | R\$ |
| | 5 | CPSB-NGFW-9400-PLUS CPCES-CO-PREMIUM | Cluster de alta disponibilidade Firewall NGFW - Tipo II Subscrição (licenças), garantia e suporte anual | Ano | 5 | R\$ | R\$ |
| | 6 | - | Serviços de Instalação, migração e Configuração / Parametrização de Software do Cluster Tipo II | Unidade | 1 | R\$ | R\$ |
| Cluster Tipo III | 7 | CPAP-SG9100-SNBT CPSB-MOB-50* | Cluster de alta disponibilidade Firewall NGFW - Tipo III | Unidade | 1 | R\$ | R\$ |
| | 8 | CPSB-NGFW-9100-PLUS CPCES-CO-PREMIUM | Cluster de alta disponibilidade Firewall NGFW - Tipo III Subscrição (licenças), garantia e suporte anual | Ano | 5 | R\$ | R\$ |
| | 9 | - | Serviços de Instalação, migração e Configuração / Parametrização de Software do Cluster Tipo III | Unidade | 1 | R\$ | R\$ |
| Gerência | 10 | CPSM-NGSM10-EVNT* CPSM-NGSM10-LOG* | Servidor de Gerência Unificada | Unidade | 1 | R\$ | R\$ |
| | 11 | - | Garantia e suporte anual | Ano | 5 | R\$ | R\$ |
| | 12 | - | Serviços de Instalação, migração e Configuração / Parametrização de Software da Gerência | Unidade | 1 | R\$ | R\$ |

*As licenças da Gerência, Firewall e Virtual Private Network (VPN) deverão ser perpétuas.


1.2 A Tabela 1 apresenta o quantitativo estimado dos itens que precisam ser adquiridos para realizar a atualização da planta de Firewalls.

1.3 A implantação da solução deve contemplar todos os acessórios de hardware e software necessários à sua perfeita instalação e funcionamento, incluindo: todos os cabos necessários para conectividade lógica, cabos de força padrão internacional IEC, interfaces, suportes, gbics (transceivers) ou rede ethernet (a depender da conectividade de rede do equipamento), conjuntos de trilhos para instalação do *Appliance* em rack padrão de 19" (dezenove polegadas), drivers de controle, softwares de configuração, fontes de alimentação, além dos equipamentos e licenças de subscrição de software para proteção de dados e atendimento a todas funcionalidades requeridas neste documento, não se limitando aos Part Numbers listados na Tabela 1.

2. LICENCIAMENTO E HARDWARE

2.1 Por cada *gateway* entenda-se o hardware e as licenças de softwares necessárias para o seu funcionamento.



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

2.2 Por console de gerência e monitoração entenda-se os servidores de gerência e as licenças de software necessária para seu funcionamento.

2.3 A licitante deve especificar o(s) modelo(s) em sua proposta comercial, indicando a qual perfil de capacidade ele(s) atende(m).

2.4 A contratada deverá utilizar os equipamentos e licenças já contratados pela Telebras como parte da solução desde que atendam aos perfis sendo contratados.

2.5 O licitante vencedor fica obrigado a fazer **trade in** dos dois (2) cluster de firewall (clusters checkpoint) que a Telebras possui em seu parque tecnológico. O desconto referente ao aproveitamento dos equipamentos deve estar expresso nestes reaproveitados pelo período da garantia previsto no novo contrato. Os modelos dos equipamentos antigos que serão substituídos são:

2.5.1 Um (1) cluster de firewall Checkpoint modelo 15000;

2.5.2 Um (1) cluster de firewall Checkpoint modelo Power-1 5070.

2.5.3 O cronograma das atividades de desinstalação e migração deverão estar previstas no plano de implantação.

2.5.4 Nos preços deverão estar computados os impostos, taxas e demais despesas que, direta ou indiretamente tenham relação com o objeto, bem como o desconto do valor de **trade in** dos equipamentos antigos.

2.6 Cada solução de alta disponibilidade (HA) deverá ser composta por dois (2) equipamentos (*appliances*) funcionando em cluster, construídos especificamente para exercer a função de *Next Generation Firewall*, com hardware e software fornecidos pelo mesmo fabricante.

2.7 Todas as funcionalidades de proteção de rede devem funcionar integradas em um mesmo equipamento, de forma simultânea.

2.8 O hardware e software que executem as funcionalidades de proteção de rede devem ser de um mesmo fabricante.


2.9 As consoles de gerência e monitoração devem ser compatíveis com os *gateways* de proteção de rede.

2.10 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário, e 2 cabos de alimentação por fonte: 1 padrão NBR 14136 e 1 IEC c320-13/14.

2.11 As licenças da Gerência, Firewall e VPN deverão ser perpétuas.

2.12 Cluster Tipo I de alta disponibilidade Firewall NGFW – Itens 1 e 2



| | | |
|--|--|--------------------------------|
|  TELEBRAS | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD |
| | | TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | | |

2.12.1 Especificações mínimas:

- 2.12.1.1 *Threat Prevention Throughput* de 13 Gbps de tráfego. O *Throughput* deverá ser atendido com todas as funcionalidades do equipamento ativas;
- 2.12.1.2 *Next Generation Firewall NGFW Throughput* de 25 Gbps de tráfego;
- 2.12.1.3 8.000.000 conexões simultâneas;
- 2.12.1.4 400.000 novas conexões por segundo;
- 2.12.1.5 Duas (2) fontes redundantes;
- 2.12.1.6 Pelo menos duas (2) interfaces de rede 10/100/1000 base-TX;
- 2.12.1.7 Pelo menos seis (6) interfaces de rede 10 GBase-SR, incluindo os transceivers se necessários;
- 2.12.1.8 Deverá possuir um (1) slot disponível para expansão de interface 100/40/25G QSFP28.

2.12.2 Licenciamento de: IPS, Application Control e URL Filtering, Anti-Spam, Data Loss Prevention, VPN mobile access, HTTPS Inspection e Anti-virus (anti-malware).

2.12.3 O licenciamento da VPN deverá ser de usuários ilimitados.

2.12.4 Item 1 - Part Number: CPAP-SG9700-SNBT PLUS; CPSB-MOB-U.

2.12.5 Item 2 - Part Number: CPSB-SNBT-9700-PLUS; CPCES-CO-PREMIUM.


- 12.12.5.1 As subscrições, o suporte técnico e a garantia devem vigor por 60 (sessenta) meses, com pagamento anual;
- 12.12.5.2 Os critérios de atendimento do suporte e garantia estão descritos no Termo de Referência.

2.13 Cluster Tipo II de alta disponibilidade Firewall NGFW – Itens 4 e 5

2.13.1 Especificações mínimas:

- 2.13.1.1 *Next Generation Firewall NGFW Throughput* de 20 Gbps de tráfego;
- 2.13.1.2 4.000.000 conexões simultâneas;
- 2.13.1.3 300.000 novas conexões por segundo;
- 2.13.1.4 Duas (2) fontes redundantes;
- 2.13.1.5 Pelo menos dez (10) interfaces de rede 10/100/1000 base-TX;



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

2.13.1.6 Pelo menos duas (2) interfaces de rede 10 GBase-SR, incluindo os transceivers se necessários.

2.13.1.7 Deverá possuir um (1) slot disponível para futura expansão de interface 100/40/25G QSFP28

2.13.2 Item 4 - Part Number: CPAP-SG9400-SNB PLUS

2.13.3 Item 5 - Part Number: CPSB-NGFW-9400-PLUS; CPCES-CO-PREMIUM.

12.13.3.1 As subscrições, o suporte técnico e a garantia devem vigor por 60 (sessenta) meses, com pagamento anual;

12.13.3.2 Os critérios de atendimento do suporte e garantia estão descritos no Termo de Referência.

2.14 Cluster Tipo III de alta disponibilidade Firewall NGFW – Itens 7 e 8

2.14.1 Especificações mínimas:

2.14.1.1 *Next Generation Firewall* NGFW *Throughput* de 3,5 Gbps de tráfego

2.14.1.2 Dois milhões (2.000.000) de conexões simultâneas;

2.14.1.3 Sessenta e cinco mil (65.000) novas conexões por segundo;

2.14.1.4 Pelo menos seis (6) interfaces de rede 10/100/1000 base-TX;

2.14.1.5 Licenciamento de: Firewall e VPN *remote access* para pelo menos 30 usuários.

2.14.2 Item 7 - Part Number: CPAP-SG9100-SNBT; CPSB-MOB-50.

2.14.3 Item 8 - Part Number: CPSB-NGFW-9100-PLUS; CPCES-CO-PREMIUM.

12.14.3.1 As subscrições, o suporte técnico e a garantia devem vigor por 60 (sessenta) meses, com pagamento anual;

12.14.3.2 Os critérios de atendimento do suporte e garantia estão descritos no Termo de Referência.


2.15 Servidor de Gerência Unificada – Itens 10 e 11

2.15.1 Console de Gerência e Monitoração:

2.15.1.1 Item 10 - Part Number: CPSM-NGSM10-EVNT; CPSM-NGSM10-LOG.

2.15.2 A console de gerência deve possuir pelo menos as seguintes funcionalidades:



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

2.15.2.1 Centralizar a administração de regras e políticas para todos os *gateways* de proteção de rede, usando uma única interface gráfica ou web;

2.15.2.2 Acesso concorrente de administradores;

2.15.2.3 Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

2.15.2.4 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.15.2.5 Autenticação integrada ao Microsoft Active Directory ou servidor Radius;

2.15.2.6 Criação de objetos globais, que possam ser utilizados em todos os *gateways* de proteção de rede;

2.15.2.7 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

2.15.2.8 Criação de regras que fiquem ativas em horário definido;

2.15.2.9 Criação de regras com data de expiração;

2.15.2.10 Atualização centralizada e remota do software dos *gateways* de proteção de rede;

2.15.2.11 Backup das configurações e *rollback* de configuração para a última configuração Salva;

2.15.2.12 Validação da política, avisando quando houver regras que, ofusquem ou conflitem com outras (*shadowing*);

2.15.2.13 Instalação de uma mesma política em mais de um *gateway*, podendo especificar, para cada *gateway*, um conjunto de regras adicionais;

2.15.2.14 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;


2.15.2.15 Os diversos *gateways* deverão operar com todas as suas funcionalidades, mesmo na ocorrência de falha de comunicação com a ferramenta de gerenciamento.

2.15.3 A console de monitoração deve possuir pelo menos as seguintes funcionalidades:

2.15.3.1 Visualização dos logs de todos os *gateways* na console centralizada, em uma única pesquisa;

2.15.3.2 Arquivamento e rotação do log;



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

2.15.3.3 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma contínua a cada 1 minuto):

- 2.15.3.3.1 Situação do gateway e do cluster;
- 2.15.3.3.2 Principais IPs por número de conexões;
- 2.15.3.3.3 Principais IPs por consumo de banda;
- 2.15.3.3.4 Conexões por IP de origem e destino;
- 2.15.3.3.5 Consumo de banda por IP de origem e destino;
- 2.15.3.3.6 Conexões por serviço;
- 2.15.3.3.7 Consumo de banda por serviço.

2.15.4 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

- 2.15.4.1 Resumo gráfico de aplicações utilizadas;
- 2.15.4.2 Principais aplicações por utilização de largura de banda de entrada e saída.

2.16 Serviços de instalação – Itens 3, 6, 9 e 12

2.16.1 O serviço de instalação e migração das políticas para os novos equipamentos da solução precisará contemplar no Plano de Implantação os seguintes itens:

2.16.1.1 Avaliação e Planejamento:

- inventário completo de todos os dispositivos conectados;
- documentação das regras e políticas existentes; e
- análise das necessidades atuais e futuras de segurança, o qual devem considerar contemplar condições do ambiente interno e externo, como por exemplo, o uso do *remote access* para trabalho híbrido.

2.16.1.2 Requisitos Técnicos:


- compatibilidade do novo firewall com a infraestrutura existente;
- configuração inicial do hardware e software do novo firewall; e
- preparação de interfaces de rede e segmentos de rede.

2.16.1.3 Migração de Políticas:

- tradução das políticas do firewall atual para o novo;
- teste das políticas antes da implantação; e
- e ajustes de políticas para otimização de desempenho e segurança.

2.16.1.4 Procedimentos de Backup:



| | | |
|--|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD |
| | | TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | | |

- backup completo das configurações e regras do firewall atual; e
- desenvolvimento de um plano de *rollback* em caso de falha na migração.

2.16.1.5 Implementação:

- instalação física e configuração básica do novo firewall;
- migração das regras e políticas, garantindo a mínima interrupção do serviço; e
- teste funcional para garantir que todas as políticas estejam operacionais.

2.16.1.6 Documentação:

- atualização da documentação de segurança para refletir as novas configurações.

2.16.1.6 Monitoramento e Ajustes Pós-Implantação:

- monitoramento contínuo do novo firewall após a implantação e ajustes necessários com base nos logs de segurança e *feedback* da equipe técnica da CONTRATANTE.

2.16.2 O plano de Trabalho, a ser entregue após a reunião de *kick-off* deverá contemplar as informações detalhadas nos serviços de instalação, o cronograma de todas as atividades que serão realizadas, bem como a arquitetura da solução que será implantada.

2.17. Quantidades:

2.17.1 Três (3) clusters de Firewall NGFW com subscrição, suporte e garantia por 60 meses;

2.17.1.1 Cada cluster será composto por dois (2) *gateways* ativo/passivo;

2.17.2 Uma (1) console de gerência com alta disponibilidade e monitoração ativa;

2.17.3 Quatro (4) serviços de instalação para os clusters e a gerência.

3. FUNCIONALIDADES BÁSICAS DE PROTEÇÃO DE REDE

3.1 Os gateways de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

3.1.2 VLAN's 802.1q;


3.1.3 Agregação de links 802.3ad;

3.1.4 *Policy based routing* ou *policy based forwarding*;

3.1.5 Roteamento multicast (PIM-SM);

3.1.6 Roteamento IPv4 e IPv6;




| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

- 3.1.7 DHCP Relay;
- 3.1.8 Suportar NAT dinâmico (N-to-1 e N-to-N);
- 3.1.9 Suportar NAT estático (N-to-1 e N-to-N);
- 3.1.10 Suportar NAT estático bidirecional (1-to-1);
- 3.1.11 Suportar tradução de porta (PAT);
- 3.1.12 Suportar NAT de origem e NAT de destino, simultaneamente;
- 3.1.13 Enviar log para múltiplas consoles de monitoração, simultaneamente;
- 3.1.14 Proteção contra anti-spoofing;
- 3.1.15 Roteamento BGP e OSPF;
- 3.1.16 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:
 - 3.1.16.1 Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 e camada 3.
 - 3.1.16.2 Modo *sniffer*, para inspeção via porta espelhada do tráfego de dados da rede.
 - 3.1.16.3 Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.
 - 3.1.16.4 Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como *default gateway* das redes protegidas.
 - 3.1.16.5 Modo Misto de trabalho *sniffer*, L2 e L3, em diferentes interfaces físicas.
- 3.2 Os *appliances* deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência.
- 3.3 Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário.

4. RECONHECIMENTO DE APLICAÇÕES E CONTROLE GRANULAR

- 4.1 Os gateways de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:



| | | |
|--|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD |
| | | TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | | |

4.1.1 Reconhecer pelo menos mil (1.000) 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, compartilhamento de arquivos, e-mail;

4.1.2 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, ultrasurf, 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, bgp, gre, ospf, rip.

4.2 Permitir decifrar tráfego SSL e SSH para o reconhecimento da aplicação que está tunelada.

4.3 Detectar e reconhecer aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.

4.4 Detectar funcionalidades específicas dentro de aplicações, como a transferência de Arquivos em Webex ou *Instant Messaging*.

4.5 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias da TELEBRAS, sem a necessidade de ação do fabricante.

4.6 Identificar o uso de táticas evasivas via comunicações criptografadas.

4.7 Atualizar a base de assinaturas de aplicações automaticamente.

4.8 Reconhecer aplicações em IPv6.

4.9 Limitar a banda (*download/upload*) usada por aplicações (*traffic shaping*), baseado no IP de origem ou nome/grupo de usuários.

4.10 Os gateways de proteção de rede deve 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* ou nas estações dos usuários.


4.11 Os gateways deverão suportar a criação de regras por: porta de destino, endereço de origem e destino (IP, Range de IP e FQDN), protocolo (TCP, UDP, ICMP, etc.), usuários e/ou grupos do Microsoft Active Directory, aplicações e categorias de aplicações.

5. PREVENÇÃO DE AMEAÇAS

5.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus, Anti-Malware, URL *filtering*, Anti-Bot e DNS *security* integrados no próprio equipamento de firewall.

5.2 Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos.



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

5.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo.

5.4 Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

5.5 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 e memória do dispositivo.

5.6 Deve possuir os seguintes mecanismos de inspeção de IPS:

5.6.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP *Defragmentation*, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

5.6.2 Detectar e bloquear a origem de *portscans*;

5.6.3 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

5.6.4 Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

5.6.5 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

5.6.6 Suportar bloqueio de arquivos por tipo;

5.6.7 Identificar e bloquear comunicação com *botnets*;

5.6.8 Deve suportar referência cruzada com CVE (*Common Vulnerabilities and Exposures*);

5.6.9 Em cada proteção de segurança, deve estar incluso informações como:

5.6.10 Código CVE, não sendo aceito outro código de referência;

5.6.11 Severidade;


5.6.12 Tipo de ação a ser executada.

5.7 O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

5.8 O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

5.9 O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

5.10 O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor).

5.11 A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas, incluindo ataques de dia zero (*zero-day*).

5.12 A solução Antivírus deve suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede.

5.13 Suportar a criação de políticas por Geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado.

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

5.15 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

5.16 A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

5.17 A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (*command & Control*).

5.18 A solução Antivírus deverá suportar a análise de links no corpo de emails.

6. ALTA DISPONIBILIDADE

6.1 Todos os elementos da solução devem funcionar em alta disponibilidade, incluindo a gerência.


6.2 A alta disponibilidade dos *gateways* de proteção de rede deve ser na forma de cluster ativo-passivo(s).

6.3 Os *gateways* ativo-passivo(s) devem manter as tabelas de conexões sincronizadas, evitando a interrupção de conexões em caso de um dos *gateway*(s) secundário(s) assumir a operação do cluster.

6.4 Os *gateways* do cluster devem ser capazes de funcionar por meio de uma rede única (mesmo domínio de *broadcast*), mas geograficamente separada.

6.5 Deve ser possível configurar uma interface de rede ou VLAN, para efetuar todas as comunicações de sincronização e comunicação entre os *gateways* de um cluster, podendo ainda usar uma ou mais interfaces como redundância para este processo.



| | | |
|---|--|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

6.6 A console de gerência e monitoração deve ser capaz de operar de forma redundante.

6.7 As políticas devem ser sincronizadas entre os módulos de gerência.

6.8 Os *gateways* devem enviar os logs e outras informações para estatística histórica para os módulos de monitoração simultaneamente.

7. VPN

7.1 Os *gateways* de proteção de rede com as funcionalidades de VPN cliente-a-*gateway* IPSec e SSL, devem suportar as seguintes características:

7.2 A VPN cliente-a-*gateway* deve suportar autenticação usando dispositivos seguros para armazenamento de certificados digitais: *smartcard* e *token*.

7.3 O cliente VPN deve ser compatível com Windows 10 32 e 64 bits, Mac OS X, e versões superiores desses sistemas operacionais.

7.4 A autenticação dos usuários na VPN cliente-a-*gateway* deverá permitir o uso de certificado digital emitido pelo *Microsoft Certificate Server*.

7.5 A autorização dos usuários na VPN cliente-a-*gateway* deverá se basear em grupos do Microsoft Active Directory, sem a necessidade de instalação de qualquer software adicional no *Domain Controller*.

7.6 Deve suportar a conexão do cliente móvel automaticamente através do *gateway* secundário, quando o primário estiver indisponível.

7.7 O cliente e o *gateway* devem ser capazes de operar adequadamente quando um elemento (modem xDSL, cable modem, firewall, etc.) efetuar a tradução de endereço do cliente (NAT Traversal).

7.8 Registrar em log, na console de monitoração, detalhes da conexão à VPN, como:

7.8.1 Usuário;

7.8.2 Horário;


7.8.3 Serviços acessados;

7.8.4 Serviços bloqueados;

7.8.5 protocolos de criptografia e endereço IP do cliente.

7.9 Possibilitar a alocação de endereços IP da rede interna da Telebras aos clientes remotos da VPN, possibilitando aos recursos internos reconhecerem os clientes da VPN como parte da rede interna.



| | | |
|---|---|--------------------------------|
|  | ANEXO A ESPECIFICAÇÕES TÉCNICAS | DOD TLB-NTE-2023/00681 |
| | | DATA Janeiro de 2025 |
| | Contratação de empresa especializada para atualização, aquisição e instalação de equipamentos Firewall compatível e serviços de suporte on-site e manutenção de hardware e software | |

7.10 A VPN gateway-a-gateway deverá suportar: IKE, 3DES, AES, SHA1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.



Assinado com senha por THIAGO FERREIRA PORTELA - 14/02/2025 às 13:56:53.
Documento Nº: 750737-6531 - consulta à autenticidade em
<https://extranet.telebras.com.br/sigaex/public/app/autenticar?n=750737-6531>

