OBJETO

O presente Termo de Referência tem por objeto o Registro de Preços para a aquisição de uma solução de cibersegurança pelo período de 60 meses, conforme o escopo descrito neste documento.

A licitação será realizada em um lote, abrangendo todos os itens descritos neste documento. A licitante deverá apresentar proposta para todos os itens que compõem o lote.

O critério de julgamento adotado será o menor preço GLOBAL, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto. Ressalta-se que o valor unitário dos itens não poderá estar acima do valor estimado.

Deverá ser entregue, em cada item, todos as soluções, sejam elas hardware, software ou serviço, para atendimento pleno de todas as especificações técnicas contidas neste documento.

ITEM	DESCRIÇÃO	Unid	Quant. Mínima	Quant. Maxima
01	Solução de proteção de perímetro com NGFW (Next Generation Firewall) “tipo 01”, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.	Unid	01	04
02	Solução de proteção de perímetro com NGFW (Next Generation Firewall) “tipo 02”, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.	Unid	01	04
03	Solução de proteção de perímetro com NGFW (Next Generation Firewall) “tipo 03”, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.	Unid	01	10
04	Solução de proteção de perímetro com NGFW (Next Generation Firewall) “tipo 04”, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.	Unid	01	10
05	Solução de proteção de perímetro com NGFW (Next Generation Firewall) “tipo 05”, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.	Unid	01	10

06	Solução de GESTÃO DE LOGS E RELATÓRIOS de ambiente unificado de NGFW (Next Generation Firewall), com log/rate de 25GB/Dia, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.	Unid	01	02
07	Solução de GESTÃO CENTRALIZADA de ambiente unificado de NGFW (Next Generation Firewall), com implantação, garantia do fabricante, repasse de conhecimento e suporte, para até 10 dispositivos físicos, pelo período de 60 meses.	Unid	01	04
08	Banco de Horas de Serviços Técnicos Especializados - USTs	Horas	2000	4000

1. ESPECIFICAÇÕES TÉCNICAS

1.1. CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW (NEXT GENERATION FIREWALL), ITENS 01, 02, 03, 04 e 05 (TIPOS 01 a 05).

1.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

1.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

1.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

1.1.6. Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS,

Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN;

1.1.7. Os appliances deverão ser instalados e configurados e/ou ser feita a migração dos dispositivos atuais do contratante para as novas tecnologias de forma presencial, por técnico certificado pela fabricante, nas dependências da CONTRATANTE, Somente para os appliances da Capital, as demais serão de responsabilidade da CONTRATANTE a instalação com suporte remoto da CONTRATADA .

1.2. FUNCIONALIDADES DE REDE E FIREWALL

1.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

1.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

1.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

1.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

1.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

1.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (*Network Address Translation*), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

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

1.2.8. Deverá suportar sFlow ou Netflow;

1.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

1.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

1.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

1.2.12. Deve implementar o protocolo ECMP;

1.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

1.2.14. Enviar log para sistemas de monitoração externos;

1.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

1.2.16. Deve possui mecanismos de proteção anti-spoofing;

1.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

1.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.2.19. Suportar OSPF graceful restart;

1.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

1.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

1.2.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

1.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

1.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

1.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

1.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

1.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

1.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

1.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

1.2.31. Deverá suportar controle por zonas de segurança;

1.2.32. Deverá suportar controles de políticas por porta e protocolo;

1.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

1.2.34. Deverá suportar Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização;

1.2.35. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

1.2.36. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

1.2.37. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

1.2.38. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

1.2.39. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

1.2.40. Suporte a objetos e regras IPV6;

1.2.41. Suporte a objetos e regras multicast;

1.2.42. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

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

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

1.3.3. Reconhecer pelo menos 4.000 (quatro mil) 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;

1.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

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

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

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

1.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

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

1.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.3.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.3.12. 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;

1.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

1.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

1.3.15. 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;

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

1.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;

1.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

1.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

1.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

1.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

1.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

1.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

1.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

1.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

1.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

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

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

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

1.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

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

1.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

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

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

1.4.9. Deve permitir o bloqueio de vulnerabilidades;

1.4.10. Deve permitir o bloqueio de exploits conhecidos;

1.4.11. Deve incluir proteção contra-ataques de negação de serviços;

1.4.12. Ser imune é capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

1.4.13. Detectar e bloquear a origem de port scans;

1.4.14. Bloquear ataques efetuados por worms conhecidos;

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

1.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

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

1.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

1.4.20. Identificar e bloquear comunicação com botnets;

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

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

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

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

1.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando

usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

1.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante

1.4.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

1.4.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

1.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

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

1.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

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

1.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

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

1.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

1.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;

1.5.8. Deve possuir a função de exclusão de URLs do bloqueio;

1.5.9. Permitir a customização de página de bloqueio;

1.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

1.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

1.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

1.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

1.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

1.6.1. 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, eDirectory e base de dados local;

1.6.2. 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;

1.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

1.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

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

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

1.6.7. 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);

1.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

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

1.7. FUNCIONALIDADE DE FILTRO DE DADOS

1.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

1.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

1.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

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

1.9. FUNCIONALIDADE DE VPN

1.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.9.2. Suportar IPSec VPN;

1.9.3. A VPN IPSEc deve suportar 3DES;

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

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

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

1.9.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

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

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

1.9.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

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

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

1.9.13. Atribuição de DNS nos clientes remotos de VPN;

1.9.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;

1.9.15. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

1.9.16. Suportar leitura e verificação de CRL (Certificate Revocation List);

1.9.17. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis VPN;

1.9.18. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

1.9.19. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

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

1.9.21. O agente de VPN client-to-site deve ser compatível com pelo menos:

1.9.21.1. Windows 10 e superior;

1.9.21.2. Linux Ubuntu 22.04 e superior;

1.9.21.3. Linux RedHat 9;

1.9.21.4. Linux CentOS 9;

1.9.21.5. MacOS 13 e superior;

1.10. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

1.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, 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;

1.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

1.10.2.1. Endereço de origem;

1.10.2.2. Endereço de destino;

1.10.2.3. Usuário e grupo;

1.10.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

1.10.2.5. Por porta;

1.10.3. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

1.10.4. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

1.10.5. O QoS deve possibilitar a definição de fila de prioridade;

1.10.5.1. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
1.10.5.2. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
1.10.5.3. Suportar modificação de valores DSCP para o Diffserv;
1.10.5.4. Suportar priorização de tráfego usando informação de ToS (Type of Service);
1.10.5.5. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
1.10.5.6. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
1.10.5.7. Deve possibilitar a definição de bandas distintas para download e upload;

1.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

1.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
1.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
1.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
1.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
1.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
1.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
1.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

1.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

1.11.8.1. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

1.11.8.2. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

1.11.8.3. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

1.11.8.4. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

1.11.9. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

1.11.10. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

1.11.11. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

1.11.12. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

1.11.13. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

1.11.14. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

1.11.15. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

1.11.16. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

1.11.17. A solução deve suportar nativamente conectores com clouds públicas;

1.11.18. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

1.11.19. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

1.11.20. Deve implementar balanceamento de link por hash do IP de origem;

1.11.21. Deve implementar balanceamento de link por hash do IP de origem e destino;

1.11.22. Deve-se implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

1.11.23. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

1.11.24. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

2. ITEM 01: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA PROTEÇÃO DE BORDA COM NGFW "TIPO 01", COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PELO PERÍODO DE 60 MESES.

2.1. Deve suportar, no mínimo, 140 (cento e quarenta) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

2.2. Deve suportar, no mínimo, 15 (quinze) milhões de conexões simultâneas;

2.3. Deve suportar, no mínimo, 685.000 (seiscentas e oitenta e cinco) novas conexões por segundo;

2.4. Deve Suportar, no mínimo, 50 (cinquenta) Gbps de throughput VPN IPSec;

2.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.800 (mil e oitocentos) túneis de VPN IPSEC Site-to-Site simultâneos;

2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 45.000 (quarenta e cinco mil) túneis de clientes VPN IPSEC simultâneos;

2.7. Deve suportar, no mínimo, 37 (trinta e sete) Gbps de throughput de IPS;

2.8. Deve suportar, no mínimo, 13,5 (treze vírgula cinco) Gbps de throughput de Inspeção SSL;

2.9. Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as

assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e AntiMalware.

2.10. Deve possuir, pelo menos, 6 (seis) interfaces MultiGigabit Ethernet 5GBase-T RJ-45;

2.11. Deve possuir, pelo menos, 12 (doze) interfaces Gigabit Ethernet SFP;

2.12. Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet SFP+;

2.13. Deve possuir, pelo menos, 4 (quatro) interfaces 25 Gigabit Ethernet SFP+;

2.14. Deverá ser disponibilizado com cada appliance NGFW 04 (quatro) transceivers SFP+ 10GBase-SR, da mesma marca do NGFW proposto.

2.15. Deverá ser disponibilizado com cada appliance NGFW 02 (dois) transceivers SFP+ 25GBase-SR, da mesma marca do NGFW proposto.

2.16. Deve possuir fonte de alimentação AC redundante;

2.17. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

3. ITEM 02: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA PROTEÇÃO DE BORDA COM NGFW "TIPO 02", COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PELO PERÍODO DE 60 MESES.

3.1. Deve suportar, no mínimo, 26 (vinte e seis) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

3.2. Deve suportar, no mínimo, 10 (dez) milhões de conexões simultâneas;

3.3. Deve suportar, no mínimo, 390.000 (trezentos e noventa mil) novas conexões por segundo;

3.4. Deve Suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput VPN IPSec;

3.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.800 (mil e oitocentos mil) túneis de VPN IPSEC Site-to-Site simultâneos;

3.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 15.000 (quinze mil) túneis de clientes VPN IPSEC simultâneos;

3.7. Deve suportar, no mínimo, 8 (oito) Gbps de throughput de IPS;

3.8. Deve suportar, no mínimo, 6 (seis) Gbps de throughput de Inspeção SSL;

3.9. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e AntiMalware.

3.10. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T RJ-45;

3.11. Deve possuir, pelo menos, 4 (quatro) interfaces Gigabit Ethernet SFP;

3.12. Deve possuir, pelo menos, 6 (seis) interfaces 10 Gigabit Ethernet SFP+;

3.13. Deverá ser disponibilizado com cada appliance NGFW 04 (quatro) transceivers SFP+ 10GBase-SR, da mesma marca do NGFW proposto.

3.14. Deve possuir fonte de alimentação AC redundante;

3.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

4. ITEM 03: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA PROTEÇÃO DE BORDA COM NGFW "TIPO 03", COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PELO PERÍODO DE 60 MESES.

4.1. Deve suportar, no mínimo, 26 (vinte e seis) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
4.2. Deve suportar, no mínimo, 2,8 (dois vírgula oito) milhões de conexões simultâneas;
4.3. Deve suportar, no mínimo, 138.000 (cento e trinta e oito mil) novas conexões por segundo;
4.4. Deve Suportar, no mínimo, 33 (trinta e três) Gbps de throughput VPN IPSec;
4.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.800 (mil e oitocentos) túneis de VPN IPSEC Site-to-Site simultâneos;
4.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 15.000 (quinze mil) túneis de clientes VPN IPSEC simultâneos;
4.7. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput de IPS;
4.8. Deve suportar, no mínimo, 2,8 (dois vírgula oito) Gbps de throughput de Inspeção SSL;
4.9. Deve suportar, no mínimo, 2,7 (dois vírgula sete) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e AntiMalware.
4.10. Deve possuir, pelo menos, 12 (doze) interfaces Gigabit Ethernet 1000Base-T RJ-45;
4.11. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet SFP;
4.12. Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet SFP+;
4.13. Deverá ser disponibilizado com cada appliance NGFW 04 (quatro) transceivers SFP+ 10GBase-SR, da mesma marca do NGFW proposto.
4.14. Deve possuir fonte de alimentação AC redundante;
4.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

5. ITEM 04: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA PROTEÇÃO DE BORDA COM NGFW "TIPO 04", COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PELO PERÍODO DE 60 MESES.

5.1. Deve suportar, no mínimo, 24 (vinte e quatro) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

5.2. Deve suportar, no mínimo, 2,7 (dois vírgula sete) milhões de conexões simultâneas;

5.3. Deve suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo;

5.4. Deve Suportar, no mínimo, 24 (vinte e quatro) Gbps de throughput VPN IPSec;

5.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 180 (cento e oitenta) túneis de VPN IPSEC Site-to-Site simultâneos;

5.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2000 (dois mil) túneis de clientes VPN IPSEC simultâneos;

5.7. Deve suportar, no mínimo, 4,3 (quatro vírgula três) Gbps de throughput de IPS;

5.8. Deve suportar, no mínimo, 2,4 (dois vírgula quatro) Gbps de throughput de Inspeção SSL;

5.9. Deve suportar, no mínimo, 2 (dois) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e AntiMalware.

5.10. Deve possuir, pelo menos, 6 (seis) interfaces Gigabit Ethernet 1000Base-T RJ-45;

5.11. Deve possuir, pelo menos, 2 (dois) interfaces MultiGigabit Ethernet 5GBase-T RJ-45;

5.12. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

6. ITEM 05: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA PROTEÇÃO DE BORDA COM NGFW "TIPO 05", COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PELO PERÍODO DE 60 MESES.

6.1. Deve suportar, no mínimo, 9 (nove) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

6.2. Deve suportar, no mínimo, 1,2 (um vírgula dois) milhões de conexões simultâneas;

6.3. Deve suportar, no mínimo, 90000 (noventa mil) novas conexões por segundo;

6.4. Deve Suportar, no mínimo, 7 (sete) Gbps de throughput VPN IPSec;

6.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 160 (cento e sessenta) túneis de VPN IPSEC Site-to-Site simultâneos;

6.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 400 (quatrocentos) túneis de clientes VPN IPSEC simultâneos;

6.7. Deve suportar, no mínimo, 2,4 (dois virgula quatro) Gbps de throughput de IPS;

6.8. Deve suportar, no mínimo, 1,2 (um vírgula dois) Gbps de throughput de Inspeção SSL;

6.9. Deve suportar, no mínimo, 1,2 (um virgula dois) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e AntiMalware.

6.10. Deve possuir, pelo menos, 6 (seis) interfaces Gigabit Ethernet 1000Base-T RJ-45;

6.11. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

7. ITEM 06: SOLUÇÃO DE GESTÃO DE LOGS E RELATÓRIOS DE AMBIENTE UNIFICADO DE NGFW, COM LOG/RATE DE 25GB/DIA, COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PELO PERÍODO DE 60 MESES.

7.1. CARACTERÍSTICAS PARA GERENCIAMENTO DE LOGS E RELATÓRIOS

7.1.1. Aquisição de solução de gestão de logs e relatórios, para todos os appliances disponibilizados nos itens 01, 02, 03, 04 e 05, com implantação, garantia do fabricante, repasse de conhecimento e sustentação, pelo período de 60 meses.

7.1.2. Deverá ser implantado presencialmente, por técnico certificado pela fabricante, nas dependências da CONTRATANTE.

7.1.3. Deverá ser do mesmo fabricante dos itens 01, 02, 03, 04, 05 e 07, deste termo.

7.1.4. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

7.1.5. A solução de gerenciamento centralizado deverá ser ofertada em formato de appliance virtual, e será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

7.1.6. Deverá ser compatível com, no mínimo, os Hypervisors: VMware ESXi, Microsoft Hyper-V 2016/2019/2022, Redhat, Nutanix e Linux KVM;

7.1.7. Deverá possuir licenciamento perpétuo, incluindo suporte do fabricante pelo período mínimo de 60 meses;

7.1.8. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

7.1.9. Não deve possuir limite na quantidade de múltiplas vCPU;

7.1.10. Não deve possuir limite para suporte a expansão de memória RAM;

7.1.11. A solução entregue em appliance virtual, não deverá impor limite de armazenamento, limitando-se apenas ao tamanho do disco alocado.

7.1.12. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

7.1.13. Possuir suporte para SNMP versão 2 e 3;

7.1.14. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

7.1.15. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

7.1.16. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

7.1.17. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;

7.1.18. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

7.1.19. Deve permitir gerar alertas de eventos a partir de logs recebidos;

7.1.20. A solução deve ter relatórios predefinidos;

7.1.21. Permitir importação e exportação de relatórios

7.1.22. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

7.1.23. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

7.1.24. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

7.1.25. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

7.1.26. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

7.1.27. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

7.1.28. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

7.1.29. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

7.1.30. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

7.1.31. Deve possuir mecanismos de remoção automática para logs antigos;

7.1.32. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

7.1.33. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

7.1.34. Permitir o envio por e-mail relatórios automaticamente;

7.1.35. Deve permitir que o relatório seja enviado por Email para o destinatário específico;

7.1.36. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

7.1.37. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
7.1.38. Deve permitir o uso de filtros nos relatórios;
7.1.39. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
7.1.40. Permitir especificar o idioma dos relatórios criados;
7.1.41. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
7.1.42. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
7.1.43. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
7.1.44. Deve permitir exportar os logs no formato CSV;
7.1.45. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
7.1.46. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
7.1.47. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
7.1.48. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
7.1.49. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
7.1.50. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
7.1.51. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo de caracteres permitidos;
7.1.52. Deve permitir visualizar em tempo real os logs recebidos;
7.1.53. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);
7.1.54. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
7.1.55. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
7.1.56. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

7.1.57. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

7.1.58. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

7.1.59. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

7.1.60. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)

7.1.61. Deve permitir a criação de paineis personalizados para monitorar operações de segurança e rede;

7.1.62. Deve possuir relatório de uso de aplicações e mídias sociais;

7.1.63. Deve possuir relatório de prevenção de perda de dados (DLP);

7.1.64. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

7.1.65. Deve possuir relatório resumido diário de eventos e incidentes de segurança;

7.1.66. Deve possuir um relatório de tráfego DNS e e-mail;

7.1.67. Deve possuir relatório das 10 principais aplicações utilizadas na rede;

7.1.68. Deve possuir relatório dos 10 principais sites web utilizados na rede;

7.1.69. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

7.1.70. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

7.1.71. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

7.1.72. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

7.1.73. Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

7.1.74. Deve permitir a correlação de eventos, provendo paineis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

7.1.75. A solução deve suportar receber, no mínimo, 25 (vinte e cinco) GB de logs diários;

7.1.76. Deve suportar a capacidade de logs diários ora requisitados.

8. ITEM 07: SOLUÇÃO DE GESTÃO CENTRALIZADA DE AMBIENTE UNIFICADO DE NGFW, COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, REPASSE DE CONHECIMENTO E SUPORTE, PARA ATÉ 10 DISPOSITIVOS FÍSICOS, PELO PERÍODO DE 60 MESES.

8.1. CARACTERÍSTICAS PARA GERENCIAMENTO CENTRALIZADO

8.1.1. Aquisição de solução de gestão centralizada, para todos os appliances disponibilizados nos itens 01, 02, 03, 04 e 05, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.

8.1.2. Deverá ser do mesmo fabricante dos itens 01, 02, 03, 04, 05 e 06 deste termo.

8.1.3. Deverá possuir licenciamento perpétuo, incluindo suporte do fabricante pelo período mínimo de 60 meses;

8.1.4. Deverá ser implantado presencialmente, por técnico certificado pela fabricante, nas dependências da CONTRATANTE.

8.1.5. Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados para os Tipo 01, 02, 03, 04 e 05 e atendendo aos requisitos deste Item;

8.1.6. A solução de gerenciamento centralizado deverá ser ofertada em formato de appliance virtual, e será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

8.1.7. Deverá ser compatível com, no mínimo, os Hypervisors: VMware ESXi, Microsoft Hyper-V 2016/2019/2022, Redhat, Nutanix e Linux KVM;

8.1.8. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

8.1.9. Não deve possuir limite na quantidade de múltiplas vCPU;

8.1.10. Não deve possuir limite para suporte a expansão de memória RAM;

8.1.11. Possibilitar a criação e administração de políticas de Firewall, Controle de Aplicação, Sistema de Prevenção a Intrusão (IPS - Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL e Balanceamento inteligente de Links (SD-WAN);

8.1.12. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

8.1.13. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;

8.1.14. Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

8.1.15. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

8.1.16. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

8.1.17. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

8.1.18. Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;

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

8.1.20. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

8.1.21. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

8.1.22. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

8.1.23. Permitir criação de regras que fiquem ativas em horário definido;

8.1.24. Permitir criação de regras com data de expiração;

8.1.25. Realizar o backup das configurações para permitir o retorno de uma configuração salva;

8.1.26. Possui mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.

8.1.27. Gerar alertas automáticos via Email, SNMP e Syslog;

8.1.28. Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.

8.1.29. Permitir backup das configurações e rollback de configuração para a última configuração salva;

8.1.30. Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;

8.1.31. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

8.1.32. Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;

8.1.33. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

8.1.34. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.

8.1.35. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.

8.1.36. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.

8.1.37. Deve suportar o gerenciamento de pontos de acesso de forma centralizada.

8.1.38. Deve suportar o gerenciamento centralizado de switches.

8.1.39. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.

9. REPASSE DE CONHECIMENTO (OPERAÇÃO ASSISTIDA) E SUPORTE ESPECIALIZADO INCLUÍDO. (ITENS 01, 02 , 03, 04, 05, 06 e 07)

9.1. O repasse de conhecimento (ou operação assistida) é feito após a implantação e/ou migração das soluções, com duração máxima de 8 horas. Toda a documentação da implantação deverá ser entregue para a CONTRATANTE em formato digital.

9.2. Além da garantia do fabricante, com intuito de garantir apoio ao time desta CONTRATANTE, plena operação, sustentação e uso de melhores práticas de todos os equipamentos (e soluções) contidos neste termo, a empresa contratada deverá prestar suporte técnico especializado on-line reativo, durante todo o período de licenciamento, ou seja, 60 meses, a partir da emissão do Termo de Recebimento dos equipamentos, com a possibilidade de ter a sua duração prorrogada, conforme a lei 14.133.

9.3. O suporte, no mínimo, contemplará:

9.3.1. Monitoramento 24x7x365 (24 horas, 7 dias por semana, 365 dias por ano) básico de forma preventiva, utilizando infraestrutura própria de SOC, de no mínimo os parâmetros dos dispositivos quanto à: Disponibilidade; Processamento, memória e consumo de recursos e de banda;

9.3.2. Interação, auxílio e orientações com a abertura de chamados junto ao fabricante para solução de problemas e falhas técnicas nos equipamentos;

9.3.3. Atualização das versões de firmware das soluções implantadas;

9.3.4. Esclarecimentos de dúvidas sobre configurações e utilização dos equipamentos;

9.3.5. Disponibilização de canal para abertura de chamados via chamada telefônica local ou gratuita, e-mail ou website, em qualquer caso em português, a qualquer horário e em qualquer dia da semana (24x7), sem custos para a CONTRATANTE, sem limites de chamados abertos.

9.3.6. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento

e controle da execução dos serviços.

9.3.7. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá à CONTRATADA fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários à execução dos serviços.

9.4. A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de solução de chamados			
Severidade	**Descrição**	**Tempo para o primeiro contato após a abertura**	**Tempo de resolução do chamado**
Urgente	Serviço crítico parado em produção	15 Minutos	Até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção	45 Minutos	Até 03 (três) horas
Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto	90 Minutos	Até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam significativamente no ambiente em produção	120 Minutos	Até 08 (oito) horas
Informações	Consulta Técnica, dúvidas em geral, monitoramento	150 Minutos	Até 24 (vinte e quatro) horas

9.5. O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do chamado.

9.6. O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável da CONTRATANTE.

9.7. A CONTRATADA deve apresentar relatório de atendimento para cada solicitação de suporte técnico, contendo a data e hora da solicitação de suporte técnico, o início e o término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes.

9.8. A CONTRATADA deve emitir relatório mensal em arquivo eletrônico ou em sistema de consulta online, com informações dos chamados abertos e fechados no período.

9.9. O relatório deve possuir os seguintes parâmetros (no mínimo):

9.9.1. Quantidade de ocorrências (chamados) registradas no período;

9.9.2. Número do chamado registrado e nível de severidade;
9.9.3. Data e hora de abertura;
9.9.4. Data e hora de início e conclusão do atendimento;
9.9.5. Identificação do técnico que fez o registro do chamado;
9.9.6. Descrição do problema;
9.9.7. Descrição da solução;
9.9.8. Lista de chamados concluídos fora do prazo de solução estabelecido.

9.10. Problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução, não deverão se encaixar nos prazos estabelecidos no item 6.4;

9.11. O ambiente da CONTRATADA VENCEDORA poderá ser objeto de diligência, para análise de infraestrutura mínima do SOC que atenderá a CONTRATANTE conforme item 6.3.1, a mesma deverá possuir, no mínimo:

9.11.1. Ser configurado de forma que a falha de equipamentos isolados NÃO interrompa a prestação dos serviços;

9.11.2. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;

9.11.3. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador ou possuir outro SOC redundante para garantia de prestação de suporte ininterrupta.

9.12. Suporte para customização de regras, melhorias, resposta a incidentes, projetos específicos, entre outros, poderão ser realizados fazendo uso das USTs disponíveis no item 7 deste termo.

10. ITEM 8 - LOTE 01: BANCO DE HORAS PARA SERVIÇOS TÉCNICOS ESPECIALIZADOS – UST´s

10.1. Objetiva apoiar e assegurar a correta utilização das soluções garantindo o melhor aproveitamento e o uso adequado das funcionalidades, provendo atividades de reestruturação, troubleshooting e prospecção;

10.2. O consumo das USTs (Unidade de Serviço Técnico) será realizado mediante apresentação de uma ordem de serviço que deverá ser aprovada pelo fiscal do contrato;

10.3. A CONTRATANTE poderá utilizar até 4.000 (quatro mil) USTs destinadas a solicitação de serviços especializados na área da infraestrutura e segurança da informação que tenham relação com o objeto deste Termo de Referência, visando a resolução de problemas, testes e implantação de novos artefatos;

10.4. As USTS poderão ser consumidas na sua totalidade dentro de um período de 60 meses com possibilidade de renovação e/ou prorrogação de uso por iguais e sucessíveis períodos conforme a lei 14.133.

10.5. A CONTRATADA deverá enviar em até 48 (quarenta e oito) horas, após a recepção da solicitação de serviço, a estimativa do quantitativo de usts necessárias para o atendimento da solicitação conforme tabela abaixo;

QUADRO UST		COMPLEXIDADE		
		Alta (3)	Média (2)	Baixa (1)
URGÊNCIA	Alta (3)	6 UST'S	5 UST'S	4 UST'S
	Média (2)	5 UST'S	4 UST'S	3 UST'S
	Baixa (1)	4 UST'S	3 UST'S	2 UST'S

10.6. A CONTRATANTE irá avaliar a estimativa e quando aprovada, comunicará a CONTRATADA que poderá iniciar o atendimento da Ordem de Serviço de forma PRESENCIAL E/OU REMOTA;

10.7. A CONTRATADA poderá também prestar consultoria e atendimento às melhorias na infraestrutura do ambiente como um todo da CONTRATANTE;

10.8. A CONTRATADA quando concluir o atendimento deverá enviar em até 2 (dois) dias o relatório descrevendo como a solicitação foi atendida;

10.9. A CONTRATADA deverá apresentar à CONTRATANTE até o 5º (quinto) dia útil do mês subsequente um relatório contendo todas as solicitações de serviço atendidas bem como suas soluções e o volume de horas consumido no período;

10.10. A prestação do serviço poderá ocorrer tanto durante o horário comercial, quanto fora deste, à critério exclusivo da CONTRATANTE;

10.11. A CONTRATANTE procederá com o pagamento do quantitativo de USTS consumidas ao longo do mês;

10.12. A CONTRATADA deve dispor de especialistas na tecnologia ofertada ou no serviço que irá prestar de modo a garantir o suporte na realização de testes, análises, medidas e ajustes, assegurando que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos pelo fabricante, visando a melhoria contínua do gerenciamento do ciclo de vida e a conformidade da mesma, bem como garantir a excelência na execução do serviço;

10.13. As seguintes atividades mínimas poderão serem contempladas:

10.13.1. Customização, implementação de novas funcionalidades, análises, etc...

10.13.2. Execução de atividades operacionais, utilizando os procedimentos recomendados a cada rotina;

10.13.3. Execução de atividades de manutenção corretiva, utilizando os procedimentos que permitam maior eficiência e eficácia na solução de falhas;

10.13.4. Execução de atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando os procedimentos que assegurem mínima interferência na operação e máxima disponibilidade dos produtos;

10.13.5. Elaboração de procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;

10.13.6. Elaboração de relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário.
10.13.7. Consultorias;
10.13.8. Treinamentos;
10.13.9. Implantação de processos de Gestão de vulnerabilidades;
10.13.10. Execução de Pentests (Testes de Intrusão);
10.13.11. Qualquer atividade complementar, relacionada ao objeto (cibersegurança), que não esteja contemplada através deste Termo de Referência.

11. LOTE 01: REQUISITOS MÍNIMOS PARA HABILITAÇÃO

11.1. A CONTRATADA deverá apresentar declaração e/ou certidão comprovando que é fabricante, distribuidora ou representante credenciada dos equipamentos e serviços objeto deste pregão (itens de 1 a 6) e, no caso das duas últimas hipóteses que a CONTRATADA está autorizada a fornecer, instalar e a prestar assistência técnica e manutenção;

11.2. A CONTRATADA deverá apresentar atestado(s) de capacidade técnica expedido por pessoa jurídica de direito público ou privado, onde comprove ter desenvolvido atividades pertinentes e compatíveis aos constantes com o objeto deste edital (itens de 1 a 6); O(s) atestado(s) deverão ser compatíveis em características e quantidades com o objeto deste Pregão;

11.3. A CONTRATADA deverá pagar todos os impostos e taxas devidas sobre as atividades prestadas ao Tribunal, bem como as contribuições à previdência social, encargos trabalhistas, prêmios de seguro e acidentes de trabalho, emolumentos, quaisquer insumos e outras despesas diretas e indiretas que se façam necessárias à execução dos serviços contratados. A não comprovação do pagamento desobriga o CONTRATANTE do pagamento da fatura até a regularização;

11.4. A CONTRATADA deverá ter em seu quadro funcional, pelo menos 1 (um) profissional com certificação de gerenciamento de projetos PMP (Project Management Professional) do PMI (Project Management Institute). Esta solicitação visa garantir que a CONTRATADA possui profissionais aptos para desenvolver os serviços de gerenciamento do projeto do CONTRATANTE, durante o período de implantação da solução ofertada;

11.5. A CONTRATADA deverá ter em seu quadro funcional, pelo menos 1 (um) profissional com certificação de especialista do fabricante proposto. Esta solicitação visa garantir que a CONTRATADA possui profissionais aptos para entregar, implantar e sustentar as soluções propostas nos itens 01 e 06.

11.6. A contratada deverá apresentar, para fins de aceitação do objeto, a comprovação integral de atendimento a todos os requisitos técnicos estabelecidos neste Termo de Referência, por meio de documentação estruturada no formato ponto a ponto, devendo as evidências apresentadas ser provenientes exclusivamente de fontes oficiais do fabricante, tais como

documentação técnica, manuais, catálogos, datasheets ou publicações institucionais, não sendo admitidas declarações genéricas, materiais de terceiros ou informações sem comprovação oficial.

11.7. Fica vedada a subcontratação, total ou parcial, do objeto deste Termo de Referência, não sendo admitida, em nenhuma hipótese, a transferência de quaisquer responsabilidades da contratada a terceiros. A execução do objeto deverá ser realizada direta e integralmente pela contratada, que assumirá plena e exclusiva responsabilidade por todas as obrigações de natureza técnica, operacional, trabalhista, previdenciária e contratual. Nos termos do art. 15 da Lei nº 14.133/2021, fica igualmente vedada a participação de empresas sob a forma de consórcio, considerando que o objeto possui natureza comum e não demanda a conjugação de capacidades técnicas ou operacionais distintas, sendo plenamente exequível por empresa individual.