



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

Contratação de empresa especializada para fornecimento de solução corporativa padronizada de segurança da informação NGFW (Next Generation FireWall) contemplando servidor (hardware) e software do tipo UTM (Unified Threat Management) - com a capacidade de integrar todos os recursos em um único dispositivo, com garantia, atualizações e suporte por 12 meses.

1- A CONTRATADA DEVERÁ FORNECER 1 (UM) APPLIANCE NOVO, DE PRIMEIRO USO, EM LINHA DE FABRICAÇÃO E EM PERFEITO ESTADO DE CONSERVAÇÃO COM AS SEGUINTE CARACTERÍSTICAS MÍNIMAS:

- 1.1 O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm) do referido rack;
- 1.2 Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;
- 1.3 Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- 1.4 Possuir painel do tipo LCD com informações do Sistema, data/hora e Endereçamento IP;
- 1.5 Possuir painel/led indicador on/off, disco e devices de rede;
- 1.6 Possuir throughput de no mínimo 34 Gbps para tráfego UDP;
- 1.7 Suportar no mínimo 18.000.000 (dezoito milhões) conexões simultâneas;
- 1.8 Suportar no mínimo 120.000 (cento e vinte mil) novas conexões por segundo;
- 1.9 Possuir throughput de no mínimo 2.2 Gbps para tráfego HTTP/HTTPS com inspeção SSL via proxy;
- 1.10 Possuir throughput de no mínimo 6 Gbps para tráfego IPS/IDS;
- 1.11 Possuir throughput de no mínimo 5 Gbps para tráfego VPN IPSEC com criptografia (AES-256 + SHA256);
- 1.12 Possuir throughput de no mínimo 2 Gbps para tráfego VPN SSL com criptografia (AES-256);
- 1.13 Possuir throughput mínimo de 6 Gbps/2 Gbps para tráfego Proxy Web filter/SSL Inspection;





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 1.14 Possuir throughput mínimo de 2.5 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- 1.15 Suportar no mínimo 400 conexões de usuários concorrentes para VPN SSL;
- 1.16 Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade; as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- 1.17 Possuir no mínimo 16 GB de memória RAM;
- 1.18 Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;
- 1.19 Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;
- 1.20 Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos; a interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet.

2 FUNÇÕES BÁSICAS:

- 2.1 Hardware (Appliance) que atua na segurança e performance do ambiente de rede;
- 2.2 VPN SSL, VPN IPsec (Client-to-site e Site-to-site);
- 2.3 Controle de Aplicações;
- 2.4 Proxy Web e Filtro de Conteúdo Web (URL Filtering);
- 2.5 Detecção e prevenção de intrusos - IPS;
- 2.6 Qualidade de serviço - QOS;
- 2.7 Anti-Malware;
- 2.8 SD-WAN;
- 2.9 Cluster.

3 CARACTERÍSTICAS GERAIS:

- 3.1 O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de maior capacidade.
- 3.2 A plataforma deve ser otimizada para análise de conteúdo de



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- aplicações em camada 7;
- 3.3 Interface em português e inglês;
- 3.4 Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;
- 3.5 O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- 3.6 O software deverá ser fornecido em sua versão mais atualizada;
- 3.7 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução;
- 3.8 Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3;
- 3.9 Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;
- 3.10 A Solução deverá prover inspeção SSL;
- 3.11 A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho;
- 3.12 Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- 3.13 Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;
- 3.14 Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:
- Endereço do servidor;
 - Porta do servidor;
 - Usuário;
 - Senha;
- 3.15 Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:
- Desempenho total (throughput);
 - Conexões simultâneas;





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- Usuários autenticados;
 - Serviços habilitados ou desabilitados;
 - Quantidade de endereços distribuídos pelo DHCP.
- 3.16 Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, mesmo antes do equipamento ser conectado à rede, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;
- 3.17 A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site aonde ele será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;
- 3.18 Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;
- 3.19 A solução ofertada deverá permitir a criação de perfis de proteção, tais como e não limitado a perfil de IPS, perfil de controle WEB/aplicações e perfil de SD-WAN e dever ser possível utilizá-los nas políticas de segurança;
- 3.20 Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;
- 3.21 Implementar protocolo de coleta de informações de fluxos que circulem pelo equipamento, como Netflow v5, v9 e v10 (IPFIX);
- 3.22 A solução deverá possuir uma única janela para a criação, configuração e edição dos recursos de segurança;
- 3.23 Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única policy;
- 3.24 Deve implementar o protocolo ECMP;
- 3.25 O sistema deverá implementar otimização de fluxos TCP em



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.

- 3.26 Deve possuir suporte ao protocolo de encapsulamento de redes MPLS; esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

4 FUNCIONALIDADES DO FIREWALL:

- 4.1 Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- 4.2 Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita salvar em pen drive local;
- 4.3 Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- 4.4 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;
- 4.5 O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- 4.6 As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- 4.7 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;
- 4.8 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;





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 4.9 Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
- 4.10 Possuir controle de acesso à internet por endereço IP de origem e destino;
- 4.11 Possuir controle de acesso à internet por sub-rede;
- 4.12 Possuir suporte a tags de VLAN (802.1q);
- 4.13 Suportar agregação de links, segundo padrão IEEE 802.3ad;
- 4.14 Possuir ferramenta de diagnóstico do tipo tcpdump;
- 4.15 Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- 4.16 Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- 4.17 Possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um, N-para-um e vários para um.
- 4.18 Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- 4.19 Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- 4.20 Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
- 4.21 Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
- 4.22 Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 4.23 Deverá suportar aplicações multimídia como: H.323, SIP;
- 4.24 Possuir tecnologia de firewall do tipo Stateful;
- 4.25 Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- 4.26 Permitir o funcionamento em modo transparente tipo "bridge";
- 4.27 Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
- 4.28 Possuir conexão entre estação de gerência e appliance



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

criptografada tanto em interface gráfica quanto em CLI (linha de comando);

- 4.29 Deverá suportar forwarding de multicast;
- 4.30 Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- 4.31 Permitir o agrupamento de serviços;
- 4.32 Permitir o filtro de pacotes sem a utilização de NAT;
- 4.33 Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 4.34 Possuir mecanismo de anti-spoofing;
- 4.35 Permitir criação de regras definidas pelo usuário;
- 4.36 Permitir o serviço de autenticação para HTTP e FTP;
- 4.37 Possuir a funcionalidade de balanceamento e contingência de links;
- 4.38 Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, padrões de uso atual.

5 IDENTIFICAÇÃO DE USUÁRIO:

- 5.1 Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACACS e Radius;
- 5.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 5.3 Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- 5.4 Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- 5.5 A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- 5.6 Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados



[Handwritten signature]



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

de maneira simples e sem utilização de scripts de comando;

- 5.7 A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- 5.8 A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;
- 5.9 O UTM deve permitir gerenciar múltiplas políticas de controles no serviço de autenticação. As políticas devem permitir criar controles para autenticação, e deve permitir ou bloqueia o acesso ao serviço de autenticação baseado em condições e para sessão, ou seja, uma vez que o usuário esteja permitido se autenticar no serviço, a política deve definir os parâmetros de sessão do usuário;
- 5.10 Para o sistema de controles no serviço de autenticação o produto deve possuir, no mínimo, as seguintes condições para o Controle de Autenticação:
 - Usuários e Grupos de Usuários;
 - Datas (Objetos de Datas);
 - Horários (Objetos de Horário);
 - Plataformas (Objetos de Dicionários);
 - Endereços Remotos (Objetos de IPv4 e IPv6);
 - Zona de Rede (Múltiplas Zonas).

6 FUNCIONALIDADES DA VPN:

- 6.1 VPN baseada em appliance;
- 6.2 Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 6.3 Suporte a certificados PKI X.509 para construção de VPNs;
- 6.4 Possuir suporte a VPNs IPsec site-to-site;
- 6.5 Criptografia, 3DES, AES128, AES256, AES-GCM-128
- 6.6 Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 6.7 Algoritmo Internet Key Exchange (IKE) versões I e II;
- 6.8 AES 128 e 256 (Advanced Encryption Standard);
- 6.9 Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;
- 6.10 Possuir suporte a VPN SSL;
- 6.11 Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- 6.12 Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:
 - RDP;
 - VNC;
 - SSH;
 - WEB;
 - SMB.
- 6.13 Deve permitir a arquitetura de vpn hub and spoke;
- 6.14 Suporte a VPNs IPsec client-to-site;
- 6.15 Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
- 6.16 Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- 6.17 Possuir funcionalidades de Auto-Discovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub);
- 6.18 A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:
 - Site-to-Site;
 - Full-Mesh;
 - Star.



7 FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:

- 7.1 A Detecção de Intrusão deverá ser baseada em appliance;



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 7.2 Possuir no mínimo 25.000 (vinte e cinco mil) assinaturas ou regras de IPS/IDS;
- 7.3 O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- 7.4 Possuir tecnologia de detecção baseada em assinatura;
- 7.5 Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;
- 7.6 Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;
- 7.7 O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- 7.8 Possuir opção para administrador nas listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.
- 7.9 Possuir capacidade de remontagem de pacotes para identificação de ataques;
- 7.10 Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- 7.11 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 7.12 Mecanismos de detecção/proteção de ataques;
- 7.13 Reconhecimento de padrões;
- 7.14 Análise de protocolos;
- 7.15 Detecção de anomalias;
- 7.16 Detecção de ataques de RPC (Remote procedure call);
- 7.17 Proteção contra ataques de Windows ou NetBios;
- 7.18 Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- 7.19 Proteção contra ataques DNS (Domain Name System);
- 7.20 Proteção contra ataques a FTP, SSH, Telnet e rlogin;
- 7.21 Proteção contra ataques de ICMP (Internet Control Message Protocol);
- 7.22 Alarmes na console de administração;
- 7.23 Alertas via correio eletrônico;



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 7.24 Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- 7.25 Capacidade de resposta/logs ativa a ataques;
- 7.26 Terminação de sessões via TCP resets;
- 7.27 Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 7.28 O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- 7.29 Possuir filtros de ataques por anomalias;
- 7.30 Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- 7.31 Permitir filtros de anomalias de protocolos;
- 7.32 Suportar reconhecimento de ataques de DDoS, reconnaissance, exploits e evasion;
- 7.33 Suportar verificação de ataque nas camadas de aplicação.

8 FUNCIONALIDADES DE QOS:

- 8.1 Adotar solução de Qualidade de Serviço baseada em appliance;
- 8.2 Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- 8.3 Permitir modificação de valores DSCP;
- 8.4 Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- 8.5 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 8.6 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;



[Handwritten signature]



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 8.7 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- 8.8 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- 8.9 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

9 FUNCIONALIDADES DO THREAT PROTECTION:

- 9.1 Possuir funções de Antivírus, Anti-spyware;
- 9.2 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- 9.3 Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- 9.4 Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;
- 9.5 Permitir o bloqueio de download de arquivos por tamanho.

10 FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB:

- 10.1 Possuir solução de filtro de conteúdo web integrado a solução de segurança;
- 10.2 Possuir pelo menos 80 categorias para classificação de sites web;
- 10.3 Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;
- 10.4 Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
 - Webmail;
 - Instituições de Saúde;
 - Notícias;
 - Pornografia;
 - Restaurante;
 - Mídias Sociais;
 - Esporte;
 - Educação;
 - Games;



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- Compras.
- 10.5 Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
 - 10.6 Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
 - 10.7 Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;
 - 10.8 Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
 - 10.9 Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
 - 10.10 Possibilitar a integração com servidores de cache WEB externos;
 - 10.11 Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®, Youtube®, Facebook®, Google Maps®;
 - 10.12 Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;
 - 10.13 Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
 - 10.14 Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
 - 10.15 Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
 - 10.16 Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de base de URL própria atualizável;
 - 10.17 Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
 - 10.18 Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

válido;

- 10.19 Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- 10.20 Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- 10.21 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 10.22 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- 10.23 Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- 10.24 Deverá permitir o bloqueio de páginas web por classificação como páginas que facilitam a busca de áudio, vídeo e URLs originadas de Spam;
- 10.25 Deverá permitir a criação de listas personalizadas de URLs permitidas - lista branca e bloqueadas - lista negra;
- 10.26 Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- 10.27 Deverá permitir configurar a porta do Proxy Explícito.

11 FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES:

- 11.1 As funcionalidades devem ser baseadas em appliance;
- 11.2 Deverá reconhecer no mínimo 2000 aplicações;
- 11.3 Deverá possuir pelo menos 15 categorias para classificação de aplicações;
- 11.4 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
 - P2P;
 - Web;
 - Transferência de arquivos;
 - Chat;
 - Social.
- 11.5 Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 11.6 Deverá integrar-se ao serviço de diretório padrão



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

- 11.7 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- 11.8 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- 11.9 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- 11.10 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 11.11 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- 11.12 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

12 SD-WAN:

- 12.1 Entende-se como tecnologia SD-WAN (Software Defined-WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;
- 12.2 Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- 12.3 Permitir utilizar VPN IPsec para interligar unidades remotas;
- 12.4 Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;
- 12.5 O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

monitoramento do consumo de banda, perda de pacotes, jitter e latência;

- 12.6 Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN;
- 12.7 O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação;
- 12.8 O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado seja avaliado. Deve suportar especificar um valor variando de 1 a 100;
- 12.9 O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;
- 12.10A solução de SD-WAN UTM deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;
- 12.11 Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:
 - Consumo de banda;
 - Perda de pacotes;
 - Jitter;
 - Latência.

13 ALTA DISPONIBILIDADE:

- 13.1 Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over;
- 13.2 Deverá haver possibilidade de criação de uma VM (máquina virtual) com as mesmas características do appliance, para uso emergencial, mantida em Standby (custos com licenciamento, se houver, deverão estar inclusos);
- 13.3 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

modificação de parâmetro/configuração seja realizada pelo administrador;

- 13.4 O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

14 SERVIÇO DE INSTALAÇÃO:

- 14.1 Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;
- 14.2 Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;
- 14.3 A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;
- 14.4 Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada.

15 TREINAMENTO PARA O SISTEMA DE FIREWALL UTM

- 15.1 Deverá ser fornecido treinamento referente a solução de firewall adquirida (hardware e software) para a equipe de TI do SEMAE (no mínimo 2 colaboradores);
- 15.2 Carga Horária mínima de 30 horas;
- 15.3 O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação na assinatura do contrato;
- 15.4 Poderá ser de forma remota (desde que não haja prejuízos operacionais) ou presencial; caso seja presencial, toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação, instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;
- 15.5 O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- 15.6 Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;
- 15.7 Este treinamento poderá ser realizado em ambiente externo ao do SEMAE, inclusive com os recursos para laboratórios (hands on) salvo em caso de necessidade e acordo entre CONTRATADA e CONTRATANTE;
- 15.8 Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE, de forma imediata após o recebimento do equipamento;
- 15.9 A CONTRATADA deverá realizar o treinamento nas dependências da CONTRATANTE com os requisitos mínimos de infraestrutura de sala de treinamento (caso haja necessidade de treinamento presencial).

16 SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO:

- 16.1 Serviço de suporte para os equipamentos de segurança de borda contratados, no esquema 14x6 (de segunda à sábado, das 8h às 22h), com banco de 10 horas de suporte/mês, pelo tempo de contrato, com as seguintes características:
- A CONTRATADA deve possuir serviço de abertura de chamados remoto capaz de permitir registrar chamados pela CONTRATADA de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
 - A contratada deverá iniciar o atendimento de suporte em no máximo 8 (oito) horas úteis após a abertura do chamado;
 - A contratada deverá fornecer atestado comprovando a existência de equipe técnica de pessoas (no mínimo duas) capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante, apresentado no ato de assinatura do contrato;
 - Na impossibilidade de solução de forma remota, a CONTRATADA deverá providenciar suporte presencial, com todos os custos de deslocamento por conta da CONTRATADA;



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

- Em caso de defeito no hardware, o mesmo deverá ser substituído imediatamente pela solução de VM (máquina virtual), o qual permitirá a retirada do equipamento com defeito, com todos os custos de retirada e envio por parte da CONTRATADA.

16.2 A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações:

- Quando constatado que o problema está relacionado a "bug" no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno.

17 DOCUMENTOS PARA PARTICIPAÇÃO:

17.1 Atestado de Capacidade Técnica, em nome da LICITANTE, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de equipamentos similares aos ofertados, de mesma finalidade, com serviços de instalação, treinamento e suporte técnico, devendo estar explícita a marca, modelo e a quantidade fornecida;

17.2 A LICITANTE deverá emitir declaração que cumprirá todos os requisitos técnicos do edital e seus anexos.

18 DOCUMENTOS PARA CONTRATO:

18.1 Declaração do fabricante do equipamento informando que a CONTRATADA está autorizada a prestar suporte técnico na solução ofertada;

18.2 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 da solução.





DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

19 REQUISITOS:

- 19.1 Os produtos que compõe a Solução de Segurança devem todos ser produzidos pelo mesmo fabricante;
- 19.2 A CONTRATADA deverá prestar suporte para a instalação dos produtos de segurança contratados.

20 DA GESTÃO E FISCALIZAÇÃO DO CONTRATO:

- 20.1 Fica designado o servidor José Odivaldo Chitolina Junior, funcional 1829-6, Chefe de Divisão de Tecnologia da Informação, para os serviços de gestão e fiscalização do contrato.

21 CONDIÇÕES DE ENTREGA E INSTALAÇÃO:

- 21.1 A solução objeto do presente termo deverá ser entregue na Divisão de TI do SEMAE, na Rua XV de Novembro, 2200, Bairro Alto, Piracicaba - SP, para ser regularmente instalada sob orientação técnica da empresa CONTRATADA.
- 21.2 O prazo de entrega e instalação deverá ser de até 30 (trinta) dias - no local informado, após a emissão de Ordem de Serviço.
- 21.3 Após a entrega, será feita a verificação das condições e características dos equipamentos. Havendo irregularidades a empresa deverá repor o equipamento defeituoso ou em desconformidade com o que foi solicitado no prazo máximo de 48 (quarenta e oito) horas a partir da data do comunicado efetuado pelo SEMAE.
- 21.4 O equipamento ofertado deverá possuir prazo de garantia legal de no mínimo 12 (doze) meses, contado a partir do recebimento definitivo.
- 21.5 Durante a garantia deverão ser substituídas, sem nenhum ônus adicional, peças ou partes defeituosas, salvo quando o defeito for provocado por uso indevido do equipamento, devidamente comprovado.
- 21.6 Os equipamentos deverão ser entregues devidamente embalados



DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

e com seus respectivos manuais e certificados de garantia.

21.7 Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 12 meses; deverá permitir a atualização do software e do sistema operacional, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

22 CONDIÇÕES DE CONSERVAÇÃO E MANUTENÇÃO:

22.1 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.

22.2 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.

22.3 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.

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

22.5 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.

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



[Handwritten signature]



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

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


José Odivaldo Chitolina Junior
Divisão de Tecnologia da Informação