LOTE	ITEM	QTD.	PRODUTO
1	1	1	Firewall de Próxima Geração - Solução composta por 1 (um) appliance conforme termo de referência.
	2	1	Pacote de licenças do Console de Gerência Administrativa e Centralização de Logs e Relatórios. Pacote de licenças de Firewall, IPS, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas de firewall de próxima geração por 12 (doze) meses.
	3	1	Instalação e configuração.
	4	1	Treinamento profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoramento de Logs Centralizado.

1. Firewall

1.1 Firewall de Próxima Geração (NGFW).

1.1.1. O equipamento deverá ter as seguintes características e condições obrigatórias:

1.2. Requisitos de Hardware:

1.2.1. Deverá possuir licenciamento baseado nos recursos de hardware;

1.2.2. Deverá fornecer relatórios baseados em usuário e em endereço IP;

1.2.3. Deverá suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet;

1.2.4. Não deverá haver restrição quanto ao número de usuários/IP conectados;

1.2.5. Deverá suportar no mínimo 140.000 (cento e quarenta mil) novas conexões por segundo;

1.2.6. Deverá suportar minimamente 2.000 (dois mil) túneis SSL VPN;

1.2.7. Deverá suportar minimamente 15.000 (quinze mil) Mbps de throughput de VPN IPsec;

1.2.8. Performance mínima de throughput do Firewall: 35.000 (trinta e cinco mil) Mbps;

1.2.9. Performance mínima de throughput de NGFW: 6.000 (seis mil) Mbps;

1.2.10. Performance mínima de throughput de IPS: 6.000 (seis mil) Mbps;

1.2.11. Deverá possibilitar no mínimo 6.000.000 (seis milhões) de conexões simultâneas;

1.2.12. Deverá possuir no mínimo 120 GB de espaço em disco para o armazenamento de eventos e relatórios;

1.2.13. Deverá possuir no mínimo uma porta COM (RJ45);

1.2.14. Deverá possuir painel de LCD na parte frontal do equipamento;

1.2.15. Deverá possuir slot de FleXi Port;

1.2.16. Quantidade mínima de memória RAM: 8Gb;

1.2.17. Deverá possuir no mínimo 8 (oito) interfaces de rede GbE;

1.2.18. Deverá possuir 1 (uma) interface do tipo console ou similar;

1.2.19. Possuir fonte 100-240VAC;

1.2.20. Equipamento com 1U para montagem em rack.

1.3. Proteção:

1.3.1. Deverá proporcionar transparência total de autenticação no proxy, provendo segurança anti-malware e filtragem web;
1.3.2. Deverá realizar autenticação dos usuários nos modos transparente e padrão;
1.3.3. As autenticações devem ser feitas via NTLM;
1.3.4. Deverá possuir sistema de quotas com possibilidade de aplicação por usuários e grupos;
1.3.5. Deverá permitir a criação de políticas por horário, aplicado a usuários e grupos;
1.3.6. Deverá permitir a criação de regras customizadas baseadas em usuário e host;
1.3.7. Deverá permitir a criação de exceções de URLs, usuários e host para que não sejam verificados pelo proxy;
1.3.8. Deverá prover proteção em tempo real de todos os acessos web, baseando-se constantemente na base de dados na nuvem do fabricante, que deverá manter-se atualizada;
1.3.9. Deverá possuir minimamente dois modos diferentes de escaneamento durante o acesso do usuário;
1.3.10. Deverá prevenir infecção por malwares, trojans e spywares em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acessos via navegador;
1.3.11. Deverá prover minimamente duas engines diferentes de anti-malware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web;
1.3.12. Deverá proporcionar proteção avançada com emulação de Java script;
1.3.13. Deverá realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (Activex, applets, cookies, etc.);
1.3.14. Deverá bloquear o trafego que não segue os padrões do protocolo HTTP;
1.3.15. Deverá permitir a criação de exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS;
1.3.16. Deverá permitir definir nas exceções de não realizar escaneamento contra malware, de não realizar escaneamento HTTPS e de não realizar escaneamento baseado em critérios especificados por políticas;
1.3.17. Deverá permitir a criação de regras de exceções por grupo de usuários, por categorias de sites, por endereços IPs de origem e de destino;
1.3.18. Deverá permitir a criação de agrupamento de categorias definidas pelo administrador do equipamento;
1.3.19. Deverá permitir editar grupos de categorias preestabelecidos pela solução;
1.3.20. Deverá permitir a criação de novas categorias com as seguintes especificações: nome da regra e descrição para identificação da regra;
1.3.21. Deverá haver a possibilidade de importar uma base com domínios e palavras chaves quando da criação da categoria. A base de sites e categorias deverá ser atualizada automaticamente pelo fabricante;
1.3.22. Deverá permitir que o administrador possa definir um certificado autoritário próprio para ser utilizado no escaneamento HTTPS;
1.3.23. Deverá filtrar imagens apresentadas pelos buscadores, reduzindo os riscos de exposição a conteúdo inapropriado;
1.3.24. Deverá permitir que em uma mesma política sejam aplicadas ações diferentes de acordo com o usuário autenticado;
1.3.25. Deverá permitir a criação de cotas de navegação por limite de tempo de acesso ou especificação de data limite para o acesso.

1.4. Controle e Segurança de Aplicações:

1.4.1. Deverá reconhecer no mínimo as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy,
Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Vídeo, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy,
Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web. As aplicações deverão ser classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares;

1.4.2. Deverá haver a possibilidade de criar regras de controle por usuário e host;

1.4.3. Deverá haver a possibilidade de que as regras criadas baseadas em aplicação permitam bloquear e liberar o tráfego para as aplicações;

1.4.4. Deverá ser possivel a categorização das aplicações por risco: muito baixo, baixo, médio, alto e muito alto;

1.4.5. Deverá permitir granularidade quando da criação de regra baseada em aplicação, exemplo: bloqueio de anexo dentro de um post do Facebook, bloqueio de upload de vídeos no Youtube, etc...

1.4.6. Deverá realizar escaneamento e controle de micro app, incluindo, mas não limitado, a Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions,
Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download,
File Upload), Google Earth Application, Google Plus, Linkedin (Company Search, Compose Webmail,Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Vídeo Search, Vídeo Streaming, Upload, Website);

1.4.7. Deverá reconhecer aplicações em IPv6;

1.4.8. Em tráfego criptografado SSL, deverá descriptografar pacotes, possibilitando assim, a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.4.9. Deverá haver a possibilidade de agendamento de horário e data especificos para a aplicação das regras de controle de aplicativos;

1.4.10. A base de assinaturas de aplicações deverá ser atualizada automaticamente;

1.4.11. Os dispositivos de proteção de rede deverão possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory;

1.4.12. Deverá ser permitido o uso individual de diferentes aplicativos para usuários que p ertencem ao mesmo grupo, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo, que não possuírem acesso a estes aplicativos, deverão ter a utilização bloqueada.

1.5. Segurança WiFi:

1.5.1. Deverá permitir a criação de SSIDs com bridge para LAN, bridge para VLAN e zona separada;

1.5.2. Deverá haver suporte a IEEE 802.1X (RADIUS authentication). Suporte a 802.11r (fast transition);

1.5.3. Deverá suportar múltiplas SSIDs, incluindo hidden SSIDs;

1.5.4. Deverá haver suporte a hotspot, customização de voucher, senha do dia e termos de aceitação;

1.5.5. Deverá suportar WPA2 Personal e Enterprise;

1.5.6. A ferramenta deverá definir o melhor canal automaticamente, buscando a melhor performance;

1.5.7. Deverá ser possível a definição de acesso a rede wireless baseado em horário;

1.5.8. Deverá suportar login em HTTPS.

1.6. Proteção para e-mail:

1.6.1. Deverá ter proteção em tempo real, com a solução devendo realizar consultas na nuvem para verificar a integridade e segurança dos e-mails;

1.6.2. Deverá ser realizado o bloqueio de spam e malwares durante a transação SMTP;

1.6.3. Possuirá necessáriamente serviço de reputação para monitoramento dos fluxos de e-mails. O AntiSpam deverá bloquear e-mails considerados de má reputação na internet e pelo fabricante;

1.6.4. Deverá suportar escaneamento de protocolos SMTP, POP3 e IMAP;

1.6.5. Deverá possuir duas engines de antivírus para duplo escaneamento;

1.6.6. Deverá detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo;

1.6.7. Haverá necessáriamente suporte a criptografia TLS para SMTP, POP e IMAP;

1.6.8. Deverá haver a possibilidade de agregar RBLs do fabricante e de terceiros, complementando a composição de segurança da ferramenta;

1.6.9. Permitir a visualização de e-mails que se encontrem na fila para serem enviados;

1.6.10. Deverá ser possível definir um prefixo no subject de cada e-mail considerado spam;

1.6.11. Deverá permitir a adição de um banner no final dos e-mails analisados pela solução;

1.6.12. Deverá possuir funcionalidade de allowlist e blocklist;

1.6.13. Deverá possuir funcionalidade para rejeição de e-mails com HELO inválido e/ou que não possuam RDNS;

1.6.14. O escaneamento deverá ser realizado tanto para e-mails de entrada quanto para os de saída;

1.6.15. Deverá possuir quarentena para os e-mails;

1.6.16. Deverá possuir funcionalidade de criptografia de e-mails e DLP para os dados;

1.6.17. Deverá haver a funcionalidade de encriptação de e-mails. Os e-mails criptografados poderão ter seu conteúdo armazenado em um arquivo PDF;

1.6.18. Deverá ser permitido enviar anexos junto aos e-mails criptografados;

1.6.19. Deverá possuir templates de dados considerados sensíveis preestabelecidos pelo fabricante (CCLs) com os padrões PII, PCI, HIPAA, com a intenção de ajudar o administrador na criação das regras desejadas e seguir as principais normas do mercado, elas deverão ser mantidas pelo fabricante;

1.6.20. Deverá ser permitido bloquear e liberar ranges IP.

1.7. Administração, Autenticação e Configurações:

1.7.1. A solução proposta deverá suportar administração via comunicação segura (HTTPS, SSH) e console;

1.7.2. Deverá haver a possibilidade de importar e exportar cópias de segurança(backup) das configurações, incluindo os objetos de usuário;

1.7.3. A solução proposta deverá suportar implementações em modo Router (camada 3) e transparente (camada 2), individualmente ou simultâneamente;

1.7.4. A solução proposta deverá suportar integração com Active Directory, LDAP, Radius, TACACS+ e Banco de Dados Local para autenticação do usuário;

1.7.5. Deverá suportar em modo automático e transparente “Single Sign On” na autenticação dos usuários do active directory e eDirectory;

1.7.6. Deverá suportar 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;

1.7.7. Deverá permitir autenticação nos modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64;

1.7.8. Deverá suportar integração com Dynamic DNS de terceiros;

1.7.9. A solução proposta deverá disponibilizar gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual;

1.7.10. A solução proposta deverá suportar Parent Proxy com suporte a IP/FQDN;

1.7.11. Deverá suportar NTP;

1.7.12. Deverá haver suporte multilíngue para console de administração web;

1.7.13. A solução proposta deverá suportar a criação de usuário baseada em ACL para fins de administração;

1.7.14. A solução proposta deverá suportar cliente PPPOE e deverá ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOE trocar;

1.7.15. Deverá suportar SNMP v1, v2c;

1.7.16. Deverá suportar SSL/TLS para integração com o Active Directory ou LDAP;

1.7.17. A solução proposta deverá possuir serviço de “Host Dynamic DNS” sem custo e com segurança reforçada;

1.7.18. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular, baseado em perfis de acesso;

1.7.19. Deverá fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades, exemplo: para firewall um tipo de autenticação, para VPN outro tipo de autenticação;

1.7.20. Deverá suportar autenticação de usuário de diferentes sessões, originando do mesmo endereço IP;

1.7.21. A solução proposta deverá ter suporte a ambientes de terminais (Microsoft e
Citrix).

1.7.22. Deverá suportar serviço de DHCP/DHCPv6, serviço de DHCP/DHCPv6 Relay Agent;

1.7.23. Deverá haver suporte a DHCP sobre VPN IPSec;

1.7.24. Deverá possuir controle de acesso e dispositivos por zoneamento;

1.7.25. Deverá permitir o factory reset e troca do idioma via interface gráfica;

1.7.26. Deverá haver a possibilidade de reutilização de definições de objetos de rede, host, serviços, período de tempo, usuários, grupos, clientes e servers;

1.7.27. Deverá possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes;

1.7.28. Deverá ter funcionalidade que permita ao administrador atribuir e/ou distribuir cores do CPU para uma interface em particular;

1.7.29. A solução proposta deverá fornecer gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting;

1.7.30. Deverá haver a opção de habilitar acesso remoto do appliance para suporte diretamente com o fabricante através de um túnel seguro, esta funcionalidade deve estar embarcada no próprio appliance.

1.8. Balanceamento de Carga e Redundância:

1.8.1. A solução proposta deverá suportar balanceamento de carga e redundância para mais de 2 (dois) links de internet;

1.8.2. Deverá ter suporte a roteamento com base em origem, destino, nome de usuário e aplicação;

1.8.3. A solução proposta deverá enviar e-mail de alerta ao administrador sobre a mudança do status de gateway;

1.8.4. Deverá permitir ativo/ativo utilizando algoritmo de “Round Robin” e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover);

1.8.5. A solução proposta deverá fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

1.9. Especificações de Disponibilidade:

1.9.1. A solução proposta deverá suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo;

1.9.2. Os administradores deverão ser notificados sobre o estado (status) dos gateways, mantendo a Alta Disponibilidade;

1.9.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado;

1.9.4. A solução deverá detectar falha em caso de link de internet, hardware e sessão;

1.9.5. A solução proposta deve suportar sincronização automática e manual entre os appliances em “cluster”;

1.9.6. Deverá suportar Alta Disponibilidade (HA) em “Bridge Mode” e Mixed Mode" (Gateway + Bridge).

1.10. Proteção Básica:

1.10.1. Deverá suportar controles por porta e protocolos TCP/UDP, origem/destino e identificação de usuários;

1.10.2. A solução deverá ser Standalone Appliance e com sistema operacional fortalecido “Hardening” para aumentar a segurança;

1.10.3. Deverá ter suporte a objetos e regras IPV6 e objetos e regras multicast;

1.10.4. A solução proposta deverá suportar “Stateful Inspection” baseado no usuário “oneto-one”, NAT dinâmico e PAT;

1.10.5. A solução deverá usar a “identidade do usuário” como critério de origem/destino, IP/subnet/grupo e porta de destino na regra do firewall;

1.10.6. A solução proposta deverá unificar as políticas de ameaças de forma granular, como antivírus/antispam, IPS, filtro de conteúdo, políticas de largura de banda e política de balanceamento de carga, baseado na mesma regra do firewall;

1.10.7. A solução anti-malware deverá realizar a proteção com emulação JavaScript;

1.10.8. Deverá permitir o bloqueio de vulnerabilidades;

1.10.9. Deverá permitir o bloqueio de exploits conhecidos;

1.10.10. A solução proposta deverá suportar arquitetura de segurança baseado em zonas, as zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis;

1.10.11. A solução proposta deverá ter predefinidas aplicações baseadas na “porta/assinatura” e também suporte à criação de aplicativo personalizado baseado na “porta/número de protocolo”;

1.10.12. Deverá suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP;

1.10.13. A solução proposta deverá suportar 802.1q (suporte a marcação de VLAN);

1.10.14. A solução proposta deverá suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4;

1.10.15. O sistema proposto deve prover regras de firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI;

1.10.16. Deverá haver suporte a implementações de IPv6 Dual Stack;

1.10.17. A solução proposta deverá suportar tuneis 6in4, 6to4, 4in6, 6rd;

1.10.18. Toda a configuração de IPv6 deverá ser suportada através da interface gráfica;

1.10.19. A solução deverá suportar DNSv6;

1.10.20. A solução deverá prover proteção DoS contra ataques IPv6;

1.10.21. A solução deverá oferecer prevenção contra Spoof em IPv6;

1.10.22. A solução deverá suportar 802.3 ad para Link Aggregation;

1.10.23. A solução proposta deverá suportar gerenciamento de banda baseado em aplicação, que permite a administradores criarem políticas de banda de utilização de link baseado por aplicação;

1.10.24. Deverá possibilitar o bloqueio de Países baseados em GeoIP;

1.10.25. Deverá ter suporte a Upstream proxy;

1.10.26. Deverá ter suporte a VLAN DHCP e tagging;

1.10.27. Deverá ter suporte a multiple bridge;

1.10.28. Deverá suportar autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI);

1.10.29. Deverá possibilitar a autonomia de troca de senha do usuário;
1.10.30. Deverá possibilitar a visualização do uso de internet do usuário conectado;
1.10.31. A solução deverá suportar autenticação via AD/LDAP, Token e base de usuários local;
1.10.32. Deverá haver a possibilidade de criação de regras que limitem e garantam upload e download;
1.10.33. Deverá permitir a criação de regra de QoS individualmente e de forma compartilhada.

1.11. Proteção de Redes:

1.11.1. Deverá prover funcionalidade de Intrusion Prevention System (IPS);
1.11.2. Deverá suportar a customização de assinaturas, permitindo ao administrador agregar novas; sempre que desejado;
1.11.3. Deverá proporcionar flexibilização na criação das regras de IPS, permitindo que as regras possam ser aplicadas tanto para usuários quanto para redes;
1.11.4. Deverá possuir funcionalidade Anti-DoS;
1.11.5. Deverá ser imune e capaz de impedir ataques básicos, como: SYN flood, ICMP flood, UDP Flood, etc;
1.11.6. A solução deverá possuir templates pré-configurados, havendo sugestões de fluxo dos pacotes, exemplo: LAN para DMZ, WAN para LAN, LAN para WAN, WAN para DMZ;
1.11.7. Deverá haver funcionalidade para o administrador criar by-pass de DoS;
1.11.8. Deverá haver a possibilidade de o administrador clonar templates existentes para ter como base quando da criação de sua política customizada;
1.11.9. A solução deverá possuir proteção avançada contra ameaças persistentes (APT);
1.11.10. A solução deverá detectar e bloquear tráfego de pacotes suspeitos e maliciosos que trafeguem pela rede tentando realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, firewall e outros;
1.11.11. A solução deverá disponibilizar logs e relatórios que informem todos eventos de APT;
1.11.12. Em casos de falso positivo, deverá ser permitido ao administrador criar exceções para o fluxo considerado como APT.

1.12. Proteção para Servidores Web (WAF):

1.12.1. Deverá possuir:
1.12.1.1. Funcionalidade de proxy reverso;
1.12.1.2. Engine de URL hardening e prevenção a directory traversal;
1.12.1.3. Engine Form hardening;
1.12.1.4. Proteção contra SQL injection;
1.12.1.5. Proteção contra Cross-site scripting;
1.12.1.6. Bloqueio de conteúdo considerado unscannable;
1.12.1.7. HTTPS (SSL) encryption offloading;
1.12.1.8. Proteção para cookie signing com assinaturas digitais;
1.12.1.9. Path-based routing;
1.12.1.10. Suporte ao protocolo do Outlook anywhere;
1.12.1.11. Autenticação reversa para acesso aos servidores web;

1.12.1.12. Possibilidade de criação de templates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação;

1.12.1.13. Função de load balancer para que os visitantes possam ser jogados para diversos servidores de maneira transparente; 1.12.1.14. Bloqueio de clientes com má reputação; 1.12.1.15. Bloqueio de protocolos com anomalias.

1.13. Relatórios:

1.13.1. Deverá possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de um único console central;

1.13.2. Deverá ser possível a customização dos relatórios padrão da solução;

1.13.3. Deverá ser permitido que o administrador realize agendamentos de relatórios para que estes sejam enviados para todos os e-mails cadastrados;

1.13.4. Os relatórios customizados deverão estar em conformidade com, pelo menos, estes órgãos: HIPAA, SOX, PCI;

1.13.5. A solução deverá armazenar histórico dos relatórios em disco local;

1.13.6. Deverá ser possível exportar relatórios para PDF, Excel;

1.13.7. Deverá possuir multiformato de relatórios, ao menos tabular e gráfico;

1.13.8. Deverá possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipédia, Google;

1.13.9. Deverá possuir relatórios que informem as principais atividades em cada módulo;

1.13.10. A solução deverá produzir logs em tempo real;

1.13.11. A solução deverá arquivar os logs para consulta posterior;

1.13.12. Deverá possuir mecanismo de procura de logs arquivados;

1.13.13. O administrador deverá poder acessar os relatórios de qualquer lugar através de um navegador;

1.13.14. Deverá haver total gerencia sobre a retenção dos dados armazenados no equipamento.

1.14. Suporte a Virtualizadores:

1.14.1. A solução deverá possuir, no minimo, suporte aos virtualizadores: VMware, HyperV, Citrix, KVM e Proxmox;

1.14.2. Deverá possuir capacidade de armazenamento ilimitado, tendo apenas o disco como limitador;

1.14.3. Deverão ser fornecidas soluções virtuais ou via appliance desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 500GB de dados;

1.15. Serviços de Instalação e Treinamento:

1.15.1. O equipamento deverá ser instalado em rack, localizado no Setor de TI da Prefeitura Municipal de Carlos Barbosa;

1.15.2. Deverá ser realizada a ativação do sistema operacional, com instalação da licença e demais particularidades do equipamento;

1.15.3. Deverão ser criados usuários para administração e gerência do equipamento;

1.15.4. Deverão ser configurados 2 (dois) links de internet, configurações de endereços IPv4 e IPv6 públicos dos respectivos links;

1.15.5. Todas as regras, usuários, particularidades e configurações do atual firewall em uso na Prefeitura, Sophos XG 230, deverão ser migradas para o novo equipamento;

1.15.6. Deverão ser criados 4 (quatro) perfis de navegação, bloqueando conteúdos específicos por determinado perfil;
1.15.7. A CONTRATADA deverá ministrar treinamento relativo à instalação, operacionalização, manuseio, configuração e utilização da solução de segurança, visando garantir a transferência de conhecimento para até 4 (quatro) pessoas indicadas pela CONTRATANTE;
1.15.8. O treinamento deverá possuir carga horária mínima de 8 (oito) horas, observandose que deverá conter todo o conteúdo sobre a solução;
1.15.9. As datas e horários para realização dos treinamentos serão definidos pela CONTRATANTE em comum acordo com a CONTRATADA;
1.15.10. O instrutor deverá possuir experiência em treinamentos desta natureza e pleno conhecimento da solução de segurança;
1.15.11. Deverá ser emitido certificado aos participantes do treinamento que cumprirem frequência mínima de 80%;
1.15.12. Treinamento deve ser ministrado por um técnico Nível Architect Next Generation Firewall.

1.16. Qualificação Técnica:

1.16.1. Para o fornecimento de suporte e atualizações, assim como a implementação, a empresa responsável pela execução dos serviços deverá possuir as seguintes certificações, atestados ou declarações:
1.16.1.1. No mínimo 1 (um) técnico nível Engineer Next Generation Firewall;
1.16.1.2. No mínimo 1 (um) técnico nível Architect Next Generation Firewall;
1.16.1.3. No mínimo 1 (um) técnico com certificação MCSA Windows Server 2016 ou superior;
1.16.1.4. No mínimo 1 (um) técnico com certificação Fundamentos de Azure;
1.16.1.5. No mínimo 1 (um) técnico com certificação LPI-2;
1.16.1.6. No mínimo 1 (um) DPO Data Protection Officer ou Encarregado de Dados;
1.16.1.7. Comprovação de aptidão da empresa por meio de, no mínimo, 1 (um) atestado de capacidade técnica, comprovando serviços de suporte, atualização e fornecimento do Next-Generation Firewall (NGFW) e de consultoria especializada;
1.16.1.8. Declaração emitida pelo fabricante da solução, para suporte, atualização e fornecimento do NextGeneration Firewall (NGFW);
1.16.1.9. Comprovação de localização em um raio máximo de 100 km (cem) quilômetros da sede do município de Carlos Barbosa para atendimento de demandas presenciais urgentes, quando necessário;
1.16.1.10. As empresas interessadas em participar do certame poderão promover visita técnica junto ao Setor de TI da Prefeitura Municipal, devendo previamente agendá- la e realizá-la com antecedência de até 48 horas antes da data de abertura do certame (recebimento e abertura dos envelopes), e será atestado que a empresa visitou o local onde será instalado o equipamento, bem como tomou conhecimento das particularidades e do treinamento, ficando assim ciente das condições estruturais para o bom cumprimento do objeto desta licitação, acatando a estrutura existente como suficiente, não podendo fazer alegações futuras quanto ao que foi verificado. A visita técnica deverá ser acompanhada por servidor (a) municipal, que ao final da visita, deverá emitir o referido atestado, devendo constar o nome completo, assinatura e nº matrícula;

1.16.1.11. O documento poderá ser substituído por Declaração de que não foi efetuada a vistoria no local onde serão executados os serviços, visto que, dispensado por manifesta vontade, aceita as condições que se apresentarem, bastando os esclarecimentos e informações concedidas pela Municipalidade, as quais dirimiram as dúvidas anteriormente à abertura do certame (se for o caso), e para tanto, cientes de todas as condições necessárias para a perfeita e completa execução
dos serviços licitados, acatam a estrutura existente como suficiente, não podendo fazer alegações futuras quanto ao que foi verificado.

1.17. Informações:

1.17.1. A LICITANTE vencedora se obriga a fornecer soluções em Appliance de firewall com Gerenciamento Unificado de Ameaças (UTM – Unified Threat Mangement), entendendo-se como tais, o conjunto de hardware e software dedicados, necessários e suficientes para o funcionamento da solução, atualização e treinamento para capacitação técnica da equipe da Prefeitura Municipal de Carlos Barbosa, de acordo com as especificações descritas no Termo de Referência;

1.17.2. A licitante vencedora deverá iniciar a instalação dos equipamentos em até 15 (quinze) dias após a assinatura do contrato, podendo esse prazo ser extendido mediante justificativa e com aceitação da CONTRATANTE;

1.17.3. A instalação e entrega deverão ocorrer junto ao Setor de TI, no centro administrativo da Prefeitura Municipal de Carlos Barbosa;

1.17.4. O fabricante deverá fornecer garantia dos equipamentos pelo período de vigência das licenças;

1.17.5. Verificando-se problema que cause impedimento para o pleno funcionamento do equipamento, deverá ser realizada a manutenção corretiva ou substituição do mesmo por equipamento reserva fornecido pela CONTRATADA, sem custo adicional para a CONTRATANTE, no prazo máximo de 4 (quatro) horas, a contar da comunicação do problema pela CONTRATANTE. A solução definitiva, seja por manutenção corretiva ou substituição por equipamento novo, de igual modelo ou
superior, deverá ser realizada no prazo máximo de 2 (dois) dias, a contar da comunicação do problema pela CONTRATANTE;

1.17.6. A vigência contratual será de 12 (doze) meses, contados da data de assinatura do contrato;

1.17.7. Todas as despesas (de qualquer natureza), sejam elas tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), fornecimento de mão-de-obra especializada, leis sociais, administração, lucros, equipamentos e ferramentas, transporte de material e de pessoal, acomodações e despesas com os funcionários da contratada que executarão os serviços (alojamento, transporte, refeição, encargos sociais, trabalhistas, etc.) e demais despesas referentes à execução do objeto da presente licitação, ficarão a cargo da licitante vencedora.