Prefeitura Municipal de Pedro Leopoldo
Secretaria Municipal de Administração
Rua Dr. Cristiano Otoni, 555 - Centro
33250-006 - Pedro Leopoldo/MG
Telefone: (31) 3660-5114
E-mail: administracao@pedroleopoldo.mg.gov.br

ESTUDO TÉCNICO PRELIMINAR

Área Requisitante: Secretaria Municipal de Administração

1. DESCRIÇÃO E JUSTIFICATIVA DA NECESSIDADE

1.1. A implementação de um firewall em uma prefeitura é fundamental para garantir a segurança de dados sensíveis, como informações pessoais de cidadãos e registros financeiros, protegendo-os contra acessos não autorizados e ataques cibernéticos. Além de filtrar o tráfego de entrada e saída, prevenindo invasões e malware, um firewall é essencial para a conformidade com legislações como a LGPD, que exige medidas rigorosas de proteção de dados. Ele também contribui para a estabilidade e o desempenho dos serviços públicos online, permitindo um gerenciamento eficiente do tráfego de rede. Com a capacidade de monitorar atividades suspeitas e gerar relatórios, o firewall facilita auditorias e análises de segurança, protegendo ainda mais a infraestrutura crítica da prefeitura, incluindo servidores e sistemas de gerenciamento. Assim, um firewall robusto é uma etapa indispensável para assegurar a integridade e a segurança dos sistemas e dados municipais.

2. ALINHAMENTO COM PAC (PLANO ANUAL DE CONTRATAÇÕES)

2.1. A presente demanda encontra-se preconizada no Plano de Contratação Anual - PAC/2024

3. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

3.1. Requisitos técnicos:

3.1.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.

3.1.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

3.1.3. Desempenho mínimo de 3.3 Gbps de IPS.

3.1.4. Suporte mínimo de 500.000 conexões simultâneas/concorrentes no modo DPI.

3.1.5. Suporte mínimo de 20.000 novas conexões por segundo.

3.1.6. Deve suportar expansão de armazenamento interno para até 256Gb.

3.1.7. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

3.1.8. Deve possuir 16 interfaces 1 GbE padrão RJ-45.

3.1.9. Deve possuir 3 interfaces 10GbE SFP+; Deve possuir 1 do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

3.1.10. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

3.1.11. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos, com aquisição de licença complementar.

3.1.12. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos, com aquisição de licença complementar.

3.1.13. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

3.1.14. Deve suportar, no mínimo, 2.1 Gbps de desempenho de VPN IPSEC.

3.1.15. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

3.1.16. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

3.1.17. O Equipamento deverá ser homologado pela ANATEL.

3.1.18. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

3.1.19. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 12(doze) meses, renováveis de acordo com o prazo da prestação e execução dos serviços.

3.1.20. A garantia do hardware deverá ser de 12 (doze) meses.

3.1.21. É imprescindível que a solução possua um limite mínimo de tamanho de arquivos de, ao menos, 400Mb, no uso da tecnologia 'gateway antimalware' liveprotection, já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

3.2.Características Gerais Dos Firewalls Físicos

3.2.1.Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

3.2.2.Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

3.2.3.A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

3.2.4.Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

3.2.5.Não serão aceitas soluções baseadas em PCs (personal computers) de uso geral, assim como soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

3.2.6.Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 12(doze) meses, incluindo garantia e suporte, renováveis de acordo com o prazo da prestação e execução dos serviços.

3.3.Características Diversas

3.3.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

3.3.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do túnel IPSec.

3.3.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

3.3.5. Deve possuir proteção anti-spoofing.

3.3.6. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP.

3.3.7. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

3.3.8. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

3.3.9. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

3.3.10. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

3.3.10.1. Latência;

3.3.10.2. Jitter;

3.3.10.3. Perda de pacotes.

3.3.11. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.

3.3.12. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

3.3.13. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

3.3.14. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

3.3.15. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

3.3.16. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

3.3.17. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

3.3.18. Deve suportar DHCP relay.

3.3.19. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

3.3.20. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

3.3.21. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares P2P (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

3.3.22. Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

3.3.23. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

3.3.24. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

3.3.25. Detectar e bloquear a origem de portscans.

3.3.26. Deve permitir o bloqueio de ataques.

3.3.27. Deve permitir o bloqueio de exploits conhecidos.

3.3.28. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP.

3.3.29. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.

3.3.30. Implementar DSCP (Differentiated Services Code Points).

3.3.31. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

3.3.32. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice Over IP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

3.3.33. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

3.3.34. Possuir suporte ao protocolo SNMP versões 2 e 3.

3.3.35. Possuir suporte a log via syslog.

3.3.36. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

3.3.37. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

3.3.38. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

3.3.39. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

3.3.40. Para tráfego criptografado SSL/TLS, deve decriptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

3.3.41. Controle, inspeção e decriptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

3.3.42. Deve permitir a funcionalidade de ARP bridging.

3.3.43. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".

3.4 **Características De VPN**

3.4.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

3.4.2. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256

3.4.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

3.4.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

3.4.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

3.4.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

3.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

3.4.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

3.4.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

3.4.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

3.4.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

3.4.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

3.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

3.4.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

3.4.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

3.4.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

3.5. **Alta Disponibilidade**

3.5.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

3.5.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

3.5.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

3.5.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

3.5.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

3.5.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

3.5.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

3.5.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

3.5.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

3.6. **Controle De Ameaças**

3.6.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

3.6.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

3.6.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

3.6.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

3.6.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

3.6.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

3.6.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

3.6.8. Implementar interface CLI segura através do protocolo SSH.

3.6.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

3.6.10. A solução deve permitir criar regras de exceção de acordo com a proteção.

3.6.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

3.6.12. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

3.6.13. A solução deve ser capaz de proteger contra ataques a DNS.

3.6.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

3.6.15. A solução deve ser capaz de prevenir acesso a websites maliciosos.

3.6.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

3.6.17. A solução deverá receber atualizações de um serviço baseado em cloud.

3.6.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

3.6.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

3.6.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

3.6.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

3.6.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

3.7. Proteção Contra Ataques Avançados

3.7.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

3.7.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

3.7.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

3.7.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

3.7.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

3.7.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

3.7.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

3.7.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

3.7.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

3.7.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este

3.8. **Características De Filtro De Conteúdo Web**

3.8.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.

3.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local.

3.8.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

3.8.4. Permitir a customização de página de bloqueio.

3.8.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

3.8.6. Deve permitir submissão de novos sites para categorização.

3.8.7. Permitir a classificação dinâmica de sites web, URLs e domínios.

3.8.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

3.8.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

3.8.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

3.9. Características De Autenticação

3.9.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

3.9.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

3.9.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

3.9.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

3.9.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

3.9.6. Deve 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 NGFW.

3.9.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

3.9.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

3.9.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

3.9.10. A solução deve possibilitar SSO via API

3.10. Características De Administração

3.10.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

3.10.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

3.10.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

3.10.4. Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração.

3.10.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

3.10.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

3.10.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

3.10.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

3.10.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

3.10.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.

3.10.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

3.10.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real, estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

3.10.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

3.10.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

3.10.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

3.10.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

3.10.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

3.10.18. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

3.10.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

3.10.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

3.10.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

3.10.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

3.10.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

3.10.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

3.10.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

3.10.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto-provisionamento da plataforma através de ponto central de gerenciamento.

3.10.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações.

3.10.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

3.10.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

3.11 Gerenciamento Unificado e Relatórios

3.11.1. Deve possuir solução de gerenciamento centralizado em nuvem do mesmo fabricante, para gerenciamento de toda solução.

3.11.2. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que determinem usuários

a. Grupos de firewalls permitidos

b. Funcionalidades permitidas por firewall ou grupo de firewalls de acordo com o perfil de uso designado

c. Perfil de nível de acesso (escrita, leitura, administração, relatórios)

3.11.3. Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual

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

3.11.5. Deve apresentar estado dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

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

3.11.7. O gerenciamento deve permitir/possuir:

a. Criação e administração de políticas de firewall e controle de aplicação

b. Monitoração de logs;

c. Investigação de evendos de segurança e falhas (debugging)

d. Acesso concorrente de administradores, conforme políticas e perfis previamente definidos

3.11.8. Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). Os firewalls devem se conectar automaticamente à plataforema de gerencia, e à partir desta conexão receberem as configurações previamente determinadas pelos operadores da plataforma.

3.11.9. A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL

3.11.10. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

3.11.11. A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador:

a. nome do firewall

b. número de série

c. modelo

d. versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline.

3.11.12. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;

3.11.13. Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento, possibilitando comparação de configurações que evitem sobreposição de regras e conflitos de configuração.

3.11.14. A solução deve possuir Dashboard com sumario de alertas e informação de status de licença

3.11.15. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo

3.11.16. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência

3.11.17. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN

3.11.18. A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls

3.11.19. A solução deve possibilitar a geração de templates de configuração à partir da configuração vigente em um firewall selecionado pelo administrador da plataforma, e possibilitar que este template possa ser editado e utilizado em outros firewalls gerenciados pela plataforma.

3.11.20. Os modelos de configuração (templates) devem suportar configurações de interfaces físicas ou virtuais

3.11.21. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

3.11.22. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

3.11.23. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;

3.11.24. Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

3.11.25. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

3.11.26. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

3.11.27. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, este processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente

3.11.28. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

3.11.29. A solução deve oferecer monitor de auditoria de configuações aplicadas aos firewalls gerenciados pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas.

3.11.30. A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações dos firewalls gerenciados.

3.11.31. A solução deve oferecer possibilidade de auditoria de configurações.

3.11.32. A solução deve possibilitar o monitoramento em tempo real dos firewalls gerenciados, informando minimamente:

3.11.33. a. Utilização de CPU/Processamento

b. Aplicações em uso e seu consumo de banda

c. Interfaces em uso e utilizaçào de banda

d. Conexões concorrentes em uso

3.11.34. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls

3.11.35. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a geração de relatórios e monitoramento em tempo real.

3.11.36. A solução deverá prover relatórios com no mínimo histórico de 365 dias

3.11.37. A solução deverá prover relatórios referente as atividades dos usuários

3.11.38. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações:

a. nome da aplicação

b. quantidade de conexões

c. percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados

3.11.39. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:

a. nome do usuário

b. quantidade de conexões

c. percentual que tráfego do usuário representa na rede

d. quantidade de Megabytes trafegados

3.11.41. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

a. endereço IP

b. quantidade de conexões

c. percentual que tráfego que o IP representa na rede

d. quantidade de Megabytes trafegados

3.11.42. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede

3.11.43. A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF

3.11.44. A solução deverá permitir geração e envio agendado de relatórios

3.11.45. A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-Mail com as informações relativas a este evento.

3.11.46. A solução deve possibilitar configuração e monitoramento centralizados de VPNs entre os firewalls gerenciados

3.11.47. A solução deve apresentar consoles de indicação com os principais eventos, riscos e ameaças contendo:

a. Aplicações de maior risco, e volume de dados consumido por estas

b. Aplicações de maior utilização, por volume de dados transferidos e conexões consumidas

c. Aplicações de maior utilização, por categoria

3.11.48. A solução deve apresentar consoles de indicação dos principais usuários contendo:

3.11.49. a. Usuários utilizando mais conexões

3.11.48. b. Usuários consumindo mais dados

3.11.50. A solução deve apresentar console de indicação de:

a. Virus/Spyware blockeados

b. Intrusões bloqueadas

c. Botnets bloqueados

d. Origens e destinos mais utilizados

3.11.51. A solução deve apresentar console de indicação de Aplicações indicando:

a. Aplicações identificadas

b. Categorização e uso das aplicações

c. Risco das aplicações

3.11.52. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

a. Lista de eventos correlacionados com opção de navegação "drilldown"; ou

b. Modo gráfico; ou

c. Lista de logs

3.11.53. A solução deve apresentar console de monitoramento de produtividade dos usuários, indicando suas características de navegação de acordo com políticas previamente estabelecidas e categorizadas como:

a. Produtivas

b. Não produtivas

c. Aceitáveis para a política de uso corporativa

d. Inaceitáveis para a política de uso corporativa

e. Customizadas

3.11.54. A solução deve permitir visualização de topologia do firewal e elementos a ele conectados (dispositivos de rede complementares, dispositivos de usuários, Access Points)

3.11.55. O Fabricante deverá comprovar que possui tecnologia holística capaz de integrar suas principais soluções em uma base centralizada gráfica com informações e alertas, comprovando integração de pelo menos 2 de suas plataformas de segurança.

3.12. **Treinamento de Capacitação:**

3.12.1.Deverá ser realizado um treinamento para solução integrada de Firewall e Service Gateway a ser utilizada na prestação dos serviços, ministrado por profissional certificado na solução. Este será realizado na Prefeitura para até 8 (oito) pessoas em uma única turma. A duração deverá ser de no mínimo 16 (dezesseis) horas, abordando as os seguintes tópicos:

- Introdução à plataforma e funcionalidades do equipamento;
- Introdução ao software de gerenciamento;

- Introdução à interface gráfica de usuário;
- Regras de Firewall;
- Zonas de segurança;
- Políticas de segurança;
- Autenticação de usuários;
- Proteção de rede;
- NAT (Network Addres Translation).

3.12.2.O treinamento deve ser vinculado as plataformas vencedoras do item 1;

3.12.3.Qualquer despesa incorrida tais como escopo do serviço, passagens aéreas, locação de veículos, hospedagens e alimentação do instrutor será de responsabilidade exclusiva do contratado.

3.12.4.Será de responsabilidade da Prefeitura a disponibilização de infraestrutura e dos equipamentos para montagem da sala de aula e laboratório.

3.12.5.Os treinamentos serão ministrados no idioma português. Os materiais fornecidos podem estar no idioma português ou inglês.

3.12.6.Após a realização do treinamento, deverá ser fornecido um certificado formal de participação para cada participante do evento.

3.12.7.A proponente vencedora deverá apresentar, durante a sessão do pregão, catálogo ou manual impresso publicado pelo fabricante do equipamento ofertado, em língua portuguesa ou inglesa, com identificação precisa da página onde se encontram as informações sobre o atendimento de cada requisito exigido na especificação técnica;

3.12.8.Poderá ser aceita cópia de documento publicado no sítio do fabricante na Internet que comprove as especificações do equipamento, desde que da mesma conste o endereço eletrônico de acesso irrestrito, devendo estar disponível para acesso ao público em geral e passível de verificação durante a sessão do pregão.

3.12.9.Todas as declarações deverão ser apresentadas com firma reconhecida em cartório e acompanhadas dos documentos que comprovem a capacidade legal de quem as assinou;

3.12.10.Todos os documentos deverão estar vigentes no dia previsto para realização deste pregão.

3.13. Sustentabilidade:

3.13.1. A presente aquisição não possui relevantes impactos ambientais, contudo, os licitantes deverão ofertar, no que couber, visando a atender ao disposto na legislação aplicável, a CONTRATADA deverá priorizar, para o fornecimento do objeto, a utilização de bens que sejam no todo ou em parte compostos por materiais recicláveis, atóxicos e biodegradáveis.

3.14. Da Visita Técnica

3.14.1. Para o correto dimensionamento e elaboração de sua proposta, é facultado ao licitante realizar visita técnica ao local de execução dos serviços. A visita técnica, quando realizada, deverá ser acompanhada pelo responsável técnico da Divisão de T.I.

3.14.2. As vistorias técnicas poderão ser realizadas de segunda à sexta-feira, no horário entre 09:00 horas às 17:00 horas, devendo o agendamento ser efetuado previamente pelo telefone (31) 3660-5122 ou através do e-mail ti@pedroleopoldo.mg.gov.br.

3.14.3. Realizada a visita técnica, será emitida uma Declaração de Vistoria Técnica, conforme modelo constante do Anexo II, a Declaração de Visita Técnica comprovará que a empresa tomou ciência de todas as informações necessárias para a execução do objeto em questão.

3.14.4. Caso a licitante opte pela não realização da vistoria técnica, esta não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante, caso seja vencedora, assumir os ônus dos serviços decorrentes; e optado pela não

realização da vistoria técnica, será emitida uma Declaração de Dispensa de Visita Técnica, conforme modelo constante do Anexo III.

3.15. Da Responsabilidade Técnica:

3.15.1. A empresa prestadora dos serviços deverá possuir em seu quadro de funcionários ou sócios, no mínimo 01 (um) técnico, certificado pelo fabricante, comprovado através da apresentação da cópia do documento válido. .

3.15. Do Suporte, Garantia e Assistência Técnica:

3.15.1. Todos os serviços de suporte e manutenção preventiva ou corretiva, assim como a substituição de peças e suprimentos necessários ao perfeito funcionamento do bem durante a vigência do contrato, serão prestados pelo fornecedor.

3.15.2. O suporte técnico será realizado remoto ou "on-site", de acordo com a necessidade e requisição da Prefeitura, sem ônus adicional durante a vigência do contrato.

3.15.3. A Contratada deverá disponibilizar um aplicativo via web para abertura de chamados de suporte técnico, ou Central de Atendimento ou correio eletrônico do prestador de serviços;

3.15.4. O prazo de atendimento para solução deverá ser respeitado de acordo com a tabela de prioridades e prazos abaixo:

Serviços	Prioridade	Prazo
Atendimento Telefônico Abertura de Chamados WEB	**1,2 e 3**	24x7 (24 Horas / 7 Dias Semana)
Horário de Atendimento	**1,2 e 3**	24x7 (24 Horas / 7 Dias Semana)
Tempo de Resposta para Serviços Remotos	**2**	Até 2 Horas Úteis
	3	Até 4 Horas Úteis
Atendimentos "On Site"	**1**	Até 4 Horas Úteis

Descrição das Prioridades:

1 - Não conformidades que restringem completamente (80 a 100%) o funcionamento de todo o sistema ou apresentem-se como ameaças concretas. *Ex.:* Paralisação do Firewall ou da rede WAN.

2 - Não conformidades que restringem parcialmente (26 a 80%) o funcionamento de todo o sistema ou apresentam-se como vulnerabilidades para possíveis ameaças. *Ex.:* Lentidão na performance

3 - Não conformidades que não restringem (0 a 25%) o funcionamento de todo o sistema, mas sim de usuários isolados *Ex.:* Um usuário bloqueado

4. ESTIMATIVA DAS QUANTIDADES E PRAZO DA CONTRATAÇÃO

4.1. Com base na análise realizada pela Divisão de Tecnologia da Informação, ficou estimado o quantitativo constante no Anexo I deste estudo.

4.2. No que se refere ao prazo de vigência da contratação, o mesmo deverá ser de 60 meses considerando as seguintes informações:

4.2.1. A contratação de uma empresa especializada em segurança da informação pelo prazo de 60 meses fundamenta-se na natureza contínua dos serviços prestados, além de serviços estruturantes de Tecnologia da Informação, sendo indispensáveis para garantir a proteção e a integridade dos ativos digitais e das informações estratégicas da instituição em tempo integral.

4.2.2. Os serviços de segurança da informação englobam atividades críticas e de caráter permanente, como:

4.2.2.1. Monitoramento contínuo de sistemas e redes para detecção e resposta a ameaças cibernéticas em tempo real.

4.2.2.2. Gestão de vulnerabilidades, incluindo a realização periódica de análises de riscos, testes de invasão (pentests) e implementação de correções.

4.2.2.3. Atualização e manutenção de ferramentas de segurança, como firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), e soluções de antivírus e antimalware.

4.2.2.4. Conformidade regulatória, assegurando que a instituição atenda às normas e legislações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).

4.2.2.5. Capacitação e conscientização dos colaboradores, com treinamentos regulares sobre boas práticas de segurança e proteção contra phishing e outras ameaças.

4.2.3. Devido à complexidade e à criticidade desses serviços, é imprescindível garantir sua execução de maneira ininterrupta e com a qualidade necessária, o que demanda um contrato de longo prazo com uma empresa especializada. Esse modelo permite:

4.2.3.1. Continuidade operacional, evitando interrupções que poderiam comprometer a segurança e o

desempenho dos sistemas.

4.2.3.2. Economia de escala, ao firmar um contrato estendido com condições favoráveis de investimento em soluções tecnológicas e especializadas.

4.2.3.3. Planejamento estratégico, permitindo maior previsibilidade e alinhamento das ações de segurança ao planejamento de longo prazo da instituição.

4.2.4. Além disso, o prazo de 60 meses é adequado para a maturação e aprimoramento contínuo das estratégias e processos de segurança, considerando a rápida evolução das ameaças cibernéticas e das tecnologias de proteção.

4.2.5. Assim, justifica-se a contratação pelo período proposto como medida essencial para assegurar a proteção contínua das informações e a conformidade da instituição com as melhores práticas e exigências do mercado.

4.2.6. A presente contratação se encontra alinhada com o Plano Anual de Contratação.

5. LEVANTAMENTO DE MERCADO

5.1. A escolha de um firewall específico para uma prefeitura deve ser fundamentada na singularidade das necessidades de segurança e na complexidade dos dados geridos. Ao avaliar as opções disponíveis no mercado, é evidente que não existe uma solução única que atenda a todos os requisitos exigidos por uma entidade pública.

5.2. Primeiramente, as prefeituras lidam com informações altamente sensíveis e reguladas, que demandam um nível de proteção personalizado e adaptado às suas operações. Soluções genéricas frequentemente não oferecem as especificidades necessárias para garantir a conformidade com legislações como a LGPD, além de não atenderem aos protocolos de segurança exigidos para a proteção de dados públicos.

5.3. Além disso, o firewall deve integrar-se com outros sistemas existentes na prefeitura, como plataformas de gestão pública e bancos de dados, requerendo uma personalização que muitas soluções de mercado não oferecem. As necessidades de monitoramento e registro em tempo real, assim como a capacidade de gerar relatórios detalhados, também são cruciais e podem não ser plenamente atendidas por alternativas disponíveis.

5.4. Por fim, a resposta a incidentes e suporte técnico devem ser adaptáveis ao contexto específico da prefeitura, algo que soluções padronizadas frequentemente falham em proporcionar. Portanto, a única solução viável é a contratação de uma empresa especializada na prestação de serviços de segurança de rede de computadores, que ofereça um firewall com funcionalidades de UTM (Unified Threat Management), incluindo serviços de suporte especializado. Essa

abordagem garantirá não apenas a proteção necessária, mas também um suporte contínuo e adaptado às demandas específicas da prefeitura, assegurando a integridade e a segurança dos dados geridos.

6. ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

6.1. A estimativa do valor de contratação dos serviços levou em consideração o Contrato atual, de número 018/2022. Os valores estão previstos no Anexo I deste Estudo Técnico Preliminar.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

7.1. A implementação de um firewall em uma prefeitura é um passo essencial para a proteção da infraestrutura de TI e dos dados sensíveis dos cidadãos. Com a crescente ameaça de ataques cibernéticos, um firewall atua como a primeira linha de defesa, filtrando o tráfego de entrada e saída para bloquear acessos não autorizados e prevenir a infiltração de malware. Isso é crucial para salvaguardar informações pessoais, registros financeiros e documentos públicos, garantindo que dados sensíveis permaneçam protegidos.

7.2. Além de garantir a segurança, o firewall contribui para a conformidade com legislações como a LGPD, que exige que entidades públicas adotem medidas rigorosas de proteção de dados. Ele também melhora a estabilidade e o desempenho dos serviços públicos online, otimizando o tráfego de rede e assegurando que as operações funcionem de forma eficiente e contínua.

7.3. O firewall permite o monitoramento constante da rede, ajudando a identificar atividades suspeitas e gerando relatórios valiosos para auditorias e análises de segurança. Isso não apenas fortalece a segurança, mas também promove uma cultura de responsabilidade e transparência na gestão de dados.

7.4. Em resumo, um firewall robusto é uma ferramenta indispensável para prefeituras, proporcionando segurança, conformidade legal, desempenho otimizado e proteção da infraestrutura crítica. Com essa proteção em vigor, as prefeituras podem operar com maior confiança, assegurando a integridade e a privacidade dos dados dos cidadãos.

8. JUSTIFICATIVA PARA PARCELAMENTO

8.1. Optar por um **lote único** para a contratação de empresa especializada para prestar serviço de rede de computadores composta por firewall proporciona significativas vantagens em termos de economia de escala, simplicidade administrativa, e uniformidade. A compra em volume permite negociar melhores preços e condições com fornecedores, reduzindo custos e facilitando o gerenciamento através de um único contrato. Além disso, garante que todos os equipamentos atendam às mesmas especificações e padrões técnicos, simplificando a logística e armazenamento, e assegurando uma entrega coordenada e eficiente. Essa abordagem também fortalece a posição de negociação e melhora a conformidade com normas e regulamentos, promovendo um processo mais eficaz e transparente.

9. DEMONSTRAÇÃO DOS RESULTADOS PRETENDIDOS

9.1. A contratação de uma empresa especializada para fornecer um firewall para esta prefeitura visa alcançar uma série de resultados significativos, entre os quais:

9.2. Proteger informações sensíveis, como dados pessoais de cidadãos e registros financeiros, contra acessos não autorizados e ataques cibernéticos;

9.3. Garantir que a prefeitura atenda a legislações como a LGPD, implementando medidas de segurança adequadas para a proteção de dados;

9.4. Estabelecer um sistema de monitoramento em tempo real para identificar e responder rapidamente a atividades suspeitas ou incidentes de segurança;

9.5. Utilizar funcionalidades de UTM (Unified Threat Management) para integrar diversas medidas de segurança, como filtragem de conteúdo, prevenção de intrusões e proteção contra malware, em uma única solução;

9.6. Garantir acesso a suporte técnico qualificado e personalizado, capaz de resolver problemas e ajustar as configurações conforme as necessidades da prefeitura;

9.7. Otimizar o tráfego de rede, garantindo que os serviços públicos online operem de maneira eficiente e estável;

9.8. Desenvolver um plano de resposta a incidentes que permita agir de forma rápida e eficaz em caso de uma violação de segurança;

9.9. Produzir relatórios detalhados sobre o tráfego de rede e eventos de segurança, facilitando auditorias e avaliações de conformidade;

9.10. Proporcionar treinamento para a equipe da prefeitura, aumentando a conscientização sobre segurança cibernética e melhores práticas;

9.11. Assegurar que a infraestrutura de TI permaneça operante e segura, minimizando o risco de interrupções em serviços essenciais para a comunidade;

9.12. Esses resultados não apenas fortalecerão a segurança da informação, mas também promoverão uma gestão mais eficiente e confiável dos dados públicos, contribuindo para a confiança da população nos serviços prestados pela prefeitura.

10. PROVIDÊNCIAS PRÉVIAS AO CONTRATO

10.1. Não verificou-se providências prévias a serem adotadas, tendo em vista a natureza da contratação.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1. No objeto contratado, não há necessidade de adequação e providências a serem adotadas para a contratação do objeto deste estudo.

12. POSSÍVEIS IMPACTOS AMBIENTAIS

12.1. Considerando a natureza do objeto em questão, não foram identificados impactos ambientais significativos. Entretanto, é imprescindível que a licitante esteja em conformidade com os critérios estabelecidos pelos órgão fiscalizadores

13. POSICIONAMENTO CONCLUSIVO

13.1. A equipe de Planejamento responsável por este estudo afirma a viabilidade e a razoabilidade do mesmo, fundamentando-se nos elementos apresentados no estudo técnico preliminar.

14. RESPONSÁVEL(IS) PELA ELABORAÇÃO DO ETP

Pedro Leopoldo, 10 de Julho de 2024

_____

Luiz Otávio de Assis Martins

Responsável pela elaboração do documento

(Baseado nas informações Técnicas da Divisão de Tecnologia da Informação)

_____

Victor Hugo Pereira Reis

Fiscal do Contrato (Substituto)

_____

Alexandre Thadeu Clemenete Bassouto

Prefeitura Municipal de Pedro Leopoldo
Secretaria Municipal de Administração
Rua Dr. Cristiano Otoni, 555 - Centro
33250-006 - Pedro Leopoldo/MG
Telefone: (31) 3660-5114
E-mail: administracao@pedroleopoldo.mg.gov.br

Responsável Técnico

Fiscal Técnico do Contrato

_____

Paula Poliana Gonçalves Braga

Fiscal Administrativo do Contrato

Aprovo este ETP e declaro que tenho conhecimento de todas as suas características, ratificando, neste ato, o seu integral conteúdo.

Pedro Leopoldo, 10 de Julho de 2024

_____

Helder Sebastião Santos

Secretário Municipal de Administração

Prefeitura Municipal de Pedro Leopoldo
Secretaria Municipal de Administração
Rua Dr. Cristiano Otoni, 555 - Centro
33250-006 - Pedro Leopoldo/MG
Telefone: (31) 3660-5114
E-mail: administracao@pedroleopoldo.mg.gov.br

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

ANEXO I

Item	Descrição	Valor Mensal do Serviço	Valor Total do Serviço (60 Meses)
01	Contratação de empresa especializada em prestação de serviços de segurança da Informação, incluindo equipamentos UTM necessários para prestação dos serviços, monitoramento e suporte especializado em modalidade 24x7, incluindo instalação de equipamentos, configuração, documentação e capacitação de no mínimo 16(dezesseis) horas aos servidores da Divisão de Tecnologia da Informação.	R$ 3.500,00	R$ 210.000,00