ANEXO V.D

ESPECIFICAÇÃO DO CORE DE SEGURANÇA

ÍNDICE

1. ESPECIFICAÇÃO DO CORE DE SEGURANÇA

1.1 CARACTERÍSTICAS DO OBJETO

1.1.a) Os equipamentos de segurança deverão ter características de *Next Generation Firewall* (NGFW), e oferecer camadas de proteção para redes internas de *data center.* Devem estar totalmente capacitados para operar em redundância e em alta disponibilidade.

1.1.b) Aquisição de solução de proteção de rede com características de NGFW, para segurança de informação que inclui filtro de pacotes, controle de aplicações, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, *spywares e malwares "Zero Day",* Filtro de URL, bem como controle de transmissão de dados e acesso à *internet* compondo uma plataforma de segurança integrada e robusta.

1.1.c) *Throughput de Firewall para*/ pacotes 64 bytes: mínimo de 1.000 Gbps;

1.1.d) *Throughput de VPN IPsec:* mínimo de 600 Gbps;

1.1.e) Suporte a, no mínimo, 100.000 novas conexões HTTP por segundo;

1.1.f) Deverá estar licenciada para ou suportar sem o uso de licença, 40.000 clientes de VPN SSL simultâneos.

1.1.g) Deverá estar licenciada para ou suportar sem o uso de licença, 20.000 túneis de VPN IPSEC simultâneos.

1.1.h) Deverá suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no *firewall* físico.

1.1.i) Os contextos virtuais deverão suportar as funcionalidades nativas do *gateway* de proteção incluindo: Firewall, IPS, Antivírus, Antispyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QoS, NAT e Identificação de usuários.

1.1.j) Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de *end-of-life e end-of-sale,* ou qualquer outra forma de lista de descontinuidades.

1.1.k) O *firewall* deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota *default* com a definição de um endereço IP de destino que deverá estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deverá ter a capacidade de usar rota alternativa para estabelecer a comunicação:

1.1.l) Deverá 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 endereço de porta (PAT);
g) NAT de Origem e NAT de Destino;
h) Suportar NAT de Origem e NAT de Destino simultaneamente;
i) A solução deverá possuir as seguintes funcionalidades:
j) Suporte a 4094 VLAN *Tags* 802.1q;
k) Agregação de links 802.3ad e LACP;
l) *Policy based routing* or policy-based *forwarding;*
m) DHCP Relay;
n) DHCP Server;

1.1.m) Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

1.1.n) Deverá implementar *Network Prefix Translation (NPTv6),* prevenindo problemas de roteamento assimétrico.

1.1.o) Deverá implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD.

1.1.p) Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino.

1.1.q) Deverá implementar o protocolo *Link Layer Discovery (LLDP)*, permitindo que o *appliance,* e outros ativos da rede se comuniquem para identificação da topologia da rede, em que estão conectados, e a função deles, facilitando

o processo de *troubleshooting.* As informações aprendidas e armazenadas pelo *appliance* deverão ser acessíveis via SNMP.

1.1.r) Deverá gerar os registros de *logs* para sistemas de monitoração externos, simultaneamente. Deverá haver a opção de enviar *logs* via protocolo TCP e SSL.

1.1.s) Deverá permitir configurar certificado, caso necessário, para autenticação no sistema de monitoração externo de *logs.*

1.1.t) Deverá exibir nos logs de tráfego o motivo para o término da sessão no *firewall*, incluindo sessões finalizadas onde houver descriptografia de SSL e SSH.

1.1.u) Deverá implementar proteção contra *anti-spoofing.*

1.1.v) Deverá permitir bloquear sessões TCP que usarem variações do *3-way handshake*, como 4 *way e 5 way split hand-shake*, prevenindo desta forma possíveis tráfegos maliciosos.

1.1.w) Deverá permitir bloquear conexões que contenham dados no *payload* de pacotes TCP-SYN e SYN-ACK, durante o *three-way handshake.*

1.1.x) Deverá suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC *(Stateless address* auto *configuration*), NAT64 ou *Dual stack* IPv4/IPv6, Identificação de usuários a partir do LDAP/AD, *Captive Portal*, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (*Denial of Service),* Descriptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 *Relay,* IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, *Neighbours Discovery* (ND), *Recursive* DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicações.

1.1.y) Os dispositivos de proteção deverão ter a capacidade de operar de forma simultânea em uma única instância de *firewall,* mediante o uso de suas interfaces físicas nos seguintes modos:

a) Modo *Sniffer,* para inspeção via porta espelhada do tráfego de dados da rede;

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

c) Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicações operando como *default gateway* das redes protegidas.

d) Modo misto de trabalho *Sniffer,* L2 e L3 em diferentes interfaces físicas.

1.1.z) Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente e em modo layer 3 (L3) e deverá sincronizar:

a) Sessões;

b) Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QoS e objetos de rede;

c) Certificados descriptografados;

d) Associações de Segurança das VPNs;

e) Tabelas FIB;

f) O HA (modo de Alta-Disponibilidade) deverá possibilitar a monitoração de falha de link.

1.1.aa) As funcionalidades de *firewall*, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPSec e SSL, QoS, descriptografia SSL e SSH, DHCP servidor, DHCP *relay*, NAT, suporte a VLAN e protocolos de roteamento dinâmico deverão 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.

1.2 CONTROLE DE POLÍTICAS

1.2.a) Deverá suportar controles e criação de políticas por zona de segurança, porta/protocolo e aplicações, categorias de aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações usuários, grupos de usuários, endereço IP e redes.

1.2.b) Deverá 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.

1.2.c) Deverá permitir autenticação segura, através de certificado nas fontes externas de endereços IP, domínios e URLs.

1.2.d) Deverá permitir consultar e criar exceção para objetos das listas externas, a partir da interface de gerência do próprio *firewall*.

1.2.e) Deverá permitir controle, inspeção e *descriptografia* de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*).

1.2.f) Deverá permitir *offload* de certificado em inspeção de conexões SSL de entrada (Inbound).

1.2.g) Deverá permitir *descriptografar* tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.

1.2.h) Deverá permitir *descriptografar* sites e aplicações que utilizam certificados *ECC*, incluindo *Elliptical Curve Digital Signature Algorithm (ECDSA).*

1.2.i) Deverá permitir Controle de inspeção e descriptografia de *SSH* por política.

1.2.j) A descriptografia de SSH deverá possibilitar a identificação e bloqueio de tráfego, caso o protocolo esteja sendo usado como técnica evasiva para burlar os controles de segurança.

1.2.k) Deverá permitir espelhamento de tráfego descriptografado (SSL e TLS) para soluções externas de análise.

1.2.l) Deverá permitir bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg.

1.2.m) Deverá suportar objetos e regras IPV6.

1.2.n) Deverá suportar objetos e regras *multicast.*

1.2.o) Deverá permitir no mínimo três tipos de negação de tráfego nas políticas de *firewall:*

a) Drop sem notificação do bloqueio ao usuário;

b) *Drop* com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego;

c) TCP-Reset para o client, TCP-Reset para o *server* ou para os dois lados da conexão.

1.2.p) Deverá suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas, em horários prédefinidos automaticamente.

1.3 CONTROLE DE APLICAÇÕES

1.3.a) A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades.

1.3.b) Deverá permitir a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

1.3.c) Deverá permitir a inspeção do 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.

1.3.d) A checagem de assinaturas também deverá determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389.

1.3.e) Deverá aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a *Encrypted Bittorrent* e aplicações VOIP, VoBB ou VOLTE que utilizam criptografia proprietária.

1.3.f) Deverá 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.

1.3.g) Para tráfego criptografado SSL, deverá *descriptografar* pacotes a fim de possibilitar a leitura de *payload*, para checagem de assinaturas de aplicações conhecidas pelo fabricante.

1.3.h) Deverá permitir decodificação de protocolos com o objetivo de detectar aplicações encapsuladas, dentro do protocolo e validar, se o tráfego corresponde com a especificação do protocolo. A decodificação de

protocolo também deverá identificar funcionalidades específicas dentro de uma aplicação, além de detectar arquivos e outros conteúdos que deverão ser inspecionados de acordo com as regras de segurança implementadas.

1.3.i) Deverá permitir identificar o uso de táticas evasivas via comunicações criptografadas.

1.3.j) Deverá atualizar a base de assinaturas de aplicações automaticamente.

1.3.k) Deverá reconhecer aplicações em IPv6.

1.3.l) Deverá permitir limitar a banda (*download/upload)* usada por aplicações (*traffic shaping)*, baseado no IP de origem.

1.3.m) Deverá permitir 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

1.3.n) Deverá permitir múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística.

1.3.o) Deverá permitir o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

1.4 PREVENÇÃO DE AMEAÇAS

1.4.a) Para proteção do ambiente contra-ataques, a solução deverá possuir módulo de IPS, Antivírus e *Anti-Spyware* integrados no próprio *appliance de Firewall.*

1.4.b) Deverá ser capaz de identificar e bloquear as seguintes ameaças: vírus, *trojans, spywares, ransomwares* e demais tipos de malwares.

1.4.c) Deverá permitir a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware).*

1.4.d) As funcionalidades de IPS, Antivírus e *Anti-Spyware* deverão 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.

1.4.e) Deverá permitir sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware*.

1.4.f) Deverá permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.

1.4.g) 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 e usando *decoder*s de pelo menos os seguintes protocolos: *HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, , MS-RPC, RTSP e File body.*

1.4.h) O fabricante deverá permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

1.4.i) Deverá permitir alertar o usuário quando uma aplicação for bloqueada.

1.4.j) Deverá permitir que o controle de portas seja aplicado para todas as aplicações.

1.4.k) Deverá permitir regras que permitam passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego dela em determinada regra. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias.

1.4.l) Deverá possibilitar a diferenciação de aplicações *Proxies (ghostsurf, freegate, etc.)* possuindo granularidade de controle/políticas para as mesmas.

1.4.m) Deverá permitir os seguintes tipos de ações para ameaças detectadas pelo IPS e *Antispyware:* permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *tcp-reset.*

1.4.n) Deverá permitir detectar e prevenir ameaças em tráfegos HTTP.

1.4.o) Deverá permitir ativar ou desativar as assinaturas, ou ainda habilitá-las apenas em modo de monitoração.

1.4.p) Deverá permitir exceções por IP de origem ou de destino deverão ser possíveis nas regras, de forma geral e assinatura a assinatura.

1.4.q) Deverá permitir granularidade nas políticas de IPS Antivírus e *Anti-Spyware* , possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

1.4.r) Deverá permitir o bloqueio de vulnerabilidades.

1.4.s) Deverá permitir o bloqueio de *exploits* conhecidos.

1.4.t) Deverá incluir proteção contra-ataques de negação de serviços (DoS).

1.4.u) Deverá permitir a inspeção e criação de regras de proteção de DOS e QoS para o conteúdo de tráfego tunelado pelo protocolo GRE.

1.4.v) Deverá ser imune e capaz de impedir ataques básicos como: *Synflood, ICMPflood, UDPflood etc.*

1.4.w) Deverá detectar e bloquear a origem de *port scans*, com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização.

1.4.x) Deverá bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões.

1.4.y) Deverá 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.

1.4.z) Deverá possuir assinaturas para bloqueio de ataques de *buffer overflow;*

1.4.aa) Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

1.4.bb) Deverá permitir usar operadores de negação na criação de assinaturas customizadas de IPS e *anti-spyware,* permitindo a criação de exceções com granularidade nas configurações.

1.4.cc) Deverá permitir o bloqueio de vírus e *spywares* em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

1.4.dd) Deverá suportar bloqueio de arquivos por tipo.

1.4.ee) Deverá identificar e bloquear comunicação com *botnets.*

1.4.ff) Deverá suportar várias técnicas de prevenção, incluindo *Drop* e tcp-rst (Cliente, Servidor e ambos).

1.4.gg) Deverá registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

1.4.hh) Deverá suportar a captura de pacotes (PCAP), por assinatura de IPS e *Antispyware.*

1.4.ii) Deverá permitir que na captura de pacotes por assinaturas de IPS e *Antispyware* seja definido o número de pacotes a serem capturados. Esta captura deverá permitir selecionar, no mínimo, 50 pacotes

1.4.jj) Deverá 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.

1.4.kk) Deverá incluir proteção contra vírus em conteúdo *HTML e javascript, software espião (spyware) e worms.*

1.4.ll) Deverá incluir proteção contra *downloads* involuntários usando HTTP de arquivos executáveis maliciosos.

1.4.mm) Deverá incluir rastreamento de vírus em PDF.

1.4.nn) Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate (zip, gzip etc.).*

1.4.oo) Deverá 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 regra de *firewall* poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança

1.4.pp) Deverá possuir a capacidade de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (*Domain generation algorithm* - DGA).

1.4.qq) Deverá mostrar nos logs as seguintes informações sobre domínios DGA:

a) Domínio suspeito identificado;

b) ID de assinatura de detecção;

c) Usuário logado na estação/servidor que originou o tráfego;

d) Aplicação;

e) Porta de destino;

f) IP de origem e IP de destino;

g) Ação do firewall;

h) Severidade.

1.5 ANÁLISE DE *MALWARES* MODERNOS

1.5.a) Devido aos *Malwares*, atualmente, 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 deverá possuir funcionalidades para análise de *Malwares* não conhecidos incluídas na própria ferramenta.

1.5.b) Deverá aplicar o conceito de *Sandbox,* que funciona como um ambiente isolado para análise de ameaças desconhecidas e que não estejam nas assinaturas do fabricante.

1.5.c) Deverá ser capaz de enviar arquivos trafegados de forma automática para análise, onde o arquivo será executado e simulado em ambiente controlado.

1.5.d) Deverá ser capaz de selecionar, através de políticas granulares, quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do *LDAP,* aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente.

1.5.e) Deverá possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixam o sistema operacional lento, que alteram parâmetros do sistema etc.

1.5.f) Deverá suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, IOS e Windows 7.

1.5.g) Deverá suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: *Sniffer*, transparente e L3.

1.5.h) Deverá possuir a capacidade de analisar em *sandbox links* (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deverá ser gerado um relatório caso a abertura do link pelo *sandbox* o identifique como site hospedeiro de *exploits.*

1.5.i) A análise de links em *sandbox* deverá ser capaz de classificar sites falsos na categoria de *phishing* e atualizar a base de filtro de URL da solução.

1.5.j) Para ameaças trafegadas em protocolo SMTP e POP3, a solução deverá ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque.

1.5.k) O sistema de análise deverá 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).

1.5.l) O sistema de análise deverá emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o *malware.*

1.5.m) Deverá permitir a visualização de resultados das análises *de malwares Zero Day* nos diferentes sistemas operacionais suportados.

1.5.n) Deverá permitir exportar o resultado das análises de *malwares* de dia Zero em PDF e CSV a partir da própria interface de gerência.

1.5.o) Deverá permitir o *download* dos *malwares* identificados a partir da própria interface de gerência.

1.5.p) Deverá permitir informar ao fabricante quanto à suspeita de ocorrências de falso-positivo e falso-negativo na análise de *malwares Zero Day* a partir da própria interface de gerência.

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

1.5.r) Deverá suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.

1.5.s) Deverá 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.*

1.5.t) Deverá permitir o envio de arquivos e *links* para análise no ambiente controlado de forma automática via API.

1.5.u) Deverá permitir o envio para análise em *sandbox* de malwares bloqueados pelo antivírus da solução.

1.5.v) A solução deverá possuir as seguintes funcionalidades de filtro de URL:

a) Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da
b) semana e hora);
c) Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;
d) Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
e) Deverá incluir 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-directory e base de dados local;
f) Deverá permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
g) Deverá permitir bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção *Safe Search* esteja desabilitada. Deverá ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;
h) Deverá suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
i) Deverá permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

j) Deverá permitir classificar sites em mais de uma categoria, de acordo com a necessidade.

1.5.w) A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório.

1.5.x) Deverá permitir a criação categorias de URLs customizadas.

1.5.y) Deverá permitir a exclusão de URLs do bloqueio, por categoria.

1.5.z) Deverá permitir a customização de página de bloqueio.

1.5.aa) Deverá proteger contra o roubo de credenciais, usuários e senhas.

1.5.bb) Deverá permitir identificação através da integração com *Active Directory* submetidos em sites não corporativos. Deverá ainda permitir criação de regra onde usuários do *Active Directory* só possam enviar informações de login para sites autorizados na solução.

1.5.cc) Deverá permitir bloquear o acesso do usuário caso ele tente fazer o envio de suas credenciais em sites classificados como *phishing* pelo filtro de URL da solução.

1.5.dd) Deverá permitir o bloqueio e continuação (possibilitando que o usuário;

1.5.ee) Os equipamentos devem trabalhar com base na aplicação de políticas de segurança para proteção de redes em IPv4 e IPv6. As configurações de políticas de segurança devem utilizar o conceito de objetos e grupos de objetos.

1.5.ff) Possuir capacidade de controle de tráfego para os protocolos TCP, UDP e ICMP baseados nos endereços de origem e de destino, porta e serviço.

1.5.gg) Deve permitir ao administrador criar objetos e grupo de objetos personalizados para usuários, hosts, redes, sub-redes, intervalos de endereço IP, serviços e protocolos.

1.5.hh) As políticas de segurança devem ser aplicadas a qualquer momento, sem prejuízo ao usuário. Sessões não afetadas por novas políticas de segurança aplicadas no equipamento não devem ser interrompidas

1.5.ii) Autenticar e autorizar acesso à usuários ou grupos de usuários, utilizando ou não certificados digitais, em uma determinada política de segurança.

1.5.jj) Os tráfegos de origem e destino das políticas de segurança deverão estar vinculados a alguma interface ou a alguma zona de segurança do equipamento.

1.5.kk) As políticas de segurança devem estar classificadas em ordem de prioridade. O administrador deverá poder alterar essa ordem a qualquer momento e de acordo com a sua necessidade.

1.5.ll) Utilizar simultaneamente políticas de segurança em IPv4 e IPv6;

1.5.mm) Gravar log detalhado do tráfego de rede permitindo a sua análise (esteja ele bloqueado ou não) e identificação da política de segurança responsável pelo bloqueio.

1.5.nn) Implementar *switch virtual* utilizando as interfaces do equipamento.

1.5.oo) Possuir a funcionalidade de roteamento dinâmico, para redes IPv4 e IPv6, por meio dos protocolos RIP, OSPF v2, OSPF v3 e BGP v4.

1.5.pp) Os equipamentos deverão operar em modo “transparente” (camada 2) e em modo “roteador” (camada 3). Em ambas as opções, o cluster formado pelos equipamentos deverá operar em alta disponibilidade nas modalidades ativo-ativo e ativo-passivo. Quando estiver em modo “transparente” o cluster de segurança deverá permitir a utilização e propagação do protocolo OSPF na rede.

1.5.qq) Possui funcionalidade DHCP server e DHCP relay agent.

1.5.rr) Possui funcionalidade DHCPv6.

1.5.ss) Criar e configurar *subinterfaces* lógicas do tipo ethernet.

1.5.tt) Permitir a limitação de largura de banda por meio de *traffic shapping,* aplicada por política, com ativação e desativação automática da funcionalidade por meio de agendamento por dia da semana, horário e com opção de recursividade.

1.5.uu) A política de *traffic shapping* deverá ser efetiva mesmo em conexões já estabelecidas.

1.5.vv) Deverá possuir a funcionalidade *Network Address Translation* (NAT) nos modos estático e dinâmico.

1.5.ww) Deverá possuir a funcionalidade NAT64 e NAT46 para redes IPv6.

1.5.xx) Deverá possuir funcionalidade *Port Address Translation* (PAT).

1.5.yy) Deverá possuir funcionalidade de tags VLAN 802.1Q, 802.11 e 802.x.

1.5.zz) Deverá realizar roteamento por meio de *Policy Based Routing* (PBR).

1.5.aaa) Utilizar o protocolo *Network Time Protocol* (NTP)

1.5.bbb) Possuir funcionalidade de roteamento de protocolo *multicast* PIM nos modos *sparse* e *dense.*

1.5.ccc) Propagar o protocolo *multicast* IGMP.

1.5.ddd) Realizar inspeção *stateful* dos protocolos de sinalização de telefonia H.323 (v1, v2, v3 e v4), *Session Initiation Protocol* (SIP), *Media Gateway Control Protocol* (MGCP) e Skinny *Client Control Protocol* (SCCP).

1.5.eee) Deve implantar o protocolo SIP em conformidade com a RFC3261.

1.5.fff) Deve ser possível criar e terminar dinamicamente conexões SIP com sinalização criptografada (SIP over TLS) e mídia criptografada (SRTP);

1.5.ggg) *Realizar Policy Based Routing* (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.

1.5.hhh) O Módulo licenciado deverá buscar automaticamente a licença no equipamento de gerenciamento centralizado.

1.5.iii) As políticas de segurança deverão ser capazes de identificar e controlar o usuário de aplicações através de integração com serviços de diretório e autenticação por meio de LDAP e base de dados local.

1.5.jjj) Deverá integrar com LDAP para identificar usuários e grupo de usuários, permitindo a granularidade de controle e de políticas baseadas em usuários e grupo de usuários;

1.5.kkk) Deverá receber eventos de autenticação de controladoras *wireless*, dispositivos 802.1x e soluções de NAC (*Network Access Control*) por meio de *syslog* para identificação de endereços IP e usuários.

1.5.lll) Deverá autenticar usuários por meio de *captive portal*, sem a necessidade de instalação de aplicativos clientes;

1.5.mmm) Deverá permitir a inclusão nos *logs* do produto de informações das atividades dos usuários.

1.5.nnn) Deverá salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: *User Agent,* Referer, e X- Forwarded. Deverá 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, E-*directory* e base de dados local.

1.5.ooo) Deverá permitir integração com *Radius,* para identificação de usuários e grupos, permitindo granularidade de controle/políticas, baseadas em usuários e grupos de usuários.

1.5.ppp) Deverá permitir integração com LDAP, para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

1.5.qqq) Deverá permitir que a autenticação da rede com fio seja realizada através de *captive portal.*

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

1.5.sss) Deverá permitir a autenticação via Kerberos.

1.5.ttt) Deverá permitir autenticação via Kerberos para administradores da solução, *Captive Portal* e usuário de VPN SSL.

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

1.5.vvv) Deverá permitir a criação de grupos customizados de usuários no *firewall,* baseado em atributos do LDAP.

1.5.www) Deverá permitir a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores *Windows.*

1.5.xxx) Deverá permitir controlar aplicações e tráfego, cujo consumo possa ser excessivo e ter um alto consumo de largura de banda.

1.5.yyy) Deverá permitir a criação de filtros para arquivos e dados prédefinidos.

1.5.zzz) Os arquivos deverão ser identificados por extensão e assinaturas.

1.5.aaaa) Deverá permitir identificar e prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados.

1.5.bbbb) Deverá permitir a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

1.5.cccc) Deverá permitir listar o número de aplicações suportadas para controle de dados.

1.5.dddd) Deverá permitir a criação de redes seguras (VPN), de forma simples para que os usuários e os administradores possam utilizar da infraestrutura remotamente.

1.5.eeee) Deverá suportar VPN Site-to-Site e Client-To-Site.

1.5.ffff) Deverá suportar IPSec VPN.

1.5.gggg) Deverá suportar SSL VPN.

1.5.hhhh) Deverá possuir interoperabilidade com os seguintes fabricantes: Fortinet.

1.5.iiii) Deverá permitir 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 porta;
e) Banda Garantida;
f) Banda Máxima;
g) Fila de Prioridade.

1.5.jjjj) Deverá permitir centralizar a administração de regras e políticas, inclusive quando configurado em um cluster, usando uma única interface de gerenciamento.

1.5.kkkk) O gerenciamento da solução deverá suportar acesso via SSH, cliente ou WEB (HTTPS).

1.5.llll) Deverá permitir substituir o certificado de fábrica no acesso HTTPS à gerência do *firewall,* com a possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa.

1.5.mmmm) Caso haja a necessidade de instalação de cliente para administração da solução, este deverá ser compatível com sistemas operacionais Windows e/ou Linux.

1.5.nnnn) O gerenciamento deverá 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;*
c) Criação e administração de políticas de Filtro de URL;
d) Monitoração de logs;
e) Ferramentas de investigação de logs;
f) *Debugging;*
g) Captura de pacotes.

1.5.oooo) Deverá permitir acesso concorrente de administradores.

1.5.pppp) Deverá permitir que administradores façam modificações, validem configurações e revertam configurações do *firewall*, simultaneamente, e que cada administrador consiga aplicar apenas as suas alterações, de forma independente, das realizadas por outro administrador.

1.5.qqqq) Deverá mostrar ao administrador do *firewall*, a hora e data do último *login* e tentativas de *login* com falha para acessos.

1.5.rrrr) Deverá permitir busca global na solução onde possa se consultar por: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso deles na configuração do dispositivo.

1.5.ssss) Deverá permitir busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

1.5.tttt) Deverá permitir usar palavras chaves e cores para facilitar identificação de regras.

1.5.uuuu) Deverá permitir autenticação integrada ao servidor *Radius.*

1.5.vvvv) Deverá permitir a localização de em quais regras um endereço IP, IP Range, *subnet* ou objetos estão sendo utilizados.

1.5.wwww) Deverá definir sequencialmente um número a cada regra de *firewall,* NAT, QoS e regras de DOS.

1.5.xxxx) Deverá permitir a criação de regras que fiquem ativas em horário definido.

1.5.yyyy) Deverá permitir a criação de regras com data de expiração.

1.5.zzzz) Deverá permitir *backup* das configurações e *rollback* de configuração para a última configuração salva.

1.5.aaaaa) Deverá permitir *Rollback* de Sistema Operacional para a última versão local.

1.5.bbbbb) Deverá permitir *upgrade* via SCP, TFTP e interface de gerenciamento.

1.5.ccccc) Deverá permitir a análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

1.5.ddddd) Deverá permitir validação de regras antes da aplicação.

1.5.eeeee) Deverá permitir validação de configurações antes da aplicação delas, permitindo identificar erros, tais como: rota de destino inválida, regras em *shadowing* etc.

1.5.fffff) Deverá permitir análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (*shadowing)* e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve realizar também a análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão dela para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente.

1.5.ggggg) Deverá permitir a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

1.5.hhhhh) Deverá permitir auditar regras de segurança, exibindo quadro comparativo das alterações de uma regra em relação à versão anterior.

1.5.iiiii) Deverá permitir a integração com outras soluções de SIEM de mercado;

1.5.jjjjj) Deverá permitir geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

1.5.kkkkk) Deverá permitir gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações, na rede no que se refere a um período anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.

1.5.lllll) Deverá permitir geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

1.5.mmmmm) Deverá permitir a criação de *Dashboards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, Antivírus, *Anti-spyware, malwares "Zero Day"* detectados em *sandbox* e tráfego bloqueado;

1.5.nnnnn) Deverá permitir a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.

1.5.ooooo) Deverá permitir o armazenamento de logs sem limite de tempo para retenção.

1.5.ppppp) Deverá permitir o armazenamento de logs sem limite de tempo e reconhecer e/ou permitir alocar um tamanho de disco de pelo no mínimo 80 TB.

1.5.qqqqq) Deverá permitir armazenar no mínimo 8TB de logs por mês.

1.5.rrrrr) Deverá permitir armazenar no mínimo 100GB de logs por dia.

2. APLICAÇÃO E ESPECIFICAÇÕES DO DPI E ANTIDDOS

Objeto deste escopo é a aquisição de *hardware e software* para contratação de solução de defesa, tipo contra-ataque de negação do serviço *DoS (Denial of Service) e DDoS (Distributed Denial of Service).*

Ataques de negação de serviços e ataques distribuídos por negação de serviços são ações maliciosas, executadas com o objetivo de exaurir os recursos disponíveis de uma rede, aplicativo ou serviço, afetando a sua disponibilidade. A contratada deverá entregar testes de funcionalidade dos sistemas propostos:

2.a) Máximo desempenho de limpeza (baseado em pacotes): 100G.

2.b) Deverá ter detecção e defesa de ataques/requisições de conexão baseada em fluxo: *netflow V5/V9, netstream V5/V9, IPFIX*, contra inundação SYN, inundação SYN-ACK, inundação ACK, inundação FIN/RST, TCP Malformado, Inundação de Conexão TCP, Inundação de Fragmentos TCP, Inundação UDP, Inundação de Fragmento UDP, inundação ICMP, outra inundação e vários amplificação de reflexão UDP.

2.c) Deverá ter capacidade de defesa contra-ataques de inundação SYN com base na autenticação de desafio de origem com números de sequência incorretos e corretos.

2.d) Deverá atender defesa contra SYN, SYN-ACK e ACK primeiro pacote de verificação para defesa contra-ataques de inundação de origem forjada.

2.e) Deverá ter capacidade de defesa contra-ataques SYN de origem real, com base na taxa SYN, limitação de taxa SYN de origem e verificação de sessão.

2.f) Deverá suportar verificação de sessão para se defender contra-ataques de inundação ACK, FIN e RST.

2.g) O sistema pode verificar o comprimento dos pacotes *SYN, SYN-ACK, FIN e RST*. O intervalo válido do comprimento do pacote pode ser personalizado.

2.h) O sistema deverá verificar o sinalizador TCP, filtrar o conteúdo da carga útil ACK e personalizar o intervalo de verificação do campo Carga útil.

2.i) Deverá suporta detecção de sessão e defesa contra vários ataques de exaustão de conexão e conexão anormal, incluindo exaustão de conexão TCP, *Sockstress*, retransmissão TCP e ataques de conexão vazia, com base em sessões de origem simultâneas e novas sessões.

2.j) Deverá suportar identificação e filtragem de ataques comuns de ataques cibernéticos com grande solicitação de requisições de um servidor DNS ou ping ICMP ou ainda com requisições de autenticação amplificada tipo *SSDP, NTP e MemCached.*

2.k) Deverá suportar filtragem de novos ataques de amplificação de reflexão UDP com base em características de ataque definidas pelo usuário sem atualização de versão.

2.l) Deverá suportar filtragem automática de novas reflexões UDP, com base nas características do tráfego.

2.m) Deverá suportar filtragem automática da reflexão TCP, com base nas características do tráfego.

2.n) Deverá ter capacidade de detecção de ataque de DNS.

2.o) Deverá suportar defesa passiva de sub-domínios (CNAME) para defender ataques de inundação de origem forjada, contra servidores de autorização DNS.

2.p) Deverá suportar limitação de taxa baseada na origem, e limitação de taxa baseada em nome de domínio, para se defender de ataques de inundação de DNS de origem real.

2.q) Deverá suportar ataques de sites *HTTP Get/Post Flood* , com base em Cookie e autenticação *JavaScript.*

2.r) Deverá suportar defesa baseada em verificação de sessão contra vários tipos de ataques anormais de sessão HTTP, incluindo

ataques de massivos, ataques de amplificação de vários métodos, ataques de conexão vazia e ataques de conexão lenta.

2.s) O mecanismo de inspeção de endereço IP (com proxy) será suportado para evitar a interrupção do serviço causada pela comutação frequente de endereços IP de proxy e que ampliem ou façam sobrecarga dos DataCenters.

2.t) Deverá dispor de proteção refinada para aplicativos HTTPS, e defesa contra-ataques de inundação contra a porta 443, com base na autenticação de origem. Além disso, a análise de comportamento será usada para defender de contra-ataques de acesso de alta frequência.

2.u) Deverá suportar aprendizado dinâmico refinado de linhas de base de tráfego. O resultado da aprendizagem poderá ser usado como o limite de defesa.