

**MINISTÉRIO DA CULTURA****SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO**

Esplanada dos Ministérios, Bloco B, - Bairro Zona Cívica Administrativa, Brasília/DF, CEP 70068-900

Telefone: - <http://www.cultura.gov.br>**CADERNO DE ESPECIFICAÇÕES TÉCNICAS****PROCESSO: 01400.000997/2023-52****DOCUMENTOS
RELACIONADOS****OBJETO - Registro de preços para aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) com garantia e suporte**

ESTUDO TÉCNICO PRELIMINAR 03/2023

CONTRATAÇÃO: 420001/000047/2023

QUADRO DE COMPOSIÇÃO - GRUPO/LOTE E ITENS.

LOTE	ITEM	DESCRIÇÃO
01	1	MÓDULO DE SEGURANÇA (CLUSTER) - TIPO I
	2	MÓDULO DE SEGURANÇA - TIPO II
	3	MÓDULO DE SEGURANÇA - TIPO III
	4	SISTEMA DE GERÊNCIA CENTRALIZADA COM ARMAZENAMENTO DE LOGS
	5	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO PARA A SOLUÇÃO
	6	TREINAMENTO "HANDS ON" SOBRE SOLUÇÃO DE FIREWALL

1. ITEM 01 - MÓDULO DE SEGURANÇA (CLUSTER) - TIPO I - CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO

- 1.1. A solução deve possuir throughput de, no mínimo, 19 (dezenove) Gbps de Next Generation Firewall, considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público;
- 1.2. Deve possuir throughput de, no mínimo, 10 (Dez) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware e log habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
- 1.3. ~~Deve possuir, no mínimo, 2 (duas) interfaces físicas de rede de 40G/100G QSFP/QSFP28 (ITEM REMOVIDO)~~
- 1.4. ~~Deve possuir, no mínimo, 2 (duas) interfaces físicas dedicadas para o recurso de alta disponibilidade não sendo permitido o uso de interfaces do quantitativo já solicitado; (ITEM REMOVIDO)~~
- 1.5. Deve suportar, no mínimo, 2.000.000 (dois milhões) sessões simultâneas;
- 1.6. Deve suportar, no mínimo, 215.000 (Duzentos e quinze mil) novas conexões por segundo;
- 1.7. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1/10 Gbps do tipo RJ-45;
- 1.8. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+;
- 1.9. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 25 Gbps do tipo SFP28;
- 1.10. Deve possuir, no mínimo, 2 (duas) interfaces físicas de rede de 40G/100G QSFP/QSFP28, devendo ser fornecido 2(dois) transceiver 40G QSFP+ SR
- 1.11. Deve possuir, no mínimo, 8 (oito) interfaces fixas de rede de 10Mbps/100Mbps/1Gbps do tipo RJ-45;

- 1.12. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1Gbps dedicada para gerenciamento;
- 1.13. Deve possuir, no mínimo, 2 (duas) interface física dedicada para o recurso de alta disponibilidade não sendo permitido o uso de interface de propósito geral para essa finalidade.
- 1.14. Deve ser possível, configurar de maneira individual, as características de velocidade de cada interface do equipamento.
- 1.15. O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação.
- 1.16. Deve possuir disco do tipo Solid State Drive (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB para armazenamento do sistema operacional e registro de logs;
- 1.17. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;
- 1.18. Deve suportar, no mínimo, 1.800 (mil e oitocentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;

2. ITEM 02 - MÓDULO DE SEGURANÇA DO - TIPO II - CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO

- 2.1. Deve possuir throughput de, no mínimo, 9 (nove) de Gbps de Next Generation Firewall considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público;
- 2.2. Deve possuir throughput de, no mínimo, 4.5 (quatro, cinco) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware e log habilitados simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
- 2.3. Deve suportar, no mínimo, 1.200.000 (um milhão e duzentos mil) sessões simultâneas;
- 2.4. Deve suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo;
- 2.5. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1Gbps do tipo RJ-45;
- 2.6. Deve possuir, no mínimo, 2 (duas) interfaces físicas de rede de 1Gbps do tipo SFP;
- 2.7. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 10Gbps do tipo SFP+;
- 2.8. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1Gbps dedicada para gerenciamento;
- 2.9. Deve possuir, no mínimo, 2 (duas) interface física dedicada para o recurso de alta disponibilidade;
- 2.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
- 2.11. Deve ser possível, configurar de maneira individual, as características de velocidade de cada interface do equipamento.
- 2.12. Deve possuir disco do tipo Solid State Drive (SSD) de, no mínimo, 240 (duzentos e quarenta) GB para armazenamento do sistema operacional e registro de logs;
Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;
- 2.13. Deve suportar, no mínimo, 1.000 (mil) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;
O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação.

3. ITEM 03 - MÓDULO DE SEGURANÇA DO - TIPO III - CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO

- 3.1. Deve possuir throughput de, no mínimo, 2 (dois) Gbps de Next Generation Firewall considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público;
- 3.2. Deve possuir throughput de, no mínimo, 1 (um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware e log habilitadas simultaneamente na solução. A comprovação se dará

através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

- 3.3. Deve suportar, no mínimo, 180.000 (cento e oitenta mil) sessões simultâneas;
Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;
- 3.4. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1Gbps do tipo RJ-45;
- 3.5. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1Gbps dedicada para gerenciamento;
- 3.6. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
- 3.7. Deve possuir disco interno de no mínimo, 128 (cento, vinte e oitenta) GB para armazenamento do sistema operacional e registro de logs;
- 3.8. O equipamento deve suportar fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC;
- 3.9. Deve suportar, no mínimo, 500 (quinhentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;
- 3.10. O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação.

4. **FUNCIONALIDADES GERAIS DOS MÓDULOS DE SEGURANÇA TIPO I, TIPO II e TIPO III**

- 4.1. A solução de deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 4.2. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 4.3. A solução de segurança, deve possuir nativamente funcionalidade de Machine Learning capaz de bloquear grande volume dos ataques nas suas redes.
- 4.4. Os Firewalls de segurança físico, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP;
- 4.5. O hardware e software que executem as funcionalidades de proteção de rede, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 4.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
 - 4.6.1. agregação de links 802.3ad e LACP para o equipamento do tipo I;
 - 4.6.2. Policy based routing ou policy based forwarding;
 - 4.6.3. Roteamento multicast (PIM-SM);
 - 4.6.4. DHCP Relay;
 - 4.6.5. DHCP Server;
 - 4.6.6. Jumbo Frames;
 - 4.6.7. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3
Suportar sub-interfaces ethernet logicas
- 4.7. Deve suportar os seguintes tipos de NAT:
 - 4.7.1. Nat dinâmico (Many-to-1);
 - 4.7.2. Nat dinâmico (Many-to-Many);
 - 4.7.3. Nat estático (1-to-1);
 - 4.7.4. NAT estático (Many-to-Many);
 - 4.7.5. Nat estático bidirecional 1-to-1;
 - 4.7.6. Tradução de porta (PAT);
 - 4.7.7. NAT de Origem;

- 4.7.8. NAT de Destino;
- 4.7.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.8. Deve implementar Network Prefix Translation (NPTv6), NAT66 ou similar que traduza prefixos de endereços de rede IPv6;
- 4.9. Enviar log para sistemas de monitoração externos;
- 4.10. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 4.11. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- 4.12. Proteção contra anti-spoofing;
- 4.13. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.14. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 4.15. Suportar a OSPF graceful restart;
- 4.16. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
- 4.17. O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 4.18. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.19. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 4.20. 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;
- 4.21. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.22. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
 - 4.22.1. Em modo transparente;
 - 4.22.2. Em layer 3;
- 4.23. A configuração em alta disponibilidade deve sincronizar:
 - 4.23.1. Sessões;
 - 4.23.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
Certificados de-criptografados;
 - 4.23.3. Associações de Segurança das VPNs;
 - 4.23.4. Tabelas FIB;
- 4.24. No modo HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- 4.25. **SD-WAN**
 - 4.25.1. Deve operacionalizar no mínimo os seguintes critérios de SD-WAN;
 - 4.25.2. A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal.
 - 4.25.3. As configurações de perfis de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades.
 - 4.25.4. A solução deve permitir operar em caráter de diagrama hub-spoke.
 - 4.25.5. É considerado diferencial dispositivos que tenham a capacidade de exibir impactos por aplicação.
 - 4.25.6. A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo os seguintes itens em porcentagem ou contadores, jitter, latência e perda de pacote.

- 4.25.7. O dispositivo deve compreender o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garantir que a experiência do usuário sofra o menor impacto possível.
- 4.25.8. O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.
- 4.25.9. A solução deve ter inteligência para executar no mínimo as seguintes lógicas de operação:
- a) Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS.
 - b) Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresenta resultados abaixo dos limites definidos.
 - c) Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes.
- 4.25.10. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponíveis, que está orientado ao mesmo destino.
- 4.25.11. O dispositivo de SD-WAN deve utilizar "*Forward Error Correction*" (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.
- 4.25.12. O SD-WAN deve permitir combinar vários serviços ISP em uma interface Ethernet Agregada (AE) para redundância de link. A interface agregada deve oferecer suporte a subinterfaces para que seja possível marcar diferentes serviços ISP usando tags. de VLAN de camada 3 a fim de obter segmentação de tráfego de ponta a ponta.
- 4.25.13. O SD-WAN deve permitir o monitoramento de integridade do caminho de aplicativos SaaS para garantir decisões com base em confiabilidade e experiência do usuário. Nos cenários onde o SD-WAN com link de acesso direto à Internet (DIA), deve permitir o failover para um caminho de desempenho mais alto com base em medições precisas da qualidade da aplicação.
- 4.25.14. Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste "path" para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes.

4.26. **CONTROLE POR POLÍTICA DE FIREWALL**

- 4.26.1. Deverá suportar controles por zona de segurança.
- 4.26.2. Controles de políticas por porta e protocolo.
- 4.26.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- 4.26.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- 4.26.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- 4.26.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
- 4.26.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- 4.26.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
- 4.26.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- 4.26.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- 4.26.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2 , TLS 1.2 e TLS 1.3;

Controle de inspeção e de-criptografia de SSH por política;

4.26.12. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

4.26.13. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

4.26.14. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

4.26.15. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

Suporte a objetos e regras IPV6.

4.26.16. Suporte a objetos e regras multicast.

4.26.17. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.26.18. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

4.27. **CONTROLE DE APLICAÇÕES**

4.27.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

- a) Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
- b) Reconhecer pelo menos 3000 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;
- c) 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 ataques mediante a porta 443.
- d) 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;
- e) Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
- f) Identificar o uso de táticas evasivas via comunicações criptografadas;
- g) Atualizar a base de assinaturas de aplicações automaticamente;
- h) Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- i) 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;
- j) Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- k) Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
- l) Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- m) O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- n) Deve alertar o usuário quando uma aplicação for bloqueada;
- o) Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.27.2. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

- a) Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
- b) Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
- c) Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

4.27.3. Deve possuir mecanismo para controlar vazamento de dados, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos: * PDF; * EXE; * .Doc; * .PPT; * Excell.

4.27.4. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload"

4.27.5. A solução de controle de dados deve permitir ações como permitir, alertar ou bloquear do envio de arquivos.

4.27.6. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estiverem sendo trafegados através de aplicações como: Dropbox-uploading, filedropper e outros.

4.28. **PREVENÇÃO DE AMEAÇAS**

4.28.1. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.28.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;

4.28.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado com a última base de assinatura instalada no momento em que a licença expirou, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.28.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.28.5. As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.28.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

4.28.7. Deve permitir o bloqueio de vulnerabilidades.

4.28.8. Deve permitir o bloqueio de exploits conhecidos.

4.28.9. Deve incluir proteção contra ataques de negação de serviços.

4.28.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:

- a) Análise de padrões de estado de conexões;
- b) Análise de decodificação de protocolo;
- c) Análise para detecção de anomalias de protocolo;
- d) Análise heurística;
- e) IP Defragmentation;
- f) Remontagem de pacotes de TCP;
- g) Bloqueio de pacotes malformados.

4.28.11. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

4.28.12. Detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

4.28.13. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

4.28.14. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: 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;

- 4.28.15. Possuir assinaturas específicas para a mitigação de ataques DoS;
- 4.28.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 4.28.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 4.28.18. Identificar e bloquear comunicação com botnets;
- 4.28.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 4.28.20. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware, ou assinatura de IPS ou aplicação;
- 4.28.21. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 4.28.22. Os eventos devem identificar o país de onde partiu a ameaça;
- 4.28.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 4.28.24. Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças;
- 4.28.25. Proteção contra downloads involuntários usando HTTP de arquivos executáveis.
- 4.28.26. Rastreamento de vírus em pdf.
- 4.28.27. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

4.29. **FILTRO DE URL**

- 4.29.1. Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 4.29.2. Deve possuir a função de exclusão de URLs do bloqueio;
- 4.29.3. Deve permitir a customização de página de bloqueio;
- 4.29.4. Deverá 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 o usuário continuar acessando o site);
- 4.29.5. A solução de segurança deve possuir a capacidade de bloquear o envio de credenciais corporativas para sites maliciosos;
- 4.29.6. A solução deve possuir mecanismos de fazer bloqueio de tipos de arquivos para upload e download, assim evitando exposição de arquivos básicos da infraestrutura.
- 4.29.7. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;
- 4.29.8. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs;

4.30. **PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY)**

- 4.30.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 4.30.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;
- 4.30.3. A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW através de mecanismos de Machine Learning. Não serão aceitas soluções que utilizem equipamentos externos;
- 4.30.4. Suportar a análise dinâmica de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional, Windows 10, Mac OS X, Android, Linux;

- 4.30.5. A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
- 4.30.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
- 4.30.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
- 4.30.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
- 4.30.9. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência;
- 4.30.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
- 4.30.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 4.30.12. 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;
- 4.30.13. Permitir o envio de arquivos para análise no ambiente controlado de forma automática, podendo ser via API;
- 4.30.14. Implementar, identificar e bloquear malwares de dia zero que trafegam pela rede;
- 4.30.15. As funcionalidades de sandbox tem como objetivo, analisar e bloquear em tempo real de Ameaças Avançadas Persistentes - APT. Essas funcionalidades têm o objetivo de proteger o ambiente contra a entrada de malwares não conhecidos, e para que ela seja efetiva é necessário que a inspeção e bloqueio sejam feitas em linha (inline), através de features de machine learning;
- 4.30.16. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;
- 4.30.17. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.
- 4.30.18. Deve prevenir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript;
- 4.30.19. Deve ser capaz de aplicar de forma complementar às assinaturas de antivírus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos.

4.31. IDENTIFICAÇÃO DE USUÁRIOS

- 4.31.1. 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 base de dados local;
- 4.31.2. 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;
- 4.31.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
- 4.31.4. Deve possuir integração com ldap para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em Usuários e Grupos de usuários;
- 4.31.5. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 4.31.6. 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);
- 4.31.7. Suporte a autenticação Kerberos;

4.31.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

4.31.9. 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 por usuário sobre o uso das aplicações que estão nestes serviços;

4.31.10. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

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

4.32. **SEGURANÇA DE DNS**

4.32.1. solução deve mostrar nos logs as seguintes informações sobre domínios DGA (Domain Generation Algorithm):

- a) Domínio suspeito identificado;
- b) ID de assinatura de detecção;
- c) Usuário logado na estação/servidor que originou o tráfego; Aplicação;
- d) Porta de destino;
- e) IP de origem;
- f) Horário; Ação do firewall;
- g) Severidade;
- h) A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

4.33. **QoS**

4.33.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

4.33.2. Suportar a criação de políticas de QoS por:

- a) Endereço de origem;
- b) Endereço de destino;
- c) Por usuário e grupo do LDAP/AD;
- d) Por aplicações;
- e) Por porta;

4.33.3. O QoS deve possibilitar a definição de classes por:

- a) Banda Garantida;
- b) Banda Máxima;
- c) Fila de Prioridade.

4.33.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

4.33.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

4.33.6. Deve implementar QOS (traffic-shaping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);

4.33.7. Disponibilizar estatísticas RealTime para classes de QoS.

- 4.33.8. Deve suportar QOS (traffic-shaping), em interface agregadas;
- 4.33.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.34. VPN

- 4.34.1. ~~A solução de VPN client-to-site deverá ser atendido apenas para o equipamento do tipo H;~~ (ITEM REMOVIDO)
- 4.34.2. Suportar VPN Site-to-Site e Client-To-Site;
- 4.34.3. Suportar IPSec VPN;
- 4.34.4. Suportar SSL VPN;
- 4.34.5. A VPN IPSEC deve suportar:
 - a) 3DES;
 - b) Autenticação MD5 e SHA-1;
 - c) Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
 - d) Algoritmo Internet Key Exchange (IKEv1 e v2);
 - e) AES 128 e 256 (Advanced Encryption Standard);
 - f) Autenticação via certificado IKE PKI.
- 4.34.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 4.34.7. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 4.34.8. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- 4.34.9. Deve suportar a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- 4.34.10. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 4.34.11. O cliente da solução de VPN client-to-site deve suportar a instalação nos seguintes tipos de sistema operacionais:
 - a) Microsoft Windows;
 - b) Apple macOS e IOS;
 - c) Android;
 - d) Linux.
- 4.34.12. A solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site para no mínimo as seguintes opções:
 - a) Sistema operacional;
 - b) Antivírus instalado;
 - c) Firewall no host;
 - d) Chaves de registros (quando aplicável);
 - e) Processos ativos.
- 4.34.13. Os mecanismos de conformidade da solução de VPN client-to-site deverá monitorar durante a conexão do usuário remoto qualquer tipo de atividade não autorizada pelo administrador em tempo real. Por exemplo: Após o usuário ser conectado e admitido pela VPN client-to-site, o seu acesso ao ambiente corporativo pode ser negado caso ele manualmente desative alguma funcionalidade especificada nos testes de conformidade da solução;
- 4.34.14. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

4.35. ANALÍTICOS

- 4.35.1. Configuração dos NGFW referente a versão do Software, modelo do equipamento e a saúde do equipamento;
- 4.35.2. Utilização das subscrições de Segurança apresentando o que possui licenciamento expirado;
- 4.35.3. Recomendação de ações e/ou comandos via CLI para remediar os gaps de segurança;
- 4.35.4. Visibilidade de alertas de segurança de forma consolidada;
- 4.35.5. Alertas de hardware e limites de configuração;
- 4.35.6. Identificação e notificação de anormalidades no estado geral de funcionamento da solução;

4.36. RELATÓRIOS

- 4.36.1. A plataforma de segurança deverá possuir relatório de avaliação de boas práticas por meio de análise das configurações atuais;
- 4.36.2. O relatório de boas práticas deverá mostrar o estado atual da solução e a adoção de práticas recomendadas de segurança com sugestões de adequações específicas alinhadas com práticas recomendadas;
- 4.36.3. O relatório deverá mostrar onde melhorar a postura de segurança e definir uma linha de base para comparação posterior, fornecendo links para documentação técnica que mostram como configurar as recomendações;
- 4.36.4. Além de mostrar um comparativo de boas práticas das configurações atuais e posteriores, o relatório deverá apresentar na comparação o grau de boas práticas adotado por instituições do setor público ou similares;
- 4.36.5. O relatório deverá possuir avaliação de melhores práticas recomendadas com base no CIS (Critical Security Controls) e do NIST Security Controls (National Institute of Standards and Technology) sobre as configurações atuais da solução, identificando os riscos e fornecendo recomendações. Exemplo: A solução deverá apontar quais são as configurações que deverão ser ajustadas e indicar local com exemplo de configuração a ser realizada para melhorar a adoção e elevar o grau de segurança;
- 4.36.6. A avaliação de práticas recomendadas deverá mostrar a adoção de recursos de segurança como por exemplo a porcentagem de adoção de regras por usuários e por aplicações;
- 4.36.7. Deverá mostrar informações de adoção da solução, apontando configurações individuais para verificar como os recursos de segurança estão sendo aproveitados. Exemplo: Análise da base de regras para identificar se as mesmas estão sendo aproveitadas e se são relevantes;
- 4.36.8. O relatório poderá ser emitido diretamente na solução ou por meio de portal WEB do fabricante da solução.

5. ITEM 04 - SISTEMA DE GERÊNCIA CENTRALIZADA COM ARMAZENAMENTO DE LOGS CONSOLE DE GERÊNCIA, MONITORAÇÃO E RELATORIA

- 5.1. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possui todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com com Hyper-V e VMware ESXi;
- 5.2. Caso a solução de gerenciamento, monitoração e relatoria, possua licenciamento relacionado a armazenamento, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;
- 5.3. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
- 5.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
- 5.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
- 5.6. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por

funcionalidade (por exemplo, IPS), e distribuição;

- 5.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
- 5.8. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
- 5.9. Deve permitir a criação de objetos e políticas compartilhadas;
- 5.10. Deve consolidar logs e relatórios de todos os dispositivos administrados;
- 5.11. Deve permitir que exportar backup de configuração automaticamente via agendamento;
- 5.12. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
- 5.13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;
- 5.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- 5.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 5.16. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
- 5.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
- 5.18. O gerenciamento deve permitir/possuir:
 - 5.18.1. Criação e administração de políticas de firewall e controle de aplicação;
 - 5.18.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
 - 5.18.3. Criação e administração de políticas de Filtro de URL;
 - 5.18.4. Monitoração de logs;
 - 5.18.5. Ferramentas de investigação de logs;
 - 5.18.6. Debugging;
 - 5.18.7. Captura de pacotes;
 - 5.18.8. Acesso concorrente de administradores.
- 5.19. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- 5.20. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
- 5.21. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- 5.22. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
- 5.23. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
- 5.24. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
- 5.25. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- 5.26. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

- 5.27. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
- 5.28. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- 5.29. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
- 5.30. Criação de regras que fiquem ativas em horário definido;
- 5.31. Criação de regras com data de expiração;
- 5.32. Backup das configurações e rollback de configuração para a última configuração salva;
- 5.33. Suportar Rollback de Sistema Operacional para a última versão local;
- 5.34. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
- 5.35. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
- 5.36. Deve suportar interface de configuração baseada no padrão Openconfig, podendo ser feito por meio de utilização de API fornecido pelo fabricante.
- 5.37. Validação de regras antes da aplicação;
- 5.38. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
- 5.39. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
- 5.40. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 5.41. Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada.
- 5.42. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 5.43. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
- 5.44. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação à versão anterior;
- 5.45. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
- 5.46. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- 5.47. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- 5.48. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- 5.49. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
- 5.50. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;
- 5.51. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- 5.52. Deve permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.
- 5.53. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
- 5.54. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

- 5.55. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
- 5.56. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
- 5.57. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
- 5.58. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
- 5.59. Deve ser possível exportar os logs em CSV;
- 5.60. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
- 5.61. Rotação do log;
- 5.62. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
- 5.63. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
 - 5.63.1. Situação do dispositivo e do cluster;
 - 5.63.2. Principais aplicações;
 - 5.63.3. Principais aplicações por risco;
 - 5.63.4. Administradores autenticados na gerência da plataforma de segurança;
 - 5.63.5. Número de sessões simultâneas;
 - 5.63.6. Status das interfaces;
 - 5.63.7. Uso de CPU;
- 5.64. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
 - 5.64.1. Resumo gráfico de aplicações utilizadas;
 - 5.64.2. Principais aplicações por utilização de largura de banda de entrada e saída;
 - 5.64.3. Principais aplicações por taxa de transferência de bytes;
 - 5.64.4. Principais hosts por número de ameaças identificadas;
- 5.65. 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-Spware), de rede vinculadas a este tráfego;
- 5.66. Deve permitir a criação de relatórios personalizados;
- 5.67. Gerar alertas automáticos via:
 - 5.67.1. Email;
 - 5.67.2. SNMP;
 - 5.67.3. Syslog;

6. ITEM 05 - SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

- 6.1. Refere-se ao serviço de instalação física e lógica para 02 (dois) appliances para a composição do Item 01 e de 01 (um) appliance para o caso do Item 02 desta contratação, sua configuração em modo de alta disponibilidade, configuração de seu sistema operacional, ativação de seus módulos e respectivas licenças de uso, configuração de regras de segurança baseadas tanto nas regras implementadas na solução de Firewall utilizada hoje no CONTRATANTE quanto em novas regras a serem especificadas neste item, assim como em regras acordadas posteriormente entre a equipe técnica do CONTRATANTE e da CONTRATADA, incluindo a migração dos clientes de VPN ativos na solução Firewall utilizada hoje no ambiente para a nova solução Firewall NGFW, além da migração da solução atual de filtro de conteúdo Web Squid/LightSquid, para a solução de filtro de URL disponível pela nova solução de Firewall NGFW.
- 6.2. Os serviços de instalação deverão ser realizados pela CONTRATADA sob acompanhamento da equipe de infraestrutura do CONTRATANTE, conforme projeto apresentado pela CONTRATADA e aprovado pelo CONTRATANTE, atendendo todos os requisitos e exigências constantes deste Termo de

Referência e demais anexos, além de seguir as orientações do fabricante e melhores práticas relacionadas ao uso de equipamentos similares em ambientes críticos.

6.3. O processo de implantação deverá ser devidamente documentado pela CONTRATADA ao longo de todo o período de execução. Ao fim do processo a CONTRATADA deverá apresentar um relatório com o detalhamento da implantação, contendo todas as etapas, histórico de mudanças, diagramas e detalhamento da estrutura da solução, procedimentos adotados, configurações efetuadas e resultado dos testes e homologação, **o período de operação assistida deverá iniciar a partir do primeiro dia após a instalação do equipamento, conforme projeto aprovado; (Texto ajustado)**

6.4. A entrega deste relatório é obrigatória, sendo este o principal artefato comprobatório de conclusão da execução do serviço, a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.

7. ITEM 06 - TREINAMENTO "HANDS ON" SOBRE A SOLUÇÃO DE FIREWALL

7.1. Treinamento oficial do fabricante com repasse de conhecimento específico sobre a solução instalada para, no mínimo, 05 (cinco) servidores/ colaboradores indicados pela CONTRATADA, conforme requisitos e demais exigências especificadas neste Termo de Referência e demais documentos anexos.

7.2. O treinamento deverá oferecer material didático de apoio gratuito aos participantes, seja por meio de mídia física (livros, apostilas, etc.) ou digital (PDF). O material deverá ser cedido individualmente a cada participante, de modo que ele possa levar consigo e consultá-lo posteriormente;

7.3. O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração e gerenciamento, além de tratamento de problemas típicos envolvendo a operação da solução;

7.4. O escopo básico do treinamento deverá conter:

- 7.4.1. Arquitetura da solução;
- 7.4.2. Configurações iniciais básicas;
- 7.4.3. Alta disponibilidade;
- 7.4.4. Controle de acesso dos administradores da solução;
- 7.4.5. Configuração de Interfaces;
- 7.4.6. Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT;
Controle por Identificação de Aplicações;
- 7.4.7. Controle por Identificação de Usuários, com conexão a fontes externas de autenticação;
Criação e gerenciamento de Filtro URL;
- 7.4.8. Decriptografia de tráfego;
- 7.4.9. Configurações de VPN (SSL e IPSec);
- 7.4.10. Monitoramento e Relatórios;
- 7.4.11. Logging e Auditoria;

7.5. Ao final do treinamento, deverá ser emitido certificado comprobatório da participação de cada participante do treinamento.

7.6. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.



Documento assinado eletronicamente por **Jaime Heleno Correa de Lisboa, Subsecretário(a) de Tecnologia da Informação e Inovação**, em 17/11/2023, às 14:12, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



A autenticidade deste documento pode ser conferida no site https://sei.cultura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1505182** e o código CRC **BB8F800C**.

