Ao
Tribunal de Justiça do Amazonas – TJAM
Comissão Permanente de Licitação – CPL

Pregão Eletrônico SRP nº 017/2020 – TJAM
Processo Administrativo nº 2019/34139
Objeto: Registro de preços para eventual Renovação e Aquisição de Solução de Firewall da Nova Geração visando atender as necessidades do atual cenário e aumento da capacidade operacional do site principal do TJAM, para atender ao Tribunal de Justiça do Amazonas, por um período de 12 (doze) meses, conforme especificações e condições definidas no Termo de Referência do edital.

PROPOSTA COMERCIAL

A empresa Servix Informática Ltda., inscrita no CNPJ sob o nº 01.134.191/0003-09, estabelecida na Rua Santos Dumont nº 57, Sala 202, Centro, Ilhéus – BA, CEP 45653-380, por intermédio de seu representante legal o Sr. Vanderlei Arcanjo Carnielo Calejon, empresário, portador da Carteira de Identidade RG nº 5412384 e inscrito no CPF sob o nº 736.875.028-72, telefone nº (11) 3525-3420, e-mail editais@servix.com, apresenta sua proposta nas condições que seguem:

LOTE 01					
Item	**Descrição**	**Unid.**	**Qtd.**	**Valor Unitário**	**Valor Total**
1	Renovação de Suporte e Garantia com 3 anos de suporte 24x7 em Alta Disponibilidade – Código do Produto: PAN-SVC-PREM-3060-3YR-R.	Un	2	R$230.796,00	R$461.592,00
2	Renovação de Licença de Filtro de URL com 3 anos em Alta Disponibilidade - Código do Produto: PAN-PA-3060-URL4-3YR-HA2-R.	Un	2	R$171.342,00	R$342.684,00
3	Renovação de Licença de Funcionalidade Prevenção à Ameaças com 3 anos em Alta Disponibilidade - Código do Produto: PAN-PA-3060-TP-3YR-HA2-R.	Un	2	R$171.342,00	R$342.684,00
4	Renovação de Licença de Funcionalidade Análise de Malware com 3 anos em Alta Disponibilidade -	Un	2	R$171.342,00	R$342.684,00

	Código do Produto: PAN-PA-3060-WF-3YR-HA2-R.				
5	Renovação de Licença de Gerência Centralizada com 3 anos de suporte 24x7 - Código do Produto: PAN-SVC-PREM-PRA-25-3YR	Un	1	R$72.780,00	R$72.780,00
6	PAN 210 - Firewall 9.x: Essentials - Configuration and Management - Presencial ou Online em Tempo Real.	Un	3	R$21.414,00	R$64.242,00
7	PAN- 330 Firewall: Troubleshooting v 9 - Presencial ou Online em Tempo Real.	Un	3	R$14.832,00	R$44.496,00
				VALOR TOTAL DO LOTE	R$ 1.671.162,00
LOTE 02					
1	Firewall de Próxima Geração Palo Alto Modelo 5220 - Código do Produto: PAN-PA-5220-AC.	Un	2	R$ 1.002.222,00	R$ 2.004.444,00
2	Suporte e Garantia com 3 anos de suporte 24x7 em Alta Disponibilidade – Código do Produto: PAN-SVC-PREM-5220-3YR.	Un	2	R$ 399.169,00	R$ 798.338,00
3	Licença de Filtro de URL com 3 anos em Alta Disponibilidade - Código do Produto: PAN-PA- 5220-URL4-3YR-HA2.	Un	2	R$ 212.676,00	R$ 425.352,00
4	Licença de Prevenção à Ameaças com 3 anos em Alta Disponibilidade - Código do Produto: PAN-PA-5220-TP-3YR-HA2-.	Un	2	R$ 212.676,00	R$ 425.352,00
5	Licença de Análise de Malware com 3 anos em Alta Disponibilidade - Código do Produto: ANPA-5220- WF-3YR-HA2-.	Un	2	R$ 212.676,00	R$ 425.352,00
				VALOR TOTAL DO LOTE	R$ 4.078.838,00
				VALOR GLOBAL	R$ 5.750.000,00

Valor total da proposta: R$ 5.750.000,00 (Cinco milhões e setecentos e cinquenta mil reais)

Dados Bancários: Itaú(341), Agência nº 0383, Conta Corrente nº 14835-0.

Validade da proposta: 60 (sessenta) dias.

Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer

tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Ilhéus, 17 de agosto de 2020.

VANDERLEI ARCANJO CARNIELO CALEJON:73687502872

Digitally signed by VANDERLEI ARCANJO CARNIELO CALEJON:73687502872
Date: 2020.08.17 10:30:06 -03'00'

Servix Informática Ltda.

Proposta Técnica:

Especificações Básicas:
Solução de proteção de rede com características de Próxima Geração (NGFW) para segurança de informação perimetral que inclui filtro de pacote, 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, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta;
Compatível com a ferramenta de gerenciamento centralizada de segurança de rede panorama.
Por plataforma de segurança entende-se hardware e software integrados do tipo appliance.
Caracteristicas gerais:
A plataforma de segurança possui a capacidade e as características abaixo, por equipamento:
Throughput de 16 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possui;
Throughput de 8 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possui devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware.
Os throughputs são comprovados por documento de domínio público do fabricante.
Os documentos públicos comprovam os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend);

Suporta, no mínimo, 3.800.000 de conexões simultâneas;
Suporta, no mínimo, 110.000 novas conexões HTTP por segundo;
Possui Fonte 120/240 AC ou DC, redundante e hot-swappble;
Possui Cooler hot-swappble;
Possui Disco Solid State Drive (SSD) redundante de, no mínimo, 240 GB.
Possui Discos de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de firewall;
Possui No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;
Possui No mínimo, 08 (oito) interfaces de rede 1 Gbps SFP;
Possui No mínimo, 08 (oito) interfaces de rede 10 Gbps SFP+;
Possui No mínimo, 04 (quatro) interfaces de rede 40 Gbps QSFP+;
Possui 2 (duas) Gbps interfaces dedicadas para alta disponibilidade sendo pelo menos uma do tipo 40 Gbps QSFP+;
Possui 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
Possui 1 (uma) interface do tipo console ou similar;
Suporta, no mínimo, 60 (sessenta) zonas de segurança;
Esta licenciada para, 10.000 (dez mil) clientes de VPN SSL simultâneos;
Esta licenciada para, 3.000 (três mil) túneis de VPN IPSEC simultâneos;
Suporta, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;
Os contextos virtuais suportam as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;
A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, interface de rede e sistema operacional dedicados para esta função;
Nenhum dos modelos ofertados estão listados no site do fabricante em listas de end-of-life e end-of-sale;
A solução consiste de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) e console de gerência e monitoração;
Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
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;
A plataforma é otimizada para análise de conteúdo de aplicações em camada 7;
O hardware e software que executam as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, são do tipo appliance.
Todos os equipamentos serão fornecidos com trilho para montagem em rack 19 incluindo o kit de adaptação se necessário e cabos de alimentação;
O software será fornecido em sua versão mais atualizada;
Os dispositivos de proteção de rede possuem pelo menos as seguintes funcionalidades:
Suporte a 4094 VLAN Tags 802.1q;
Possui Agregação de links 802.3ad e LACP;
Possui Policy based routing ou policy based forwarding;
Possui Roteamento multicast (PIM-SM);
Possui DHCP Relay;
Possui DHCP Server;
Possui suporte a Jumbo Frames;

Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
Suporta sub-interfaces ethernet logicas.
Suporte a, no mínimo, 15 (quinze) roteadores virtuais na mesma instância de firewall;
O firewall tem a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve esta comunicável através de uma rota. Caso haja falha na comunicação o firewall tem a capacidade de usar rota alternativa para estabelecer a comunicação;
Suporta os seguintes tipos de NAT:
Nat dinâmico (Many-to-1);
Nat dinâmico (Many-to-Many);
Nat estático (1-to-1);
NAT estático (Many-to-Many);
Nat estático bidirecional 1-to-1;
Tradução de porta (PAT);
NAT de Origem;
NAT de Destino;
Suporta NAT de Origem e NAT de Destino simultaneamente;
Implementa Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
Implementa o protocolo ECMP;
Implementa balanceamento de link por hash do IP de origem;
Implementa balanceamento de link por hash do IP de origem e destino;
Implementa balanceamento de link através do método round-robin;
Implementa balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Suporta o balanceamento de, no mínimo, quarto links;
Implementa balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

Implementa balanceamento de link através de políticas por aplicação e porta de destino;
Implementa o protocolo Link Layer Dicovery (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 dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
Pode enviar log para sistemas de monitoração externos, simultaneamente;
Existe opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
Permite configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
Proteção contra anti-spoofing;
Permite bloquear sessoes TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
Permite bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
Exibe nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
Para IPv4, suporta roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
Para IPv6, suporta roteamento estático e dinâmico (OSPFv3);
Suporta a OSPF graceful restat;
Suporta o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
Suporta 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 e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

O dispositivos de proteção tem a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
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;
Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
Em modo transparente;
Em layer 3;
A configuração em alta disponibilidade sincroniza:
Sessões;
Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
Certificados de-criptografados;
Associações de Segurança das VPNs;
Tabelas FIB;
O HA (modo de Alta-Disponibilidade) possibilita monitoração de falha de link.
As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico operam 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.
Controle de Politica por Firewall
Suporta controles por zona de segurança.
Suporta controles de políticas por porta e protocolo.

Suporta controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
Suporta controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
Suporta a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.
Permite autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
Permite consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
Suporta controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
Suporta controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
Suporta offload de certificado em inspeção de conexões SSL de entrada (Inbound);
Suporta de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
Suporta de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
Suporta controle de inspeção e de-criptografia de SSH por política;
A de-criptografia de SSH possibilita a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
A plataforma de segurança implementa espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
Suporta bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
Possui Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
Possui QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
Possui Suporte a objetos e regras IPV6.

Possui Suporte a objetos e regras multicast.
Suporta no mínino três tipos de negação de tráfego nas políticas de firewall: 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;
Suporta a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
Controle de Aplicações
Os dispositivos de proteção de rede possuem a capacidade de reconhece aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
Suporta a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
Reconhece pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
Reconhece pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
Inspeciona o payload de pacote de dados com o objetivo de detectar através 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 389;
Aplica heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

Identifica o uso de táticas evasivas, ou seja, tem 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.
Para tráfego criptografado SSL, pode de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
Realiza 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 pode 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;
Permite a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Permite também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
Permite habilitar aplicacões SAAS apenas no modo corporativo e bloquea-las para uso pessoal, tais como: office 365, Skype, aplicativos do Google e etc.
Identifica o uso de táticas evasivas via comunicações criptografadas;
Atualiza a base de assinaturas de aplicações automaticamente;
Reconhece aplicações em IPv6;
Limita a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
Os dispositivos de proteção de rede possuem a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
Pode 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;

Suporta múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
Para manter a segurança da rede eficiente, suporta o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
Permite 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;
Permite o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
Permite a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
Pode alertar o usuário quando uma aplicação for bloqueada;
Pode possibilitar que o controle de portas seja aplicado para todas as aplicações;
Permite criar filtro na tabela de regras de segurança para exibir somente:
Pode conter regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta de- terminada regra;
Possui aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
Possui acesso a regras de segurança onde não houve passagem de tráfego nos últi- mos 90 dias.
Possibilita a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, ne- onet, etc.) possuindo granularidade de controle/politicas para os mesmos;
Possibilita a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;

Possibilita a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
Possibilita a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;
Possibilita a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
Possui Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).
Possui Nível de risco da aplicação.
Possui Categoria e sub-categoria de aplicações.
Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.
Prevenção de ameaças
Para proteção do ambiente contra ataques, os dispositivos de proteção possuem módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance.
Inclui assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
As funcionalidades de IPS, Antivírus e Anti-Spyware podem 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.
Sincroniza as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo
Implementa 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;
Possui a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;
As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
Suporta granularidade nas politicas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
Permite o bloqueio de vulnerabilidades.
Permite o bloqueio de exploits conhecidos.
Inclui proteção contra ataques de negação de serviços.
Suporta a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
Posssui os seguintes mecanismos de inspeção de IPS:
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;
Bloqueio de pacotes malformados.
É imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
Detecta e bloqueia a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
Bloqueia ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
Suporta 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;

Possui assinaturas específicas para a mitigação de ataques DoS e DDoS;
Possui assinaturas para bloqueio de ataques de buffer overflow;
Pode possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
Permite usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
Permite o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
Permite 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;
Suporta bloqueio de arquivos por tipo;
Identifica e bloquear comunicação com botnets;
Suporta varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
Suporta referencia cruzada com CVE;
Registra 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;
Suporta a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;
Permite que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura Permite selecionar, no mínimo, 50 pacotes;
Possui 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;
Permite o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
Os eventos devem identificar o país de onde partiu a ameaça;
Inclui proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

Possui proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.
Possui rastreamento de vírus em pdf.
Permite a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
Permite a configuração de diferentes políticas de controle de ameaças e ataques baseado em politicas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada politica de firewall poderá ter uma configuração diferentes de IPS, sendo essas politicas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
Análise de malwares modernos
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 possui funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
O dispositivo de proteção é capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
Seleciona através 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;
Possui 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 deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;
Suporta a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
Suporta a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7;

Suporta 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;
A solução possui a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;
A análise de links em sand-box deve é capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
Para ameaças trafegadas em protocolo SMTP e POP3, a solução tem a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
O sistema de análise “In Cloud” ou local provê 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);
O sistema automático de analise "In Cloud" ou local permite emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;
Permite exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
Permite o download dos malwares identificados a partir da própria interface de gerência;
Permite visualizar o resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
Permite informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.
Suporta a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

Suporta a análise de arquivos do pacote office (.doc, .docx, xls, xlsx, ppt, pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-0, DMG e PKG), Linux (ELF), RAR e 7zip no ambiente sandbox;
Pode atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequencia de pelo menos 5 minutos;
Permite o envio de arquivos e links para analise no mabiente controlado de forma automatica via API
Permite o envio para analise em sand-box de malwares bloqueados pelo antivirus da solucão.
Filtro de url
A plataforma de segurança possui as seguintes funcionalidades de filtro de URL:
Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
Permite a criação de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
Permite 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.
Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
Permite bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;
Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
Possui pelo menos 60 categorias de URLs;
Permite classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
Possui categoria especifica para classificar domínios recém registrados (com menos de 32 dias);
A solução tem a capacidade de classificar sites em mais de uma catego- ria, de acordo com a necessidade;

A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
Suporta a criação categorias de URLs customizadas;
Suporta a exclusão de URLs do bloqueio, por categoria;
Permite a customização de página de bloqueio;
Permite proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
Permite bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução;
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);
Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
Permite salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;
Identificação de Usuários
Permite incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
Possui integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
Possui integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

Implementa a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
Possui integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
Suporta o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
Permite 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);
Permite a autenticação Kerberos;
Suporta autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
Possui 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;
Permite identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
Permite a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;
Suporta e opera com 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 detarminados acessos internos e externos a organização.
Implementa a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

Possui suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.
QOS
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, a solução, além de poder permitir ou negar esse tipo de aplicações, tem 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.
Suporta a criação de políticas de QoS por:
Endereço de origem
Endereço de destino
Por usuário e grupo do LDAP/AD.
Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
Por porta;
O QoS possibilita a definição de classes por:
Banda Garantida
Banda Máxima
Fila de Prioridade
Suporta priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
Suporta marcação de pacotes Diffserv, inclusive por aplicação;
Permite implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);
Disponibilizar estatísticas RealTime para classes de QoS.
Suporta QOS (traffic-shapping), em interface agregadas;
Permite o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

Filtro de dados
Permite a criação de filtros para arquivos e dados pré-definidos;
Os arquivos podem ser identificados por extensão e assinaturas;
Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
Suporta identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;
Permite 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;
Permite listar o número de aplicações suportadas para controle de dados;
Permite listar o número de tipos de arquivos suportados para controle de dados;
Geo-Localização
Suporta a criação de politicas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.
Possibilita a visualização dos países de origem e destino nos logs dos acessos.
Permite visualizar nos logs e criar politicas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;
Possibilita a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.
VPN
Suporta VPN Site-to-Site e Cliente-To-Site;
Suporta IPSec VPN;
Suporta SSL VPN;
A VPN IPSEc suporta:
DES e 3DES;
Autenticação MD5 e SHA-1;

Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
Algoritmo Internet Key Exchange (IKEv1 e v2);
AES 128, 192 e 256 (Advanced Encryption Standard)
Autenticação via certificado IKE PKI.
Possui interoperabilidade com os seguintes fabricantes:
Cisco;
Checkpoint;
Juniper;
Palo Alto Networks;
Fortinet;
Sonic Wall;
Permite habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
A VPN SSL suporta:
O usuário pode realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
A funcionalidades de VPN SSL podem ser atendidas com ou sem o uso de agente;
Atribuição de endereço IP nos clientes remotos de VPN SSL;
Permite a atribuição de IPs fixos nos usuários remotos de VPN SSL;
Permite a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
Permite 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;
Atribuição de DNS nos clientes remotos de VPN;
Permite que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);

A solução de VPN pode verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
Possui lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
Permite a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
Exibe mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Permite que o usuário desabilite a exibição da mensagem nas conexões seguintes;
Permite avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Permite também a customização da mensagem com informações relevantes para o usuário;
Permite criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
A VPN SSL suporta proxy arp e uso de interfaces PPPOE;
Suporta autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
Permite a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
Possui lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
Suporta leitura e verificação de CRL (certificate revocation list);
Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
O agente de VPN a ser instalado nos equipamentos desktop e laptops, pode ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

O agente pode comunicar-se com o portal para determinar as políticas de segurança do usuário,
Permite que a conexão com a VPN SSL seja estabelecida das seguintes formas:
Antes do usuário autenticar na estação;
Após autenticação do usuário na estação;
Sob demanda do usuário;
Permite manter uma conexão segura com o portal durante a sessão.
O agente de VPN SSL client-to-site é compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;
O portal de VPN pode enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
Permite a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
Possui a capacidade de identificar se a origem da conexão de VPN é externa ou interna;
Console de gerência e monitoração
Permite a adminis tração de regras e políticas do cluster, usando uma única interface de gerenciamento;
O gerenciamento da solução suporta acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
Permite 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;
O gerenciamento permite:
Criação e administração de políticas de firewall e controle de aplicação;
Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
Criação e administração de políticas de Filtro de URL;
Monitoração de logs;
Ferramentas de investigação de logs;

Debugging;
Captura de pacotes.
Acesso concorrente de administradores;
Permite que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador
Pode 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.
Possui mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
Possui um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
Permite usar palavras chaves e cores para facilitar identificação de regras;
Permite monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
Suporta também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
Permite a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
Permite a Autenticação integrada ao Microsoft Active Directory e servidor Radius;
Permite a Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

Pode atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
Permite a Criação de regras que fiquem ativas em horário definido;
Permite a Criação de regras com data de expiração;
Permite a Backup das configurações e rollback de configuração para a última configuração salva;
Suporta Rollback de Sistema Operacional para a ultima versão local;
Tem a habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
Possui mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
Permite a validação de regras antes da aplicação
Implementa mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
Permite a validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
Possibilita a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
Permite auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
Possibilita a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
Permite a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
Tem a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

Permite a geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
Permite prover relatórios com visão correlacionada de aplicações e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
Permite a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários e tráfego bloqueado;
Permite o gerenciamento da solução possibilita a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
Permite a visualização dos logs de tráfego e malwares modernos (IP de origem, destino, usuário e porta), aplicação e filtro de arquivos em uma única tela;
Possui relatórios de utilização dos recursos por aplicações, URL, ameaças que passaram pela solução;
Provê uma visualização sumarizada de todas as aplicações que passaram pela solução;
Possui mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
Nas opções de "Drill-Down", é possível identificar o usuário que fez determinado acesso;
Possui relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também pode mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
Os relatórios de visibilidade e uso sobre aplicativos (SaaS) podem ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
Permite exportar os logs em CSV;
Permite acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
Rotação do log;
Permite que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

Permite fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
Permite a exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
Permite a exibição da Situação do dispositivo e do cluster
Permite a exibição das Principais aplicações;
Permite a exibição das Principais aplicações por risco;
Permite a exibição dos Administradores autenticados na gerência da plataforma de segurança;
Permite a exibição do Número de sessões simultâneas
Permite a exibição do Status das interfaces;
Permite a exibição do Uso de CPU;
Realiza a Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
Mostra um Resumo gráfico de aplicações utilizadas;
Permite a exibição das Principais aplicações por utilização de largura de banda de entrada e saída;
Permite a exibição das Principais aplicações por taxa de transferência de bytes;
Permite a exibição dos Principais hosts por número de ameaças identificadas;
Permite a exibição das Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas de rede vinculadas a este tráfego;
Permite a criação de relatórios personalizados;
Em cada critério de pesquisa do log pode incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde pode definir um faixa de tempo como critério de pesquisa;
Pode gerar alertas automáticos via:
Email;
SNMP;
Syslog;

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