ANEXO I

TERMO DE REFERÊNCIA

1 – OBJETO

1.1 – Registro de preço para aquisição de aquisição de **solução de proteção de rede com características de *Next Generation Firewall (NGFW)* para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, *spywares e malwares "Zero Day"*, Filtro de URL, funcionalidade de *Sandbox,* bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança[1] integrada** com garantia e respectiva subscrição por, pelo menos, 36 (trinta e seis) meses, serviços de instalação e treinamento, de acordo com as características e quantitativos constantes neste Termo de Referência.

2 – DAS ESPECIFICAÇÕES E CARACTERÍSTICAS DO OBJETO

2.1 – Poderão ser adquiridos os itens abaixo informados:

	Item	Descrição	Quantidade	Valor unitário máximo estimado
LOTE 1	1	*Appliance Next Generation Firewall (NGFW)*, com interface de gerência e respectivas licenças, garantia, suporte e atualizações por 36 meses	02	R$ 402.916,26
	2	Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1	02	R$ 256.971,46
	3	Serviços de instalação, configuração e repasse de conhecimento	02	R$ 41.837,55
	4	Treinamento	06	R$ 12.994,50

2.2 - Descrição dos itens e requisitos técnicos mínimos:

2.2.1 – ITEM 1 - *Appliance Firewall* NGFW:

2.2.1.1 - Entende-se por "*Appliance Firewall* NGFW", conjunto formado por *hardware* e respectivas licenças de *software* necessárias para seu funcionamento, incluídas as consoles de gerência e monitoramento.

2.2.1.1.1 - Para atendimento a esse item será aceito o fornecimento do *hardware* em *appliance* composto por 02 (dois) equipamentos, desde que atendidas todas as características, as funcionalidades e as capacidades descritas neste termo de referência.

2.2.1.2 - Cada *"Appliance* NGFW" deve possuir as seguintes características, licenciadas para uso:

[1] Por plataforma de segurança entende-se hardware e software integrados do tipo *appliance*

2.2.1.2.1 - Possuir *throughput* mínimo de 2 Gbps 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, Antivírus e *Anti-spyware*. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.

2.2.1.2.2 - Os *throughputs* devem ser comprovados por documento de domínio público do fabricante. A localização destes documentos deve ser informada na proposta detalhada (conforme item 8.3 do edital). A ausência/inexistência de tais documentos resultará desclassificação da proposta.

2.2.1.2.3 - Os documentos públicos devem comprovar os *throughputs* aferidos com tráfego HTTP ou **blend** de protocolos definidos pelo fabricante como tráfego real (*real-world traffic blend*).

2.2.1.2.4 - Não será aceita aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

2.2.1.2.5 - Deve ser capaz de suportar, no mínimo, 1.000.000 conexões simultâneas.

2.2.1.2.6 - Deve ser capaz de suportar, no mínimo, 55.000 novas conexões por segundo.

2.2.1.2.7 - Deve ser fornecido com fontes 120/240 AC, redundantes, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

2.2.1.2.8 - Deve ser fornecido com *coolers* ou *fans hot-swappables*, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

2.2.1.2.9 - Deve ser fornecido com disco *Solid State Drive* (SSD) com no mínimo 2400 GB.

2.2.1.2.10 - *Deve possuir, no mínimo, 08 (oito) interfaces de rede* 10/100/1000 base-TX.

2.2.1.2.11 - Deve possuir, no mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+, fornecidos com seus respectivos *transceivers* do tipo SR.

2.2.1.2.12 - Deve possuir 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento.

2.2.1.2.13 - Deve possuir 01 (uma) interface do tipo console ou similar.

2.2.1.2.14 - Deve ser capaz de operar em alta disponibilidade nos modos Ativo/Ativo ou Ativo/Passivo.

2.2.1.2.15 - Os equipamentos (*appliances)* fornecidos (Alta disponibilidade) devem possuir o mesmo fabricante, modelo e configuração.

2.2.1.2.16 - Deve suportar, no mínimo, 50 (cinquenta) zonas de segurança.

2.2.1.2.17 - Deve permitir a expansão futura de, no mínimo, 04 (quatro) instâncias virtuais de *firewall*.

2.2.1.2.18 - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 300 (trezentos) clientes de VPN SSL simultâneos.

2.2.1.2.19 - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 50 (cinquenta) túneis de VPN IPSEC simultâneos.

2.2.1.3 - Por cada equipamento que compõe a plataforma de segurança, entende-se o *hardware* e as licenças de *softwares* necessárias para o seu funcionamento.

2.2.1.4 - Por console de gerência e monitoração, entende-se as licenças de *software* necessárias para as duas funcionalidades.

2.2.1.5 - A console de gerência e monitoramento não pode residir no mesmo *appliance* de proteção de rede, devendo ser segregadas dos equipamentos dos *appliances* de proteção.

2.2.1.5.1 - A console de gerência e monitoramento deve ser virtual e deve rodar em ambiente VMWare ESXi 6.0 ou superior.

2.2.1.6 - Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em como *end-of-life* ou *end-of-sale*.

2.2.1.7 - Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, e devem incluir kit tipo trilho para adaptação, se necessário, e cabos de alimentação.

2.3.1.8 - A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência e monitoração.

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

2.2.1.10 - As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

2.2.1.11 - A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

2.2.1.12 - O *hardware* e *software* que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

2.2.1.13 - O *software* deverá ser fornecido em sua versão mais atualizada recomendada pelo fabricante.

2.2.1.14 - Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

a) Suporte a 1024 VLAN Tags 802.1q
b) Agregação de links 802.3ad e LACP
c) Policy based routing ou policy based forwarding
d) Roteamento multicast (PIM-SM)
e) DHCP Relay
f) DHCP Server
g) Suporte à criação de objetos de rede

2.2.1.15 - Suportar sub-interfaces ethernet logicas.

2.2.1.15.1 - Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de *firewall* ou roteamento baseado em políticas (PBR).

2.2.1.16 - O *firewall* deve ter a capacidade de testar o funcionamento de rotas estáticas ou rota *default* com a definição de um endereço IP de destino que deve estar comunicável por meio de uma rota. Caso haja falha na comunicação o *firewall* deve ter a capacidade de usar rota alternativa para estabelecer a comunicação.

2.2.1.17 - Deve suportar os seguintes tipos de NAT:

a) Nat dinâmico (*Many-to-1*);
b) Nat dinâmico (*Many-to-Many*);
c) Nat estático (1-to-1);
d) NAT estático (*Many-to-Many*);
e) Nat estático bidirecional 1-to-1;
f) Tradução de porta (PAT);
g) NAT de Origem;
h) NAT de Destino;
i) Suportar NAT de Origem e NAT de Destino simultaneamente.

2.2.1.18 - Deve implementar o protocolo ECMP.

2.2.1.19 - Deve implementar balanceamento de link por pelo menos um dos métodos a seguir: IP de origem, IP de origem e destino ou *round-robin*.

2.2.1.20 - Enviar log para sistemas de monitoração externos, simultaneamente.

2.2.1.21 - Deve haver a opção de enviar logs para os sistemas de monitoração externos.

2.2.1.22 - Proteção de *anti-spoofing*;

2.2.1.23 - Dever permitir bloquear conexões que contenham dados no *payload* de pacotes durante o *three-way hand-shake*;

2.2.1.24 - Deve exibir nos logs de tráfego o motivo para o término da sessão no *firewall*, incluindo sessões finalizadas onde houver de-criptografia de SSL ou SSH.

2.2.1.25 - Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

2.2.1.26 - Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

2.2.1.27 - Suportar a OSPF *graceful restart*;

2.2.1.28 - Deve suportar o protocolo BGP permitindo que o *firewall* possa anunciar rotas para IPv6.

2.2.1.28.1 - Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (*address auto configuration*), NAT64, Identificação de usuários a partir do LDAP/AD, *Captive* Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (*Denial of Service*), De-criptografia SSL ou SSH, PBF (*Policy Based Forwarding*), DHCPv6 *Relay*, IPSec, VPN SSL, Ativo/Passivo, SNMP, NTP, DNS e controle de aplicação.

2.2.1.29 - Os dispositivos de proteção devem ter a capacidade de operar 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).

2.2.1.29.1 - Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

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

2.2.1.29.3 - 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.

2.2.1.30 - Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

a) Em modo transparente;
b) Em layer 3.

2.2.1.31 - A configuração em alta disponibilidade deve sincronizar:

a) Sessões;
b) Configurações, incluindo, mas não limitado a políticas de *Firewall*, NAT, QOS e objetos de rede;
c) Associações de Segurança das VPNs;
d) Tabelas FIB.

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

2.2.1.33 - As funcionalidades de filtro de pacotes, NAT, VPN IPSec e protocolos de roteamento dinâmico 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.

2.2.1.34 - Controle por política de *Firewall*

2.2.1.34.1 - Deverá suportar controles por zona de segurança.

2.2.1.34.2 - Controles de políticas por porta e protocolo.

2.2.1.34.3 - Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras.

2.2.1.34.4 - A solução deve identificar de forma automática quais interfaces o tráfego irá ser direcionado, evitando assim que as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.

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

2.2.1.34.6 - Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

2.2.1.34.7 - Deve permitir consultar ou criar políticas para objetos das listas externas ou nuvem de inteligência do fabricante a partir da interface de gerência do próprio firewall.

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

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

2.2.1.34.10 - Deve de-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2.

2.2.1.34.11 - Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo *Elliptical Curve Digital Signature Algorithm (ECDSA);*

2.2.1.34.12 - Controle de inspeção e de-criptografia de SSH ou SSL por política.

2.2.1.34.13 - Bloqueio de, no mínimo, os seguintes tipos de arquivos: cab, msi e exe.

2.2.1.34.14 - *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo).

2.2.1.34.15 - Suporte a objetos e regras IPV6.

2.2.1.34.16 - Suporte a objetos e regras *multicast.*

2.2.1.34.17 - Deve suportar no mínimo dois dos tipos de negação de tráfego nas políticas de *firewall* a seguir: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.

2.2.1.34.18 - Suportar a atribuição de agendamento das políticas (ou regras) com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

2.2.1.35 - Controle de aplicações

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

2.2.1.35.2 - Deve ser possível efetuar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

2.2.1.35.3 - Deve reconhecer nativamente aplicações relacionadas a tráfego *peer-to-peer*, redes sociais, acesso remoto, *update* de *software*, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

2.2.1.35.4 - Deve reconhecer pelo menos as seguintes aplicações: *bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer*, rdp ou ms-rdp, vnc, gmail*, youtube*, *http-tunnel*, *facebook chat, gmail chat, whatsapp*, *4shared, dropbox, google drive, onedrive*, db2, mysql, *oracle, kerberos, ldap, radius, itunes,* dhcp, ftp, dns, *wins*, ntp, snmp, *gotomeeting, webex, evernote* e *google* ou *google-docs*;

2.2.1.35 - Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar por meio de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389;

2.2.1.35.6 - Deve detectar aplicações por meio de análise comportamental do tráfego observado, incluindo, pelo menos, *Encrypted Bittorrent* e aplicações VOIP.

2.2.1.35.7 - 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 ataques mediante a porta 443.

2.2.1.35.8 - 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.

2.2.1.35.9 - 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, incluindo, mas não limitado a *Yahoo Instant Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do *Webex*. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

2.2.1.35.10 - 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;

2.2.1.35.11 - Deve permitir controle granular para aplicações SaaS, tais como: *Office* 365, *Skype*, aplicativos *google, gmail*, etc.;

2.2.1.35.12 - Identificar o uso de táticas evasivas via comunicações criptografadas;

2.2.1.35.13 - Atualizar a base de assinaturas de aplicações automaticamente.

2.2.1.35.14 - Reconhecer aplicações em IPv6.

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

2.2.1.35.16 - 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 nas estações dos usuários.

2.2.1.35.17 - 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.

2.2.1.35.18 - Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos.

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

2.2.1.35.20 - Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da instituição.

2.2.1.35.20.1 - A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no *payload* dos pacotes TCP e UDP ou usando *decoders* de pelo menos os seguintes protocolos: HTTP, FTP, SMTP, Telnet, SSH, IMAP, IMAP e RTSP.

2.2.1.35.21 - O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

2.2.1.35.22 - Deve alertar o usuário quando uma aplicação for bloqueada.

2.2.1.35.23 - Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

2.2.1.35.24 - Deve possibilitar a diferenciação de tráfegos *Peer2Peer* (*Bittorrent*, *emule*, *neonet*, etc.) possuindo granularidade de controle/políticas para os mesmos.

2.2.1.35.25 - Deve possibilitar a diferenciação de tráfegos de *Instant Messaging* (AIM, *Gtalk*, *Facebook Chat*, etc.) possuindo granularidade de controle/políticas para os mesmos.

2.2.1.35.26 - Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o *Gtalk* chat e bloquear a transferência de arquivos.

2.2.1.35.27 - Deve possibilitar a diferenciação de aplicações *Proxies* (*ghostsurf, freegate*, etc.) possuindo granularidade de controle/políticas para os mesmos.

2.2.1.35.28 - Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

a) Tecnologia utilizada nas aplicações (*Client-Server, Browser Based, Network Protocol*, etc.);
b) Nível de risco da aplicação;
c) Categoria e subcategoria de aplicações;
d) Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

2.2.1.36 - Prevenção de ameaças

2.2.1.36.1 - Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e *Anti-Spyware* (ou *antimalware*) integrados no próprio *appliance* de *Firewall* ou entregue por meio de composição com outro equipamento ou fabricante.

2.2.1.36.2 - Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware* ou *antimalware*).

2.2.1.36.3 - Deve sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware* (ou *antimalware*) quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo.

2.2.1.36.4 - Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e *Anti-spyware* ou *antimalware*: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *reset* ou tcp-*reset*.

2.2.1.36.5 - Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2.

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

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

2.2.1.36.8 - Deve suportar granularidade nas políticas de IPS, Antivírus e *Anti-Spyware* (ou *antimalware*), possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

2.2.1.36.9 - Deve permitir o bloqueio de vulnerabilidades.

2.2.1.36.10 - Deve permitir o bloqueio de *exploits* conhecidos.

2.2.1.36.11 - Deve incluir proteção contra ataques de negação de serviços.

2.2.1.36.12 - Deverá possuir os seguintes mecanismos de inspeção de IPS:

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

2.2.1.36.13 - Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood e UDPfloof.

2.2.1.36.14 - Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da instituição.

2.2.1.36.15 - Bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões.

2.2.1.36.16 - Possuir tecnologia ou assinaturas para a mitigação de ataques DoS e DDoS.

2.2.1.36.17 - Possuir assinaturas para bloqueio de ataques de buffer overflow.

2.2.1.36.18 - Deverá possibilitar a criação de assinaturas customizadas pelo órgão.

2.2.1.36.19 - Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS, permitindo a criação de exceções com granularidade nas configurações.

2.2.1.36.20 - Permitir o bloqueio de vírus e *spywares* (ou *malwares*) em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMB ou SMB (NetBios-ssn) e SMTP;

2.2.1.36.20.1 - É permitido uso de *appliance* externo (antivírus de rede), para o bloqueio de vírus e **spywares** em protocolo SMB de forma a conter *malwares* se espalhando horizontalmente pela rede.

2.2.1.36.21 - Suportar bloqueio de arquivos por tipo.

2.2.1.36.22 - Deve estar apto a identificar e bloquear comunicação com botnets.

2.2.1.36.23 - Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst.

2.2.1.36.24 - Registrar na console de monitoração as seguintes informações sobre ameaças identificadas.

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

2.2.1.36.25 - Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Anti-spyware*.

2.2.1.36.26 - Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 ou IPv6), previamente definidos.

2.2.1.36.27 - Os eventos devem identificar o país de onde partiu a ameaça.

2.2.1.36.28 - Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

2.2.1.36.29 - Rastreamento de vírus em pdf.

2.2.1.36.30 - Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.).

2.2.1.36.31 - 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 diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

2.3.1.37 - Análise de *malwares*

2.2.1.37.1 - Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de *Malwares* não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.

2.2.1.37.2 - 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.

2.2.1.37.3 - A solução deve ser capaz de selecionar por meio de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

2.2.1.37.4 - Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos duas das três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis (como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.).

2.2.1.37.5 - Suportar a análise com pelo menos 50 (cinquenta) tipos de comportamentos maliciosos para a análise da ameaça não conhecida.

2.2.1.37.6 - Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional *Windows* 7 e *Windows* 10;

2.2.1.37.7 - Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, HTTP e SMTP).

2.2.1.37.8 - A solução deve possuir a capacidade de analisar em *sandbox links* (http e HTTPs) presentes no corpo de e-mails trafegados em SMTP. Deve ser gerado um relatório caso a abertura do link pela *sandbox* o identifique como site hospedeiro de *exploits*.

2.2.1.37.9 - Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos *e-mails* permitindo identificação ágil do usuário vítima do ataque.

2.2.1.37.10 - O sistema de análise *"In Cloud"* ou local deve prover informações sobre as ações do *Malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *Malware,* gerar assinaturas de Antivírus e *Anti-spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo *Malware* e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede).

2.2.1.37.11 - Deve permitir o download dos *malwares* identificados a partir da própria interface de gerência.

2.2.1.37.12 - Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de *malwares* de dia zero.

2.2.1.37.13 - Caso a solução de análise de *malware* seja fornecida em *appliance* local, deve possuir, no mínimo, 25 ambientes controlados *(sandbox)* independentes para execução simultânea de arquivos suspeitos.

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

2.2.1.37.15 - Suportar a análise de arquivos executáveis, ZIP e criptografados em SSL no ambiente controlado.

2.2.1.37.16 - Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar), Linux (ELF), RAR e 7-ZIP no ambiente de *sandbox*;

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

2.3.1.38- Filtro de URL

2.2.1.38.1 - A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL.

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

2.2.1.38.1.2 - Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

2.2.1.38.1.3 - Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs por meio da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

2.2.1.38.1.4 - Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

2.2.1.38.1.5 - Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

2.2.1.38.1.6 - Suportar base ou cache de URLs local no *appliance*, evitando **delay** de comunicação/validação das URLs.

2.2.1.38.1.7 - Possui pelo menos 50 categorias de URLs.

2.2.1.38.1.8 - Deve classificar o nível de risco de URLs ou aplicações em, pelo menos, três níveis: baixo, médio e alto.

2.2.1.38.1.9 - A categorização de URL deve analisar toda a URL e não somente até o nível de diretório.

2.2.1.38.1.10 - Permitir a criação categorias de URLs customizadas.

2.2.1.38.1.11 - Permitir a exclusão de URLs do bloqueio, por categoria.

2.2.1.38.1.12 - Permite a customização de página de bloqueio.

2.2.1.38.1.13 - Permite 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).

2.2.1.38.1.14 - Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

2.2.1.39- Identificação de usuários

2.2.1.39.1 - Deve ser capaz de criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, *Active Directory* e base de dados local.

2.2.1.39.2 - 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.

2.2.1.39.3 - Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

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

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

2.2.1.39.5 - Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no *firewall* (*Captive* Portal).

2.2.1.39.6 - Suportar a autenticação *Kerberos*.

2.2.1.39.7 - Deve suportar autenticação via *Kerberos* para administradores da plataforma de segurança, *Captive* Portal e usuário de VPN SSL;

2.2.1.39.8 - 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.

2.2.1.39.9- Deve implementar a criação de grupos customizados de usuários no *firewall,* baseado em atributos do LDAP/AD;

2.2.1.39. 10 - Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente.

2.2.1.40 - QoS

2.2.1.40.1 - 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*.

2.2.1.40.2 - Suportar a criação de políticas de QoS por:
a) Endereço de origem;
b) Endereço de destino;
c) Por usuário e grupo do LDAP/AD;
d) Por aplicações, incluindo, mas não limitado a *Skype, Bittorrent* e *Youtube*;
e) Por porta.
f) O QoS deve possibilitar a definição de limite de *Upload e Download* ou de classes por: banda garantida, banda máxima e fila de prioridade.

2.2.1.40.3 - Suportar a limitação de upload e download ou a priorização *Real Time* de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

2.2.1.40.4 - Disponibilizar estatísticas *Real Time* para classes de QoS.

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

2.2.1.41 - Filtro de dados

2.2.1.41.1 - Permitir a criação de filtros para arquivos e dados pré-definidos.

2.2.1.41.2 - Os arquivos devem ser identificados por extensão e assinaturas.

2.2.1.41.3 - Permitir a identificação e opcionalmente prevenir a transferência de vários tipos de arquivos (*Office*, PDF, etc.) identificados sobre aplicações (P2P, *Instant Messaging* etc.).

2.2.1.41.4 - Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

2.2.1.41.5 - 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.

2.2.1.41.6 - Permitir listar o número de aplicações suportadas para controle de dados.

2.2.1.41.7 - Permitir listar o número de tipos de arquivos suportados para controle de dados.

2.2.1.42 - Geo-localização

2.2.1.42.1 - Suportar a criação de políticas por Geo-localização, permitindo que o tráfego de determinado Pais/Países seja bloqueado.

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

2.2.1.42.3 - Deve possibilitar a criação de regiões geográficas, caso a solução ofertada não possua as regiões pré-cadastradas, e criar políticas utilizando as mesmase criar políticas utilizando as mesmas.

2.2.1.43 - VPN IPSEC/SSL

2.2.1.43.1 - Suportar VPN Site-to-Site e Cliente-To-Site.

2.2.1.43.2 - Suportar IPSec VPN.

2.2.1.43.3 - Suportar SSL VPN.

2.2.1.43.4 - A VPN IPSec deve suportar:

a) DES e 3DES;
b) Autenticação MD5 e SHA-1;
c) *Diffie-Hellman Group* 1*, Group* 2, *Group* 5 e *Group* 14;
d) Algoritmo *Internet Key Exchange* (IKEv1 e v2);
e) AES 128 e 256 (*Advanced Encryption Standard*);
f) Autenticação via certificado IKE PKI.

2.2.1.43.5 - A VPN SSL deve suportar:

2.2.1.43.5.1 - O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

2.2.1.43.5.2 - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

2.2.1.43.5.3 - Atribuição de endereço IP nos clientes remotos de VPN SSL.

2.2.1.43.5.4 - Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

2.2.1.43.5.5 - Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário.

2.2.1.43.5.6 - 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*.

2.2.1.43.5.7 - Atribuição de DNS nos clientes remotos de VPN;

2.2.1.43.5.8 - Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-spyware* (ou *antimalware*) e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

2.2.1.43.5.9 - Suportar autenticação via AD/LDAP, certificado e base de usuários local.

2.2.1.43.5.10 - Permitir o estabelecimento de túnel VPN *client-to-site* do cliente a plataforma de segurança, integrando-se com as ferramentas de *Windows-logon*.

2.2.1.43.5.11 - Suportar leitura e verificação de CRL (*certificate revocation list*).

2.2.1.43.5.12 - O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory ou ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

2.2.1.43.5.13 - O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

2.2.1.43.5.14 - Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

a) Após autenticação do usuário na estação;
b) Sob demanda do usuário.

2.2.1.43.5.15 - Deve manter uma conexão segura com o portal durante a sessão.

2.2.1.43.5.16 - O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: *Windows Vista, Windows* 7, *Windows* 8, *Windows* 10, Mac OSx, Android e IOS.

2.2.1.43.5.17 - Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

2.2.1.43.5.18 - Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

2.2.1.43.5.19 - Para atendimento as funcionalidades de VPN IPSEC/SSL, será permitido a composição com solução de concentrador VPN por meio de *appliance* físico ou virtual desde que a solução proposta seja do mesmo fabricante e não implique em custo ou licença adicional.

2.2.1.44 - Console de gerência e monitoramento

2.2.1.44.1 - Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos *appliances*.

2.2.1.44.2 - O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos *appliances* da plataforma de segurança.

2.2.1.44.3 - Controle sobre todos os *appliances* da plataforma de segurança em uma única console, com administração de privilégios e funções, salvo o concentrador VPN.

2.2.1.44.4 - O gerenciame
nto centralizado deverá ser entregue como *appliance* virtual e deve ser compatível com *VMware ESXi* 6.0 ou superior.

2.2.1.44.5 - Deve permitir controle global de políticas para todos os *appliances* que compõe a plataforma de segurança.

2.2.1.44.6 - Deve suportar organizar os *appliances* administrados em grupos: os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição.

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

2.2.1.44.8 - 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.

2.2.1.44.9 - Deve permitir a criação de objetos.

2.2.1.44.10 - Deve consolidar logs e relatórios de todos os *appliances* dispositivos administrados.

2.2.1.44.11 - Deve permitir que exportar backup de configuração automaticamente via agendamento.

2.2.1.44.12 - Deve permitir que a configuração ou pacote de atualização de versão dos *firewalls* seja importada de forma automática, ou manual, na plataforma de gerenciamento centralizado e que possa ser usada em outros *firewalls* e grupos *de firewalls*.

2.2.1.44.13 - Deve mostrar os status dos *firewalls* em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

2.3.1.44.14 - Deve centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

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

2.2.1.44.16 - 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.

2.2.1.44.17 - Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais *Windows.*

2.2.1.44.18 - O gerenciamento deve permitir/possuir:

a) Criação e administração de políticas de *firewall* e controle de aplicação;
b) Criação e administração de políticas de IPS, Antivírus e *Anti-Spyware* ou *Antimalware*;
c) Criação e administração de políticas de Filtro de URL;
d) Monitoramento de logs;
e) Ferramentas de investigação de logs;
f) Debugging;
g) Captura de pacotes.

2.2.1.44.19 - Acesso concorrente de administradores.

2.2.1.44.20 - Deve permitir que administradores concorrentes façam modificações, validem e/ou revertam configurações do *firewall* simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador.

2.2.1.44.21 - Deve mostrar ao administrador do *firewall* a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

2.2.1.44.22 - Deve possuir mecanismo busca global na solução onde possa se consultar, por uma *string*, elementos como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas e endereços IPs. Permitindo a localização e uso dos mesmos na configuração do dispositivo.

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

2.2.1.44.24 - Deve permitir monitorar via SNMP falhas de hardware e o uso de recursos do equipamento.

2.2.1.44.25 - Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

2.2.1.44.26 - Permitir a definição de perfis de acesso à console com permissões granulares como: acesso de escrita e acesso de leitura.

2.2.1.44.27 - Efetuar a autenticação integrada ao *Microsoft Active Directory* e servidor *Radius*.

2.2.1.44.28 - Permitir efetuar buscas para localizar em quais regras um endereço IP, IP *Range, subnet* ou objetos estão sendo utilizados.

2.2.1.44.29 - Deve atribuir sequencialmente um número a cada regra de *firewall*, NAT e QoS.

2.2.1.44.30 - Permitir a criação de regras que fiquem ativas em horário definido.

2.2.1.44.31 - Permitir a criação de regras com data de expiração.

2.2.1.44.32 - Efetuar *backup* das configurações e *rollback* de configuração para a última configuração salva.

2.2.1.44.33 - Permitir o *Rollback* de Sistema Operacional para a última versão local.

2.3.1.44.34 - Permitir o upgrade via SCP ou interface de gerenciamento.

2.2.1.44.35 - Permitir a validação regras antes da aplicação.

2.2.1.44.36 - Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros.

2.2.1.44.36.1 - Caso necessário, será aceito o uso de *appliance* externo para permitir a validação de regras antes da aplicação.

2.2.1.44.37 - Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

2.2.1.44.38 - Deve possibilitar a integração com a solução de SIEM em uso no TRE-PR, QRadar.

2.2.1.44.39 - Deve gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

2.2.1.44.40 - Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede.

2.2.1.44.41 - Emitir relatórios em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

2.2.1.44.42 - Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, *Antimalware* ou Antivírus e *Anti-spyware*), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.

2.2.1.44.43 - 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* (ou *anti-malware*), *malwares "Zero Day"* detectados em *sandbox* e tráfego bloqueado.

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

2.2.1.44.45 - Dever permitir a visualização dos *logs* de *malwares* modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, *anti-spyware* (ou *anti-malware*), Filtro de URL e filtro de arquivos.

2.2.1.44.46 - Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e *Anti-spyware* ou *Anti-malware*), etc..

2.2.1.44.47 - Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), e URLs que passaram pela solução.

2.2.1.44.48 - Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em *Real Time*.

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

2.2.1.44.50 - 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* por meio de aplicativos SaaS com a informação do usuário responsável pelo acesso.

2.2.1.44.51 - Permitir a rotação dos logs.

2.2.1.44.52 - 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.

2.2.1.44.53 - Exibição das seguintes informações, de forma histórica e em tempo real:

a) Situação do dispositivo e do cluster;
b) Principais aplicações;
c) Administradores autenticados na gerência da plataforma de segurança;
d) Status das interfaces;
e) Uso de CPU;

2.2.1.44.54 - No mínimo os seguintes relatórios devem ser gerados:

a) Resumo gráfico de aplicações utilizadas;
b) Principais aplicações por utilização de largura de banda de entrada e saída;
c) Principais aplicações por taxa de transferência de bytes;
d) Principais hosts por número de ameaças identificadas;
e) Atividades de um usuário específico do AD/LDAP, incluindo aplicações acessadas, categorias de URL, e ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), de rede vinculadas a este tráfego;
f) Deve permitir a criação de relatórios personalizados.

2.2.1.44.55 - Gerar alertas automáticos via, pelo menos, por e-mail e SNMP.

2.2.1.44.56 - A plataforma de segurança deve permitir através de API (*Application Program Interface*) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em Real Time com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

2.2.1.44.57 - Para comprovação de atendimento aos requisitos técnicos previstos neste termo **não** serão aceitas declarações e/ou cartas de fabricantes ou licitantes. Serão considerados os documentos de domínio público dos respectivos equipamentos e softwares. Caso a documentação de domínio pública seja omissa ou dúbia, poderá ser solicitada amostra para comprovação do atendimetno das características (conforme item 9 do edital).

2.2.1.44.58 - Os equipamentos ofertados devem obrigatoriamente ter certificação da ANATEL.

2.2.1.44.59 - Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a de capacidade ilimitada.

2.2.1.44.60 - Caso a solução possua módulo de relatórios estendida, deverá ser entregue junto com a solução.

2.2.1.44.61 - As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 36 (trinta e seis) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.

2.2.1.44.62 - Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em até 3 (três) dias úteis, para todos os componentes da solução.

2.2.2 – ITEM 2 – Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1:

2.2.2.1 - Este item visa estender, por 24 meses, o funcionamento da solução de proteção de rede com características de Next Generation Firewall (NGFW) e da console de gerência, com todas as garantias de funcionamento do hardware, licenciamentos e respectivas assinaturas de serviço necessárias para seu funcionamento, incluindo, mas não se restringindo a:

2.2.2.1.1 - Extensão do prazo de garantia da solução por 24 (vinte e quatro) meses, com envio de peças/equipamentos de reposição em até 3 dias úteis, para todos os componentes da solução;

2.2.2.1.2 - Extensão do prazo de uso do serviço de atualização automática da base de classificação e categorização de aplicações conhecidas, sites e URLs, pelo período de 24 (vinte e quatro) meses;

2.2.2.1.3 - Extensão do prazo de uso do serviço de atualização automática da base de assinaturas, utilizada pelo serviço de classificação e categorização de arquivos, pelo período de 24 (vinte e quatro) meses;

2.2.2.1.4 - Extensão do prazo de atualizações das assinaturas do serviço de classificação e categorização de arquivos, pelo período de 24 (vinte e quatro) meses.

2.2.3 – ITEM 3 - Serviços de instalação, configuração e repasse de conhecimento.

2.2.3.1 - Os serviços de instalação, configuração e repasse de conhecimento deverão compreender, no mínimo, as seguintes atividades:

a) Reunião para definição dos requisitos, arquitetura e topologia de instalação;
b) Instalação física dos appliances em rack;
c) Energização e conexão dos appliances em rede;
d) Atualização de firmware dos appliances;
e) Configuração das interfaces de gerenciamento;
f) Ativação das licenças adquiridas;
g) Configuração das interfaces de rede e regras de roteamento;
h) Configuração dos objetos e regras de firewall e NAT;

i) Ativação e configuração das funcionalidades de console de gerenciamento, URL Filter, controle de aplicação, VPN, prevenção contra ameaças, antivírus e malwares e sandbox;
j) Migração de todo o ambiente atual para a nova solução
k) Acompanhamento do processo de migração para a nova solução;
l) Elaboração da documentação do ambiente implementado;
m) Repasse de conhecimento, abordando o funcionamento geral da solução e a utilização da console de gerenciamento, com no mínimo 2 horas de duração.

2.2.3.2 - Os serviços devem ser executados de segunda a sexta-feira, das 12 às 19 horas, na sede do TRE-PR.

2.2.3.3 - A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 (trinta) dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência.

2.2.3.4 - Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada.

2.2.3.5 - Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.

2.2.4 – ITEM 4 - Treinamento

2.2.4.1 - Voucher para treinamento oficial do fabricante, a ser ministrado pelo fabricante ou por um de seus parceiros credenciados.

2.2.4.2 - A carga horária mínima do treinamento não poderá ser inferior a 32 (trinta e duas) horas;

2.2.4.3 - O treinamento deverá ser realizado no Brasil, em português, contando com aulas teóricas e práticas.

2.2.4.4 - O treinamento deve abordar, no mínimo:

a) Principais funcionalidades;
b) Configuração inicial;
c) Configuração de políticas de segurança;
d) Métodos de integração e autenticação de usuários;
e) Configurações de NAT e QoS;
f) Configurações de VPN (IPSec e SSL);
g) Emissão e personalização de relatórios.

2.2.4.5 - Deve ser emitido um certificado para cada servidor que participar da capacitação e tiver frequência mínima de 70% (setenta por cento).

2.2.5 - Do suporte técnico durante a garantia contratual:

2.2.5.1- Durante o período de Garantia, a CONTRATADA deverá prestar suporte técnico, atender às solicitações do TRE-PR, efetuadas pela Seção de Rede, respeitando as condições e níveis de serviço especificados a seguir;

2.2.5.2- A severidade dos chamados de suporte e garantia serão determinadas conforme abaixo e o prazo de atendimento será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir:

2.2.5.3- Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 (seis) horas	12 (doze) horas	08 (oito) horas	16 (dezesseis) horas

2.2.5.4- Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade.

Dias úteis		Sábados, domingos e feriados	
Prazo atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 (seis) horas	48 (quarenta e oito) horas	10 (dez) horas	48 (quarenta e oito) horas

2.2.5.5 - Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.

Dias úteis		Sábados, domingos e feriados	
Prazo atendimento	Prazo de solução definitiva	Prazo atendimento	Prazo de solução definitiva
30 (trinta) horas	72 (setenta e duas) horas	-	-

2.2.5.6- Serão considerados para efeitos dos prazos exigidos:

2.2.5.6.1. Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção.

2.2.5.6.2. Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e a efetiva recolocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

2.2.5.7 - A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação ao licitante vencedor, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica do TRE-PR;

2.2.5.8 - O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da TRE-PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais ao TRE-PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar em aplicação de sanções previstas.

2.2.5.9- As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como sanções previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar na aplicação das sanções previstas.

2.2.5.10- Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica do TRE-PR e solicitará autorização para o fechamento do chamado. Caso o TRE-PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pelo licitante vencedor. Nesse caso, o TRE-PR fornecerá as pendências relativas à solicitação em aberto.

2.2.5.11- O TRE-PR encaminhará a contratada, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.

2.2.5.12 - Por necessidade excepcional de serviço, o TRE-PR também poderá solicitar a escalação de chamado para níveis superiores de severidade. Nesse caso, a escalação deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

3 - DAS OBRIGAÇÕES DA CONTRATADA

3.1 – Da entrega:

3.1.1 – Do prazos:

3.1.1.1 – Prazo de entrega da solução: a solução deverá ser entregue em um prazo de até **60 (sessenta) dias corridos**, a contar da assinatura do contrato.

3.1.1.2 – **Prazo de instalação e configuração**: a solução deverá ser instalada e configurada em um prazo de até **60 (sessenta) dias corridos**, contados da data de recebimento provisório.

3.1.2 – Do local de entrega: a solução deverá ser entregue no Tribunal Regional Eleitoral do Paraná, Rua João Parolin, nº 224, Curitiba-PR, Seção de Rede, agendamento pelos telefones (41) 3330-8628 ou 3330-8629.

3.2 - – Do recebimento do objeto:

3.2.1 – Do recebimento provisório: em até 10 (dez) dias corridos a solução será recebida, provisoriamente, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

3.2.2 – O recebimento provisório será realizado pela Seção de Gestão de Equipamentos de Microinformática.

3.2.3 - Na hipótese de constatação de anomalias que comprometam a utilização adequada da solução, ela será rejeitada, em todo ou em parte, conforme dispõe o Art. 76 da Lei n° 8.666/93, sem qualquer ônus para o TRE-PR, devendo o licitante vencedor reapresentá-la (s) no prazo máximo de até 30 (trinta) dias, após o comunicado.

3.2.4 – Do recebimento definitivo: a verificação da conformidade das especificações da solução ocorrerá no prazo de até 10 (vinte) dias corridos, contados a partir do recebimento provisório. Atestada a conformidade quantitativa e qualitativa, a solução será recebida definitivamente.

3.2.4.1- O recebimento definitivo será realizado pela Coordenadoria de Infraestrutura.

3.3 – Da garantia:

3.3.1 - A solução ofertada deverá estar coberta por garantia total fornecida pelo fabricante, pelo prazo de 36 (trinta e seis) meses.

3.3.1.1 - A garantia iniciará a partir da data de recebimento definitivo da solução.

3.3.2 - A contratada deverá apresentar o Certificado de Garantia emitido pelo fabricante, no prazo de até 30 (trinta) dias corridos, a contar da data de recebimento definitivo da solução.

3.3.3 - A contratada deverá possibilitar a abertura de chamado técnico diretamente no fabricante da solução ou por centro de suporte devidamente autorizado pelo fabricante.

3.3.4 - O atendimento de primeiro nível deve ser realizado em português do Brasil.

3.3.5 - Deve ser disponibilizado pelo menos um dos seguintes canais de atendimento para suporte:

a) Telefone 0800;
b) Sistema Web de abertura de chamados;
c) E-mail.

3.3.6 - A Contratada deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de *firmware e software*, aplicação de correções (patches), diagnóstico, avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

3.3.7 – A Contratada deverá, semestralmente, revisar as atualizações de drivers, firmwares e microcódigos de todos os *appliances* contratados. Os serviços de atualizações de *firmwares* somente deverão ocorrer para os eventos classificados como críticos.

3.3.8 - Os serviços cobertos pela garantia deverão ser prestados nas instalações do TRE-PR, em Curitiba/PR.

3.3.9 - Os serviços cobertos pela garantia deverão ser prestados pela empresa fabricante, pela contratada ou parceiro autorizado/credenciado, através da disponibilização de técnicos certificados pelo fabricante da solução.

3.3.10 - A Contratada deverá fornecer a seus técnicos as ferramentas e instrumentos necessários à execução dos serviços, bem como produtos ou materiais indispensáveis à manutenção do equipamento.

3.3.11 - Os discos rígidos que forem substituídos ou no caso de troca de equipamento ficarão retidos e serão de propriedade do TRE-PR.

3.3.12 - A Contratada deverá garantir atualizações do produto e suporte técnico do fabricante (telefone, e-mail ou acesso remoto) pelo período de vigência da garantia.

3.3.13 - A substituição de equipamento defeituoso deverá ocorrer em até 30 (trinta) dias corridos, após a abertura de Ordem de Serviço pelo gestor de contrato ou notificação automática do sistema na central de atendimento do licitante vencedor ou fabricante.

3.4 – A Contratada deverá apresentar, ao gestor da contratação, em até 30 (trinta) dias corridos contados da assinatura do contrato, no momento da entrega dos equipamentos, os documentos abaixo:

a) Certificação/declaração emitida pelo fabricante do equipamento ofertado (ou credenciado) para, no mínimo, 02 (dois) funcionários, atestando participação em curso/treinamento específico relacionado à utilização/configuração/suporte do equipamento ofertado.

b) Comprovação do vínculo dos funcionários certificados (conforme alínea a) com a empresa contratada, mediante apresentação de carteira profissional ou contrato de prestação de serviços.

3.5 – Da sustentabilidade:

3.5.1 - Será exigida a compatibilidade do produto com a diretiva RoHS (RoHS - Restriction of Certain Hazardous Substances ou Restrição de Certas Substâncias Perigosas), a qual limita a um percentual máximo o uso de substâncias perigosas nos processos de fabricação dos produtos, entre elas: cádmio (Cd), mercúrio (Hg), cromo hexavalente (CrVI), bifenilos polibromados (PBBs), éteres difenil-polibromados (PBDEs) e chumbo (Pb), de modo a contribuir para a redução do impacto ambiental.

3.5.2 - Os produtos deverão ser preferencialmente, acondicionados em embalagem individual adequada, com menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento. As condições deste item serão objeto de verificação *in loco* no momento da entrega dos produtos.

3.6 - A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

4 - DISPOSIÇÕES GERAIS

4.1 - As licitantes deverão efetuar suas cotações seguindo rigorosamente as especificações solicitadas, abstendo-se de participar da licitação aqueles que não puderem atender às condições do edital.

4.2 - Dúvidas referentes à contratação poderão ser sanadas com o servidor Breno Schult, pelo telefone: (41) 3330-8621 ou 3339-8681, das 12h às 19:00.