CIDADE DE SÃO PAULO
EDUCAÇÃO

Consulta Pública n° 29/SME/2021

TERMO DE REFERÊNCIA

Processo nº 6016.2022/0078383-4

1 OBJETO

1.1 Contratação de empresa especializada para fornecimento de solução e serviços, equipamentos e licenciamento de software, garantia e suporte técnico de solução de "Software Defined Wide Area Network" (SD-WAN), visando atender as necessidades da Secretaria Municipal de Educação de São Paulo (SME/SP).

2 DESCRIÇÃO

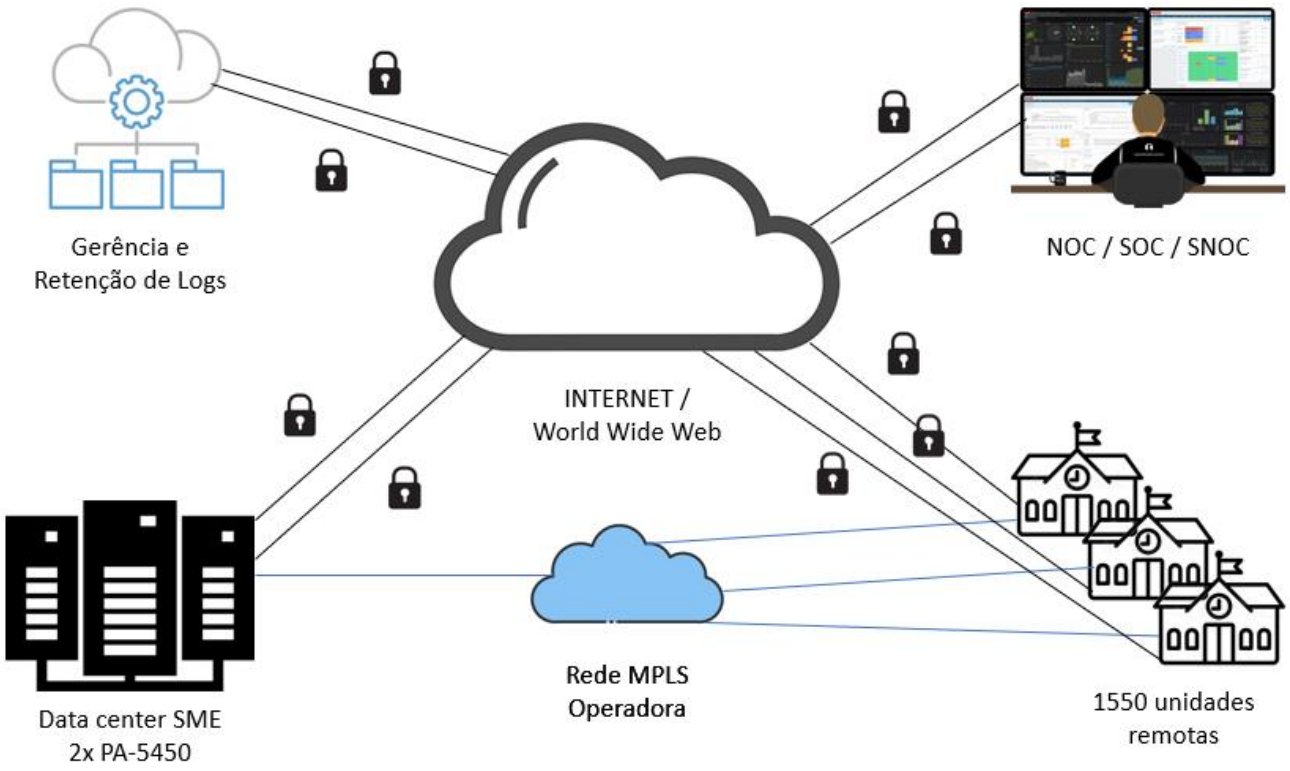
2.1 Este termo refere-se à contratação de empresa especializada para fornecimento de serviços, equipamentos e licenciamento de software, garantia e suporte técnico de solução de "Software Defined Wide Area Network" (SD-WAN), visando atender as necessidades da Secretaria Municipal de Educação de São Paulo (SME/SP), pelo período de 60 meses.

2.2 Atualmente a SME possui em sua infraestrutura uma solução de Segurança da Informação composta por Chassis de Next Generation Firewalls, Relatoria e Autenticação Centralizada, que deve ser integrada a solução proposta:

Quantidade	Produto	Descrição	Part Number
02	PA-5450	Palo Alto Networks PA-5450	PAN-PA-5450-AC-SYS

2.3 A solução ofertada deve ter todas as suas funcionalidades compatíveis com os equipamentos descritos na tabela acima, sendo possível gerenciar, monitorar, coletar logs, autenticar, terminar SD-WAN e garantir a total interoperabilidade entre eles, mesmo após atualizações.

2.4 O cenário desejado é representado no esquema abaixo:



2.5 O serviço deve contemplar os seguintes itens:

	ITEM	DESCRIÇÃO	QUANTIDADE
LOTE ÚNICO	01	Equipamento para terminação de SD-WAN, licenciado e suportado por 60 meses	1550 unidades
	02	Serviço de instalação para equipamento de terminação SD-WAN	1550 unidades
	03	Solução de gerência centralizada e retenção de logs para os 1550 equipamentos de terminação SD-WAN, licenciado e suportado por 60 meses	1 unidade
	04	Serviço de instalação para solução de gerência centralizada e retenção de logs	1 unidade
	05	Expansão para aumento de processamento e licenciamento de solução centralizadora de SD-WAN pelo período de 60 meses	2 unidades
	06	Serviço de instalação para expansão e licenciamento de SD-WAN por 60 meses	1 unidade
	07	Treinamento oficial do fabricante da solução de SD-WAN para configuração, gerências e resolução de problemas dos equipamentos	65 Horas
	08	Serviço mensal de manutenção e monitoramento e correlacionamento de eventos (SNOC) para 1550 terminadores SD-WAN e 2 concentradores SD-WAN, incluindo toda a infraestrutura (hardware, software, serviço, pessoal e datacenter ou cloud) para a plena realização do serviço	60 meses
	09	Garantia e suporte técnico on-site	60 meses

3 CARACTERISTICAS GERAIS

3.1 Equipamento para terminação de SD-WAN, licenciado e suportado por 60 meses

3.1.1 Características de desempenho

3.1.1.1 Throughput de pelo menos 2.9 Gbps de Next Generation Firewall

3.1.1.2 Throughput de pelo menos 1 Gbps de proteção contra ameaças conhecidas, desconhecidas, filtro de URL ativo e log habilitado

3.1.1.3 Throughput de pelo menos 1.5 Gbps para VPN IPSec

3.1.1.4 Capacidade de pelo menos 200 mil sessões simultâneas

3.1.2 Disco interno de pelo menos 128Gb

3.1.3 As características devem ser comprovadas por documentos de domínio público do fabricante

3.1.4 Deve ser fornecido, pelo período mínimo de 60 meses, as licenças exigidas para o completo atendimento das especificações deste termo de referência;

3.1.5 O equipamento deve estar coberto por suporte e garantia do fabricante pelo período mínimo de 60 meses;

3.1.6 Os equipamentos devem suportar se conectar diretamente pelos protocolos de SD-WAN com os equipamentos já disponíveis no datacenter da SME, sendo eles duas unidades de Palo Alto Networks PA-5450.

3.1.7 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

3.1.8 A solução deverá consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW);

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

3.1.10 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

3.1.11 A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7;

3.1.12 O hardware e software que executem as funcionalidades de proteção de rede deverão ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3.1.13 Em caso de perda ou vencimento de licenciamento o equipamento deverá ser capaz de manter a sua operação de funcionamento, e configurações não causando indisponibilidade nos serviços de conectividade da unidade qual está instalado, até a regularização ou inserção de novas licenças.

3.1.14 O software deverá ser fornecido em sua versão mais atualizada recomendada pelo fabricante;

3.1.15 Os dispositivos de proteção de rede deverão possuir pelo menos as seguintes funcionalidades:

3.1.15.1 Suporte a 4094 VLAN Tags 802.1q;

3.1.15.2 Agregação de links 802.3ad e LACP;

3.1.15.3 Policy based routing ou policy based forwarding;

3.1.15.4 Roteamento multicast (PIM-SM);

3.1.15.5 DHCP Relay;

3.1.15.6 DHCP Server;

3.1.15.7 Jumbo Frames;

3.1.15.8 Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3.

3.1.15.9 Suportar sub-interfaces ethernet lógicas;

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

3.1.16 Deverá suportar os seguintes tipos de NAT:

3.1.16.1 NAT dinâmico (Many-to-1);

3.1.16.2 NAT dinâmico (Many-to-Many);

3.1.16.3 NAT estático (1-to-1);

3.1.16.4 NAT estático (Many-to-Many);

3.1.16.5 NAT estático bidirecional 1-to-1;

3.1.16.6 Tradução de porta (PAT);

3.1.16.7 NAT de Origem;

3.1.16.8 NAT de Destino;

3.1.16.9 Suportar NAT de Origem e NAT de Destino simultaneamente;

3.1.17 Deverá implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico.

3.1.18 Deverá implementar o protocolo ECMP:

3.1.18.1 Deverá implementar balanceamento de link por hash do IP de origem;

3.1.18.2 Deverá implementar balanceamento de link por hash do IP de origem e destino;

3.1.18.3 Deverá implementar balanceamento de link através do método round-robin;

3.1.19 Deverá ser capaz de receber e gerenciar individualmente, com implementação de conceito SDWan no mínimo 3 portas WAN, para saídas de internet de tecnologias diferentes, idênticas ou mistas.

3.1.20 Deverá implementar balanceamento de link por peso. Nesta opção deverá ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deverá suportar o balanceamento de, no mínimo, quatro links;

3.1.21 Deverá implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

3.1.22 Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino;

3.1.23 Deverá implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance deverão ser acessíveis via SNMP;

3.1.24 Enviar log para sistemas de monitoração externos, simultaneamente;

3.1.25 Deverá haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

3.1.26 Deverá permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

3.1.27 Proteção contra anti-spoofing;

3.1.28 Deverá permitir bloquear sessões TCP que usarem variações do 3-way hand shake, como 4 way e 5 way split handshake, prevenindo desta forma possíveis tráfegos maliciosos;

3.1.29 Deverá permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

3.1.30 Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver descriptografia de SSL e SSH;

3.1.30.1 Para IPv4, deverá suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.1.30.2 Para IPv6, deverá suportar roteamento estático e dinâmico (OSPFv3)

3.1.31 Suportar a OSPF graceful restart;

3.1.32 Deverá suportar o protocolo mp-bgp (multiprotocol bgp) permitindo que o firewall possa anunciar rotas multicast para ipv4 e rotas unicast para ipv6;

3.1.33 Suportar no mínimo as seguintes funcionalidades em ipv6: slaac (address auto configuration), nat64, identificação de usuários a partir do ldap/ad, captive portal, ipv6 over ipv4 ipsec, regras de proteção contra dos (denial of service), descriptografia ssl e ssh, pbf (policy based forwarding), qos, dhcpv6 relay, ipsec, vpn ssl, ativo/ativo, ativo/passivo, snmp, ntp, syslog, dns, neighbour discovery (nd), recursive dns server (rdnss), dns search list (dnssl) e controle de aplicação;

3.1.34 A funcionalidade nat64 é extremamente importante para este momento de transição entre ipv4 e ipv6, por tanto é requisitado que o dispositivo ofertado tenha suporte, devido a iminente escassez de endereços ipv4, juntamente com a crescente demanda para conectar usuários, máquinas e dispositivos iot, sendo que, implantar puramente o protocolo ipv6 em paralelo com ipv4 (dual-stack) não garante a continuidade de expansão, tendo em vista que o número de endereços ipv4 é infinitamente menor comparado com a oferta do ipv6, uma vez que as duas pilhas de protocolos deverão muitas vezes coexistir;

3.1.35 Os dispositivos de proteção deverão ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3):

3.1.35.1 Modo Sniffer para inspeção via porta espelhada do tráfego de dados da rede;

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

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

3.1.35.4 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.1.36 Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

3.1.36.1 Em modo transparente;

3.1.36.2 Em layer 3.

3.1.37 A configuração em alta disponibilidade deverá sincronizar:

3.1.37.1 Sessões;

3.1.37.2 Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

3.1.37.3 Associações de Segurança das VPNS;

3.1.37.4 Tabelas FIB;

3.1.37.5 HA (modo de Alta-Disponibilidade) deverá possibilitar monitoração de falha de link.

3.1.38 Deverá possuir nativamente ou ferramentas externas que indique as regras sobrepostas e objetos não utilizados para permitir a otimização das regras em uso, facilitando a eliminação de elementos em desuso ou a possibilidade de mesclar os elementos no aspecto de gerenciamento;

3.1.39 Deverá permitir nativamente ou, através de composição com ferramentas líderes de mercado, a revisão periódica de regras aplicadas e as respectivas aplicações em uso, sugerindo pelo contratado quais modificações deverão ser realizadas para filtrar o tráfego de acordo com as aplicações mais utilizadas, em detrimento das regras iniciais migradas, desta maneira, substituindo gradativamente as regras de porta e protocolo para aplicação, evitando técnicas de by-pass de controles de camada 3 e 4. O fluxo mínimo de análise de regras deverá trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso em regras primariamente mantidas por porta/protocolo. A solução deverá permitir a análise de tráfego das aplicações por regra em um período de até 30 dias;

3.1.40 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.1.41 Controle por política de firewall:

3.1.41.1 Deverá suportar controles por zona de segurança;

3.1.41.2 Controles de políticas por porta e protocolo;

3.1.41.3 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

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

3.1.41.5 Deverá suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

3.1.41.6 Deverá permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

3.1.41.7 Deverá permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

3.1.41.8 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

3.1.41.9 Controle, inspeção e descriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

3.1.41.10 Deverá suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

3.1.41.11 Deverá descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

3.1.41.12 Deverá descriptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

3.1.41.13 Controle de inspeção e descriptografia de SSH por política;

3.1.41.14 A descriptografia de SSH deverá possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

3.1.41.15 A plataforma de segurança deverá implementar espelhamento de tráfego de criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

3.1.41.16 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

3.1.41.17 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

3.1.41.18 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações; 3.1.43.19. Suporte a objetos e regras IPV6;

3.1.41.19 Suporte a objetos e regras multicast;

3.1.41.20 Deverá suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

3.1.41.21 Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

3.1.42 Controle de aplicações

3.1.42.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.1.42.2 Deverá ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

3.1.42.3 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.1.42.4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, Linkedin, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, OneDrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs etc.;

3.1.42.5 Deverá inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deverá determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

3.1.42.6 Deverá aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

3.1.42.7 Identificar o uso de táticas evasivas, ou seja, deverá ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

3.1.42.8 Para tráfego criptografado SSL, deverá descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.1.42.9 Deverá realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deverá identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que deverão ser inspecionados de acordo as regras de segurança implementadas;

3.1.42.10 Deverá permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deverá permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

3.1.42.11 Deverá permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Microsoft 365, Skype, aplicativos Google, Gmail etc.;

3.1.42.12 Identificar o uso de táticas evasivas via comunicações criptografadas;

3.1.42.13 Atualizar a base de assinaturas de aplicações automaticamente;

3.1.42.14 Reconhecer aplicações em IPv6;

3.1.42.15 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

3.1.42.16 Os dispositivos de proteção de rede deverão possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

3.1.42.17 Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

3.1.42.18 Deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

3.1.42.19 Para manter a segurança da rede eficiente, deverá suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

3.1.42.20 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.1.42.21 A criação de assinaturas personalizadas deverá permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

3.1.42.22 HTTP, FTP, SMB, SMTP, IMAP e POP3.

3.1.42.23 O fabricante deverá permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

3.1.42.24 Deverá alertar o usuário quando uma aplicação for bloqueada;

3.1.42.25 Deverá permitir a customização da mensagem de bloqueio;

3.1.42.26 Deverá possibilitar que o controle de portas seja aplicado para todas as aplicações

3.1.42.27 Deverá permitir criar filtro na tabela de regras de segurança para exibir somente:

3.1.42.27.1 Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

3.1.42.27.2 Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

3.1.42.27.3 Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

3.1.42.28 Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.42.29 Deverá possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.42.30 Deverá possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Messenger do Facebook e bloquear a transferência de arquivos ou permitir o WhatsApp e bloquear a transferência de arquivos;

3.1.42.31 Deverá possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.42.32 Deverá ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

3.1.42.32.1 Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol etc.).

3.1.42.32.2 Nível de risco da aplicação;

3.1.42.32.3 Categoria e subcategoria de aplicações;

3.1.42.32.4 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda etc.

3.1.42.33 Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). O fluxo mínimo de análise de regras legadas deve trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

3.1.43 Prevenção de ameaças

3.1.44 Para proteção do ambiente contra ataques, os dispositivos de proteção deverão possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

3.1.45 Deverá incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.1.46 As funcionalidades de IPS, Antivírus e Anti-Spyware deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.1.47 Deverá implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Anti Spyware: permitir, permitir e gerar log, bloquear, bloquear ip do atacante por um intervalo de tempo e enviar tcp-reset;

3.1.48 Deverá possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;

3.1.49 As assinaturas deverão poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

3.1.50 Exceções por IP de origem ou de destino deverão ser possíveis nas regras, de forma geral e assinatura a assinatura.

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

3.1.52 Deverá permitir o bloqueio de vulnerabilidades.

3.1.53 Deverá permitir o bloqueio de exploits conhecidos.

3.1.54 Deverá incluir proteção contra ataques de negação de serviços.

3.1.55 Deverá suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE.

3.1.56 Deverá possuir os seguintes mecanismos de inspeção de IPS:

3.1.56.1 Análise de padrões de estado de conexões;

3.1.56.2 Análise de decodificação de protocolo;

3.1.56.3 Análise para detecção de anomalias de protocolo;

3.1.56.4 Análise heurística;

3.1.56.5 IP Defragmentation;

3.1.56.6 Remontagem de pacotes de TCP;

3.1.56.7 Bloqueio de pacotes malformados.

3.1.56.8 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof etc.;

3.1.56.9 Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

3.1.56.10 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

3.1.56.11 Possuir assinaturas específicas para a mitigação de ataques DoS;

3.1.56.12 Possuir assinaturas para bloqueio de ataques de buffer overflow;

3.1.56.13 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

3.1.56.14 Deverá permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

3.1.56.15 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

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

3.1.56.17 Suportar bloqueio de arquivos por tipo;

3.1.56.18 Identificar e bloquear comunicação com botnets;

3.1.56.19 Deverá suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

3.1.56.20 Deverá suportar referência cruzada com CVE;

3.1.57 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

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

3.1.58 Deverá suportar a captura de pacotes (PCAP), por assinatura de IPS e Anti-Spyware;

3.1.59 Deverá permitir que na captura de pacotes por assinaturas de IPS e Anti-Spyware seja definido o número de pacotes a serem capturados. Esta captura deverá permitir selecionar, no mínimo, 50 pacotes;

3.1.60 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

3.1.61 Os eventos deverão identificar o país de onde partiu a ameaça;

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

3.1.63 Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

3.1.64 Rastreamento de vírus em pdf.

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

3.1.66 Se tratando do Microsoft Office365 a solução contratada deverá permitir a restrição de domínios não vinculados à instituição para os funcionários administrativos, desta maneira evitando que o acesso a contas pessoais de e-mails, sejam bloqueadas garantindo que dados possam ser apenas trocados por intermédio do domínio Microsoft contratado pela instituição.

3.1.67 Deverá ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

3.1.68 **Análise de malwares modernos:**

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

3.1.68.2 O dispositivo de proteção deverá ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

3.1.68.3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

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

3.1.68.5 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida; S

3.1.68.6 uportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10 e MacOS;

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

3.1.68.8 A solução deverá possuir a capacidade de analisar em sandbox links (http e HTTPs) presentes no corpo de e-mails trafegados em SMTP e POP3. Deverá ser gerado um relatório caso a abertura do link pela sandbox o identifique como site hospedeiro de exploits;

3.1.68.9 A análise de links em sandbox deverá ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

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

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

3.1.68.12 O sistema automático de análise "In Cloud" ou local deverá emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

3.1.68.13 Deverá permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

3.1.68.14 Deverá permitir o download dos malwares identificados a partir da própria interface de gerência;

3.1.68.15 Deverá permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

3.1.68.16 Deverá permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência.

3.1.68.17 Caso a solução seja fornecida em appliance local, deverá possuir, no mínimo, 28 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;

3.1.68.18 Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas deverão ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

3.1.68.19 Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

3.1.68.20 Suportar, pelo menos, a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP, no ambiente de sandbox;

3.1.68.21 Deverá atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox com frequência de, pelo menos, a cada minuto;

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

3.1.68.23 Deverá permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;

3.1.68.24 Deve prevenir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.

3.1.69 Proteção de DNS:

3.1.69.1 Deverá prover segurança automática para tráfego de DNS, com análise em cloud, provendo aos equipamentos, acesso a assinaturas de DNS, geradas utilizando análise preditiva e aprendizado de máquina, fornecendo dados de domínios maliciosos;

3.1.69.2 Deverá permitir configuração de categorias de assinaturas de DNS, para possibilitar a criação de políticas de segurança distintas, baseadas em fatores de risco associados com certos tipos de tráfego DNS;

3.1.69.3 Deverá proteger contra ameaças baseadas em DNS, incluindo aquelas baseadas em DNS dinâmico, domínios registrados recentemente e domínios de phishing;

3.1.69.4 Deverá proteger contra comunicações de command and control e roubo de dados baseadas em DNS.

3.1.69.5 O Dispositivo de próxima geração deverá, em sua característica de proteção de DNS, permitir o bloqueio de técnicas de Domain generation algorithms (DGA), evitando assim, que uma máquina contaminada possa tentar estabelecer em um curto espaço de tempo sessão com domínios maliciosos ou inexistentes.

3.1.70 Filtro de URL

3.1.70.1 A plataforma de segurança deverá possuir as seguintes funcionalidades de filtro de URL:

3.1.70.1.1 Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.1.70.2 Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança;

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

3.1.70.4 Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

3.1.70.5 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.1.70.6 Deverá bloquear o acesso à sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deverá ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

3.1.70.7 Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

3.1.70.8 Possuir pelo menos 60 categorias de URLs;

3.1.70.9 Deverá classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

3.1.70.10 Deverá possuir categoria específica para classificar domínios recém registrados (com menos de 30 dias);

3.1.70.11 A solução deverá ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;

3.1.70.12 A solução deverá permitir que sites classificados com a categoria errada sejam reavaliados pelo fabricante;

3.1.70.13 A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

3.1.70.14 Suportar a criação categorias de URLs customizadas;

3.1.70.15 Suportar a exclusão de URLs do bloqueio, por categoria;

3.1.70.16 Permitir a customização de página de bloqueio;

3.1.70.17 Deverá proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deverá ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

3.1.70.18 Deverá permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

3.1.70.19 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

3.1.70.20 Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

3.1.70.21 Deverá salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

3.1.71 Identificação de usuários

3.1.71.1 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

3.1.71.2 Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; D

3.1.71.3 Deverá possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.1.71.4 Deverá implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

3.1.71.5 Deverá possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

3.1.71.6 Deverá suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

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

3.1.71.8 Suportar a autenticação Kerberos;

3.1.71.9 Deverá suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuário de VPN SSL;

3.1.71.10 Deverá possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

3.1.71.11 Deverá identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

3.1.71.12 Deverá permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;

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

3.1.71.14 Deverá implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.1.71.15 Deverá possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

3.1.72 QOS

3.1.72.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, vimeo etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deverá ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

3.1.72.2 Suportar a criação de políticas de QoS por:

3.1.72.2.1 Endereço de origem;

3.1.72.2.2 Endereço de destino;

3.1.72.2.3 Por usuário e grupo do LDAP/AD;

3.1.72.2.4 Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

3.1.72.2.5 Por porta.

3.1.72.3 O QoS deverá possibilitar a definição de classes por:

3.1.72.3.1 Banda Garantida;

3.1.72.3.2 Banda Máxima;

3.1.72.3.3 Fila de Prioridade.

3.1.72.4 Suportar priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

3.1.72.5 Suportar marcação de pacotes Diffserv, inclusive por aplicação.

3.1.72.6 Deverá implementar QOS (traffic-shaping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deverá ser efetuada nos dois sentidos da conexão (Inbound e Outbound);

3.1.72.7 Disponibilizar estatísticas Real Time para classes de QoS.

3.1.72.8 Deverá suportar QOS (traffic-shaping), em interface agregadas;

3.1.72.9 Deverá permitir o monitoramento do uso que as

3.1.72.10 aplicações fazem por bytes, sessões e por usuário em tempo real.

3.1.73 Filtro de dados

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

3.1.73.2 Os arquivos deverão ser identificados por extensão e assinaturas;

3.1.73.3 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos, incluindo, mas não limitado a MS Office e PDF, identificados sobre aplicações (P2P, Instant Messaging, SMB etc.);

3.1.73.4 Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

3.1.73.6 Permitir listar o número de aplicações suportadas para controle de dados;

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

3.1.74 Geolocalização

3.1.74.1 Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

3.1.74.2 Deverá possibilitar a visualização dos países de origem e destino nos logs dos acessos;

3.1.74.3 Deverá permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;

3.1.74.4 Deverá possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

3.1.75 VPN

3.1.75.1 Suportar VPN Site-to-Site e Cliente-To-Site;

3.1.75.2 Suportar IPSec VPN;

3.1.75.3 Suportar SSL VPN;

3.1.75.4 A VPN IPSec deverá suportar:

3.1.75.4.1 DES e 3DES;

3.1.75.4.2 Autenticação MD5 e SHA-1;

3.1.75.4.3 Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

3.1.75.4.4 Algoritmo Internet Key Exchange (IKEv1 e v2);

3.1.75.4.5 AES 128, 192 e 256 (Advanced Encryption Standard);

3.1.75.4.6 Autenticação via certificado IKE PKI.

3.1.75.5 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

3.1.75.6 Deverá permitir a atribuição de endereço IP nos clientes remotos de VPN SL;

3.1.75.7 3.1.53.7. Deverá permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

3.1.75.8 3.1.53.8. Deverá permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

3.1.75.9 Deverá permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

3.1.75.10 Deverá permitir a atribuição de DNS nos clientes remotos de VPN;

3.1.75.11 Deverá permitir que seja definido métodos de autenticação distintos por Sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac Windows e Chrome OS);

3.1.75.12 A solução de VPN deverá verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deverá ser bloqueado caso o dispositivo não seja o correto;

3.1.75.13 Deverá possuir lista de bloqueio para dispositivos que forem reportados como roubado ou perdido pelo usuário;

3.1.75.14 Deverá haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

3.1.75.15 Deverá exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deverá permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

3.1.75.16 Deverá avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deverá permitir também a customização da mensagem com informações relevantes para o usuário;

3.1.75.17 Deverá permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.1.75.18 A VPN SSL deverá suportar proxy arp e uso de interfaces PPPOE;

3.1.75.19 Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

3.1.75.20 Deverá permitir a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada;

3.1.75.21 Permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

3.1.75.22 Suportar leitura e verificação de CRL (Certificate Revocation List);

3.1.75.23 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

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

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

3.1.75.26 Deverá permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

3.1.75.27 Antes do usuário autenticar na estação;

3.1.75.28 Após autenticação do usuário na estação;

3.1.75.29 Sob demanda do usuário.

3.1.75.30 Deverá manter uma conexão segura com o portal durante a sessão;

3.1.75.31 O Suporte do fabricante deverá contemplar atendimento para a resolução de problemas nos clientes de VPN;

3.1.75.32 O agente de VPN SSL client-to-site deverá ser compatível com os sistemas operacionais Windows XP, Vista, 7, 8, 10, e Mac OSx.

3.1.75.33 Deverá possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

3.1.76 SD-WAN

3.1.76.1 Deverá operacionalizar no mínimo os seguintes critérios de SD-WAN:

3.1.76.2 As configurações de profiles de SD-WAN deverão partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução, assim flexibilizando a configuração inicial e suas devidas manutenções;

3.1.76.3 A solução deverá permitir operar em caráter de diagrama hub-spoke;

3.1.76.4 Os dispositivos deverão ter a capacidade de exibir impactos por aplicação;

3.1.76.5 A solução deverá permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo itens em porcentagem ou contadores, jitter, latência e perda de pacote;

3.1.76.6 O dispositivo deverá compreender o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garantir que a experiência do usuário sofra o menor impacto possível;

3.1.76.7 O SD-WAN deverá suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LTE /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.

3.1.76.8 A solução deverá ter inteligência para executar no mínimo as seguintes lógicas de operação:

3.1.76.8.1 Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G deverão ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS;

3.1.76.8.2 Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deverá permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresente resultados abaixo dos limites definidos;

3.1.76.8.3 Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

3.1.76.8.4 Distribuição orientada a qualidade, o dispositivo deverá validar o melhor caminho disponível e utilizar-se deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes.

3.1.76.9 A Solução de SD-WAN deverá desempenhar a função de Forward Error Correlation (FEC).

3.1.76.10 A Solução de SD-WAN deverá desempenhar a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão.

3.1.76.11 Os dispositivos deverão suportar a funcionalidade de ZTP (Zero Touch Provisioning) para que assim, inseridos nas estruturas remotas, possam buscar automaticamente por suas configurações, com o objetivo de facilitar a instalação nas unidades remotas ou a troca de um dispositivo defeituoso.

3.2 Serviço de distribuição e instalação para equipamento de terminação SD-WAN

3.2.1 Os serviços de instalação e configuração deverão compreender, no mínimo, as seguintes atividades:

3.2.1.1 Instalação física on-site dos equipamentos nas unidades desta secretaria;

3.2.1.2 Conectorização e desconectorização e passagem de todo cabeamento necessário para a devida instalação do equipamento na infraestrutura da unidade que receber o equipamento.

3.2.1.3 Fornecimento de até 2 Patch Cord, por unidade de instalação caso necessário.

3.2.1.4 Energização e conexão dos equipamentos em rede;

3.2.1.5 Organização e identificação dos cabeamentos equivalentes a esta instalação, de forma a manter o rack devidamente organizado ao termino das instalações do novo equipamento.

3.2.1.6 Atualização de firmware dos equipamentos;

3.2.1.7 Configuração das interfaces de gerenciamento;

3.2.1.8 Ativação das licenças adquiridas;

3.2.1.9 Configuração das interfaces de rede e regras de roteamento;

3.2.1.10 Configuração dos objetos e regras de firewall e NAT;

3.2.1.11 Ativação e configuração das funcionalidades de console de gerenciamento, URL Filter, controle de aplicação, VPN, prevenção contra ameaças, antivírus e malwares, sandbox e proteção DNS;

3.2.1.12 Ativação e configuração de SD-WAN, conectando todas as localidades diretamente com o os equipamentos de Firewall já existentes no datacenter da SME;

3.2.1.13 Execução de outras configurações que se fizerem necessárias para o pleno atendimento do equipamento a necessidade de SME.

3.2.1.14 Validação e testes das instalações realizadas junto a equipe técnica de COTIC/SME ou responsável por ela determinado.

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

3.2.1.15.1 O documento de As Built deverá possuir registro fotográfico, topologias em padrão de mercado, validação dos testes e expor as configurações realizadas, comprovando a execução dos serviços;

3.2.2 O acionamento da execução dos serviços deverá ser realizado por meio de ordens de fornecimento por etapa da prestação de serviço, se forma que:

3.2.2.1 Deverá ser emitida ordem de fornecimento para o fornecimento dos equipamentos e sua devida guarda:

3.2.2.2 Deverá ser emitida ordem de Serviço para a execução das instalações, com determinação das unidades a serem atendidas.

3.2.2.3 Deverá ser emitida ordem de Serviço para o acionamento dos demais itens de contratação como, treinamentos e serviço de monitoramento.

3.2.3 A execução dos serviços deverá ser planejada de forma a tender a prazos de execução final determinados pela CONTRATANTE, o planejamento anterior ao serviço poderá ser realizado remotamente através de web conferência ou videoconferência.

3.2.4 A meta para finalização da instalação de todas as unidades escolares previstas em SME deverá ser de 6 meses, após a conclusão dos estudos e determinação das configurações necessárias e cronograma de fornecimento e execução, podendo este planejamento ser alterado em caso de necessidade da CONTRATANTE.

3.2.5 O planejamento deverá resultar em um documento contendo as configurações necessárias para atender cada tipo de unidade de SME topologias em padrão de mercado, e cronograma de fornecimento e execução das instalações, de forma que seja possível garantir a previsibilidade das ações, e da finalização das instalações.

3.2.6 A CONTRATADA deverá para cada tipo de unidade de SME, realizar instalação de equipamento como prova de conceito (POC) de forma a validar, comprovar e garantir o atendimento a todas as necessidades especificações expostas no documento de planejamento e o pleno atendimento as necessidades técnicas de SME.

3.2.7 A aprovação das instalações e execução do cronograma total de instalação deverá ser realizado após a execução das unidades de POC.

3.2.8 A entrega efetiva dos equipamentos nas unidades de SME deverá ser realizada em conjunto com a instalação.

3.2.8.1 Desta forma a CONTRATADA deverá garantir que o cronograma de instalação seja executado de acordo com a entrega dos equipamentos pela mesma, não permitindo que os equipamentos fiquem nas unidades escolares sob risco de furto ou outras avarias durante o tempo de execução do projeto.

3.2.8.2 Fica a cargo da CONTRATADA a guarda dos equipamentos durante o período de execução das ações.

3.2.8.3 Durante o período de guarda cabe a CONTRATADA, a responsabilidade quanto a evitar registros de ocorrências devido armazenamento, perdas, furtos, extravio ou outras ocorrências quais possam causar impacto no fornecimento do objeto para a unidade escolar.

3.2.8.4 Caberá a CONTRATADA em caso de ocorrência durante o período de guarda, a obrigação de garantir a reposição de equipamentos que por ventura sofrerem danos, extravios ou outras ocorrências.

3.2.9 Durante toda a implantação do projeto, a CONTRATADA deverá indicar um gerente de projeto para acompanhamento das instalações

3.2.10 O gerente de projetos provido pela CONTRATADA deverá ter, no mínimo a certificação Project Management Professional (PMP®)

3.2.11 O gerente de projetos deverá planejar e acompanhar o cronograma de instalação, interagindo com as equipes responsáveis pelo serviço

3.2.12 Durante a execução das ações o gerente de projeto e representante responsável pelo contrato deve ser o ponto focal de contato entre a CONTRATANTE e a CONTRATADA.

3.2.13 A contratada deve demonstrar como instalar e configurar os equipamentos e os softwares fornecidos, quando alinhado com os recursos do time de tecnologia da SME (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.

3.3 Solução de gerência centralizada e retenção de logs para os 1550 equipamentos de terminação sd-wan, licenciado e suportado por 60 meses

3.3.1 Solução composta por appliances físicos, com capacidade mínima licenciada de administração de 1550 unidades, permitindo futura expansão apenas por licenciamento

3.3.2 Os appliances físicos, quando compostos, devem ser idênticos

3.3.3 A solução deve suportar e estar licenciado para a ingestão de pelo menos 105.000 logs por segundo

3.3.4 A solução deve suportar e estar licenciada para a ingestão e armazenamento de pelo menos 21Tb de logs por dia

3.3.5 A solução deve ser entregue sempre em sua capacidade máxima de armazenamento, sendo não inferior 48tb

3.3.6 Os equipamentos devem estar cobertos por suporte e garantia do fabricante pelo período mínimo de 60 meses

3.3.7 Toda as configurações e operações dos terminadores SD-WAN devem ser realizados a partir de uma única interface.

3.3.7.1 Preferencialmente essa interface deve ser WEB;

3.3.8 O gerenciamento da solução deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

3.3.9 Caso a solução de gerenciamento possua licenciamento relacionado a armazenamento, este deverá ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional.

3.3.10 Deve permitir o controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

3.3.11 Deverá permitir o controle global de políticas para todos os equipamentos que compõe a plataforma de segurança.

3.3.12 Deverá suportar organizar os dispositivos administrados em grupos: os sistemas virtuais deverão ser administrados como dispositivos individuais, grupos geográficos, por funcionalidade (por exemplo, IPS), e distribuição.

3.3.13 Deverá implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.

3.3.14 Deverá implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios.

3.3.15 Deverá permitir a criação de objetos e políticas compartilhadas.

3.3.16 Deverá consolidar logs e relatórios de todos os dispositivos administrados.

3.3.17 Deverá permitir que exportar backup de configuração automaticamente via agendamento.

3.3.18 Deverá permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls.

3.3.19 Deverá mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

3.3.20 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

3.3.21 O gerenciamento da solução deverá suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

3.3.22 Deverá permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa.

3.3.23 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deverá ser compatível com sistemas operacionais Windows e Linux.

3.4 O gerenciamento deverá permitir/possuir:

3.4.1.1 Criação e administração de políticas de firewall e controle de aplicação;

3.4.1.2 Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

3.4.1.3 Criação e administração de políticas de Filtro de URL;

3.4.1.4 Monitoração de logs;

3.4.1.5 Ferramentas de investigação de logs;

3.4.1.6 Debugging;

3.4.1.7 Captura de pacotes em tempo real.

3.5 **Acesso concorrente de administradores:**

3.5.1.1 Deverá permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

3.5.1.2 Deverá mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI;

3.5.1.3 Deverá possuir mecanismo de busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;

3.5.1.4 Deverá possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

3.5.1.5 Deverá permitir usar palavras chaves e cores para facilitar identificação de regras.

3.5.1.6 Deverá permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN client-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas.

3.5.1.7 Deverá suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets.

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

3.5.1.9 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.

3.5.1.10 Autenticação integrada ao Microsoft Active Directory e servidor Radius.

3.5.1.11 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados.

3.5.1.12 Deverá atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DoS.

3.5.1.13 Criação de regras que fiquem ativas em horário definido

3.5.1.14 Criação de regras com data de expiração.

3.5.1.15 Backup das configurações e rollback de configuração para a última configuração salva;

3.5.1.16 Suportar rollback de Sistema Operacional para a última versão local;

3.5.1.17 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

3.5.1.18 Deverá possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

3.5.1.19 Validação de regras antes da aplicação;

3.5.1.20 Deverá implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.:

3.5.1.21 Permitir o uso de appliance externo para permitir a validação de regras antes da aplicação.

3.5.1.22 Deverá realizar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing):

3.5.1.23 Permitir o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

3.5.1.24 Deverá possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

3.5.1.25 Deverá permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;

3.5.1.26 Deverá possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);

3.5.1.27 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

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

3.5.1.29 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

3.5.1.30 Deverá prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-spyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

3.5.1.31 Deverá permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti spyware, malwares "Zero Day "detectados em sandbox e tráfego bloqueado;

3.5.1.32 O gerenciamento da solução deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

3.5.1.33 Deverá permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

3.5.1.34 Deverá possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-spyware), etc.;

3.5.1.35 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-spyware), e URLs que passaram pela solução;

3.5.1.36 Deverá possuir mecanismo "Drill-Down" para navegação nos relatórios em Real Time;

3.5.1.37 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

3.5.1.38 Deverá possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deverá mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

3.5.1.39 Os relatórios de visibilidade e uso sobre aplicativos (SaaS) deverão poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

3.5.1.40 Deverá ser possível exportar os logs em CSV;

3.5.1.41 Deverá ser possível acessar o equipamento e aplicar configurações durante momentos em que o tráfego é muito alto e a CPU e a memória do equipamento estiver totalmente utilizada.

3.5.1.42 Deverá permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

3.5.1.43 Deverá permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação etc. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

3.5.1.43.1 Situação do dispositivo e do cluster;

3.5.1.43.2 Principais aplicações;

3.5.1.43.3 Principais aplicações por risco;

3.5.1.44 Administradores autenticados na gerência da plataforma de segurança;

3.5.1.44.1 Número de sessões simultâneas;

3.5.1.44.2 Status das interfaces;

3.5.1.44.3 Uso de CPU;

3.5.1.44.4 Deverá permitir que os seguintes relatórios sejam gerados:

3.5.1.44.5 Resumo gráfico de aplicações utilizadas;

3.5.1.44.6 Principais aplicações por utilização de largura de banda de entrada e saída;

3.5.1.44.7 Principais aplicações por taxa de transferência de bytes;

3.5.1.44.8 Principais hosts por número de ameaças identificadas;

3.5.1.44.9 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-spyware), de rede vinculadas a este tráfego;

3.5.1.45 Deverá permitir a criação de relatórios personalizados;

3.5.1.46 Possuir capacidade de gerar diferentes tipos de relatório de acesso à internet dos usuários, com opção de exibir informação dos últimos 7 dias de logs, que considerem no mínimo itens de URL e Elementos das aplicações.

3.5.1.47 Em cada critério de pesquisa do log deverá ser possível incluir múltiplas entradas (ex. 10 redes e IPs distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deverá ser possível definir um faixa de tempo como critério de pesquisa.

3.5.1.48 Gerar alertas automáticos via:

3.5.1.48.1 E-mail;

3.5.1.48.2 SNMP;

3.5.1.48.3 Syslog.

3.5.1.49 A solução ofertada deverá permitir 100% de disponibilidade para gestão das configurações e funções administrativas durante um momento de alta carga/ataques de DDoS, ou seja, em caso de alta demanda do plano de processamento de pacotes de rede, o plano de gerenciamento não poderá ser afetado, sendo assim apenas dispositivos com plano dedicado de gerenciamento e processamento de pacotes serão aceitos neste edital.

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

3.6 Serviço de instalação para solução de gerência centralizada e retenção de logs

3.6.1 Os equipamentos, juntamente com seus discos e licenças, devem ser instalados e ativados em datacenter da CONTRATADA ou subcontratado por esta.

3.6.2 a instalação deve cobrir a integração da administração de todas as unidades instaladas e os 2 equipamentos já existentes no datacenter da SME

3.6.3 A instalação deve cobrir a integração da coleta de logs de todas as unidades instaladas e os dois equipamentos já existentes no datacenter da SME

3.7 Expansão para aumento de processamento e licenciamento de solução centralizadora de SD-WAN pelo período de 60 meses

3.7.1 A expansão deve ser realizada nos 2 equipamentos palo alto networks pa-5450, trazendo um incremento mínimo no ambiente de:

3.7.1.1 Throughput de 65 Gbps de Next Generation Firewall

3.7.1.2 Throughput de 30 Gbps de proteção contra ameaças conhecidas atuante para todas as assinaturas que a plataforma possuir, ameaças desconhecidas, filtro de URL ativo, bloqueio de arquivos e log habilitado

3.7.1.3 Throughput de 17 Gbps para VPN IPSec

3.7.1.4 Capacidade de 20 Milhões de sessões simultâneas

3.7.1.5 Licença de uso de SD-WAN para equipamento PA-5450 em cluster HA por 60 meses.

3.7.1.6 Deve ativar e ter suportada a funcionalidade de SD-WAN em todo o equipamento PA-5450 pelo período mínimo de 60 meses;

3.8 Serviço de instalação para expansão e licenciamento de SD-WAN

8.8.1 As lâminas adquiridas devem ser instaladas, licenciadas e ativadas nos equipamentos já em posse desta secretaria, localizados no seu datacenter principal.

8.8.2 A licença de SD-WAN deve ser ativada e configurada para funcionamento pleno em todo o equipamento, a fim de suportar a conexão de todas as unidades remotas.

3.9 Treinamento oficial do fabricante da solução de SD-WAN

3.9.1 O treinamento deve ser oferecido para no mínimo 15 (quinze) pessoas e ser divido em três modalidades:

3.9.2 Configuração, com no mínimo 30 horas

3.9.3 Gerenciamento, com no mínimo 15 horas

3.9.4 Resolução de problema, com no mínimo 20 horas

3.10 O treinamento deverá ser oficial do fabricante, ministrado pelo próprio ou por um de seus parceiros credenciados;

3.11 A modalidade do treinamento poderá ser presencial, em São Paulo – Capital ou em plataforma de ensino a distância, ao vivo;

3.12 O treinamento deverá ser realizado no Brasil, em português, contando com aulas teóricas e práticas;

3.13 O material do treinamento deverá ser disponibilizado nas línguas portuguesa ou inglesa;

3.14 **O treinamento de configuração deverá abordar, no mínimo:**

3.14.1 Principais funcionalidades;

3.14.2 Configuração inicial;

3.14.3 Configuração de políticas de segurança;

3.14.4 Métodos de integração e autenticação de usuários;

3.14.5 Filtro de URL;

3.14.6 Prevenção contra ameaças, antivírus;

3.14.7 Configurações de NAT e QoS;

3.14.8 Configurações DE VPN (IPSec e SSL);

3.14.9 Emissão e personalização de relatórios;

3.14.10 Disaster Recovery;

3.14.11 Gerenciamento do ambiente com Redundância.

3.15 **O treinamento de configuração deverá abordar, no mínimo:**

3.15.1 Configuração e gerência do servidor de gerenciamento

3.15.2 Administração de vários dispositivos remotos, utilizando das funcionalidades que facilitem esta administração

3.15.3 Coleta de logs e geração de reports;

3.15.4 Planejamento e design para implementação da gerência

3.16 O treinamento de configuração deverá abordar, no mínimo:

3.16.1 Uso das ferramentas disponíveis para investigar problemas

3.16.2 Metodologias conhecidas para resolução de prob

3.16.3 Análise avançada de logs para resolver problemas

3.16.4 Resolução de problemas avançados, baseado em cenários

3.17 Para cada modalidade dos treinamentos deverá ser emitido certificado para cada participante que cumprir frequência mínima de 70% (setenta por cento)

3.18 **Serviço mensal de monitoramento e correlacionamento de eventos (SNOC)**

3.18.1 Monitoramento para 1550 terminadores SD-WAN e 2 concentradores SD-WAN já instalados no datacenter desta secretaria, incluindo toda a infraestrutura (hardware, software, serviço, licenciamento, pessoal e, datacenter ou cloud) para a plena realização do serviço

3.18.2 Serviço de monitoramento 24x7 para ambiente de equipamentos e gerência, com monitoramento reativo e proativo da infraestrutura, a fim de diagnosticar problemas de performance e disponibilidade dos ativos de segurança através de ferramentas de coletas de informações para o SNOC e para análise de eventos de segurança através de uma ferramenta de SIEM e, ainda, para coletas e estatísticas para administração e otimizações de desempenho. Através de uma solução de siem composta por hardware e software fornecida pela contratada sem ônus para a contratante.

3.18.2.1 Os equipamentos que serão monitorados pelo SNOC:

3.18.2.1.1 1550x Terminadores de SD-WAN;

3.18.2.1.2 2x Palo Alto Networks PA-5450;

3.18.3 A CONTRATADA deverá:

3.18.3.1 Implantar, configurar e manter painéis de monitoração;

3.18.3.2 Detectar e endereçar problemas nos Itens de Configuração sendo monitorados;

3.18.3.3 Dar apoio e suporte nas Investigações das causas de problemas (no caso de incidentes recorrentes)

3.18.3.3.1 Em casos específicos ou a partir de solicitações, a CONTRATANTE poderá solicitar apoio e suporte On Site para a CONTRATADA.

3.18.3.4 O sistema de gerenciamento deverá fornecer as informações necessárias para avaliar, em tempo real, as características especificadas para os dispositivo e serviços contratados;

3.18.4 Atividades compreendidas:

3.18.4.1 Configuração de alertas e a abertura de incidentes e requisições que possam causar impacto nos sistemas e processos de negócios, reduzindo o risco de parada.

3.18.4.2 Análise criteriosa de relatórios produzidos, informando o desempenho e as tendências de sistemas e redes, as ocorrências pontuais e críticas, os encaminhamentos, as soluções e as medidas adotadas.

3.18.4.3 Instalação, implantação e modelagem de ferramentas de monitoração, solução de gerenciamento de disponibilidade, falhas, desempenho, aplicações e de nível de serviço.

3.18.4.4 O Registro e abertura de incidente no Service Desk da CONTRATADA, para identificar a causa raiz e tomar as medidas de apoio à resolução do incidente (troubleshooting), em conformidade com os processos de incidente e mudança do CONTRATANTE e potencial de impacto na disponibilidade do serviço.

3.18.4.5 Identificação, classificação, priorização e notificação de falhas nos serviços monitorados, ativos de rede e servidores.

3.18.4.6 Triagem e Categorização de evento: os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais incidentes com as características em comum, que podem receber tratamento padronizado. Os eventos confirmados, classificados como incidente, devem ter seu tíquete escalado para os analistas da CONTRATANTE.

3.18.4.7 Padronização de procedimentos de resposta a incidentes, os incidentes escalados devem incluir procedimentos padronizados contendo as melhores práticas para seu tratamento e contenção, de modo que viabilize a execução das medidas corretivas necessárias pela CONTRATANTE, no caso em que os ativos serão apenas monitorados.

3.18.4.8 Recebimento e processamento de alarmes, através de 'polling' aos equipamentos monitorados.

3.18.4.9 Coordenação das janelas operacionais de manutenção para atualizações de software e aplicação de patches de correção.

3.18.4.10 Disponibilização de interfaces de gerenciamento WEB para acompanhamento em tempo real dos serviços em execução, incidentes em aberto, problemas, responsáveis (equipe e analista) por cada atendimento, NMS´s definidos e mensurados.

3.18.4.11 Supervisão de atendimento e monitoramento permanente dos indicadores definidos durante a elaboração dos processos ou revisados posteriormente.

3.18.5 A CONTRATADA deverá fornecer uma estrutura de monitoramento dos dados através de:

3.18.5.1 Ferramentas de monitoramento para dados de SNOC

3.18.5.2 A solução deverá ter capacidade de coleta dos dados através de agentes, coletas via syslog ou através do Protocolo SNMP;

3.18.5.3 A CONTRATADA deverá executar o serviço de monitoração proativa e reativa dos ativos relacionados neste termo de referência, constituída do parque de dispositivos – 1550 unidades remotas e 2x Palo Alto Networks PA-5450, executando as seguintes atividades:

3.18.5.3.1 Gerenciamento de monitoramento de falhas;

3.18.5.3.2 Gerenciamento de monitoramento de desempenho;

3.18.5.3.3 Gerenciamento de monitoramento dos fluxos de rede.

3.18.5.3.4 Interface de monitoramento dos atendimentos;

3.18.5.3.5 Gestão de níveis mínimos de serviços;

3.18.5.3.6 Geração e fornecimento de relatórios mensais;

3.18.6 Monitoramento das seguintes variáveis (quando disponíveis):

3.18.6.1 Performance;

3.18.6.2 Evento crítico;

3.18.6.3 Evento repetitivo;

3.18.6.4 Serviço ativo/inativo;

3.18.6.5 Versionamento e atualizações.

3.18.6.6 Status da CPU (processadores)

3.18.6.7 Falhas nas Interfaces de rede I/O

3.18.6.8 Falhas nos Armazenamento

3.18.6.9 Status de ocupação de memória e espaço em disco

3.18.6.10 Falhas nas fontes de alimentação

3.18.6.11 Alarmes de temperatura (disponível via SNMP ou agente do fabricante do dispositivo)

3.18.7 Ferramenta de monitoramento para dados de SNOC/SIEM:

3.18.7.1 Fornecimento da ferramenta de SIEM (Security Information and Event Management), na modalidade as-a-service mantido e operado pelo provedor de SNOC. Poderá ser fornecida através de infraestrutura local, ou através de plataforma como serviço/cloud pública ou privada;

3.18.7.2 O período de retenção dos logs deverá ser de 30 dias, para processamento e tratamento;

3.18.7.3 Deverá ser fornecido funcionalidade capaz de analisar e correlacionar logs, além de trazer contextualização e enriquecimento de dados para análises, podendo ser fornecido através da plataforma especificada de monitoramento, ou através de uma plataforma adicional, contemplando no mínimo as seguintes características:

3.18.7.4 A solução deverá ser capaz de analisar e correlacionar logs, além de trazer contextualização e enriquecimento de dados para análises que serão realizadas pelo time de reposta a incidentes da CONTRATANTE.

3.18.7.5 Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenados na Solução Integrada de SNOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças

3.18.7.6 Para a monitoração de alertas de segurança, a detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados.

3.18.8 Os alertas devem indicar minimamente:

3.18.8.1 Ataques de força bruta com e sem sucesso

3.18.8.2 Falhas de autenticação que indiquem suspeita de roubo de identidade;

3.18.8.3 Infecção de equipamentos por vírus;

3.18.8.4 Comprometimento de ativos da rede;

3.18.8.5 Realização de ações suspeitas por parte de usuários privilegiados;

3.18.8.6 Alertas de operação de serviços, como interrupções e falhas;

3.18.8.7 Ataques de negação de serviço;

3.18.8.8 Ataques comuns em aplicações WEB, como XSS e SQL injection;

3.18.8.9 Atividades de botnets;

3.18.8.10 Exploração de vulnerabilidades.

3.18.9 A CONTRATADA deve configurar proativamente regras de correlacionamento, baseadas em boas práticas de segurança e bases de conhecimento próprias, customizadas para o ambiente da CONTRATANTE, monitorando minimamente

3.18.9.1 Detecção de rootkits conhecidos;

3.18.9.2 Detecção de não conformidades em ativos;

3.18.9.3 Detecção de vulnerabilidades em ativos;

3.18.9.4 Integridade de arquivos críticos e de configuração;

3.18.9.5 Detecção de anomalias de comportamento baseado em estatísticas (Statistical Behavioral Analysis);

3.18.9.6 Detecção de anomalias com base em tendências (Trend Behavior Analisys);

3.18.10 Detecção de padrões em logs:

3.18.10.1 Detecção de padrões baseados em uma sinalização específica (thresholds);

3.18.10.2 Detecção de padrões baseados em valores unitários;

3.18.10.3 Detecção de ameaças que saem de normas básicas (whitelisting).

3.18.10.4 As fontes de dados a serem utilizados pela plataforma de SIEM serão as especificadas abaixo:

3.19 DO DETALHAMENTO DA EXECUÇÃO DOS SERVIÇOS:

3.19.1 A PROPONENTE deverá possuir estrutura física, com centro de monitoramento (SNOC) funcionando em regime de 24 x 7 com operadores observando o monitoramento do ambiente de forma presencial no SNOC, a partir de onde será realizada a monitoração do ambiente da CONTRATANTE.

3.19.2 Canal de comunicação com túnel criptografado exclusivo para acesso ao ambiente da empresa, com a finalidade de monitoramento e coleta de eventos para análise;

3.19.3 A CONTRATADA deverá indicar o local onde possui sua estrutura de SNOC, sendo que este deve estar estabelecido no brasil, preferencialmente na região metropolitana de São Paulo e estará sujeito à diligência por parte da CONTRATANTE.

3.19.4 Todos os atendimentos devem ser iniciados no brasil e no idioma português do brasil.

3.19.5 As ferramentas de monitoramento de SNOC deverão possuir Dashboards adequados para a prestação dos serviços necessários ao gerenciamento centralizado da solução de TI com todos os componentes pertinentes a um ambiente de gerenciamento e monitoramento, contendo, no mínimo:

3.19.6 A monitoração do ambiente da CONTRATANTE poderá ocorrer através de comunicação VPN estabelecia entre a CONTRATADA;

3.19.7 A CONTRATADA deverá disponibilizar um número único local do tipo 0800, para a execução dos serviços, que demandarem contatos telefônicos;

3.19.8 A CONTRATADA deverá informar e acompanhar os incidentes relacionados com serviços diversos solicitados, incluindo a sugestão para a resolução de incidentes que geram indisponibilidade e problemas de desempenho nos serviços, operando em regime de 24 x 7;

3.19.9 A execução dos serviços será gerenciada pela CONTRATADA, que fará o acompanhamento diário da qualidade e dos níveis de serviços alcançados, com vistas a efetuar eventuais ajustes e correções de rumo. Quaisquer problemas, que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviços definidos, devem ser, imediatamente, comunicados, à CONTRATANTE, que colaborará, com a CONTRATADA, na busca da melhor solução para o problema.

3.19.10 O nível de serviço será acordado com a contratada e poderá ser definido em função de, no mínimo:

3.19.11 Disponibilidade;

3.19.12 Tempo médio de reparo (mttr);

3.19.13 Tempo médio entre falhas (mtbf);

3.19.14 Tempo máximo de parada;

3.19.15 Tempo de resposta

3.19.16 Relatórios de alarmes, inventário e disponibilidade

3.20 A solução de gerência de falhas deverá prover relatórios web de inventário, disponibilidade e histórico de alarmes dos ativos de rede gerenciados que possibilitem:

3.21 Determinar os ativos mais problemáticos

3.21.1 Os alarmes mais recorrentes;

3.21.2 Quais os dispositivos estão mais e menos frequentemente indisponíveis;

3.21.3 Quais os dispositivos estão entrando e saindo do gerenciamento;

3.21.4 Informações de ativos em versões detalhadas ou resumidas

3.22 Os relatórios de alarmes deverão prover, no mínimo, as seguintes informações:

3.22.1 Quantidade de alarmes por mês e por semana;

3.22.2 Quantidade diária de alarmes por hora;

3.22.3 Log detalhado de alarmes;

3.22.4 Quantidade mensal de alarmes por dia e por semana;

3.22.5 Alarmes mais comuns;

3.22.6 Ativos mais problemáticos;

3.23 Os relatórios de disponibilidade deverão prover, no mínimo, as seguintes informações:

3.23.1 Disponibilidade de todos os ativos;

3.23.2 Paradas planejadas;

3.23.3 Log de paradas;

3.23.4 Disponibilidade mensal projetada para todos os dispositivos;

3.23.5 Disponibilidade detalhada para um dispositivo selecionado;

3.23.6 Dispositivos com menor disponibilidade

3.24 Os relatórios de Serviço e Nível de Serviço deverão prover, no mínimo, as seguintes informações:

3.24.1 Informações detalhadas de cada Cliente;

3.24.2 Resumo do Nível de Serviço por Cliente;

3.24.3 Disponibilidade do Serviço por Cliente;

3.24.4 Resumo do Serviço por Cliente;

3.24.5 Detalhe do Nível de Serviço por Cliente;

3.24.6 Status do Nível de Serviço por cliente;

3.24.7 Resumo do Nível de Serviço por cliente.

3.25 Os relatórios poderão ser impressos e salvos, no mínimo, nos seguintes formatos:

3.25.1 Microsoft Excel;

3.25.2 PDF;

3.25.3 Microsoft Word;

3 GARANTIA E SUPORTE ON-SITE

3.1 Deverá ser fornecida garantia e suporte de 60 Meses contra defeito de fabricação, atendimento a correções de configuração, criação de novas configurações, alterações de projeto, mudança de localidade de equipamentos, vícios quais surjam durante o tempo de garantia dos equipamentos, problemas de softwares fornecidos junto ao equipamento, dentre outras necessidades derivadas da gestão e operação do ambiente.

3.2 Prestar assistência técnica on-site do equipamento pelo período mínimo de 60 (sessenta) meses, incluindo atendimento a fonte, bateria, cabos e outros periféricos fornecidos pela contratada.

3.3 A contratada deverá garantir a reposição de peças e originais e idênticas do equipamento, quando indisponível o fornecimento nestas condições a CONTRATANTE deverá ser notificada para a aprovação das alterações no atendimento.

3.4 As peças de reposição não deverão ser recondicionadas, recuperadas ou fruto de reutilização.

3.5 A CONTRATADA deverá fornecer mão-de-obra técnica, atendimento ON-SITE, transporte do equipamento para centro de reparo caso necessário, disponibilização de equipamento ou periférico de backup durante o período de manutenção externa, e entrega do equipamento substituído quando necessário, de forma que a unidade de SME em atendimento não seja mantida com os serviços indisponíveis durante o processo de manutenção.

3.6 A CONTRATADA fica responsável pelo laudo, análise e confirmação de problemas e falhas ora reportados dos equipamentos.

3.7 O período da prestação de serviço de garantia deverá ser contado a partir da emissão do ateste de recebimento definitivo.

3.8 Esta garantia deverá ser comprovada na Proposta, através de declaração do fornecedor para este Edital.

3.9 A CONTRATADA deverá dispor de atendimento e abertura de chamados durante horário comercial, via e-mail, via fone (0800), com viabilidade de acompanhamento de chamados via sistema online, além dos demais canais.

3.9.1 O sistema de chamados da CONTRATADA deve possuir integração com o sistema de chamados da CONTRATANTE.

3.10 A CONTRATADA deverá fornecer para cada abertura de chamado numeração única equivalente a identificação daquela solicitação.

3.11 A CONTRATADA deverá ser capaz de fornecer relatórios conforme solicitado pela contratante, comprovando o atendimento aos itens passiveis de glosa por atendimento, ou ainda quanto as ocorrências e serviços realizados como forma de comprovar o pleno atendimento as obrigações contratuais.

4 CONFIDENCIALIDADE

4.1 A CONTRATADA deverá preservar o caráter confidencial das informações dos usuários, não as aproveitando em nenhuma hipótese para fins não condizentes com o objeto licitado, inclusive uso comercial, publicitário ou estatístico;

4.2 A CONTRATADA somente poderá repassar as informações em seu poder aos órgãos da Prefeitura da Cidade de São Paulo, mediante prévia solicitação da SME/SP ou da autoridade pública competente, sob fundado pedido judicial e/ou administrativo vinculante, sempre observando os preceitos constitucionais atinentes à intimidade e ao sigilo dos dados pessoais;

4.3 O uso de informações em desacordo com a presente cláusula ou com as determinações da SME/SP implica infração contratual grave, além de sujeitar a CONTRATADA e seus prepostos às cominações administrativas, civis e criminais aplicáveis;

4.4 A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da CONTRATANTE para divulgação;

4.5 Não poderá haver nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da CONTRATANTE.

5 Qualificação técnica consistirá em:

5.1 A CONTRATADA deverá apresentar no mínimo 01 (um) atestado/declaração fornecido por pessoa jurídica de direito público ou privado, comprovando que a CONTRATADA já forneceu satisfatoriamente equipamentos compatíveis com o desta licitação. O atestado/declaração A deverá conter, no mínimo: o nome da empresa/órgão contratante, o nome do responsável por sua emissão e telefone para contato, caso necessário. O Pregoeiro(a) poderá determinar qualquer diligência que entender necessária para verificar a autenticidade e legitimidade do atestado ou de qualquer documento que lhe suscitar dúvidas.

5.2 Admite-se ao somatório dos quantitativos consignados em atestados que comprovem o fornecimento do objeto;

5.3 O somatório deve ser de, no mínimo, 5% da quantidade total de equipamentos fornecidos neste certame;

5.4 A CONTRATADA deverá apresentar no mínimo 01 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o fornecimento de serviços de monitoramento.

5.5 A CONTRATADA deverá apresentar no mínimo 01 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando a implementação e manutenção de ferramenta de SIEM.

5.6 A CONTRATADA deverá apresentar declaração oficial do fabricante que a revenda é autorizada do fabricante ofertado;

5.7 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com certificação nível profissional do fabricante ofertado.

5.8 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com a certificação "Certified Ethical Hacker" – CEH;

5.9 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com certificação em nível Administrador e/ou Arquiteto em soluções de SIEM;

5.10 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com a certificação de Auditor Lider em Sistemas de Gestão de Segurança da Informação ISO/IEC 27001;

5.11 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com a certificação ITIL Foundation v3;

5.12 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com a certificação COBIT Foundation;

5.13 A CONTRATADA deverá ter em seu corpo de funcionários ativos pelo menos 01 (um) profissional com a certificação PMP - Project Management Professional – reconhecida pelo PMI – Project Management Institute;

5.14 O(s) atestado(s) deverá(ão) conter o nome da empresa declarante, a identificação do nome e assinatura do responsável, bem como o número de telefone para contato e deverá comprovar o fornecimento e implantação de solução de segurança rede.

6 ACORDO DE NÍVEL DE SERVIÇO

6.1 Os serviços que constituem o objeto deste instrumento deverão ser prestados sem interrupções, no regime de atendimento 24 x 7 (vinte e quatro horas / sete dias por semana); O SLA será aferido mensalmente ao longo da vigência do contrato para, se cabível, aplicar descontos e multas;

6.2 O SLA deverá atender os seguintes níveis de prioridade para a resolução do Problema:

NÍVEL DE PRIORIDADE	DESCRIÇÃO	PRAZOS	
		A partir da abertura do chamado a CONTRATADA terá um prazo de:	
		ATENDIMENTO	TEMPO DE SOLUÇÃO
ALTA	Falha completa do Serviço ou degradação severa dos serviços	04h	02h
MÉDIA	Falha parcial ou degradação dos serviços	08h	04h
BAIXA	Instalação de atualização de software (upgrade)	16h	08h

6.3 As interrupções programadas para manutenções preventivas ou por necessidades da CONTRATADA, só podem ser efetuadas fora do horário comercial, desde que comunicadas e aprovadas pela CONTRATANTE com antecedência de 5 (cinco) dias úteis, ou em casos extraordinários de comum acordo entre as partes;

6.4 Interrupções ocasionadas por paradas programadas e previamente agendadas e efetuadas no prazo da janela acordada, não serão consideradas para efeito de desconto ou multa;

6.5 O SLA será gerenciado pelo tempo decorrido entre a abertura do chamado e seu fechamento por técnico da SME/SP;

6.6 Relativamente aos serviços de suporte técnico e manutenção o nível de serviço exigido e a penalidade por seu descumprimento será:

Indicador	Nível de Prioridade	Penalidade
"Tempo de solução do Problema" - Período compreendido entre o horário de chegada do técnico aolocal, ou inicio do atendimento e o horário do término com a solução, deixando o equipamento em condições normais de operação.	Alta	Multa equivalente a 10% sobre o valor mensal de consultoria técnica dos chamados que excederem o limite de tempo de solução estabelecido como meta.
	Média	Multa equivalente a 5% sobre o valor mensal de consultoria técnica dos chamados que excederem o limite de tempo de solução estabelecido como meta
	Baixa	Multa equivalente a 2% sobre o valor mensal de consultoria técnica dos chamados que excederem o limite de tempo de solução estabelecido como meta.

7 OBRIGAÇÕES DA CONTRATADA

7.6 A CONTRATADA deverá fornecer os serviços de atualização das licenças, suporte, garantia e consultoria técnica, sem ônus para a CONTRATANTE, durante a vigência do contrato, incluindo visita técnica, substituição de peças, transporte, atualizações e outras providências pertinentes à continuidade da prestação do serviço.

7.7 A CONTRATADA deverá garantir o funcionamento dos equipamentos contra possíveis defeitos de projeto, fabricação, instalação e materiais, durante a vigência do contrato.

7.8 A CONTRATADA deverá garantir que todas as licenças, serviços e peças estejam de acordo com as especificações da fabricante.

7.9 A CONTRATADA deverá disponibilizar suporte técnico remoto e/ou presencial:

7.9.1 O atendimento deverá ser realizado em um primeiro momento de forma remota, caso constatado o problema de hardware, o atendimento deverá ser realizado nos locais onde estes estiverem instalados (atendimento “on-site”);

7.9.2 Toda a garantia e demais reparos necessários, deverá obrigatoriamente respeitar o período de 60 (sessenta) meses no regime 24x7 (vinte e quatro horas por dia e sete dias por semana), incluindo feriados e finais de semana para atendimentos aos concentradores;

7.9.3 Toda garantia e suporte deverá contemplar o fornecimento da atualização dos softwares ofertados (correções, “patches”, “updates” ou novas ”releases”) sem custo adicional, sempre que solicitado pela contratante ou indicado pela contratada;

7.10 O serviço deverá ser fornecido durante a vigência do contrato, contado a partir da data da assinatura da Ordem de serviço;

7.11 O suporte on-site será utilizado pela CONTRATANTE dentro do prazo de garantia da solução em período no regime de suporte 24x7 (vinte e quatro horas por dia e sete dias por semana), incluindo feriados e finais de semana para abertura de chamados.

7.12 A CONTRATADA deverá relatar, mensalmente, de forma clara e detalhada, os serviços utilizados no período de 30 dias por meio de notas fiscais/ faturas com detalhamento de serviço impresso.

7.13 A CONTRATADA deverá:

7.13.1 Recomendar atualizações ou configurações de segurança;

7.13.2 Acompanhar, presencialmente ou remotamente, procedimentos considerados como críticos pela contratante, tais como atualização de versão do equipamento, sempre mediante agendamento e atuação imediata em caso de incidente grave de segurança ou falha irrecuperável de hardware ou software;

7.13.3 Avaliar mudanças críticas na infraestrutura da contratante;

7.13.4 Avaliar o ambiente após renovação das licenças, emitindo relatório com resultados e possíveis recomendações.

7.13.5 Orientar sobre as melhores práticas de configuração e utilização dos equipamentos;

7.13.6 Revisar o ambiente sob demanda;

7.13.7 Responder dúvidas de usabilidade do produto/interface;

7.13.8 Ser responsável por todos os técnicos que forem realizar manutenção dos equipamentos;

7.13.9 Manter, durante o prazo de vigência do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação

7.13.10 Arcar com todas as despesas relativas à entrega dos bens, inclusive, as relativas ao seu transporte, bem como a necessidade de revisitas ou reagendamentos de entrega, seja por qual motivo for.

7.13.11 Manter controle próprio, atualizado diariamente e compartilhado com a contratante, por meio de plataforma compartilhada online, das entregas e instalação dos equipamentos nas unidades constantes em ordem de fornecimento.

7.13.12 Fornecer sob a ordem de fornecimento emitida cronograma com planejamento de fornecimento dos itens nas localidades requisitadas.

7.13.13 Obter comprovantes de entrega nas unidades com a assinatura e carimbo da unidade qual receber os equipamentos.

7.13.14 Caso requisitado pela contratante os comprovantes de entrega e Notas Fiscais ou de Remessa, deverão ser digitalizados pela contratada no momento da entrega para plataforma online de controle fornecida pela contraente.

7.13.15 Acatar a recusa de aceite das unidades e recusa de assinatura do recebimento em caso de identificação de problemas de carácter qualitativo ou quantitativo.

7.13.16 Designar colaborador(es), munido de e-mail, telefone e aplicativo de mensageria, como ponto fixo de comunicação do contrato, para o atendimento as requisições da contratante.

7.13.17 Fornecer em até 24 horas corridas, quaisquer informações requisitadas pelos fiscais de contrato quanto ao Objeto Editalício e as atividades derivadas desta aquisição.

7.13.18 Ser capaz e emitir relatórios gerenciais que viabilizem a comprovação do cumprimento dos itens que compõem o objeto de contrato, tais como: índice de falhas, número de abertura de chamados, tempo de atendimento, volumetria de trocas de equipamento, tempo de resolução de problemas dentre outros quais subsidiem os fiscais de contrato a validar e comprovar a execução do objeto contratado.

7.13.19 Toda a garantia e demais reparos necessários, deveram obrigatoriamente respeitar o período de 60(sessenta) meses, contados a partir do aceite definitivo das instalações nas unidades de SME.

8 OBRIGAÇÕES DA CONTRATANTE

8.6 Fiscalizar, através do Fiscal Técnico do contrato o cumprimento das obrigações assumidas pela CONTRATADA, inclusive quanto à continuidade da prestação dos serviços que, ressalvados os casos de força maior, justificados e aceitos pela CONTRATANTE, não devem ser interrompidos;

8.7 Notificar a CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades constatadas nos serviços executados;

8.8 Relacionar-se com a CONTRATADA, exclusivamente, por meio de pessoa(s) por ela credenciada(s);

8.9 À CONTRATANTE reserva-se o direito de exercer, quando lhe convier, fiscalização sobre os serviços contratados, e ainda, aplicar as penalidades previstas neste instrumento ou rescindi-lo, caso a CONTRATADA descumpra quaisquer das cláusulas estabelecidas;

8.10 Serão nomeados os Fiscais responsáveis pelo acompanhamento da execução do objeto contratado, devendo fazer anotações e registros de todas as ocorrências, determinando o que for necessário à regularização das falhas ou defeitos observados para o fiel cumprimento das cláusulas e condições estabelecidas, O Fiscal do Contrato terá apoio do Fiscal Técnico que fiscalizará as questões técnicas do serviço;

8.11 Indicar os locais de prestação dos serviços;

8.12 Indicar o responsável pela gestão do contrato, a quem competirá a fiscalização dos serviços, a qualquer instante, solicitando à Contratada, sempre que achar conveniente, informações do seu andamento;

8.13 Efetuar pagamentos de acordo com o estabelecido em contrato;

8.14 Facilitar, por todos os meios, o exercício das funções da CONTRATADA, dando-lhe acesso às suas instalações, promovendo o bom entendimento entre seus servidores e os empregados da CONTRATADA e cumprindo suas obrigações estabelecidas neste contrato;

8.15 Prestar aos empregados da CONTRATADA informações e esclarecimentos que eventualmente venham a ser solicitados, e que digam respeito à natureza dos serviços contratados;

9 TERMOS DE RECEBIMENTO PROVISÓRIO E DEFINITIVO

10.1 Quando os serviços contratados forem concluídos, caberá à Contratada apresentar comunicação escrita informando o fato à fiscalização da Contratante, a qual competirá, no prazo de até 05 dias, a verificação dos serviços executados, para fins de recebimento provisório.

10.2 A Contratante realizará avaliação minuciosa dos serviços executados juntamente com os fiscais intermediários dos serviços, com a finalidade de mensurar os serviços prestados e avaliar a sua qualidade.

10.3 Após tal avaliação, será lavrado Termo de Recebimento Provisório, em 02 (duas) vias de igual teor e forma, ambas assinadas pelo fiscal, relatando as eventuais pendências verificadas.

10.4 A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Termo de Recebimento Provisório.

10.5 O Termo de Recebimento Definitivo dos serviços contratados será lavrado em até 15 dias após a lavratura do Termo de Recebimento Provisório, por servidor ou comissão designada pela autoridade competente, desde que tenham sido devidamente atendidas todas as exigências da fiscalização quanto às pendências observadas.

10.6 Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo, desde que o fato seja comunicado à Contratante nos 15 (quinze) dias anteriores à exaustão do prazo.

10.7 O recebimento definitivo do objeto licitado não exime a Contratada, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei n° 10.406, de 2002).

10.8 Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Anexo I deste ajuste e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, à custa da contratada, sem prejuízo da aplicação de penalidades.

11 VISTORIA TÉCNICA

11.1 A vistoria técnica é facultativa.

11.2 A vistoria técnica tem como objetivo verificar as condições locais, avaliar a quantidade e a natureza dos trabalhos, materiais e equipamentos necessários à realização do objeto da contratação, permitindo aos interessados colher as informações e subsídios que julgarem necessários para a elaboração da sua proposta, de acordo com o que o próprio interessado julgar conveniente, não cabendo à Administração nenhuma responsabilidade em função de insuficiência dos dados levantados por ocasião da visita técnica.

11.3 As empresas licitantes poderão promover quantas visitas técnicas considerar necessário, examinando os locais e demais características das instalações físicas da CONTRANTE em sua totalidade, nos endereços que serão realizados os serviços, a fim de verificar as condições locais e dirimir eventuais dúvidas, posto que não serão aceitas alegações posteriores quanto ao desconhecimento de situação existente, peculiares dos serviços ou das instalações.

11.4 As empresas interessadas deverão apresentar "Atestado de Visita Técnica", conforme o modelo constante no **ANEXO II** deste Termo de Referência. Cada visita deverá ser previamente agendada por email: smecotic@sme.prefeitura.sp.gov.br, a qual poderá ser realizada até o dia imediatamente anterior à Sessão Pública, no período das 08h00 às 17h00 horas.

11.4.1 O agendamento estará condicionado à disponibilidade de acompanhamento da equipe técnica da SME.

11.5 A CONTRATADA não poderá pleitear, em hipótese alguma, modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre o local em que serão executados os serviços, bem como pela opção de não realização da visita técnica.

11.6 Competirá a cada interessado, quando da visita técnica, fazer-se acompanhar dos técnicos e especialistas que entender suficientes para colher as informações necessárias à elaboração da sua proposta.

11.7 As prospecções, investigações técnicas, ou quaisquer outros procedimentos que impliquem interferências no local em que serão prestados os serviços deverão ser previamente informadas e autorizadas pela CONTRATADA.

11.8 Caso opte pela não realização da visita técnica, as empresas deverão apresentar o Atestado de Não Realização, conforme o modelo constante no **ANEXO III** deste Termo de Referência.

12 PENALIDADES

1.2 São aplicáveis as sanções previstas no Capítulo IV, da Lei Federal nº 8.666/93, Lei Federal nº 10.520/ 02, do Decreto Municipal nº 44.279/03, e demais normas pertinentes, devendo ser observados os procedimentos contidos no capítulo X, sendo que as multas serão aplicadas como segue:

12.1.1 Pela inexecução total do objeto contratual, multa de 20% (vinte por cento) sobre o valor global do contrato, garantida a defesa prévia;

12.1.2 Multa de 1% (um por cento) por dia de atraso na entrega do objeto, calculada sobre o valor do item em atraso, até o 10º dia de atraso;

12.1.3 Multa de 2% (dois por cento) por dia de atraso na entrega do objeto, calculada sobre o valor do item em atraso, a partir do 11° dia de atraso, limitada a 20% do valor do contrato;

12.1.4 Multa de 5% (cinco por cento) sobre o valor do contrato na hipótese de descumprimento de qualquer das condições ajustadas, cujas sanções não estejam previstas nesta cláusula;

12.1.5 As multas previstas nos incisos acima são cumulativas e serão aplicadas até o limite de 20% (vinte por cento) do valor total do contrato, quando poderá ser cancelado o contrato;

12.1.6 Pela rescisão do contrato por culpa da CONTRATADA, multa de 20% (vinte por cento) sobre o valor do contrato;

12.1.7 O período de atraso será contado em dias corridos.

12.1.8 Relativo aos serviços de suporte técnico e manutenção o nível de serviço exigido a penalidade por seu descumprimento será o contido no item 5.7 deste Termo de Referência.

12.1.9 As penalidades administrativas serão aplicadas na medida estritamente necessária, sempre observando os princípios da razoabilidade e proporcionalidade, que são basilares do direito administrativo, decorrentes dos princípios da legalidade e da finalidade e que terão lugar inclusive nos casos de eventual lacuna ou dúvida de interpretação.

12.2 Multa pela recusa da **CONTRATADA** em assinar o Contrato e/ou retirar "Nota de Empenho" e/ou "Ordem para Início dos Serviços" dentro do prazo estabelecido, ou com atraso, sem a devida justificativa aceita pela Prefeitura: 20% (vinte por cento), sobre o valor do ajuste, nos termos do art. 81 da Lei 8.666/93;

12.3 Incidirá na mesma penalidade a não apresentação dos documentos necessários, impossibilitando a entrega da Nota de Empenho, para celebração do contrato:

12.4 O procedimento para aplicação de penalidade observará o disposto no Decreto Municipal 44.279/2003.

13 VIGÊNCIA DO CONTRATO

13.1 O contrato terá vigência de 24 (vinte e quatro) meses, contados do início de vigência do Contrato e conforme Art. 57, inc. IV, da Lei 8.666/1993, renováveis até o limite legal;

13.2 A prorrogação contratual somente poderá ocorrer nos termos previstos do art. 57 da Lei 8.666/93, até o limite legal, desde que haja autorização formal da autoridade competente e observados os seguintes itens:

13.3 os serviços tenham sido prestados regularmente;

13.4 a Administração mantenha interesse na realização do serviço;

13.5 o valor do Contrato permaneça economicamente vantajoso para a Administração;

13.6 CONTRATADA manifeste expressamente interesse na prorrogação.

13.7 É facultado à SME o direito de rescindir o Instrumento Contratual, total ou parcialmente, independentemente de Notificação Judicial ou Extrajudicial, nos casos previstos nos artigos de 77 a 80 da Lei nº 8.666/1993;

13.8 A abstenção, por parte da SME, do uso de quaisquer das faculdades concedidas no Instrumento Contratual e neste Edital não importará em renúncia ao seu exercício;

14 DO PAGAMENTO

14.1 O prazo de pagamento será de 30 (trinta) dias, a contar da data em que for atestada a prestação de cada parcela do serviço, que não poderá ultrapassar o prazo de 5 (cinco) dias úteis, contados da data em que a empresa cumprir todos os requisitos necessários à tramitação do documento fiscal;

14.2 O pagamento será efetuado exclusivamente por crédito em conta corrente no BANCO DO BRASIL S/A, nos termos do disposto no Decreto nº 51.197, publicado no D.O.C. de 23/01/10;

14.3 Deverá ser apresentado relatório contendo os índices de disponibilidade do link durante o mês de vidência da fatura;

14.4 Os pagamentos mensais obedecerão ao disposto nas Portarias da Secretaria das Finanças em vigor, ficando ressalvada a possibilidade de alteração das condições contratadas em face da superveniência de normas federais ou municipais sobre a matéria.

15 FISCALIZAÇÃO/CONTROLE DA EXECUÇÃO DOS SERVIÇOS

15.1 A fiscalização dos serviços pelo Contratante não exime, nem diminui a completa responsabilidade da Contratada, por qualquer inobservância ou omissão às cláusulas contratuais;

15.2 O Contratante poderá, a seu critério e a qualquer tempo, realizar vistoria da execução dos serviços e verificar o cumprimento de normas preestabelecidas no edital/contrato.

Anexo I: Modelo de proposta de preços

À
Prefeitura do Município de São Paulo
Secretaria Municipal de Educação

Assunto: Proposta de preços
Referência: Edital de Pregão Eletrônico nº [●]/SME/[●]

[Nome do proponente], com domicílio à [endereço do licitante com logradouro, número, complemento, bairro e cidade], CNPJ nº [●], telefone [●], FAX [●], e-mail [●], neste ato representado por [nome do representante], [qualificação civil do representante, cargo e referência a instrumento de mandato, se houver], pelo presente propõe a prestação de [●], conforme as características descritas no Termo de Referência, conforme as seguintes condições:

LOTE ÚNICO

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
01	Equipamento para terminação de SD-WAN, licenciado e suportado por 60 meses	1550 unidades	[●]	[●]
02	Serviço de instalação para equipamento de terminação SD-WAN	1550 unidades	[●]	[●]
03	Solução de gerência centralizada e retenção de logs para os 1550 equipamentos de terminação SD-WAN, licenciado e suportado por 60 meses	1 unidade	[●]	[●]
04	Serviço de instalação para solução de gerência centralizada e retenção de logs	1 unidade	[●]	[●]
05	Expansão para aumento de processamento e licenciamento de solução centralizadora de SD-WAN pelo período de 60 meses	2 unidades	[●]	[●]
06	Serviço de instalação para expansão e licenciamento de SD-WAN por 60 meses	1 unidade	[●]	[●]
07	Treinamento oficial do fabricante da solução de SD-WAN para configuração, gerências e resolução de problemas dos equipamentos	65 Horas	[●]	[●]
08	Serviço mensal de manutenção e monitoramento e correlacionamento de eventos (SNOC) para 1550 terminadores SD-WAN e 2 concentradores SD-WAN, incluindo toda a infraestrutura (hardware, software, serviço, pessoal e datacenter ou cloud) para a plena realização do serviço	60 meses	[●]	[●]
09	Garantia e suporte técnico on-site	60 meses	[●]	[●]
VALOR TOTAL DOS ITENS 01 a 09			[●]	

Valor global do lote (valor total dos itens 01 a 09)	[●]
Validade da proposta	[●]
Condições de pagamento	[●]

Os preços ofertados incluem todos os custos diretos e indiretos, incluídas as despesas de frete até os locais de prestação dos serviços, os encargos sociais e trabalhistas, fiscais e demais despesas necessárias ao cumprimento integral das obrigações decorrentes da licitação.

O proponente se submete a todas as cláusulas e condições do edital, bem como às disposições da Lei Federal nº 8.666/1993, da Lei Municipal nº 13.278/02 e demais normas complementares.

São Paulo, [●] de [●] de [●]

[assinatura do responsável legal]
Nome: [●]
RG: [●]
Cargo: [●]

Anexo II: Atestado de Vistoria Técnica

Pregão Eletrônico nº. [●]/SME/20[●] - Processo Administrativo SEI nº [●]

Atestamos para os fins de comprovação junto à Comissão Permanente de Licitação, referente ao Pregão Eletrônico nº. **[●]**/SME/20**[●]**, que o(a) Sr(a) **[●]**, representante da Empresa **[●]**, esteve presente em unidade: **[●]**da Secretaria Municipal de Educação visando conhecer o ambiente, local de execução para obter subsídios para a elaboração de sua Proposta para a Licitação em questão. Sendo assim, não poderá pleitear, em hipótese alguma, modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou falta de conhecimentos e informações sobre o local em que serão executados os serviços.

São Paulo, **[●]** de **[●]** de **[●]**.

_____
(Assinatura do Representante do Proponente)

_____
NOME DO REPRESENTANTE LEGAL

_____
EMPRESA

_____
SERVIDOR DE SME:
RF: **[●]**

Anexo III: Atestado de Não Vistoria Técnica

Pregão Eletrônico nº. [●]/SME/20[●] Processo Administrativo SEI nº [●]

Atestamos para os fins de comprovação junto à Comissão Permanente de Licitação, relativamente ao Pregão Eletrônico nº. **[●]**/SME/20**[●]**, que o(a) Sr(a)**[●]** representante da Empresa **[●]**, optou pela não realização de visita técnica visando conhecer o ambiente, local de execução e, finalmente, obter subsídios para a elaboração de sua Proposta para a Licitação em questão. Sendo assim, não poderá pleitear, em hipótese alguma, modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou falta de conhecimentos e informações sobre o local em que serão executados os serviços.

São Paulo, **[●]**de **[●]**de**[●]**.

_____
(Assinatura do Representante do Proponente)

_____
NOME DO REPRESENTANTE LEGAL

_____
EMPRESA