ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. DESCRIÇÃO DOS SERVIÇOS E QUANTITATIVO

Id	Bem/Serviço	Model/Part Num-ber	Qtd.
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2
3	GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	PAN-PRA-25	1
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2
8	Implantação da solução de Firewall	---	1
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	---	1
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	---	1
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	---	1

2. ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

2.1. NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.1.1. CARACTERÍSTICAS GERAIS

2.1.1.1. A solução deve incluir um par de equipamentos (appliances) Next Generation Firewall em alta disponibilidade, bem como uma solução

de gerenciamento centralizado e relatoria, todos fornecidos pelo mesmo fabricante. Cada par de equipamentos de alta disponibilidade deve ser projetado especificamente para a função de Next Generation Firewall, com hardware e software também provenientes do mesmo fabricante.

2.1.1.2. Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, de forma integrada e simultânea, as funcionalidades de firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware Protection, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL;

2.1.1.3. O equipamento e seus componentes deverão ser novos, sem uso, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

2.1.1.4. Não será aceito equipamento em modo End of Life e End of Support.

2.1.1.5. Não serão aceitas soluções baseadas em PCs de uso geral.

2.1.1.6. A solução deve suportar a configuraçao de alta disponibilidade, podendo ser configurado ativo/passivo ou ativo/ativo, com consideração para licenciamento adicional, se necessário.

2.1.1.7. Todos os componentes necessários para o pleno funcionamento da solução devem ser fornecidos.

2.1.1.8. Todas as funcionalidades que dependam de licenciamento devem ser entregues licenciadas para 60 meses.

2.1.2. CARACTERÍSTICAS FÍSICAS MÍNIMAS

2.1.2.1. Deve possuir throughput de, no mínimo, 26 Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware 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;

2.1.2.2. Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, e estar licenciado para a criação de pelo menos 10 (dez) sistemas virtuais, independentes entre si.

2.1.2.3. Deve suportar, no mínimo, 3.500.000 conexões simultâneas;

2.1.2.4. Deve suportar, no mínimo, 250.000 novas conexões por segundo;

2.1.2.5. Deve suportar, no mínimo, 7 (sete) Gbps de throughput de Inspeção SSL;

2.1.2.6. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo RJ-45;

2.1.2.7. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+.

2.1.2.8. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 40/100 Gbps do tipo QSFP+/QSFP28.

2.1.2.9. Deve possuir, no mínimo, 2 (duas) interface física dedicada para

o sincronismo de estados da solução de alta disponibilidade;

2.1.2.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

2.1.2.11. Deve possuir, no mínimo, 1 (uma) interface dedicada para gerenciamento;

2.1.2.12. Deve possuir armazenamento interno redundante de, no mínimo, 480 GB;

2.1.2.13. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 e 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento; deverá vir acompanhado de cabo de alimentação.

2.1.2.14. O equipamento deve ser fornecido com as portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para uso, sem custos adicionais. Todas as interfaces solicitadas nos appliances devem estar licenciadas e prontas para uso imediato, incluindo os transceivers/transceptores considerando o padrão Short Range (SR).

2.1.3. FUNCIONALIDADE DE FIREWALL

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

2.1.3.2. Suporte aos protocolos IPv4 e IPv6.

2.1.3.3. Suporte a no mínimo 512 VLANs no padrão 802.1q

2.1.3.4. Agregação de links 802.3ad e LACP;

2.1.3.5. Policy based routing ou policy-based forwarding;

2.1.3.6. Roteamento multicast (PIM-SM);

2.1.3.7. Deve suportar os protocolos IGMP v2, IGMP v3;

2.1.3.8. Deve suportar os protocolos DHCP e DHCPv6;

2.1.3.9. Deve suportar o protocolo NTP;

2.1.3.10. Jumbo Frames;

2.1.3.11. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

2.1.3.12. Suportar sub-interfaces ethernet logicas;

2.1.3.13. Deve suportar Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

2.1.3.14. Deve implementar Network Prefix Translation (NPTv6) ou NAT66;

2.1.3.15. Enviar log para sistemas de monitoração externos;

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

2.1.3.17. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

2.1.3.18. Proteção contra anti-spoofing;

2.1.3.19. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

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

2.1.3.21. Suportar a OSPF graceful restart;

2.1.3.22. Deve suportar o protocolo MP-BGP (Multiprotocol BGP)

permitindo que o firewall possa anunciar rotas para IPv4 e IPv6;

2.1.3.23. Os 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);

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

2.1.3.25. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

2.1.3.26. 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;

2.1.3.27. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.1.3.28. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo

2.1.3.29. A configuração em alta disponibilidade deve sincronizar:

2.1.3.29.1. Sessões;

2.1.3.29.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

2.1.3.29.3. Certificados de-criptografados;

2.1.3.29.4. Associações de Segurança das VPNs;

2.1.3.29.5. Tabelas FIB;

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

2.1.4. CONTROLE POR POLÍTICA DE FIREWALL

2.1.4.1. Deverá suportar controles por zona de segurança;

2.1.4.2. Controles de políticas por porta e protocolo;

2.1.4.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

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

2.1.4.5. 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;

2.1.4.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

2.1.4.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

2.1.4.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

2.1.4.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

2.1.4.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

2.1.4.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS 1.2 e 1.3;

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

2.1.4.13. 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;

2.1.4.14. Bloqueios de arquivos por extensão;

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

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

2.1.4.17. Suporte a objetos e regras IPV6;

2.1.4.18. Suporte a objetos e regras multicast;

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

2.1.5. CONTROLE DE APLICAÇÕES

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

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

2.1.5.3. 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;

2.1.5.4. 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;

2.1.5.5. 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;

2.1.5.6. 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;

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

2.1.5.8. Atualizar a base de assinaturas de aplicações automaticamente;

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

2.1.5.10. 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;

2.1.5.11. 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;

2.1.5.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

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

2.1.5.14. 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 customizadas;

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

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

2.1.5.17. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

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

2.1.5.19. 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 a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

2.1.5.20. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

2.1.5.21. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

2.1.6. IDENTIFICAÇÃO DE USUÁRIOS

2.1.6.1. 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, E-directory e base de dados local;

2.1.6.2. 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;

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

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

2.1.6.5. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x ou soluções NAC via syslog, para a identificação de endereços IP e usuários;

2.1.6.6. 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);

2.1.6.7. Suporte a autenticação Kerberos;

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

2.1.6.9. 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;

2.1.6.10. 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 a organização;

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

2.1.7. QOS

2.1.7.1. 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.

2.1.7.2. Suportar a criação de políticas de QoS por:

2.1.7.3. Endereço de origem

2.1.7.4. Endereço de destino

2.1.7.5. Por usuário e grupo do LDAP/AD.

2.1.7.6. Por aplicações;

2.1.7.7. Por porta;

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

2.1.7.9. Banda Garantida

2.1.7.10. Banda Máxima

2.1.7.11. Fila de Prioridade.

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

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

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

2.1.7.15. Deve suportar QOS (traffic-shapping), em interface agregadas;

2.1.7.16. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

2.1.8. VPN

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

2.1.8.2. Suportar IPSec VPN;

2.1.8.3. Suportar SSL VPN;

2.1.8.4. A VPN IPSEc deve suportar:

2.1.8.5. 3DES;

2.1.8.6. Autenticação MD5 e SHA-1;

2.1.8.7. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

2.1.8.8. Algoritmo Internet Key Exchange (IKEv1 e v2);

2.1.8.9. AES 128 e 256 (Advanced Encryption Standard);

2.1.8.10. Autenticação via certificado IKE PKI;

2.1.8.11. 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 throubleshooting;

2.1.8.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

2.1.8.13. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

2.1.8.14. Deve suportar a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

2.1.8.15. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

2.1.8.16. O cliente de VPN SSL deve ser capaz de ser insalado e estar devidamente licenciado para criar perfis customizados de conformidade no mínimo os seguintes sistemas operacionais:

2.1.8.16.1. Windows;

2.1.8.16.2. MacOS

2.1.8.16.3. Linux;

2.1.8.16.4. Android

2.1.8.16.5. Apple iOS.

2.1.8.17. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;

2.1.8.18. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto:

2.1.8.18.1. Sistema operacional e patches instalados;

2.1.8.18.2. Antivírus e versão instalada;

2.1.8.18.3. Firewall no host;

2.1.8.18.4. Criptografia do disco;

2.1.8.18.5. Agente de DLP instalado;

2.1.8.18.6. Backup de disco;

2.1.8.18.7. Chaves de registros;

2.1.8.18.8. Processos ativos.

2.1.8.19. Deve permitir a quarentena automática e manual de dispositivos caso encontre algum comprometimento malicioso no tráfego inspecionado.

2.1.8.20. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções:

2.1.8.20.1. sistema operacional e patches instalados;

2.1.8.20.2. Antivírus e versão instalada;

2.1.8.20.3. Firewall no host;

2.1.8.20.4. Criptografia do disco;

2.1.8.20.5. Agente de DLP instalado backup de disco;

2.1.8.20.6. Chaves de registros

2.1.8.20.7. Processos ativos;

2.1.9. PREVENÇÃO DE AMEAÇAS

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

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

2.1.9.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

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

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

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

2.1.9.7. Deve permitir o bloqueio de vulnerabilidades.

2.1.9.8. Deve permitir o bloqueio de exploits conhecidos.

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

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

2.1.9.11. Análise de padrões de estado de conexões;

2.1.9.12. Análise de decodificação de protocolo;

2.1.9.13. Análise para detecção de anomalias de protocolo;

2.1.9.14. Análise heurística;

2.1.9.15. IP Defragmentation;

2.1.9.16. Remontagem de pacotes de TCP;

2.1.9.17. Bloqueio de pacotes malformados.

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

2.1.9.19. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

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

2.1.9.21. 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;

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

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

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

2.1.9.25. Identificar e bloquear comunicação com botnets;

2.1.9.26. Deve ser capaz de analisar em tempo real através de mecanismos baseados em Machine Learning o tráfego de ameaças avançadas de C2 (comando e controle) e spyware para proteção de ameaças de dia zero.

2.1.9.27. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

2.1.9.27.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

2.1.9.27.2. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação;

2.1.9.27.3. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

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

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

2.1.9.27.6. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos;

2.1.9.27.7. Rastreamento de vírus em pdf;

2.1.9.27.8. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);

2.1.10. FILTRO WEB

2.1.10.1. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

2.1.10.2. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

2.1.10.3. Deve possuir pelo menos 60 categorias de URLs;

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

2.1.10.5. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;

2.1.10.6. Deve suportar a capacidade de criação de políticas baseadas no controle por URL ou categoria de URL;

2.1.10.7. Deve suportar a criação categorias de URLs customizadas;

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

2.1.10.9. Deve permitir a customização de página de bloqueio;

2.1.10.10. Deve 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);

2.1.10.11. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;

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

2.1.10.13. Deve prover análise em tempo real do conteúdo web e dessa forma permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução;

2.1.10.14. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

2.1.11. ANÁLISE DE MALWARES MODERNOS

2.1.11.1. 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;

2.1.11.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

2.1.11.3. Suportar a análise de arquivos maliciosos em ambiente

controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X, Android, Linux.

2.1.11.4. A solução deve possuir a capacidade de extrair e analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

2.1.11.5. A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

2.1.11.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

2.1.11.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

2.1.11.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

2.1.11.9. 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.

2.1.11.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

2.1.11.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

2.1.11.12. 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;

2.1.11.13. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

2.1.11.14. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

2.1.11.15. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

2.1.11.16. 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 executem esta função.

2.1.11.17. Deve previnir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.

2.1.11.18. Deve ser capaz de aplicar de forma complementar às assinaturas de antivirus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable), ELF (executable and linked format) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos;

2.1.12. PROTEÇÃO DNS

2.1.12.1. Deve possuir a função resolução de endereços via DNS, para que

conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

2.1.12.2. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.1.12.2.1. Domínio suspeito identificado;

2.1.12.2.2. ID de assinatura de detecção;

2.1.12.2.3. Usuário logado na estação/servidor que originou o tráfego;

2.1.12.2.4. Aplicação;

2.1.12.2.5. Porta de destino;

2.1.12.2.6. IP de origem;

2.1.12.2.7. IP de destino;

2.1.12.2.8. Horário;

2.1.12.2.9. Ação do firewall;

2.1.12.2.10. Severidade;

2.1.12.2.11. 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;

2.1.12.2.12. A análise automática deve incluir, no mínimo, as seguintes características:

2.1.12.2.13. Padrões de consulta;

2.1.12.2.14. Entropia;

2.1.12.2.15. Análise de frequência n-gram de domínios;

2.1.12.2.16. Taxa de consultas.

2.1.12.2.17. Deve possuir a capacidade de analisar em tempo real a requisições de DNS e acesso a novas assinaturas de DNS;

2.1.13. SDWAN

2.1.13.1. Deve ser capaz de agregar vários links em uma interface virtual;

2.1.13.2. Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jiter e Packet Loss, onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras da interface virtual;

2.1.13.3. Deve poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNS);

2.1.13.4. Deve suportar a agregação de túneis de VPN IPSec e balancear o tráfego entre eles e inserir essa interface agregada à Interface Virtual;

2.1.13.5. Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface virtual;

2.1.13.6. Deve possibilitar a distribuição de trafego entre os links que compõe a interface virtual, a critério do administrador;

2.1.13.7. Deve suportar a critério do administrador uma topologia Full-mesh;

2.1.13.8. Deve permitir configurar acesso direto à Internet para aplicações tipo SaaS;

2.1.13.9. 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 disponiveis que

está orientado ao mesmo destino.

2.1.13.10. 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.

2.1.14. SUPORTE E GARANTIA DO FABRICANTE

2.1.14.1. Deve operar no regime 24/7;

2.1.14.2. Deve ser possivel abrir chamados telefonicos diretamente no fabricante no modelo 24/7;

2.1.14.3. Deve ter um tempo de resposta para chamados críticos de até 1 (uma hora);

2.1.14.4. Em caso de falha de hardware o envio do equipamento para a substituição deve operar no modo NBD (Next Business Day);

2.2. SOFTWARE PARA GERENCIAMENTO CENTRALIZADO DO CLUSTER DE FIREWALLS

2.2.1. O appliance virtual deve ser compatível com VMware ESXi, Microsoft Hyper-V e KVM;

2.2.2. Deve possuir capacidade de armazenamento de até 24TB;

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

2.2.4. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

2.2.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

2.2.6. 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;

2.2.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

2.2.8. 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;

2.2.9. Deve permitir a criação de objetos e políticas compartilhadas;

2.2.10. Deve consolidar logs e relatórios de todos os dispositivos administrados;

2.2.11. Deve permitir que exportar backup de configuração automaticamente via agendamento;

2.2.12. 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;

2.2.13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

2.2.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

2.2.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou

WEB (HTTPS) e API aberta;

2.2.16. 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;

2.2.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

2.2.18. O gerenciamento deve permitir/possuir:

- **2.2.18.1.** Criação e administração de políticas de firewall e controle de aplicação;
- **2.2.18.2.** Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- **2.2.18.3.** Criação e administração de políticas de Filtro de URL;
- **2.2.18.4.** Monitoração de logs;
- **2.2.18.5.** Ferramentas de investigação de logs;
- **2.2.18.6.** Debugging;
- **2.2.18.7.** Captura de pacotes.
- **2.2.18.8.** Acesso concorrente de administradores;

2.2.19. 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;

2.2.20. 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;

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

2.2.22. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

2.2.23. 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;

2.2.24. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

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

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

2.2.27. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

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

2.2.29. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

2.2.30. Criação de regras que fiquem ativas em horário definido;
2.2.31. Criação de regras com data de expiração;
2.2.32. Backup das configurações e rollback de configuração para a última configuração salva;
2.2.33. Suportar Rollback de Sistema Operacional para a ultima versão local;
2.2.34. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
2.2.35. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
2.2.36. Deve suportar interface de configuração baseada no padrão Openconfig.
2.2.37. Validação de regras antes da aplicação;
2.2.38. 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.
2.2.39. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
2.2.40. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
2.2.41. Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada.
2.2.42. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
2.2.43. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
2.2.44. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
2.2.45. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
2.2.46. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
2.2.47. Deve ter a capacidade de encaminhar todo tráfego seja ele criptografado ou não para uma cadeia de equipamentos de segurança tais como IPS, IDS e SIEM para inspeção. Esta funcionalidade pode ser entregue por ferramenta externa.
2.2.48. 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;
2.2.49. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
2.2.50. 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;
2.2.51. 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;

2.2.52. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

2.2.53. Dever 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.

2.2.54. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

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

2.2.56. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

2.2.57. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

2.2.58. 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;

2.2.59. 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;

2.2.60. Deve ser possível exportar os logs em CSV;

2.2.61. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

2.2.62. Rotação do log;

2.2.63. 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;

2.2.64. 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.;

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

- **2.2.65.1.** Situação do dispositivo e do cluster;
- **2.2.65.2.** Principais aplicações;
- **2.2.65.3.** Principais aplicações por risco;
- **2.2.65.4.** Administradores autenticados na gerência da plataforma de segurança;
- **2.2.65.5.** Número de sessões simultâneas;
- **2.2.65.6.** Status das interfaces;
- **2.2.65.7.** Uso de CPU;
- **2.2.65.8.** Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
- **2.2.65.9.** Resumo gráfico de aplicações utilizadas;
- **2.2.65.10.** Principais aplicações por utilização de largura de banda de entrada e saída;
- **2.2.65.11.** Principais aplicações por taxa de transferência de bytes;

2.2.65.12. Principais hosts por número de ameaças identificadas;

2.2.65.13. 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;

2.2.66. Deve permitir a criação de relatórios personalizados;

2.2.67. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

2.2.68. Gerar alertas automáticos via:

2.2.68.1. Email;

2.2.68.2. SNMP;

2.2.68.3. Syslog;

2.3. ZERO TRUST NETWORK ACCESS (ZTNA) COM CAPACIDADE PARA SUPORTAR 400 USUÁRIOS

2.3.1. REQUISITOS GERAIS DA SOLUÇÃO

2.3.1.1. A solução de segurança na borda deverá suportar, no mínimo, as seguintes funcionalidades:

2.3.1.1.1. ZTNA (Zero Trust Network Access).

2.3.1.1.2. Filtro de URL;

2.3.1.1.3. Controle de Aplicação;

2.3.1.1.4. Prevenção de Ameaças;

2.3.1.1.5. Solução de segurança DNS;

2.3.1.1.6. Proteção Contra Malwares Modernos (Sandbox);

2.3.1.1.7. Gerência e Relatórios.

2.3.1.2. A solução deverá ser licenciada para permitir a autenticação para acesso de 200 usuários conectados simultaneamente

2.3.1.3. A solução disponibilizada deverá ter capacidade de receber via redirecionamento ou interceptar de maneira ativa e realizar inspeção e tratamento de todo o tráfego web de forma a controlar os acessos a serviços SaaS (Gerenciados e não gerenciados), IaaS, Web e Aplicações Internas (Nuvem pública e on-premises).

2.3.1.4. A solução deve possuir console única de gestão para toda a plataforma de segurança, incluindo:

2.3.1.4.1. Painel de Política;

2.3.1.4.2. Painel de Relatório;

2.3.1.4.3. Painel de Incidentes;

2.3.1.4.4. Painel de Configuração;

2.3.1.4.5. Painel Analítico.

2.3.1.5. O fabricante da solução deverá possuir ao menos 2 gateways no Brasil com pelo menos 2 (dois) endereços IPs dedicados para cada um deles e garantir que as configurações sejam aplicadas aos mesmos localmente, não sendo permitidas soluções genéricas agregadas através de appliances físicos e/ou virtuais;

2.3.1.6. A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet, saindo apenas com IPs designados para o Brasil.

2.3.1.7. Esta funcionalidade também deverá garantir que a mesma faixa de endereço não seja compartilhada com outros clientes;

2.3.1.8. Deverá ser fornecida com no mínimo, 2 (duas) estruturas de processamento redundantes no território nacional (Brasil)

2.3.1.9. A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-2 e ISO 27001

2.3.1.10. Deverá ser possível realizar a interceptação do tráfego de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, para no mínimo as seguintes formas:

2.3.1.10.1. Túnel Seguro (IPSEC ou SSL);

2.3.1.10.2. Integração com plataformas de SDWAN;

2.3.1.10.3. Integração com NGFW/UTM (IPSEC);

2.3.1.10.4. Agente (Windows, Linux e MacOS);

2.3.1.11. Os serviços de segurança devem ser fornecidos de maneira transparente às redes/usuários remotas;

2.3.1.12. A solução deve fornecer a capacidade de associar e atribuir toda a atividade do usuário, usando uma representação de identidade conforme integrações com:

2.3.1.12.1. Active Directory;

2.3.1.12.2. Federação (SSO) utilizando SAML v2.0.

2.3.1.12.3. OpenID Connect/OAuth 2.0

2.3.1.12.4. Suportar recurso de autenticação única para todo o ambiente, utilizando o padrão de autenticação Active Directory, OpenID Connect/OAuth 2.0 ou outra plataforma com suporte à SAML;

2.3.1.13. A solução deverá ser capaz de prover acesso às aplicações internas sem a necessidade de instalação de máquinas virtuais na rede de destino como ponte de acesso;

2.3.1.14. A solução deverá executar suas funcionalidades para defender a rede/usuário contra ameaças avançadas, vírus e ameaças escondidas em tráfego HTTPS e aplicações com SSL criptografado;

2.3.1.15. A solução deverá ser capaz de descriptografar e inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.2 ou superior;

2.3.1.16. O tráfego SSL/TLS deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao tráfego não criptografado;

2.3.1.17. Deverá permitir a configuração de portas diferentes das portas padrão utilizadas pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites;

2.3.1.18. A solução deverá verificar os certificados digitais de sites acessados por meio do protocolo HTTPS. Em caso de certificados digitais inválidos, a solução deverá ser configurável para, de acordo com preferência do TJ-CE, bloquear ou permitir o acesso aos sites;

2.3.1.19. Deverá permitir configurar regras de exceção a sites HTTPS que não devem ter seu tráfego inspecionado;

2.3.1.20. O licenciamento e a garantia pelo fabricante para toda a solução deverão estar ativos durante toda a vigência do contrato;

2.3.2. ZTNA (ZERO TRUST NETWORK ACCESS)

2.3.2.1. A solução deve possuir a capacidade de controlar o acesso e aplicar controle de aplicação, proteção contra malwares modernos (Sandbox), prevenção de ameaças e segurança de DNS, de usuários remotos a aplicações internas através da nuvem do fabricante, onde o usuário remoto tenha acesso apenas a aplicação especificada na

política de segurança e não a um segmento de rede interna;

2.3.2.2. A solução deve ser implementada com agente único na estação de trabalho do usuário remoto;

2.3.2.3. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

2.3.2.4. A solução deve garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

2.3.2.5. Ser possível configurar através da console gráfica da solução quais aplicações internas serão acessadas através do Tenant da solução;

2.3.2.6. Ser autossuficiente e se ajustar automaticamente do ponto de vista de performance caso algum ponto de presença venha a falhar sem a necessidade do administrador ou cliente configurar nenhuma regra;

2.3.2.7. Trabalhar em modo híbrido, onde seja possível publicar os atalhos de acesso a aplicações presentes nos datacenters do TJ-CE e nas nuvens públicas indicadas pela mesma;

2.3.2.8. A solução deve permitir definir a conformidade de estações com sistemas operacionais Windows, Linux e MacOS, com as políticas organizacionais baseadas no mínimo nos seguintes critérios:

2.3.2.8.1. Presença de processo(s) em execução;

2.3.2.8.2. Presença de arquivos em disco;

2.3.2.8.3. Participação em domínio do AD;

2.3.2.8.4. Existência de Certificado Digital no dispositivo;

2.3.2.8.5. Que somente as máquinas que estejam com solução anti-malware ativada possam acessar os serviços internos.

2.3.2.8.6. O cliente SSL client-to-site também deve suportar dispositivos móveis (IOS e ANDROID), sistemas operacionais Linux;

2.3.2.9. A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

2.3.2.9.1. Máquinas em conformidade: A partir de uma máquina remota, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação;

2.3.2.9.2. Geolocalização: A partir de uma máquina remota tentando se conectar de um país não permitido, deverá ter sua conexão bloqueada;

2.3.2.10. Pela solução deve ser possível criar políticas de segurança onde pode ser especificado:

2.3.2.10.1. Usuário do AD;

2.3.2.10.2. Grupo do AD;

2.3.2.10.3. Aplicação Privada;

2.3.2.10.4. Perfil de segurança (por exemplo: Filtro de URLs, Controle de Aplicação e inspeção Anti-malware);

2.3.2.10.5. Ação: Permitir e/ou Bloquear.

2.3.2.11. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host,

criptografia do disco, chaves de registros e processos ativos;

2.3.2.12. A solução deve realizar verificação contínua de confiança, onde uma vez que o acesso a um aplicativo é concedido;

2.3.2.13. A confiança deverá ser continuamente avaliada com base em mudanças nas condições de segurança na estação;

2.3.2.14. Possuir capacidade de analisar dinamicamente (continuamente) os acessos dos usuários conectados remotamente a internet e recursos do próprio órgão;

2.3.2.15. Suportar políticas de permissão e negação de acesso com base em várias condições. Por exemplo: postura do dispositivo, localização do dispositivo/usuário, associação ao grupo de usuários;

2.3.2.16. Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real;

2.3.2.17. A solução deve gerar logs dos acessos realizados por usuários remotos as aplicações internas, no mínimo, com as seguintes informações:

2.3.2.17.1. Regra de segurança que foi aplicada no tráfego;

2.3.2.17.2. Ação tomada pela solução;

2.3.2.17.3. Usuário;

2.3.2.17.4. Endereço IP;

2.3.2.17.5. IP público e IP privado.

2.3.2.17.6. País de origem;

2.3.2.17.7. Porta de origem;

2.3.2.17.8. Sistema operacional;

2.3.2.17.9. Aplicação de destino;

2.3.2.17.10. Porta de destino;

2.3.2.17.11. Protocolo;

2.3.2.17.12. Bytes trafegados na sessão;

2.3.2.17.13. Hora de início e término da sessão.

2.3.2.18. Deve permitir que a conexão com o serviço SASE seja estabelecida das seguintes formas:

2.3.2.18.1. Antes do usuário autenticar na estação;

2.3.2.18.2. Após autenticação do usuário na estação;

2.3.2.18.3. Sob demanda do usuário;

2.3.2.18.4. Sempre ativo mantendo o usuário conectado assim que o usuário faz o logon.

2.3.2.18.5. A solução deve enviar a lista de gateways ativos para estabelecimento da conexão;

2.3.2.18.6. Deve haver a opção do cliente remoto escolher manualmente o gateway de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

2.3.3. FILTRO DE URLS

2.3.3.1. A solução deverá suportar a criação de políticas baseadas no controle por URL e categorias de URLs;

2.3.3.2. O perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

2.3.3.3. A solução deverá possuir:

2.3.3.3.1. Pelo menos 70 categorias distintas de URLs;

2.3.3.3.2. A capacidade de classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

2.3.3.3.3. Categoria específica para classificar domínios recém registrados (com menos de 30 dias);

2.3.3.3.4. Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

2.3.3.4. A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas de filtro de conteúdo WEB:

2.3.3.4.1. Categoria de URL;

2.3.3.4.2. Usuários e Grupos do Active Directory;

2.3.3.4.3. Profile de prevenção de malwares;

2.3.3.4.4. Atividade realizada na URL/Aplicação;

2.3.3.4.5. IP de Origem;

2.3.3.4.6. IP de Destino;

2.3.3.4.7. País de origem e destino;

2.3.3.4.8. Ação: allow, block e alert;

2.3.3.4.9. Tipo de arquivo.

2.3.3.4.10. A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

2.3.3.5. A solução deverá suportar:

2.3.3.5.1. A criação de categorias de URLs customizadas;

2.3.3.5.2. A exclusão de URLs do bloqueio, por categoria;

2.3.3.5.3. A customização de página de bloqueio;

2.3.3.5.4. A capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

2.3.3.6. A solução deverá permitir:

2.3.3.6.1. Um mecanismo para sobrescrever as categorias de URL;

2.3.3.6.2. A criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

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

2.3.3.6.4. A solução deverá possuir mecanismo de Controle de URL que apresenta contagem de utilização de regra de acordo com a utilização (hit count);

2.3.3.7. A solução deverá possibilitar:

2.3.3.7.1. Categorização e recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

2.3.3.7.2. A inspeção de tráfego HTTPS Outbound deverá efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo de descriptografia para inspeção completa do tráfego de saída para a internet;

2.3.3.7.3. Implementação de filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das estações dos usuários.

2.3.3.7.4. O cadastro manual de usuários e grupos diretamente na interface de gerência remota;

2.3.3.7.5. 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);

2.3.3.7.6. Salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

2.3.3.7.7. A solução deverá ser capaz de detectar e prevenir roubo de credenciais, controlando e bloqueando os sites que o usuário pode enviar credenciais corporativas com base na classificação do endereço, em tempo real.

2.3.3.7.8. A solução deverá possuir a capacidade de detectar técnicas de phishing ou falsificação de imagens;

2.3.3.7.9. A solução deverá utilizar modelos de inteligência preditiva no reconhecimento de URLs maliciosas em tempo real não cadastradas na base de categorização do fabricante da solução.

2.3.4. CONTROLE DE APLICAÇÕES

2.3.4.1. A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.3.4.2. A solução deverá contar com módulos de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

2.3.4.3. Pela solução deverá ser possível:

2.3.4.3.1. A liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

2.3.4.3.2. A criação de políticas por geolocalização, permitindo que o tráfego de uma aplicação para um determinado país seja bloqueado ou redirecionado;

2.3.4.3.3. Adicionar políticas de controle de aplicações e perfis de segurança para todo o tráfego web e interno através da nuvem SSE, não se limitando somente a possibilidade de habilitar controle de aplicações em parte do tráfego;

2.3.4.3.4. Adicionar controle de aplicações em todas as regras de segurança da solução, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

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

2.3.4.4. A criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

2.3.4.4.1. Nível de risco da aplicação;

2.3.4.4.2. Categoria de aplicações.

2.3.4.4.3. A solução deverá reconhecer pelo menos 3.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e webmail;

2.3.4.4.4. A solução deverá suportar múltiplos métodos de

identificação e classificação das aplicações, por pelo menos assinaturas, decoders de protocolos e heurísticas;

2.3.4.5. A solução deverá diferenciar:

2.3.4.5.1. Tráfegos peer-to-peer (bittorrent, emule, neonet, etc.), possuindo granularidade de controle para os mesmos;

2.3.4.5.2. Tráfegos de mensageiros instantâneos (facebook Chat, WhatsApp, telegram e etc.) possuindo granularidade de controle para os mesmos;

2.3.4.5.3. Aplicações proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle para eles.

2.3.4.5.4. A solução deverá diferenciar e controlar partes das aplicações, incluindo, mas não limitado: Permitir o WhatsApp WEB e bloquear a transferência de arquivos, permitir o facebook e bloquear chat;

2.3.4.6. Pela solução deverá ser possível:

2.3.4.6.1. Inspecionar o payload do pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.3.4.6.2. Realizar filtragens/inspeções dentro de portas TCP conhecidas, por exemplo porta 80 http, buscando por aplicações que potencialmente expõem o ambiente como: peer-to-peer ou mensageiros instantâneos;

2.3.4.6.3. Identificar o uso de táticas evasivas, ou seja, deverá ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como ataques utilizando comunicação TLS;

2.3.4.6.4. Aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a encrypted bittorrent e aplicações VOIP que utilizam criptografia proprietária.

2.3.4.6.5. Caso a solução não tenha assinaturas pré-definidas de uma aplicação, ela deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, HTTPS, FTP, E-mail e extensão de arquivos;

2.3.4.6.6. Pela solução deverá ser possível atualizar a base de assinaturas de aplicações automaticamente;

2.3.4.6.7. O fabricante da solução deverá disponibilizar um serviço para solicitação de inclusão de aplicações na base de assinaturas dele;

2.3.5. PREVENÇÃO DE AMEAÇAS

2.3.5.1. A solução deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto à movimentação entre nuvens (SaaS Gerenciado e SaaS não gerenciado);

2.3.5.2. Na solução deverá ser possível criar políticas de segurança baseadas no nível de risco da aplicação. Ex: selecionar na política de segurança o bloqueio de todas as aplicações de cloud storage com nível de risco alto na base do fabricante da solução;

2.3.5.3. Deve conter, no mínimo, as seguintes informações sobre as

aplicações comparadas na interface gráfica da solução:

2.3.5.3.1. Informações sobre vulnerabilidades e exploits já sofridos;

2.3.5.3.2. Certificações e normas que a aplicação está aderente. Ex: PCI, DSS, SOC-1, SOC-2 e SOC-3;

2.3.5.3.3. Informações sobre privacidade de dados. Ex: ao armazenar dados na aplicação, o cliente continua sendo proprietário dos dados.

2.3.5.3.4. A solução deverá possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

2.3.5.4. A solução deverá suportar:

2.3.5.4.1. Várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

2.3.5.4.2. Referência cruzada com CVE.

2.3.5.5. A solução deverá ser capaz de categorizar os seguintes tipos de domínio:

2.3.5.5.1. Domínios de DNS dinâmicos;

2.3.5.5.2. Domínios identificados previamente como sendo distribuidores de Malwares;

2.3.5.5.3. Domínios identificados anteriormente em campanhas de Phishing;

2.3.5.5.4. Domínios identificados previamente como Graywares os quais podem usar de técnicas de instalação de aplicações não desejadas;

2.3.5.5.5. Domínios Estacionários os quais são sites com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares;

2.3.5.5.6. Domínio de anonimização de Proxy utilizados com uma forma de driblar a análise de conteúdo.

2.3.5.5.7. A solução deverá possuir sistema de análise automática para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.3.5.5.8. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

2.3.5.5.9. A solução deverá permitir updates em tempo real para ameaças e novos ataques feitos através de DNS.;

2.3.6. SEGURANÇA DNS

2.3.6.1. A solução de segurança de DNS, tem como finalidade proteger as conexões a domínios maliciosos que muitas vezes são utilizados pelos atacantes, utilizam para interceptar a comunicação e poder ter acesso e controlar a comunicação dos usuários, causando problemas de evasão e exfiltração de dados;

2.3.6.2. Caso o fabricante não tenha solução de segurança para DNS de forma nativa, ou seja, licenciada de forma separada da solução, o mesmo pode compor com outra solução dedicada de mercado de fabricantes como (ex.: Cisco Umbrella) e deverá ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.3.6.3. A solução de segurança de DNS deve ser capaz de identificar

atividades maliciosas de comando e controle utilizado pelo menos as seguintes técnicas:

2.3.6.4. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.3.6.4.1. Domínio suspeito identificado;

2.3.6.4.2. ID de assinatura de detecção;

2.3.6.4.3. Usuário logado na estação/servidor que originou o tráfego;

2.3.6.4.4. Aplicação;

2.3.6.4.5. Porta de destino;

2.3.6.4.6. IP de origem;

2.3.6.4.7. IP de destino;

2.3.6.4.8. Horário;

2.3.6.4.9. Ação do firewall;

2.3.6.4.10. Severidade;

2.3.6.4.11. 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;

2.3.6.5. A análise automática deve incluir, no mínimo, as seguintes características:

2.3.6.5.1. Padrões de consulta;

2.3.6.5.2. Entropia;

2.3.6.5.3. Análise de frequência n-gram de domínios;

2.3.6.5.4. Taxa de consultas.

2.3.6.5.5. A solução deve permitir updates em tempo real para ameaças e novos ataques feitos através de DNS;

2.3.6.5.6. A solução deve permitir a utilização ilimitada (quantidades) de assinaturas DNS;

2.3.6.6. A solução de segurança de DNS deve ser capaz de categorizar os seguintes tipos de domínio:

2.3.6.6.1. Domínios de DNS dinâmicos

2.3.6.6.2. Domínios identificados previamente como sendo distribuidores de malwares

2.3.6.6.3. Domínios registrados recentemente

2.3.6.6.4. Domínios identificados anteriormente em campanhas de phishing

2.3.6.6.5. Domínios identificados previamente como graywares os quais podem usar de técnicas de instalação de aplicações não desejadas

2.3.6.6.6. Domínios Estacionários os quais são sítios com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares.

2.3.6.6.7. Domínio de proxy de animação utilizados com uma forma de driblar a análise de conteúdo.

2.3.7. PROTEÇÃO CONTRA MALWARES MODERNOS

2.3.7.1. A solução deverá possuir nuvem de inteligência proprietária do fabricante que seja responsável em atualizar toda a base de segurança através de assinaturas;

2.3.7.2. A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise em tempo real em uma sandbox, devendo

permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado (sandbox). Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.3.7.3. A solução deverá prevenir o uso de exploits avançados;

2.3.7.4. Na solução, a análise deverá prover:

2.3.7.4.1. Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

2.3.7.4.2. Informações sobre as ações do malware na máquina infectada;

2.3.7.4.3. Informações sobre as URLs não confiáveis utilizadas pelo novo malware;

2.3.7.4.4. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;

2.3.7.4.5. Detecção de aplicações não confiáveis, utilizadas pelo Malware;

2.3.7.4.6. Assinaturas de antivírus e antispyware de maneira automática.

2.3.7.5. A solução deverá possuir:

2.3.7.5.1. Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS;

2.3.7.5.2. Mecanismo de detecção "antibot", que inclui pelo menos, reputação de endereço IP;

2.3.7.5.3. Funcionalidade de detecção e bloqueio de call-backs.

2.3.7.5.4. A solução deverá prevenir contra ameaças de dia zero:

2.3.7.5.5. Via tráfego de internet;

2.3.7.5.6. Que possam burlar o sistema operacional emulado;

2.3.7.5.7. Através de tecnologias em nível de emulação e código de registro.

2.3.7.5.8. A solução deverá ser capaz de implementar:

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

2.3.7.5.8.2. Visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

2.3.7.5.8.3. Análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

2.3.7.5.9. A solução deverá suportar ainda:

2.3.7.5.9.1. Identificação e bloqueio de malware nas comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

2.3.7.5.9.2. 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;

2.3.7.5.9.3. Suportar a análise dinâmica de arquivos

maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10, Mac OS X, iOS, Android e Linux;

2.3.7.5.9.4. 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;

2.3.8. SUPORTE E GARANTIA DO FABRICANTE

2.3.8.1. O Serviço deverá fornecer:

2.3.8.1.1. Acesso a Especialistas Técnicos e Recursos Online:

2.3.8.1.1.1. A solução deverá fornecer acesso imediato a especialistas técnicos e recursos online, garantindo proteção ao produto oferecido. Os usuários poderão submeter, atualizar e verificar o status dos casos de suporte por meio de um Portal de Suporte ao Cliente online.

2.3.8.2. Transferência de Conhecimento Avançada:

2.3.8.2.1. A solução incluirá uma plataforma completa de transferência de conhecimento. Isso abrangerá documentação detalhada do produto, bancos de dados de resolução de problemas e um ambiente de gerenciamento de casos de suporte baseado em conhecimento, permitindo colaboração entre usuários. Além disso, serão disponibilizados manuais de produtos, guias técnicos, notas de lançamento de software e FAQs para simplificar a resolução de incidentes.

2.3.8.3. Serviço de Melhoria Contínua:

2.3.8.3.1. A solução oferecerá um serviço de melhoria contínua para maximizar o valor do produto. Isso incluirá o desenvolvimento de planos de sucesso personalizados, alinhados com metas e requisitos específicos da organização. Serão realizadas verificações periódicas da saúde da solução e aplicadas as melhores estratégias de utilização para otimização e proteção do investimento.

2.3.8.4. Integração de Fluxos de Trabalho Operacionais:

2.3.8.5. A solução garantirá a integração eficaz com fluxos de trabalho operacionais. A equipe especializada colaborará com a infraestrutura de rede e segurança, identificando pontos de integração, conduzindo verificações regulares e revisões operacionais para promover uma operação mais eficiente e aumentar a confiança na solução.

2.3.8.6. Os SLAs de para tempos de resposta, deverão obedecer aos seguintes níveis de severidade:

Severidade	Descrição	SLA
1	Grave impacto no ambiente de produção, como a perda de dados de produção ou a inoperância de sistemas.	Até 1 hora, contada a partir do registro do chamado.
2	O software opera, porém, seu desempenho em no ambiente de produção é consideravelmente limitado.	Até 2 horas, contadas a partir do registro do chamado.
3	Perda parcial e não crítica de funcionalidade de software no ambiente de produção, mas é viável continuar usando-o por meio de uma	Até 4 horas, contadas a partir do registro do chamado.

	solução alternativa	
4	Questionamento de natureza geral, notificação de discrepância na documentação ou sugestão de aprimoramento ou alteração do produto.	Até 48 horas, contadas a partir do registro do chamado.

2.4. INSTALAÇÃO PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.4.1. É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada. Os equipamentos e componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento ou componente de hardware fora das condições normais recomendadas pelo fabricante.

2.4.2. A Contratada deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off no intuito de revisar os requisitos do projeto, discutir cronogramas de marcos do projeto, membros da equipe e itens de ação de acompanhamento.

2.4.3. Deverá conduzir através de um workshop uma sessão de design profundada do cenário da implantação da solução através da colaboração das principais partes interessadas da contratante no intuito de desenvolver e concordar com os critérios de design e a estratégia de implantação;

2.4.4. Os serviços de instalação e configuração, compreendem, entre outros, os seguintes procedimentos:

2.4.4.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;

2.4.4.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

2.4.4.3. Regras de Firewall existentes e aplicáveis à solução ofertada dada a colocação desta na Rede deste parque;

2.4.4.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

2.4.4.5. Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

2.4.4.6. A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos;

2.4.4.7. Aplicação de todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável;

2.4.4.8. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

2.4.4.9. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será

considerado entregue, quando for instalado e configurado, com todas as atualizações, configurações e licenças ativadas. Deverão ser adicionados ao Sistema de Gerência Centralizada todos os equipamentos instalados contemplados na solução adquirida. Os equipamentos deverão ser monitorados e gerenciados por este Sistema de Gerência Centralizada;

2.4.4.10. Habilitação das licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução;

2.4.4.11. Inclusão de políticas de segurança encaminhadas pelo CONTRATENTE, pré-existentes em seu ambiente, para os novos equipamentos.

2.4.5. A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução, contendo:

2.4.5.1. Os procedimentos de instalação e configuração,

2.4.5.2. Cenário de implantação e integração da rede;

2.4.5.3. Diagrama/documentação de rede para referência;

2.4.5.4. Lista de materiais/inventário da solução;

2.4.5.5. Versão do Sistema Operacional;

2.4.5.6. Hardening/segurança do sistema;

2.4.5.7. Capacidades fundamentais;

2.4.5.8. Requisitos específicos do cenário de implantação;

2.4.5.9. Detalhes de design de baixo nível (por exemplo, endereços IP, nomes de dispositivos, matriz de cabeamento, pesquisa do local, configuração específica do site/dispositivo);

2.4.5.10. Estratégia de validação - principais pontos de verificação a serem testados;

2.4.5.11. Bem como fornecer um repasse sobre a solução e as configurações realizadas.

2.5. SUPORTE TÉCNICO E MONITORAMENTO 24X7 PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.5.1. O serviço de suporte técnico da CONTRATADA deverá ser contínuo na modalidade 24x7, e quando necessário realizando a intermediação com o serviço oficial de garantia e suporte do fabricante da solução, nos moldes descritos no item 2.1.14, durante todo o período de vigência do contrato.

2.5.2. O serviço de suporte técnico e monitoramento 24x7 da CONTRATADA incluirá:

2.5.2.1. Suporte técnico para identificação e resolução de problemas em software e hardware;

2.5.2.2. Resolução de problemas quanto acesso à sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

2.5.2.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.5.2.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.5.2.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

2.5.2.6. Encaminhar incidentes ao fabricante da solução;

2.5.2.7. Suporte em demais configurações de segurança, redundância e

gerência;

2.5.2.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

2.5.2.9. Apoio técnico para tarefas de auditoria e análise de logs.

2.5.2.10. Lançamentos de recursos e atualizações de software mais recentes;

2.5.2.11. Atualização dos serviços de assinatura de segurança manual ou automática;

2.5.2.12. Caso o fabricante se comunique e/ou documente em uma língua diferente do português, será de responsabilidade da contratada fornecer suporte linguístico para garantir a compreensão adequada de todas as informações pertinentes ao cumprimento deste contrato.

2.5.2.13. O suporte linguístico fornecido pela contratada deve assegurar que todas as comunicações e documentos sejam devidamente traduzidos para o idioma acordado pelas partes, garantindo assim uma comunicação clara e precisa entre as partes envolvidas no contrato.

2.5.2.14. As despesas associadas ao fornecimento do suporte linguístico serão de responsabilidade da contratada

2.5.2.15. A CONTRATANTE poderá solicitar qualquer relatório da solução a qualquer tempo, sem restrição de quantidade de solicitações, o que deverá ser provido pela contratada num prazo de 5 dias úteis, contados a partir da data de solicitação por parte da CONTRATANTE

2.5.2.16. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva.

2.5.2.17. O atendimento e suporte técnico especializado será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

2.5.2.18. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

2.5.2.19. A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

2.5.2.20. A CONTRATADA deverá disponibilizar uma ferramenta de

Service Desk que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

2.5.2.21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional, registro de ameaças e vulnerabilidades identificadas em softwares dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

2.5.2.22. A CONTRATADA deverá executar a cada 3 meses e apresentar os resultados encontrados incluindo sugestão de ações de melhoria para serem executadas, Assessments de boas práticas e de revisão de ciclo de vida de segurança, que possam resumir riscos operacionais e de segurança do TJCE, bem como a aderência a melhores práticas e configurações recomendadas pelo fabricante.

2.6. TREINAMENTO PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.6.1. Deverá fornecer treinamento para até 8 (oito) alunos, a fim de capacitar os profissionais da CONTRATANTE;

2.6.2. O serviço de capacitação deve consistir na oferta de treinamentos com abordagem prática voltada a todos os requisitos funcionais da solução contratada, tanto relativo a aspectos operacionais, que inclui a utilização prática de todas as principais funcionalidades da ferramenta, como administrativos, que inclui o gerenciamento, suporte e parametrização da solução.

2.6.3. Ministrado por profissionais da CONTRATADA com conhecimentos comprovados na solução oferecida.

2.6.4. Deve incluir fornecimento de documentação didática em papel ou mídia digital com todo o conteúdo.

2.6.5. Deve ser composto por parte teórica e prática, com uso de laboratórios virtuais da CONTRATADA ou do fabricante.

2.6.6. O treinamento deve abordar, no mínimo, os seguintes tópicos:

2.6.6.1. Conceitos, configuração, gerenciamento e diagnóstico de problemas;

2.6.6.2. Arquitetura e Componentes do NGFW;

2.6.6.3. Sistema de Prevenção de Intrusão;

2.6.6.4. Políticas de Segurança e Aplicações;

2.6.6.5. Filtragem de Conteúdo, Aplicações e URL;

2.6.6.6. Balanceamento de Carga e Alta Disponibilidade;

2.6.6.7. Relatórios, Conformidade e Regulamentações;

2.6.6.8. Customização de Relatórios e Monitoramento;

2.6.6.9. Gerenciamento de Usuários e Autenticação;

2.6.6.10. Registros de eventos;

2.6.6.11. Registro de tráfego;

2.6.6.12. Proteção contra Malware;

2.6.6.13. Controle de Acesso e VPN;
2.6.6.14. Balanceamento de Carga e Alta Disponibilidade;
2.6.6.15. Melhores Práticas de Segurança;
2.6.6.16. Atualizações e Manutenção;
2.6.6.17. Teste de Intrusão e Avaliação de Segurança;
2.6.6.18. Backup e Recuperação de Desastres;
2.6.6.19. Integração com Outras Soluções.

2.6.7. A CONTRATADA poderá incluir tópicos e funcionalidades que julgar necessários, além dos elencados acima;

2.6.8. Após o treinamento, a CONTRATADA deve fornecer certificados de participação a cada funcionário participante, incluindo tópicos abordados, duração e instrutores.

2.6.9. Custos de deslocamento, hospedagem e alimentação dos treinandos são de responsabilidade da CONTRATANTE.

2.6.10. A CONTRATADA será o responsável pela preparação do local de treinamento inclusive da disponibilização e instalação de todos os equipamentos.

2.6.11. A duração mínima do treinamento (carga horária) será de 40 (quarenta) horas em 10 (dez) dias;

2.6.12. O curso deverá ser ministrado em língua portuguesa com o material didático utilizado e fornecido preferencialmente em língua portuguesa.

2.7. INSTALAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA)

2.7.1. A Contratada deverá realizar a implementação em conjunto com o fabricante realizando a instalação, configuração e funcionamento dos componentes da solução ofertada. Os componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento fora das condições normais recomendadas pelo fabricante.

2.7.2. Este serviço deverá inclui quatro (4) etapas: Implantação, Integração, Repasse de Conhecimento e Documentação;

2.7.3. A Contratada em conjunto com o fabricante deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off para realizar o lançamento inicial do projeto. Esta reunião incluir uma revisão dos requisitos do projeto e uma discussão sobre cronogramas e plano de ação;

2.7.4. Após o kick-off, a Contratada em conjunto com o fabricante deverá gerar um Documento de Requisitos Técnico, baseado no ambiente do cliente

2.7.5. O Documento de Requisitos Técnicos descreverá o ambiente de produção planejado e os procedimentos operacionais;

2.7.6. A Contratada em conjunto com o fabricante deverá:

2.7.6.1. Realizar a configuração com base nos requisitos definidos no Documento de Requisitos Técnicos. As tarefas de configuração devem incluir no mínimo:

2.7.6.1.1. Implantação de usuários móveis;
2.7.6.1.2. Conector ZTNA (Configuração e integração de 4 conectores com até 10 alvos de aplicativos);
2.7.6.1.3. Dez (10) políticas de segurança.

2.7.6.2. Revisar e validar a implantação de acordo com os critérios

definidos no Documento de Requisitos Técnicos, apoiando a integração inicial de usuários móveis e validando o comportamento e a conectividade dos usuários, através de um Teste Piloto de Integração

2.7.6.2.1. No Teste Piloto de Integração deverão ser revisados e os registros de tráfego e ameaças e os fluxos de tráfego e garanta que os usuários possam alcançar os destinos adequados definidos pelas políticas de segurança

2.7.6.3. Realizar uma sessão de transferência de conhecimento após a conclusão dos serviços de planejamento, configuração e validação listados acima;

2.7.6.4. Realiza uma sessão de Transferência de Conhecimento deverá incluir uma descrição do ambiente as-built e uma transferência de conhecimento sobre como gerenciar e operar o ambiente. A transferência de conhecimento deverá ser realizada em uma única sessão de até duas (2) horas, para oito (8) participantes;

2.8. SUPORTE TÉCNICO E MONITORAMENTO 24X7 PARA SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA)

2.8.1. O serviço de suporte técnico da CONTRATADA deverá ser contínuo na modalidade 24x7, e quando necessário realizando a intermediação com o serviço oficial de garantia e suporte do fabricante da solução, nos moldes descritos no item 2.3.8, durante todo o período de vigência do contrato.

2.8.2. O serviço de suporte técnico e monitoramento 24x7 da CONTRATADA incluirá:

2.8.2.1. Suporte técnico para identificação e resolução de problemas em software;

2.8.2.2. Resolução de problemas quanto acesso à sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

2.8.2.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.8.2.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos a solução ofertada;

2.8.2.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

2.8.2.6. Encaminhar incidentes ao fabricante da solução;

2.8.2.7. Suporte em demais configurações de segurança, redundância e gerência;

2.8.2.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

2.8.2.9. Apoio técnico para tarefas de auditoria e análise de logs.

2.8.2.10. Lançamentos de recursos e atualizações de software mais recentes;

2.8.2.11. Atualização dos serviços de assinatura de segurança manual ou automática;

2.8.2.12. Caso o fabricante se comunique e/ou documente em uma língua diferente do português, será de responsabilidade da contratada fornecer suporte linguístico para garantir a compreensão adequada de todas as informações pertinentes ao cumprimento deste contrato.

2.8.2.13. O suporte linguístico fornecido pela contratada deve assegurar

que todas as comunicações e documentos sejam devidamente traduzidos para o idioma acordado pelas partes, garantindo assim uma comunicação clara e precisa entre as partes envolvidas no contrato.

2.8.2.14. As despesas associadas ao fornecimento do suporte linguístico serão de responsabilidade da contratada

2.8.2.15. A CONTRATANTE poderá solicitar qualquer relatório da solução a qualquer tempo, sem restrição de quantidade de solicitações, o que deverá ser provido pela contratada num prazo de 5 dias úteis, contados a partir da data de solicitação por parte da CONTRATANTE

2.8.2.16. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva.

2.8.2.17. O atendimento e suporte técnico especializado será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

2.8.2.18. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

2.8.2.19. A atualização de software quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

2.8.2.20. A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

2.8.2.21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional, registro de ameaças e vulnerabilidades identificadas em softwares dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.