SERVIÇO MUNICIPAL DE ÁGUA E ESGOTO – SEMAE
Autarquia Municipal - Lei Municipal n.º 1.657 de 30 de abril de 1969
Rua XV de Novembro, 2.200 – Piracicaba/SP – CEP 13.417-100
Fone: (19) 3403-9611 - ramal 9686
www.semaepiracicaba.sp.gov.br

DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

Contratação de empresa especializada para cessão de uso de solução corporativa padronizada de segurança da informação contemplando servidores (hardware e software) do tipo UTM (Unified Threat Management) e SMX (Secure eMail eXchange) pelo período de 24 meses, com possibilidade de renovação por mais 24 meses.

1- A CONTRATADA deverá disponibilizar 2 (dois) appliances novos, idênticos, do mesmo fabricante e modelo, de primeiro uso, em linha de fabricação e em perfeito estado de conservação com as seguintes características:

1.1 Appliance de 8000 Mbps de capacidade de firewall com garantia e atualização para 24 meses, com possibilidade de renovação por mais 24 meses.

1.2 O equipamento deve se instalar em rack com largura padrão de 19 polegadas, ocupando no máximo 1U do referido rack;

1.3 Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;

1.4 Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

1.5 Possuir painel do tipo LCD com informações do Sistema, data/hora e Endereçamento IP;

1.6 Possuir painel/led indicador on/off, disco e devices de rede;

1.7 Possuir throughput de no mínimo 8000 Mbps para tráfego TCP;

1.8 Possuir throughput de no mínimo 15000 Mbps para tráfego UDP;

1.9 Suportar no mínimo 2.000.000 (2 milhões) conexões simultâneas;

1.10 Suportar no mínimo 100.000 (cem mil) novas conexões por segundo;

1.11 Possuir throughput de no mínimo 3600 Mbps para tráfego HTTP/ HTTPS via proxy;

Procuradoria Jurídica SEMAE

1.12 Possuir throughput de no mínimo 800 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;

1.13 Possuir throughput de no mínimo 600 Mbps para tráfego HTTP/ HTTPS com inspeção SSL + Inspeção ATP via proxy;

1.14 Possuir throughput de no mínimo 2500 Mbps para tráfego IPS;

1.15 Possuir throughput de no mínimo 2000 Mbps para tráfego ATP;

1.16 Possuir throughput de no mínimo 3000 Mbps para tráfego VPN IPSEC com criptografia (AES-128);

1.17 Possuir throughput de no mínimo 1800 Mbps para tráfego VPN SSL com criptografia (AES-128);

1.18 Suportar no mínimo 400 conexões de usuários concorrentes para VPN SSL;

1.19 Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade;

1.20 Permitir expandir no mínimo 16 interfaces GbE RJ45 ou 4 LANs 10GbE SFP+;

1.21 Possuir no mínimo de 3(três) devices de rede GbE By-pass;

1.22 Possuir no mínimo 16 GB de memória RAM;

1.23 Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;

1.24 Possuir mínimo de 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;

1.25 Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

1.26 Deve suportar no mínimo 2.000 contas de e-mail.

2- Especificações gerais do software UTM:

2.1 Características da solução:

2.1.1 Solução UTM ("Unified Threat Management", Gerenciador Unificado de Ameaças), integrada com os

demais recursos e serviços, deve ser capaz de instalar todos os recursos e serviços em um mesmo hardware.

2.2 Recursos e serviços gerais:

2.2.1 Deve suportar tecnologia de Firewall Stateful Packet Inspection;

2.2.2 Possuir conexão entre a estação de gerência e Appliance no modo criptografado tanto em interface gráfica, quanto em CLI (linha de comando). O Acesso a interface de administração deve ser via WEB sob o protocolo HTTPS com ergonomia voltada a usabilidade;

2.2.3 Gerenciamento do tráfego e estatísticas sumarizadas através de um painel de controle;

2.2.4 Possuir sistemas de alertas e notificações do sistema em tempo real na interface WEB e envios automáticos por e-mail;

2.2.5 Interface responsiva compatível com dispositivos móveis;

2.2.6 Interface em português e inglês;

2.2.7 O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

2.2.8 Permitir a criação de perfis de administração baseado em ACL (Acess List), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;

2.2.9 Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

2.2.10 Permitir criar as definições de ACL (Acess List) completa por administrador, sendo possível especificar os direitos, como: somente Visualizar ou Editar "Alterar, Excluir, Cadastrar";

2.2.11 Permitir auditoria do sistema com log das ações;

dos administradores por tipo de recurso e período;

2.2.12 Possuir porta console para possíveis manutenções no produto;

2.2.13 Acesso via WEB a console shell para gerenciamento através de interface de linha de comando CLI (Command Line Interface). Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

2.2.14 A interface CLI deve suportar a configuração de roteamento dinâmico no mínimo para os protocolos BGP, OSPF, RIP1 e RIP2 com suporte a interface Vty;

2.2.15 Possuir um Certificado digital (CA - Certificado de Autoridade) padrão X.509, nativo com chaves de 2048 bits, para os processos de autenticação do usuário, utilização do proxy SSL e em todas as conexões de serviços com o Appliance.

2.2.16 A solução deve manter um canal de comunicação segura, com criptografia baseada em certificados entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

2.2.17 Permitir a integração com qualquer autoridade certificadora válida emissora de certificados X509 que deve seguir os padrões descritos na RFC 2459.

2.2.18 Capacidade para criação de objetos com a finalidade de facilitar a administração e configuração do sistema, deve atender no mínimo os seguintes tipos de objetos: endereço IP, endereço MAC, portas de serviços e protocolos, atendendo no mínimo os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP, e SCTP), tabela de horário, período com especificação de data/hora inicial e final, tabela de palavras chaves com a possibilidade de especificar expressões regulares, tipos de conteúdo de arquivos (content types);

2.2.19 Possuir um sistema de armazenamento remoto com

suporte a conexões do tipo SMB, NFS e Disco (USB-HDD);

2.2.20 Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

2.2.21 As cópias de segurança (backups) devem ser armazenadas em dispositivos remotos do tipo NFS (Network File System) ou Disco externo (USB-HDD);

2.2.22 O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

2.2.23 As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

2.2.24 O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

2.2.25 Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

2.2.26 Suporte e integração com servidores de Network Time Protocol (NTP) para atualização de data e hora do sistema, o que padroniza e evita problemas com o horário de verão;

2.2.27 Atualização automática do sistema para correções e releases. O sistema de atualização deve permitir agendamento para verificação diária da base de atualizações do fabricante.

2.2.28 As atualizações devem ser disponibilizadas no intervalo máximo de 15 dias. Não podendo ultrapassar este período;

2.2.29 Permitir desabilitar update automático;

Procuradoria Jurídica SEMAE

2.2.30 Efetuar controle de tráfego e monitor por estado de conexão no mínimo para os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP e SCTP) baseados nos endereços de origem, destino e porta;

2.2.31 Suportar o Internet Protocol Versões 4 (IPv4);

2.2.32 Suporte à Interfaces Ethernet;

2.2.33 Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;

2.2.34 Suportar o protocolo 802.1x, para autenticação RADIUS;

2.2.35 Suporte a interfaces do tipo MACVLAN;

2.2.36 Suportar o protocolo 802,1ax e 802.3ad (LACP), Link Aggregation Control Protocol;

2.2.37 Suporte à interfaces DSL;

2.2.38 Suporte à roteamento estático;

2.2.39 Suporte ao protocolo SNMP;

2.2.40 A solução deve suportar no mínimo o funcionamento com 2 (dois) equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

2.3 Autenticação:

2.3.1 Suporte à múltiplos domínios de autenticação, mínimo 3(três) domínios;

2.3.2 Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de administração WEB do dispositivo;

2.3.3 Suporte à sincronismo de usuários e grupos com servidores Windows AD® e Servidores LDAP;

2.3.4 Permitir a utilização de LDAP, LDAP/SSL para a autenticação de usuários;

2.3.5 Permitir a utilização de autenticação RADIUS para sincronismo de contas e sessões;

2.3.6 Permitir o login de usuários de forma transparente ao efetuar logon na rede para plataformas Windows 2008 e 2012 Servers (sem a necessidade de o usuário digitar novamente a senha), para todos os serviços

suportados, considerando assim a autenticação do usuário, como uma autenticação unificada entre a plataforma Windows e o Appliance Firewall NG UTM;

2.3.7 Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via portal WEB para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente carregado;

2.3.8 Possuir suporte a um sistema de autenticação do tipo Captive Portal capaz de redirecionar de forma automática a autenticação, deve ser compatível com autenticação Windows AD®, LDAP, RADIUS e LOCAL;

2.3.9 O Captive Portal deve suportar o protocolo HTTPS para a tela de autenticação do usuário e para administração dos serviços de Captive Portal para o usuário;

2.3.10 A solução deve permitir em seu portal de autenticação o cadastro de novos usuários, permitindo controle por área, para usuários convidados o Captive Portal solicitará informações para cadastro no sistema, enquadrando automaticamente à um perfil de acesso previamente configurado;

2.3.11 O sistema de Captive Portal deve ser capaz de aplicar uma política geral e gerenciar a sessão do usuário autenticado:

2.3.12 Controlar o número de sessões concorrentes por usuário;

2.3.13 Controlar o número de tentativas de autenticação não autorizada;

2.3.14 Bloquear o endereço IP de origem das tentativas de autenticação não autorizada;

2.3.15 Definir o tempo de bloqueio do endereço IP das tentativas de autenticação não autorizada;

2.3.16 Definir tempo de sessão por inatividade;

2.3.17 Identificar endereço IP;

2.3.18 Identificar endereço MAC;

Procuradoria Jurídica SEMAE

2.3.19 Permitir o administrador efetuar logout de sessão de qualquer usuário através da interface de gerenciamento WEB da solução de firewall;

2.3.20 Os usuários devem ter acesso à alguns recursos tais como: alterar dados pessoais; alterar senha para os casos de usuário do tipo local; fazer o download do Certificado de Autoridade (CA) e acesso ao Termos de Uso;

2.4 Segurança:

2.4.1 Prover a condição de configuração de uma Política padrão por agrupamento de devices ou zonas de rede, determinando origem e destino por tipo de agrupamento;

2.4.2 Possibilitar exigir autenticação para a política padrão;

2.4.3 Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022; ser capaz de aplicar mascaramento de pacotes do tipo: SNAT (source nat) por endereço IP de origem; SNAT (masquerade) por device de origem; DNAT (dnat) mascaramento de destino por endereço IP/porta de destino e Nat-T em VPN IPSec;

2.4.4 Prover mecanismos de segurança configuráveis, que permita habilitar proteção contra ataques do tipo: "Denied of Service; Portscan; Pacotes inválidos; SYN Flood; ICMP Flood";

2.4.5 Possuir mecanismo que permita habilitar e desabilitar recursos do tipo: "ICMP Echo/Request - ping; ICMP Redirect; ICMP Broadcast; Source Routing; Checksum; Log Inválidos; TCP be liberal";

2.4.6 Possuir mecanismo de configuração para o controle de tipos de conexão possibilitando definir limites máximos para cada tipo de controle das conexões do protocolo TCP;

2.4.7 Possuir mecanismo de configuração para o controle de conexão possibilitando definir limites de timeout para as conexões genéricas;

2.4.8 Possuir mecanismo de configuração para o controle de conexão do protocolo ICMP possibilitando definir limites de timeout;

2.4.9 Possuir mecanismo de configuração para o controle de conexão do protocolo UDP possibilitando definir limites de timeout;

2.4.10 Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;

2.4.11 Possuir politicas padrões de entrada para os serviços nativos do firewall, por agrupamento de device ou zonas de rede, podendo exigir ou não autenticação, com possibilidade de aplicar ações de bloqueio, permissão, inspeção IPS ou inspeção ATP;

2.4.12 Permitir definir as políticas de entrada para os serviços nativos do firewall, podendo aplicar filtros no acesso por: usuário, grupos, endereço IP de origem, endereço IP de destino e horário;

2.5 Proxy:

2.5.1 Possuir Proxy nativo para tráfego HTTP, HTTPS, versões 1.0 e 1.1, FTP;

2.5.2 Deve possibilitar a conexão de tráfego para outros serviços e que contemplem a conexão em proxys HTTP, tais como: XMPP, SIP, H323, SMTP, POP3, IMAP, RTSP, TELNET e outros;

2.5.3 Deve permitir a configuração para outras portas de serviços;

2.5.4 Deve permitir implementar proxy transparente para os protocolos HTTP e HTTPS, de forma a dispensar a configuração dos browsers dos dispositivos clientes para a utilização das características o serviço;

2.5.5 Deve permitir implementar proxy configurado para os protocolos HTTP, HTTPS, FTP e SOCKS;

Procuradoria Jurídica SEMAE

2.5.6 Deve permitir o armazenamento em cache de conteúdo trafegado pelo protocolo HTTP e HTTPS;

2.5.7 Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

2.5.8 Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

2.5.9 Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

2.5.10 Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

2.5.11 Deve permitir operar sem interceptação SSL;

2.5.12 Possibilitar a integração com servidores de cache WEB externos;

2.5.13 Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;

2.5.14 Deve ser capaz de armazenar cache dinâmicos de streaming no mínimo para endereços do Youtube® e MSN Vídeos®;

2.5.15 Deve ter capacidade de armazenar em cache dinâmicos conteúdo do Facebook®, Google Maps® e Sourceforge Downloads®;

2.5.16 Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

2.5.17 Deve ter suporte à integração com antivírus HTTP através de hierarquia de proxy;

2.5.18 Possuir mecanismos de integração à interceptação SSL com suporte a conexões de proxy transparente ou proxy configurado;

2.5.19 Ter a capacidade de análise de HTTP e HTTPS, pelo Antimalware se determinados tipos de arquivos baseados na extensão contém vírus antes de entregá-lo ao usuário e suportar ao menos 2 scanners;

2.5.20 Ter a capacidade de trabalhar como Anti-Virus de Gateway permitindo a análise de arquivos específicos por extensão;

2.5.21 Permitir o gerenciamento de quarentena de Malware;

2.5.22 Permitir realizar Filtro de Conteúdo por Autoridade Certificadora;

2.5.23 Permitir desabilitar interceptação de SSL por domínio;

2.6 Sistema de proteção avançada contra ameaças:

2.6.1 Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

2.6.2 O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.

2.6.3 Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

2.6.4 A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

2.6.5 A base de assinaturas deve possuir mínimo de 2(duas) modalidades de assinaturas, atendendo a identificação de ameaças e aplicativos;

2.6.6 Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

2.6.7 O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

2.6.8 Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

Procuradoria Jurídica SEMAE

2.6.9 Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

2.6.10 Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

2.6.11 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.

2.6.12 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;

2.6.13 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSN Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

2.6.14 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

2.6.15 Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para

6(seis) categorias, capaz de permitir seleção por categorização, elas devem atender as seguintes classificações: spam, reputation, malware, attacks, anonymous e abuse;

2.6.16 Possuir mecanismo de bloqueio e proteção por localização GeoIP para uma lista mínima de 250 Países e Repúblicas;

2.6.17 Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar aplicações criptografadas incluindo todo o payload;

2.6.18 Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

2.6.19 Suportar exceção de aplicativos por assinatura, IP de origem ou IP de destino;

2.6.20 Suportar exceção para base de reputação IP por endereço IP;

2.6.21 Suportar exceção para a base de localização GeoIp por endereço IP;

2.6.22 Ação de Bloqueio do pacote ou reset da conexão em tempo real;

2.6.23 Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";

2.6.24 Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

2.6.25 Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

2.6.26 Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

Procuradoria Jurídica SEMAE

2.6.27 Todos os logs e registros devem permitir ser gerados por período: "diário ou mensal";

2.6.28 Possuir mecanismos para inspecionar, identificar e detectar os aplicativos e sub aplicativos trafegados via proxy e classificá-los de acordo com a base de assinaturas;

2.6.29 Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy e classificá-los de acordo com a base de assinaturas;

2.6.30 Deve permitir o bloqueio em caso de detecção dos aplicativos e ou ameaças e atacantes, com base nas políticas de cada assinatura;

2.7 Sistema de prevenção contra intrusão:

2.7.1 Possuir sistema de prevenção contra intrusão de atacantes (IPS) nativo;

2.7.2 O Sistema de IPS deve monitorar, analisar o trafego e proteger a rede contra ataques internos e externos e utilizar técnicas de varredura e identificação que filtrem e bloqueie os pacotes atacantes e descarte o pacote com conteúdo de código malicioso;

2.7.3 Deve ser baseado na identificação de assinaturas de tipos de ataques e aplicações com vulnerabilidades conhecidas. O IPS deve contemplar uma base de assinaturas capaz de identificar o método de ataque com base em modelos de comportamento, características dos protocolos de rede, sistemas operacionais, inclusive comandos executados e esse conjunto de informações deve permitir que o pacote malicioso seja identificado e bloqueado em tempo real pelo IPS.

2.7.4 Possuir pelo menos 18000 mil (dezoito mil) assinaturas;

2.7.5 O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

2.7.6 Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

2.7.7 A base de assinaturas deve contemplar um mínimo de 65 (sessenta e cinco) categorias, atendendo a identificação de ameaças e atacantes;

2.7.8 A solução deve ser capaz de detectar e prevenir as seguintes ameaças: Exploits e vulnerabilidades específicas de clientes e servidores, mau uso de protocolos, comunicação outbound de malware, tentativas de tunneling, e ataques genéricos;

2.7.9 A solução deve prover mecanismos de proteção contra ataques dos serviços de rede e aplicações, protegendo pelo menos os seguintes serviços: aplicações web, serviços de, DNS, FTP, SNMP, Telnet, TFTP, serviços Windows (Microsoft Networking) e VoIP.

2.7.10 A solução deve prover mecanismos de proteção contra ataques as assinaturas relacionadas a web-server, IIS, Apache, MSSql, MySql para que seja usado para proteção específica de Servidores Web;

2.7.11 Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS), Exploits, Attack Response;

2.7.12 Detecção de ataques de RPC (Remote Procedure Call);

2.7.13 Deve prover mecanismos de Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

2.7.14 Deve prover mecanismos de Proteção contra ataques de ICMP (Internet Control Message Protocol);

2.7.15 Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar pacotes criptografados incluindo todo o payload;

2.7.16 Suportar exceção de ameaças por assinatura, IP

Procuradoria Jurídica SEMAE

de origem ou IP de destino;

2.7.17 Ação de Bloqueio do pacote ou reset da conexão em tempo real;

2.7.18 Deve possuir mecanismo para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

2.7.19 Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "ataques detectados" e os "ataques bloqueados";

2.7.20 Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre os tipos de ataques e usuários, os graus de impacto e usuários, ataques identificados e bloqueados;

2.7.21 Todos os logs e registros devem permitir ser gerados por período: "diário ou mensal";

2.7.22 Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy, e classificá-lo de acordo a base de assinaturas;

2.7.23 Deve permitir o bloqueio em caso de detecção de ameaças e atacantes, com base nas políticas de cada assinatura;

2.8 QOS:

2.8.1 Deve permitir especializar as redes de forma a melhorar sensivelmente a qualidade de conexão, tratando de forma diferenciada e especifica as transmissões que exijam maior e melhor qualidade da rede;

2.8.2 Deve possuir mecanismo que permita criar controles por fila de prioridade, mínima de 5(cinco) níveis;

2.8.3 Deve ser capaz de alterar a velocidade dos acessos por nível de prioridade;

2.8.4 Deve ser capaz de criar limites de banda máxima por fila de prioridade;

2.8.5 Deve ser capaz de criar garantia de banda mínima por

fila de prioridade;

2.8.6 Deve permitir a habilitação do controle de velocidade permitindo especificar a largura de banda ou velocidade Downstream e Upstream de cada barramento ou device;

2.8.7 Priorização de pacotes com suporte às tecnologias de tratamento ToS (Type of Service) e DSCP (DiffServ Code Point);

2.8.8 Permitir modificação de valores ToS para a priorização de roteamento dos pacotes;

2.8.9 Implementar no mínimo 5(cinco) níveis de roteamento e tipos de serviços, com configuração e marcação para códigos ToS através da interface gráfica;

2.8.10 Permitir modificação de valores DSCP dos pacotes para o DiffServ;

2.8.11 Implementar no mínimo 20 (vinte) classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;

2.9 Balanceamento de link:

2.9.1 Deve ser capaz de segmentar e priorizar o tráfego através das interfaces de rede;

2.9.2 Deve contemplar a função de roteamento por prioridade de links;

2.9.3 Deve ser "tolerante a falhas", ou seja, possuir recurso de FailOver;

2.9.4 Deve possuir mecanismos de controle de falhas de link, capaz de aplicar testes da disponibilidade em tempo real. Estes testes devem retornar para o sistema o status atual de cada link e em caso de falhas do link principal, este recurso deverá alterar o "gateway padrão" do sistema para o próximo link da lista de prioridades de links;

2.9.5 O serviço de FailOver de links deve possibilitar que os testes e monitoramento sejam realizados através do protocolo ICMP para endereços de hosts externos;

Procuradoria Jurídica SEMAE

2.9.6 O monitoramento no protocolo ICMP deve permitir inserir múltiplos endereços para verificação e o link principal somente será marcado como inativo se todos os hosts externos pararem de responder;

2.9.7 Deve possuir as seguintes opções de configurações para o monitoramento do link que fazem parte do FailOver e Balanceamento de link:

2.9.8 Intervalo de monitoramento;

2.9.9 Quantidade tentativas de testes por host ou número de falhas necessárias antes de marcar o link como inativo;

2.9.10 Permitir utilizar um link como principal e outro como secundário. O tráfego apenas será redirecionado (FailOver) quando o principal ficar indisponível, retornado ao estado anterior quando o principal ficar ativo novamente;

2.9.11 Deve suportar regras de roteamento dos serviços de saída do próprio dispositivo de firewall, podendo selecionar entre os links, inclusive definindo prioridade do tráfego;

2.9.12 Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não.

2.9.13 Permitir o balanceamento de links, inclusive com IPs dinâmicos para ADSL ou outra tecnologia de banda larga que não utilize IP Fixo;

2.9.14 Deve contemplar o recurso de balanceamento de links por políticas de segurança; podendo ser aplicadas por: origem, destino, conteúdo web, horário ou período de data e hora inicial e final, controles de tipo de conteúdo, tipo de pacote; políticas de mascaramento; políticas de proxy; usuário e grupos;

2.10 Controle de aplicativos web:

2.10.1 O controle de aplicativos web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado por tipo de aplicativo

e sub aplicativos em uso, deve ser baseado em decodificadores de assinaturas e protocolos.

2.10.2 O controle desses aplicativos devem permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamentos de devices podem utilizar ou não estes recursos, definindo inclusive dentro das suas características quais recursos de cada aplicativo poderão ser utilizados.

2.10.3 A base deve contemplar um número mínimo de 790 aplicativos e sub aplicativos diferentes, catalogados e classificados em categorias, mínima de 24 categorias;

2.10.4 Possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de especificar endereço de origem ou destino das aplicações, para as tomadas de ação;

2.10.5 Reconhecer no mínimo aplicações do tipo redes sociais, aplicativos peer to peer, acesso remoto, games, streamings, aplicativos de lojas on line, mensageiros instantâneos, colaboração, vídeo conferência, e-mails, fóruns, bloggers, storage, proxy anônimos, antivírus entre outras;

2.10.6 Deve contemplar assinaturas que identifique pelo menos os aplicativos e sub aplicativos tais como: Youtube®, Facebook®, Twitter®, Linkedin®, Tumblr®, Bittorrent®, Gnutella®, AIM®, Baidu®, Syflex®, Logmein®, Join.me®, DropBox®, Onedrive®, Apple iCloud®, Amazon®, Ebay®, ITunnes®, Blospot®, Instagram®, Flickr®, Photoshop®, Picasso®, Myspace®, Netflix®, Justin TV®, Megavideo®, Skype®, Viber®, Whatsapp®, Yahoo Messenger®, Spotify®, Wunderlist®, Webex®, Gismodo®, Google News®, Google Docs®, Google Earth®, Google Translator®, Google Finance®, Money Control®, Morningstar®, Playstation®, Wii®, Xbox

Live®;

2.10.7 Ser capaz de identificar assinaturas de aplicações de uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações de proxys que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Vtunnel, Zenguard, Privax, Proxydotorg;

2.10.8 O recurso deve de forma objetiva controlar aplicativos web 2.0 com a finalidade de melhorar o desempenho da rede e evitar improdutividade do grupo de usuários da rede;

2.11 Filtro de conteúdo web:

2.11.1 O filtro de conteúdo web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado dependendo da URL ou categoria web, deve ser baseado em uma lista de URL's classificadas por tipo de conteúdo;

2.11.2 O filtro de conteúdo web deve permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamento de devices, podem acessar ou não as diversas categorias identificadas;

2.11.3 O filtro de conteúdo web deve possuir base de dados catalogada com mínimo de 40 milhões de URL's e classificada em no mínimo 80 categorias;

2.11.4 A solução deve possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de correlacionar endereços de origem e destino das URL's ou categorias web para as tomadas de ação;

2.11.5 A solução de filtro de conteúdo deve suportar a ação de forçar a pesquisa segura independente da configuração do navegador (browser) da estação de

trabalho do usuário. Esta funcionalidade não permitirá que os sites de busca retornem resultados considerados inapropriados. Esta funcionalidade deve ser suportada no mínimo para os buscadores "Google®", "Bing®" e "Yahoo®";

2.11.6 Deve possuir mecanismos de filtragem de métodos HTTP a fim de otimizar e melhorar a eficiência do tráfego web, deve comtemplar filtros do tipo: put, get, checkout, connect, delete, head, link, post, search e trace;

2.11.7 Deve permitir criar base de categorias personalizadas a partir de listas de URL's com suporte a lista de palavras chaves e expressões regulares;

2.11.8 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

2.11.9 Permitir a criação de filtros para arquivos e dados pré-definidos;

2.11.10 Os arquivos devem ser identificados por extensão e assinaturas;

2.11.11 Suporte a identificação de arquivos compactados, executáveis, imagens e multimídias, a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

2.11.12 Deve oferecer a opção de bloquear controles ActiveX e Java Scripts que possam comprometer o acesso web dos usuários;

2.11.13 Deve oferecer a opção de cota de tempo em horas ou minutos de navegação web por dia;

2.11.14 Deve oferecer a opção de cota de tráfego em MB de navegação web por dia;

2.11.15 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs e etc) identificados sobre aplicações (HTTP, HTTPS e FTP)

inclusive oferecendo a opção de controle de tamanho máximo de download por navegação;

2.11.16 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs, etc) identificados sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de upload por navegação;

2.11.17 Deve suportar mecanismos de filtro e controle de login no Google® por domínio, permitindo ao administrador especificar os domínios permitidos;

2.11.18 O sistema de filtro de conteúdo poderá ser aplicado por definição de horário ou período de validade do filtro; podendo ou não especificar usuários, grupos de usuários, rede ou agrupamento de device para todos os recursos de filtragem e controles estabelecidos;

2.12 Políticas de segurança do firewall:

2.12.1 O sistema deve integrar os respectivos recursos e serviços de integração com o firewall: NAT, proxy; filtro de conteúdo web, filtro de aplicações web, QoS, FailOver e balanceamento de links, de acordo as especificações técnicas descritas a fim de propiciar um sistema capaz de tratar o tráfego da rede em camadas, garantindo a segurança dos dados;

2.12.2 Estes recursos integrados devem permitir o tratamento do tráfego em camadas, de modo granular com o suporte a interceptar o tráfego SSL, identificar malwares e ações mal-intencionadas que utilizam o protocolo HTTPS para burlar firewalls, o sistema deve interceptar estas conexões, analisar e enviar os pacotes para tomadas de ações;

2.12.3 Deve também permitir a inspeção destes pacotes, detectar e prevenir dos ataques de intrusos, operando em conjunto com o firewall, impedir que acessos externos e/ou remotos executem rotinas de

invasão. Executando ação pró ativa de bloqueio dos ataques;

2.12.4 Deve permitir gerar políticas de segurança capaz de filtrar os pacotes, integrar aos recursos de tratamento de filtro de conteúdo, filtro de aplicações, gerenciamento e controle dos pacotes definindo controle de banda por níveis de velocidade e garantia de banda por prioridade.

2.12.5 Deve permitir o roteamento estático por device, por endereço IP, serviços, usuários, grupos de usuários, para cada link de internet podendo distribuir o balanceamento de carga entre múltiplos links de internet ou ainda definir um roteamento exclusivo sem a opção de redundância ou FailOver;

2.12.6 As políticas de segurança devem permitir integrar em uma mesma interface interativa a definição de uma única política que atenda todos os recursos integrados com o firewall;

2.12.7 As políticas de segurança devem tomar ações do tipo: permitir, bloquear e inspecionar para o tráfego IPS ou Inspecionar para o tráfego ATP;

2.12.8 As políticas de segurança devem atender as especificações por prioridade, se o conteúdo do tráfego se enquadrar as definições da política, a mesma deve ser aplicada ignorando as políticas de menor prioridade;

2.12.9 Deve permitir o agrupamento de políticas respeitando as regras de negócio;

2.12.10 Deve permitir reordenação sempre que necessário;

2.12.11 Deve suportar mecanismos de balanceamento de links por política, inclusive com devices do tipo VLAN ou MACVLAN (endereços virtuais);

2.12.12 Deve ser permitido desabilitar uma política de segurança sem que seja necessário remove-la da lista;

2.12.13 A interação da interface ainda deve prover um recurso ou mecanismo para expandir a política, ou

Procuradoria Jurídica SEMAE

seja, permitir a visualização com as informações de filtros e a ação que compõe a regra;

2.13 VPN IPSEC:

2.13.1 A solução deve prover comunicação através de túneis VPN "Virtual Private Network" ou "Rede virtual Privada". Ter como principal finalidade utilizar os recursos da rede pública "Internet" para conectar redes remotas.

2.13.2 Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereços inválidos possam se comunicar através da Internet;

2.13.3 Deve suportar VPN IPSEC Túnel site to site ou site to client;

2.13.4 Deve suportar VPN IPSEC RAS - Acesso remoto IPSEC;

2.13.5 Deve suportar os protocolos padrões de VPN: IPSEC, ESP, IKE e IKE versão 2;

2.13.6 A solução de VPN deve operar o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

2.13.7 O suporte aos protocolos e algoritmos de autenticação e integridade IKEv1 e IKEv2 de acordo a RFC 7296, de modo a estabelecer canais de autenticação e criptografia com outros produtos que suportem tal padrão;

2.13.8 Deve possuir suporte a algoritmos de criptografia IKE: 3DES, AES, Blowfish;

2.13.9 Deve possuir suporte a algoritmos de integridade IKE: md5, sha1, sha256, sha384 e sha512;

2.13.10 Deve possuir suporte a algoritmos de criptografia ESP: DES, AES, Blowfish e Camélia;

2.13.11 Deve possuir suporte a algoritmos de integridade ESP: md5, sha1, sha256, sha384, sha512, aesxcbc e aescmac;

2.13.12 Suporte ao menos à 5 Diffie-Hellman distintos;

2.13.13 A solução deve atender a suporte IKEv2 com suporte a fragmentação, de acordo a RFC 7383;

2.13.14 Deve possuir funcionalidade que permita estabelecer túneis de VPN com Appliances da mesma solução ou outras soluções de VPN implementadas atrás de firewalls, através de encapsulamento UDP, de acordo a RFC 3947;

2.13.15 Implementar os esquemas de troca de chaves manual, para os protocolos IKE e IKEv2 através de chave compartilhada (Pré-Shared Key);

2.13.16 Suportar Main Mode e Aggressive mode em IKE v1;

2.13.17 Possuir funcionalidade Dead Peer Detection (DPD) ou similar;

2.13.18 Suportar VPN Redundante (Failover) reestabelecimento automático da VPN IPSEC sobre um segundo enlace caso haja falha no enlace principal);

2.13.19 Suporte à conexão por FQDN "Full Quality Domain Name";

2.13.20 Deve permitir habilitar, desabilitar os túneis de VPN IPSEC

2.13.21 A solução deve prover recursos de controle de conexão no tratamento do protocolo IKE que possibilite definir parâmetros dos tempos de vida das conexões e retransmissão e da autenticação IKE;

2.13.22 O sistema de VPN IPSEC RAS deve funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs não válidos, colocando-os, virtualmente, em uma rede local estendida;

2.13.23 No modo VPN IPSEC RAS deve ser possível configurar o endereço/range IP a ser atribuída a interface de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;

2.13.24 O modo VPN IPSEC RAS deve suportar autenticação integrada X-Auth (Integração Windows AD, PAM LDAP base de autenticação local) para usuários do

Procuradoria Jurídica SEMAE

firewall;

2.13.25 Deve possuir mecanismos de autenticação com suporte a EAP (MSCHAP2) para clientes VPN IPSEC Windows;

2.13.26 Compatibilidade com clientes VPN nativos para os sistemas operacionais iOS 7 ou superior, Android 4.4.4 ou superior, MacOS X 10.6 ou superior, Linux 2.6.36 ou superior, Windows 7 ou superior;

2.14 VPN SSL:

2.14.1 A solução deve prover comunicação através de VPN SSL que permita um usuário remoto devidamente autorizado a utilizar um navegador WEB moderno para acessar com segurança diversos serviços da rede privada;

2.14.2 A solução deve suportar acesso com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPNs através da Internet;

2.14.3 A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

2.14.4 O acesso deve oferecer versatilidade, facilidade de uso, e controles específicos de grupos e usuários em cada modalidade de aplicação e deve estar disponível através de um portal WEB.

2.14.5 Deve prover acesso via túnel SSL utilizando um navegador sem a necessidade de um cliente instalado na estação remota, e ser compatível com o navegador Mozilla Firefox versão 47;

2.14.6 Deve ser compatível com as plataformas operacionais: MS-Windows, Linux, MacOS;

2.14.7 Deve possuir mecanismos de tunelamento de aplicações através de um portal web, com suporte a desvio de porta (Port Forward) para as aplicações internas;

2.14.8 Permitir acesso interno e externo ao portal

web;

2.14.9 Deve suportar as seguintes modalidades de aplicações: Aplicações Túnel do tipo cliente-servidor, Aplicações de acesso remoto tais como: VNC, SSH, Terminal Service, Aplicações web do tipo HTTP e HTTPS, Compartilhamento de rede do tipo SMB;

2.14.10 Deve possuir suporte a autenticação integrada X-Auth (Integração Windows AD, PAM LDAP e base de autenticação local) para usuários do firewall;

2.15 Serviços de rede (DDNS, DNS E DHCP):

2.15.1 A solução de UTM integrada deve permitir integração à serviços do tipo DDNS (Dynamic DNS);

2.15.2 Possuir suporte à publicação de hosts dinâmicos para os provedores de serviços: NO-IP e Dyndns;

2.15.3 Deve contemplar um mecanismo de atualização automática do DDNS por agendamento (update);

2.15.4 O serviço de DDNS deve ser compatível com Interface DSL ou PPOE;

2.15.5 O sistema também deve prover um recurso de redirecionamento DNS para provedores de DNS recursivo a fim de disponibilizar acesso a serviços de resolução de nomes remotos; permitir a consulta recursiva a partir dos redirecionamentos de DNS;

2.15.6 Permitir a configuração de acesso e redirecionamento por device de rede;

2.15.7 Suporte a cache de DNS;

2.15.8 Possuir mecanismos de proteção capaz de identificar ataques que disponibilizem servidores DNS válidos com autoridades sobre domínios configurados para responder um TTL (Time to live) muito baixo, inibindo a ação de guardar cache, o sistema deve possibilitar a proteção contra ataques que alteram a resposta a pesquisa de DNS para um endereço IP dinâmico de servidores com códigos maliciosos;

2.15.9 O sistema de proteção a este tipo de resposta

Procuradoria Jurídica SEMAE

(pesquisa de domínios com TTL muito baixo) deve possuir a opção de exceção para endereços de hosts locais e por domínios possibilitando especificar hosts e domínios confiáveis que não queira guardar cache;

2.15.10 Deve permitir DNS Redirect por listas de hosts;

2.15.11 A solução de UTM integrada deve fornecer um serviço de DHCP (Dynamic Host Configuration Protocol) Server e DHCP Relay;

2.15.12 Deve possuir mecanismo de configuração e distribuição de pool de endereços IPs por device de rede, com suporte a interfaces do tipo ethernet, VLAN, inclusive interface MACVLAN (Virtuais);

2.15.13 Deve permitir a distribuição do pool de endereços IPs por filtro de grupo ou objeto de endereço MAC; permitir a distribuição de endereço IP fixado ao endereço MAC.

2.15.14 A distribuição dos dados de configurações de serviços de rede deve contemplar a distribuição de Gateway ou roteamento, a definição de um sufixo de DNS; lista de endereço de servidores de DNS e servidores Wins;

2.15.15 Deve permitir a definição do tempo de vida do DHCP para a renovação do endereço IP entregue;

2.16 Cluster:

2.16.1 A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

2.16.2 Os dois dispositivos devem ser ligados em paralelo, com réplicas das configurações entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal ficar inoperante;

2.16.3 Deverão ser capazes de manter o sincronismo de todos os itens de configuração e serviços, exemplo:

Políticas de segurança, Configurações de segurança do firewall, Certificado de autoridade, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmico, Perfis, bases de antivírus, filtros web, IPS e ATP;

2.16.4 A alta disponibilidade deve ter persistência de sessão e detecção de falhas por protocolo VRRP;

2.16.5 O Sincronismo dos servidores deve ser por interface exclusiva;

2.17 Relatórios:

2.17.1 A geração de relatórios deve ser centralizada e disponibilizada através da interface WEB da solução e disposta em um painel de controle de gerenciamento.

2.17.2 A geração dos relatórios detalhados deve ser opcional e configurável por tipo de relatório: proxy, ataques e ameaças, aplicativos e firewall;

2.17.3 A solução deve disponibilizar a geração de relatórios acessíveis, fáceis de usar e baseados na web que ofereça visão em tempo real, relatórios sumarizados, gráficos e históricos detalhados.

2.17.4 Os relatórios devem propiciar ao administrador base concreta de análise fornecendo uma visão profunda de como a rede e os computadores estão sendo utilizados, permitindo-se entender e reforçar quando necessário as regras de conformidade.

2.17.5 A solução também deve através da interface de administração web, permitir administradores visualizar os relatórios dos usuários.

2.17.6 Acesso centralizado e consistente a todos os logs sumarizados e eventos do sistema com a opção de verificação "Diária" e "Mensal" dos registros e ainda com a opção de extração no formato "PDF" e "CSV".

2.17.7 Suporte à geração em PDF para os relatórios estatísticos;

Procuradoria Jurídica SEMAE

2.17.8 Deve ser capaz de gerar e manter os relatórios detalhados no mínimo por 7(sete) dias;

2.17.9 Deve suportar exportação dos relatórios detalhados no formato CSV;

2.17.10 Possuir um mecanismo de arquivamento dos relatórios gerados para download, o arquivamento deve ser mantido pelo período mínimo de 1(hum) mês;

2.17.11 Possuir um serviço de manutenção de limpeza dos registros de estatísticas e relatórios extraídos nos formatos CSV e PDF, mantendo os registros por um período mínimo de 30(trinta) dias;

2.17.12 A manutenção dos relatórios detalhados deve ser rotacional, automático e deve manter um período mínimo de 7 dias;

2.17.13 O sistema deve possuir um mecanismo de log que permita enviar os arquivos de log para outro servidor do tipo SYSLOG, especificando IP e porta;

2.17.14 Deve ser capaz de gerar relatório Online com (B.I) Business Intelligence para filtro na busca de relatórios;

2.17.15 Deve contemplar relação de eventos entre os itens de relatórios do proxy;

2.17.16 Deve contemplar relação de eventos entre os itens de relatórios das ameaças e aplicativos;

2.17.17 Deve contemplar os eventos de detecção do AntiMalware;

2.17.18 Deve contemplar relação de eventos entre os itens de relatórios dos atacantes;

2.17.19 A empresa fabricante da solução deve garantir que todos os relatórios detalhados devem ser assinados através de uma chave de integridade (key) que garanta a confiabilidade dos dados, atendendo ao Marco Civil nº 12.965/2014;

2.18 Registros e logs do sistema:

2.18.1 Deve atender os registros e logs do sistema das respectivas informações de gerenciamento por

dispositivo: relatórios e gráficos gerais do sistema;

2.18.2 Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico diário por hora em (KB/ MB/ GB/ TB);

2.18.3 Gerar gráfico estatístico do sistema contendo informações do total de tráfego web via proxy e histórico diário por hora em (KB/ MB/ GB/ TB);

2.18.4 Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo sistema de proteção de ameaças persistentes, tipo ATP e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

2.18.5 Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo sistema de prevenção de intrusos, tipo IPS (Inspection Prevention System) e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

2.18.6 Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico mensal por dia em (KB/ MB/ GB/ TB);

2.18.7 Gerar gráfico estatístico do sistema contendo informações do total de tráfego web via proxy e histórico mensal por dia em (KB/ MB/ GB/ TB);

2.18.8 Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo ATP (Advanced Threats Protection) e histórico mensal por dia em (KB/ MB/ GB/ TB);

2.18.9 Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo IPS (Inspection Prevention System) e histórico mensal por dia em (KB/ MB/ GB/ TB);

2.18.10 Gerar histórico dos top 10 (dez) com o total do tráfego de rede em (KB/ MB/ GB/ TB) por: usuários, grupos, serviços/protocolos; regras de conformidade e categorias web;

2.18.11 Gerar histórico dos top 10 (dez) alertas de

Procuradoria Jurídica SEMAE

segurança dos ataques detectados pelo firewall com o total de hits;

2.18.12 Gerar histórico dos top 10 (dez) aplicativos web (ATP) com o total de hits;

2.18.13 Gerar histórico das top 10 (dez) ameaças APT (Advanced Persistent Threats) detectados pelo ATP com o total de hits e classificação do tipo de impacto na rede;

2.18.14 Gerar histórico dos top 10 (dez) ataques detectados pelo (IPS) com o total de hits e classificação do tipo de impacto na rede;

2.18.15 Gerar gráfico estatístico do sistema contendo informações de desempenho como: (%) percentual de uso de processamento (CPU), (%) percentual de entrada/saída (I/O), (%) percentual de carga média (LOAD), (%) percentual de utilização de disco e (%) percentual de consumo de memória (RAM);

2.18.16 Gráfico estatístico do consumo de banda, mínimo de 5 (cinco) níveis de prioridade em (B/ KB/ MB/ GB/ TB/);

2.18.17 Gráfico estatístico em tempo real do tráfego total da rede (RX/ TX);

2.18.18 Gráfico estatístico do sistema contendo histórico sobre o tráfego dos devices de rede (RX/ TX) e um serviço de monitoração em tempo real para cada device de rede;

2.18.19 A solução deve possuir um sistema de monitoração de tráfego para as novas conexões, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo. O serviço de monitoração deve retornar os dados especificados nos filtros e a respectiva regra de conformidade;

2.18.20 A solução deve possuir um sistema de monitoração de tráfego para as conexões estabelecidas, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo, inclusive

limitando o quadro de respostas até 10 (dez) conexões estabelecidas. O serviço de monitoração deve retornar os dados especificados nos filtros, o total de tráfego em (KB/ MB/ GB/ TB), a velocidade em (bps/ kbps/ Mbps/ Gbps/ Tbps) e o número de pacotes trafegados;

2.19 Relatórios e gráficos gerais do tráfego web via proxy:

2.19.1 Gerar gráficos estatísticos do tráfego WEB via Proxy contendo as seguintes informações: total das requisições, total das requisições bloqueadas;

2.19.2 Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego web via proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;

2.19.3 Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de tráfego web via proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;

2.19.4 Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego web via proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (uma) hora;

2.19.5 Gerar gráfico ou resumo mensal do total da relação de eventos entre o tráfego web via proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (hum) dia;

2.19.6 Gerar histórico dos Top Level 10 (dez) com o total do tráfego em (KB/ MB/ GB/ TB) e o total dos acessos, com a opção de ordenação por tráfego e por acessos, das regras de conformidade permitidas e tipos de conteúdo permitidos;

2.19.7 Gerar histórico dos Top Level 10 (dez) com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos) e total de acessos, com a opção de ordenação por tráfego, por tempo, e por acessos, das categorias permitidas e aplicativos permitidos;

Procuradoria Jurídica SEMAE

2.19.8 Gerar histórico dos Top Level 10 (dez) "usuários" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

2.19.9 Gerar histórico dos Top Level dos 10 (dez), inclusive a relação de eventos entre "usuários" e as "categorias web" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

2.19.10 Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "usuários" e os "aplicativos web" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

2.19.11 Gerar histórico dos Top Level 10 (dez), dos "bloqueados" com o total das tentativas de acesso, das regras de conformidade bloqueadas, categorias bloqueadas, aplicativos web bloqueados e tipos de conteúdo bloqueados;

2.19.12 A solução deve possuir um sistema de monitoração da navegação WEB via Proxy em tempo real por filtro do tipo: servidor, origem (endereço IP ou usuário), URL de destino e porta de serviço. O serviço de monitoração deve retornar o tempo de tráfego em (hora/ minuto/ segundo), a origem (endereço IP ou usuário), o total de tráfego em (B/ KB/ MB/ GB/ TB), a velocidade em (bps/ Kbps/ Mbps/ Gbps/ Tbps) e a URL de destino;

DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

2.20 Relatórios e gráficos gerais do tráfego ATP:

2.20.1 Gerar gráficos estatísticos do tráfego ATP contendo as seguintes informações: total de ameaças detectadas, total de ameaças bloqueadas, total de aplicativos detectados, total de aplicativos bloqueados;

2.20.2 Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego ATP das ameaças detectadas a as ameaças bloqueadas no intervalo de tempo de 1 (uma) hora;

2.20.3 Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (uma) hora;

2.20.4 Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de trafego ATP das ameaças detectadas e as ameaças bloqueadas no intervalo de tempo de 1 (hum) dia;

2.20.5 Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (hum) dia;

2.20.6 Gerar gráficos estatísticos do tráfego ATP contendo as informações do total de ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

2.20.7 Gerar históricos ou resumos diários do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

2.20.8 Gerar históricos ou resumos mensais do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

Procuradoria Jurídica SEMAE

2.20.9 Gerar histórico do Top Level 10 (dez) "detectados", com o total de detecções e o tipo de impacto das ameaças e aplicativos;

2.20.10 Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre as "ameaças" e os "usuários" com o tipo de impacto, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

2.20.11 Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "aplicativos" e os "usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

2.20.12 Gerar histórico dos Top Level 10 (dez) "bloqueados" com o total das detecções, das ameaças e aplicativos;

2.21 Relatório e gráficos gerais do tráfego IPS:

2.21.1 Gerar gráficos estatísticos do tráfego IPS contendo as seguintes informações: total de ataques detectados, total de ataques bloqueados;

2.21.2 Gerar gráfico, histórico ou resumo diário, do total de trafego IPS da relação de eventos entre os "ataques detectados" e os "ataques bloqueados" no intervalo de tempo de 1 (uma) hora;

2.21.3 Gerar gráfico, histórico ou resumo mensal, do total de trafego IPS da relação de eventos entre os "ataques detectados" e dos "ataques bloqueados" no intervalo de tempo de 1 (hum) dia;

2.21.4 Gerar gráficos estatísticos do tráfego IPS contendo as informações do total dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

2.21.5 Gerar gráficos, históricos ou resumos diários, do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três)

tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

2.21.6 Gerar gráficos, históricos ou resumos mensais, do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

2.21.7 Gerar histórico dos Tops 10 (dez) "ataques detectados", com o total de detecções e o tipo de risco ou impacto na rede;

2.21.8 Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "ataques" e os "endereços IP ou usuários" com o tipo de risco ou impacto na rede, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

2.21.9 Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre o "grau de risco" e os "endereços IP ou usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

2.21.10 Gerar histórico dos Tops Level 10 (dez), "categorias de ataques" com o total das detecções e total de bloqueados, com a opção de detalhar a categoria e identificar os endereços IPs ou usuários atacantes.

3 Especificações gerais do software SMX:

3.1 Características da solução:

3.1.1 Deverá possuir criptografia das caixas postais dos usuários;

3.1.2 A solução deverá possuir recursos de Antispam, Antivírus e Antimalware;

3.1.3 Deverá possuir sistema de arquivamento das caixas postais;

3.1.4 Deverá possuir Relatórios e sistema de monitoração das mensagens enviadas e recebidas;

3.1.5 A solução deve ter suporte aos seguintes recuros:

Procuradoria Jurídica SEMAE

3.1.6 Instalação distribuída em N servidores "balanceamento de recursos e serviços da solução";

3.1.7 Suporte ao protocolo SNMP;

3.1.8 Deverá possuir recurso de cluster do tipo H.A "High Availability" Alta disponibilidade;

3.1.9 Deverá permitir a atualização de data e hora com suporte a servidores NTP "Network Time Protocol";

3.1.10 Deverá permitir a atualização automática do sistema para correções e releases.

3.1.11 A solução deve permitir a administração através de uma Interface WEB HTTPS, com suporte as seguintes funções:

3.1.12 Gerenciamento através de um painel de controle;

3.1.13 Emitir alertas e notificações do sistema em tempo real na interface WEB;

3.1.14 Interface responsiva compatível com dispositivos móveis;

3.1.15 Interface em português e inglês;

3.1.16 Perfis de administradores "Super administrador e Administrador restrito".

3.1.17 Definições de ACL (Acess List) completa, "Visualizar, Editar";

3.1.18 Auditoria com log das ações dos administradores por recurso;

3.1.19 Agendamento para o envio dos alertas e notificações por e-mail;

3.1.20 Acesso a console Shell para gerenciamento através de interface de linha de comando CLI (Command Line Interface);

3.1.21 Deverá possuir funcionalidade de Backup e Restore das configurações;

3.1.22 Deverá permitir o Backup em ponto de montagem do tipo Armazenamento NFS "com suporte a tráfego TCP e UDP";

3.1.23 Deverá possuir o suporte a múltiplos domínios de autenticação;;

3.1.24 Deverá executar o sincronismo de usuários e grupos com servidores Windows AD® e Servidores LDAP;

3.1.25 Deve permitir o cadastro de usuários do tipo "local";

3.1.26 Dos recursos e serviços integrados a solução de Firewall de E-mail.

3.1.27 A solução deve atuar como servidor MTA/MRA. "Mail Transfer Agent"/ "Mail Retrieval Agent".

3.1.28 Permitir o envio e recebimentos de mensagens servidor/servidor. MTA/MTA.

3.1.29 Permitir o recebimento e acesso de mensagens cliente/servidor. MRA/MTA.

3.1.30 Deve prover um serviço inteligente capaz de decidir e tratar a confiabilidade da mensagem para sua entrega ou negação baseado nos tratamentos de conexão da origem em tempo de protocolo. Fazer a verificação e quando detectado alguma ilegitimidade a mensagem não deve ser entregue nem armazenada e não gerar mensagem de resposta de erro na entrega – "bounce";

3.1.31 A solução deverá contemplar as seguintes funcionalidades:

- Antispam com aprendizado heurístico.
- Base de dados Antimalware.
- Base de dados com reputação de endereços,
- Firewall de e-mail multicondicional.

3.1.32 A solução deverá suportar as seguintes especificações técnicas com os seguintes recursos:

- Suportar os serviços e protocolos incluindo criptografia cliente-servidor com suporte SSL/TLS.
- IMAP e IMAPs;
- POP e POPs;
- SMTP e SMTPs;

3.1.33 Deverá possuir os seguintes métodos de autenticação:

- Plain;
- Login;

3.1.34 Deverá permitir o controle de Relay (endereços confiáveis permitidos), por classe ou objeto de rede/ endereço IP;

3.1.35 Deverá possuir Integração e sincronismos de usuários de autenticação AD e LDAP.

3.1.36 Deverá suportar contas locais;

3.1.37 Deverá permitir o controle do número de mensagens;

3.1.38 Deverá possuir suporte a consulta de RBLs (Real-time Blocking List);

Procuradoria Jurídica SEMAE

3.1.39 O serviço de consulta à base de RBLs deve prover recurso de regras de exceção que contemple os seguintes filtros:

- Por servidor.
- Usuário de origem;
- Usuário de origem do grupo;
- Endereço Ip de origem;
- Remetente;
- Domínio remetente;

3.1.40 A solução deve permitir que o usuário tenha acesso a listas "Quarentena, Blacklist e Whitelist";

3.1.41 Deve suportar manipulação dos endereços de remetentes para as listas "Blacklist e Whitelist", o usuário deve conseguir manipular qualquer mensagem recebida na sua caixa de entrada (INBOX) para as respectivas listas, a partir das pastas, no próprio cliente de e-mail ou serviço similar;

3.1.42 O serviço de manipulação destas listas "Quarentena, Blacklist e Whitelist" deve ser suportado por qualquer cliente de e-mail e baseado no protocolo IMAP;

3.1.43 O sistema deve enviar relatórios diários dos endereços inseridos na "Blacklist" do usuário no último dia;

3.1.44 O sistema deve enviar relatórios diários dos endereços inseridos na "Whitelist" do usuário no último dia;

3.1.45 Suporte a conexões do tipo "Retriever" para conexões com outros servidores de e-mail.

3.1.46 Deverá possuir recurso de Cluster - Alta disponibilidade - H.A "High Availability".

3.1.47 A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo). Os dois dispositivos são ligados em paralelo, com réplicas das configurações entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal ficar inoperante;

3.1.48 Deverão ser capazes de manter o sincronismo entre as seguintes configurações como regras de firewall local, regras de conformidade de e-mail; certificado de autoridade, contas administrativas, usuários e grupos, configurações de rede,

roteamento estático, roteamento dinâmico, bases de antivírus, antimalware, de reputação e RBLs;

3.1.57 Deve atuar como um Proxy transparente, receber e inspecionar o tráfego IMAP/POP, fazer uma pesquisa para determinar qual o servidor responde pela respectiva caixa de postal e de forma transparente desviar a conexão do cliente IMAP para o servidor que corresponda a caixa postal correta para aquele usuário.

3.1.58 O serviço de antispam deve funcionar como um classificador de mensagens deve possuir tecnologia capaz de sinalizar quando uma mensagem é um SPAM ou uma mensagem normal, ou seja, de origem confiável.

3.1.59 O Antispam deve atender aos seguintes recursos:

- Analisar as mensagens durante seu recebimento, diretamente no protocolo;
- Testes automáticos baseados nas RFC's (822; 2822).
- Aprendizagem por n° de ocorrências na Blacklist/ Whitelist.
- Deve permitir parametrizações para o aprendizado heurístico;
- Aprendizagem heurística em tempo de protocolo;
- Entrada manual de conteúdo para aprendizagem heurística através das pastas IMAP através do webmail nativo do sistema ou do cliente de e-mail do usuário ou serviço similar.

3.1.60 A solução deve permitir inclusão de endereços de e-mail nas listas de consulta, "Blacklist e Whitelist" pelos usuários.

3.1.61 O sistema ainda deve possuir um recurso de regras de exceção para a análise do Antispam, que contemple os seguintes filtros:

- Por servidor;
- Usuário de origem;
- Usuário de origem do grupo;
- Endereço IP de origem;
- Remetente;
- Domínio remetente;
- Palavra chave no remetente;
- Expressão regular por palavra chave no remetente.

Procuradoria Jurídica SEMAE

3.1.62 O serviço de antimalware deve oferecer tecnologia avançada de proteção contra malwares e vírus para garantir a confiabilidade do tráfego das mensagens de E-mails recebidos e enviados.

3.1.63 O Antimalware deve atender aos seguintes recursos:

- Analisar as mensagens separando os itens do arquivo por tipo de conteúdo (Header, SMTP, HTLM, DOC, FLASH, ZIP, EXE, BATS, VBS, OCTET STREAM, JPEG, GIF, MPEG, PNG, TIF e outros);
- Bloqueio por listas de arquivos maliciosos. (Trojans, Worm, Rootkits, Adware, Spywares, Etc);
- Bloqueio de arquivos encriptados;
- Detecção de aplicativos maliciosos - PUA/API (Potential Unwanted Application/ Aplicativos potencialmente indesejados);

3.1.64 O recurso Firewall de E-mail deve atender a condição de gerenciamento das mensagens de e-mail baseadas em regras de conformidade.

3.1.65 As regras de conformidade devem permitir criar agrupamento por finalidade para gerenciamento dessas regras.

3.1.66 A solução deve permitir criar ou definir as regras de conformidade numa mesma interface interativa, ou seja, em uma mesma tela o administrador deve ter a condição de aplicar em uma mesma regra, o conjunto de todas as condições e normas para recebimento ou tratamento de uma mensagem de e-mail.

3.1.67 Deve permitir aplicar filtros que componham os seguintes recursos integrados:

- Filtro e controle por conteúdo. (Informações do cabeçalho; anexos; mime type; corpo da mensagem; links; tamanho do anexo, entre outros.);
- Mail reputation;
- AntiPhishing;
- AntiMalware;
- Antispam;
- Blacklist;
- Whitelist;
- Antivírus;
- RBL (Real-time Blocking List).

DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

3.1.68 As regras devem permitir tomadas de ações classificadas em dois tipos:

- Ações de manipulação da mensagem com suporte a: copiar para, adicionar X-header; adicionar pontos (score), resposta automática, adicionar remetente na whitelist, adicionar remetente na blacklist, adicionar destinatário na whitelist, adicionar destinatário na blacklist;

- Ações de tratamento final (recebimento ou bloqueio) da mensagem com suporte a: receber, bloquear, rejeitar, descartar, desviar para quarentena do usuário, enviar captcha, enviar captcha com ação automática para adicionar o remetente na whitelist do usuário; desviar ou redirecionar para outro servidor MTA;

3.1.69 As ações das regras devem ser aplicadas usando o método "Search Match Wins" para as ações de tratamento final;

3.1.70 Até que uma mensagem se enquadre em uma regra de ação de tratamento final a mesma deve ser analisada por todo o conjunto de regras de conformidade navegando por todos os grupos e regras definidas na lista;

3.1.71 As ações de tratamento final de recebimento ou bloqueio devem encerrar a análise de uma mensagem que se enquadre nas condições definidas na respectiva regra, abandonando o grupo e aplicando a ação final;

3.1.72 Habilitar resposta automática, inclusive personalizando a mensagem para cada tratamento.

3.1.73 Deve ser permitido manipular ou mover as regras entre os grupos, de maneira que o administrador possa deslocar uma determinada regra para outro grupo conforme a necessidade;

3.1.74 Sistema de Arquivamento de mensagens (caixas postais): O serviço de arquivamento de mensagens deve automatizar o processo de cópia e armazenamento dos e-mails, visando proteger todos os e-mails de entrada e saída, incluindo anexos com a finalidade de preservar e proteger a informação.

3.1.75 Deve prover os seguintes recursos:

- O serviço deve ser disponibilizado a partir de um ponto de armazenamento do tipo NFS ou Disco com suporte a USB-HDD;

- Gerenciamento das caixas postais por "usuário", "grupo" e "período";

Procuradoria Jurídica SEMAE

- Controle de acesso do arquivamento por regras;
- Acesso via IMAP;
- Disponibilizar toda a base de e-mail para consulta de/para algum usuário com o propósito de gerenciamento da base de conteúdo das mensagens trafegadas;
- A recuperação de e-mails excluídos acidentalmente ou não;
- Servir como processo de auditoria e proteção à propriedade intelectual contida no e-mail;
- Permitir o acompanhamento de conteúdo dos e-mails (internos/ externos);
- Gestão do tráfego de documentos anexos;
- Verificação das conformidades das regras;

3.2 Relatórios:

3.2.1 A solução deve disponibilizar a geração de relatórios acessíveis, fáceis de usar e baseados na Web que ofereça visão em tempo real, relatórios sumarizados, gráficos e históricos detalhados em um painel de controle de gerenciamento.

3.2.2 Os relatórios devem propiciar ao administrador base concreta de análise fornecendo uma visão profunda de como a rede e os computadores estão sendo utilizados, permitindo-se entender e reforçar quando necessário as regras de conformidade.

3.2.3 Acesso centralizado e consistente a todos os logs sumarizados e eventos do sistema com a opção de verificação "Diária" e "Mensal" dos registros e ainda com a opção de extração no formato "PDF" e "CSV".

3.2.4 Suporte a geração em PDF para os relatórios estatísticos;

3.2.5 Suporte CSV para exportação dos relatórios detalhados;

3.2.6 Dos relatórios e gráficos gerais do sistema:

- Gráficos estatísticos do sistema contendo informações de desempenho como: (%) percentual de uso de processamento (CPU), (%) percentual de entrada/saída (I/O), (%) percentual de carga média (LOAD), (%) percentual de utilização de disco e (%) percentual de consumo de memória (RAM);
- Gráfico do total de analises de SPAM versus Percentual (%) de acerto nas análises;

- Gráfico histórico ou resumo diário do total de mensagens entregues no intervalo de tempo de 1 (uma) hora;
- Gráfico histórico ou resumo mensal do total dos e-mails entregues no intervalo de tempo de 1 (hum) dia;
- Gráfico histórico ou resumo do total versus o motivo dos e-mails ignorados ou "não entregues";
- Gráfico histórico ou resumo do tempo dos e-mails na fila por intervalo de tempo de até: 1 (hum) dia, 12(doze) horas, 6 (seis) horas, 3 (três) horas, 1 (uma) hora, 30 (trinta) minutos, 15 (quinze) minutos, 5 (cinco) minutos, 1 (hum) minuto;
- Deverá prover a informação dos usuários que mais enviaram e receberam e-mails;
- Histórico dos TOP 10 Endereços IP rejeitados com o total dos e-mails;
- Monitor em tempo real dos e-mails na fila por filtro de remetente e destinatário agrupados por domínios, remetente ou destinatário. O serviço de monitoração deve retornar o total dos e-mails em fila, o tamanho, o tempo em fila do e-mail mais antigo, o tempo em fila do e-mail mais recente e o agrupamento;

4 Documentos para participação:

4.1 Atestado de Capacidade Técnica, em nome da LICITANTE, expedido por pessoa jurídica de direito público ou privado, que comprove a prestação de serviço de forma similar ao ofertado;

4.2 A LICITANTE deverá emitir declaração que cumpre todos os requisitos técnicos do edital se responsabilizando por isso.

5 Documentos para contrato:

5.1 Declaração do Fabricante informando que a CONTRATADA está autorizada a prestar suporte técnico na solução ofertada;

5.2 A CONTRATADA deverá apresentar carta do fabricante quanto ao fornecimento, garantia e funcionalidade dos produtos ofertados;

5.3 A CONTRATADA deverá apresentar declaração emitida pelo

Procuradoria Jurídica SEMAE

fabricante específica para este certame comprovando que a empresa faz parte do programa de parcerias e que possui autorização para comercializar os seus produtos e serviços;

5.4 A CONTRATADA deve fornecer atestado comprovando a existência de equipe técnica com pessoas capacitadas pelo fabricante em todas as soluções adquiridas. O atestado/diploma deverá ser fornecido pelo fabricante.

6 Requisitos:

6.1 Os produtos que compõe a Solução de Segurança devem todos ser produzidos pelo mesmo fabricante;

6.2 A CONTRATADA deverá prestar suporte para a instalação dos produtos de segurança contratados.

7 Condições de entrega e instalação:

7.1 Os equipamentos de informática objeto do presente termo serão entregues na Divisão de TI do SEMAE, na Rua XV de Novembro, 2200, Bairro Alto, Piracicaba - SP, para serem regularmente instalados sob orientação técnica da empresa CONTRATADA.

7.2 O prazo de entrega e instalação deverá ser de até 5 (cinco) dias no local informado, após a assinatura do contrato.

8 Condições de conservação e manutenção:

8.1 O SEMAE ficará responsável pela conservação e pela regular utilização dos bens móveis objeto do presente termo em ambiente climatizado e supridos de no-break, responsabilizando-se pelos danos decorrentes de uso inadequado, acidentes ou eventos não relacionados com o desgaste natural dos equipamentos.

8.2 A manutenção deverá ser preventiva e corretiva, com fornecimento total de peças. A manutenção corretiva

compreende todo e qualquer cuidado técnico indispensável para o perfeito funcionamento regular e permanente dos equipamentos.

8.3 Todo serviço deverá ser executado nas instalações da CONTRATADA, exceto aqueles que possam ser resolvidos de forma rápida no local onde se encontra o equipamento avariado, ou de forma remota quando o problema for lógico.

8.4 Quando retirado algum equipamento para manutenção preventiva ou corretiva, será necessária a reposição através de equipamento fornecido pela CONTRATADA com as mesmas funcionalidades do equipamento retirado.

8.5 No caso de manutenção corretiva, a CONTRATADA deverá atender ao chamado em 4 (quatro) horas e resolver o problema dentro de no máximo 72 (setenta e duas) horas, a contar do acionamento pela Divisão de TI do SEMAE.

8.6 No caso de manutenção preventiva, a mesma terá um prazo de 48 (quarenta e oito) horas para retirar e fazer a substituição temporária do equipamento.

8.7 Não será tolerada a falta de atendimento, seja por motivo de férias, licença, greve, falta ao serviço ou demissão de empregados, não tendo estes, em hipótese alguma, vínculo empregatício ou qualquer outra espécie de relação de emprego com o SEMAE.

8.8 Serão de exclusiva responsabilidade da CONTRATADA, todas as despesas referentes a encargos e obrigações sociais, trabalhistas e fiscais, decorrentes da execução do contrato.

8.9 A CONTRATADA deverá ter disponibilidade para atendimento dos chamados, no horário compreendido entre 08 e 17 horas em horário comercial, de segunda à sexta feira.

8.10 A CONTRATADA deverá indicar um telefone celular e/ou fixo que possibilite o contato imediato com o SEMAE no horário estabelecido de atendimento.

Procuradoria Jurídica SEMAE

9 Condições de uso e de devolução:

9.1 Os equipamentos de informática objeto do presente termo

serão utilizados para fins exclusivos de execução, pelo SEMAE, de softwares, sistemas e soluções em tecnologia da informação da CONTRATADA, ficando expressamente proibida sua utilização para quaisquer outras finalidades.

9.2 O SEMAE não poderá emprestar, locar, dar em garantia ou ceder, a qualquer título, parcial ou totalmente, os bens móveis descritos neste termo, nem tampouco poderá, em qualquer hipótese, utilizá-los para quaisquer finalidades não contempladas no texto do presente termo.

9.3 A CONTRATADA deverá retirar os equipamentos a partir do próximo dia útil contando a data de término do contrato.

10 Sigilo:

10.1 As partes ficam obrigadas a manter sigilo absoluto em relação a todos e quaisquer dados, informações, documentos dos contratantes a que tiverem acesso em função do contratado, sendo que o término da vigência ou a rescisão do presente contrato não afetarão a obrigação de sigilo em referência.

Clayton Luis Ramos da Silva
Setor de Controle da Tecnologia da Informação

José Odivaldo Chitolina Junior
Divisão de Tecnologia da Informação