PROJETO BÁSICO

1. DA ESPECIFICAÇÃO GERAL DOS SERVIÇOS:

1.1. Das Definições:

1.1.1. O município de Patrocínio/MG, sempre voltado para o bom atendimento à população, necessita que os servidores (colaboradores) façam uso rotineiro do link de acesso a internet, acessando serviços e sistemas nela disponibilizados. Para garantir a continuidade de serviços, torna-se indispensável a contratação de link dedicado de acesso rápido a internet e de maior potência, com recursos capazes de minimizar os problemas decorrentes de falhas pontuais ou lentidão.

1.1.2. A contratação do serviço de link para redundância do acesso a rede mundial de computadores, deve-se a busca de soluções para evitar paralisações nos trabalhos e a necessidade de ampliar a disponibilidade de serviços já existentes, também garantir a continuidade dos mesmos e ou balanceamento de carga e contingência. O município não pode dispor apenas de link sem a implementação de sistemas de backup e redundância, o qual eventualmente pode sofrer indisponibilidade.

1.1.3. Justifica-se a contratação dos serviços em regime continuado, tendo em vista serem eles essenciais ao bom e pleno desempenho das atividades meio e fim do Município, atividades como acesso a bancos, cartão SUS, bolsa família, diversos sites e sistemas do governo (estadual e federal) como educacenso e tribunal de contas, e o sistema de gestão para atendimento direto aos cidadãos, entre muitos outros.

1.1.4. Promover a Segurança da Informação no ambiente computacional da Prefeitura Municipal de Patrocínio, seguindo as diretrizes do mercado, que colocam a segurança da informação e a atualização do parque tecnológico como projeto estratégico. O advento de novas ameaças tecnológicas requer a adoção de novas soluções de segurança para garantir a integridade dos dados armazenados dentro da infraestrutura de tecnologia da informação da instituição. Para que a Prefeitura não venha a ser exposta a vulnerabilidades e novas ameaças, se faz necessário adquirir uma solução ligada a segurança dos dados.

1.1.5. As quantidades especificadas têm o objetivo de garantir alta disponibilidade dos serviços de tecnologia da informação da Prefeitura.

1.1.6. O serviço de firewall e de internet tem o propósito de interligar o Setor Administrativo da Prefeitura Municipal, local onde estão concentrados os servidores e demais equipamentos que compõem o seu Data Center com todas suas Secretarias, principalmente de Obras, Saúde, Educação, Desenvolvimento Social, Meio Ambiente e demais pontos externos ao paço municipal, garantindo o tráfego de dados, voz e vídeo, permitindo assim o compartilhamento de acesso à internet, e-mails e softwares de gestão pública e demais sistemas de gestão.

1.2. Dos Dimensionamentos:

O certame foi dimensionado de acordo com a demanda e necessidades dos locais a serem atendimento pelos produtos e serviços solicitados.

1.3. Da Viabilidade técnica:

Conforme pode-se comprovar pela visita técnica, o local e as condições elétricas e ambientais está de acordo com as características necessárias para implantação dos produtos e serviços licitados. Pois no mesmo local já existem outros links e equipamentos semelhantes em uso.

www.patrocinio.mg.gov.br – (34) 3839-1800 – Praça Olímpio Garcia Brandão 1.452, Cidade Jardim CEP 38747-050

1.4. Das Especificações Técnicas Detalhadas do Projeto Firewall:
DOS REQUISITOS TÉCNICOS MÍNIMOS A SEREM ASSEGURADOS PARA A INSTALAÇÃO DE LINK E CONFIGURAÇÃO DA SOLUÇÃO (UTM) DE FIREWALL INTEGRADO AO LINK DE DADOS PRINCIPAL (LOTE1).

A - PROJETO BÁSICO (FIREWALL)

ESPECIFICAÇÕES DETALHADAS DE EQUIPAMENTOS, INSTALAÇÃO, CONFIGURAÇÃO E TREINAMENTOS DA SOLUÇÃO (UTM) FIREWALL NGFW.

A1. Requisitos Gerais do Firewall

1.1. Dispositivo de sistema de segurança de informação perimetral que inclui firewall, administração de largura de banda de serviço de internet (QoS), suporte para conexões VPN IPSec e SSL, proteção contra ameaças de vírus e malware, bem como controle de transmissão de dados e acesso a internet.
1.2. Deve incluir um módulo de proteção contra ameaças de rede, bloqueio de vírus, spyware, controle de transferência de arquivos, controle da navegação de internet e bloqueio de arquivos por tipo.
1.3. Deve incluir licenças para no mínimo 800 (oitocentos) usuários para as funcionalidades de controle de ameaças, controle de vírus, IPS, antiransoware, antiphishing, antispyware, aplication control, filtro de URL (web filter), atualizações automáticas.
1.4. A solução deve ser ofertada em Appliance/hardware especifico para o propósito solicitado, não sendo aceitas soluções baseadas em servidores abertos.
1.5. A solução deve utilizar sistema operacional próprio "hardenizado", não sendo aceitos sistemas operacionais Linux ou baseados em distribuições abertas.
1.6. A plataforma deve ser otimizada para analise de conteúdo de aplicações em camada 7.
1.7. O firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).
1.7.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
1.7.2. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.
1.7.3. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para no mínimo 3 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes.
1.7.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
1.8. Deve suportar redes virtuais, vlans 802.1q;
1.9. Deve suportar tradução de endereços da rede (NAT) por origem e destino, por endereços IP dinâmicos e pool de portas.
1.10. Deve suportar PPPoE, BGP, OSPF e RIP2, DHCP Server e DHCP relay.
1.11. Deve suportar os protocolos de criptografia IKE, 3DES, AES (com chaves de 128, 192 e 256 bits), SHA1 e MD5.
1.12. Deve suportar pelos menos os seguintes protocolos de VOIP: H.323, SIP, SCCP e MGCP.
1.13. Deve suportar Identificação, controle e visibilidade sendo:
1.13.1. Identificação e controle para o uso de aplicações por usuário mediante interação com servidores LDAP, Active Directory ou Radius e endereço IP.
1.13.2. Identificação deve ser de modo independente à porta lógica e/ou aplicações que utilizam as

portas 80 e 443 (Implica a descrição bidirecional de SSL e Identificação de aplicações que encapsuladas em túnel SSL).
1.13.3. Visibilidade de aplicações incluindo peer-to-peer, facebook, twitter e web 2.0.
1.13.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam métodos de ocultamento via comunicações cifradas, tais como Ultrasurf, Skype e ataques mediante a porta 443.
1.14. Em caso de protocolos desconhecidos, poderão designar-se assinaturas próprias.
1.15. Deve suportar descrição e controle de tráfego SSHv2.
1.16. Deve suportar a detecção de aplicações dinâmicas dentro de sessões de proxy HTTP.
1.17. Deve suportar o controle de tráfego IPv4 e IPv6, este último inclui visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPV6 deve ser suportado em interfaces trabalhando em L2 e L3.
1.18. O fornecedor deverá descrever os controles suportados na política de acesso (zonas de segurança, usuários, IP, aplicações, agendamentos, etc).
1.19. Descartadas eventuais especificações que possam estar em desuso pelo mercado, por serem consideradas obsoletas ou substituídas por ferramentas de melhor controle e qualidade, para o mesmo fim.

A2. Controles por Políticas de Firewall
2.1. Deve suportar controles por zona de segurança.
2.2. Deve suportar as seguintes características:
2.2.1. Controle de políticas por porta e protocolo.
2.2.2. Controle de políticas por aplicações e categorias de aplicações.
2.2.3. Controle de políticas por usuários, grupos de usuários, endereços IP, redes e zonas de segurança.
2.2.4. Controle de inspeção e decifra mento do protocolo SSL por política para trafego de entrada (Inbound) e Saída (Ou pound).
2.2.5. Controle de inspeção e deciframento do protocolo SSH por política.
2.3. Deve suportar o bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
2.4. Deve suportar aplicação de QoS baseado em políticas para prioridade, garantia de banda e banda máxima.
2.5. Deve suportar QoS baseado em políticas para marcação de pacotes (diffserv marking).
2.6. Deve suportar objetos e regras IPV6.
2.7. Deve suportar objetos e regras multicast.
2.8. Deve suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

A3. Controle de Aplicações
3.1. Deve contar com ferramentas de visibilidade que permitam administrar o tráfego de aplicações, permitindo a execução de aplicações autorizadas e bloqueio de aplicações não autorizadas.
3.2. O controle de aplicações deve identificá-las independente das portas e protocolos, bem como de técnicas de evasão utilizadas.
3.3. O fornecedor deverá descrever as técnicas utilizadas pela solução para a detecção das aplicações (Assinaturas, Porta/Protocolo, Heurística, etc) e se as mesmas são baseadas em inspeção IPS ou inspeção profunda de pacotes (Deep Packet Inspection);
3.4. Deve suportar múltiplos métodos de identificação e classificação das aplicações.

3.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
3.6. Deve suportar a criação de aplicações customizadas pela interface gráfica do produto.
3.7. Deve incluir a capacidade de atualização para identificar novas aplicações.
3.8. Deve atualizar a base de assinaturas de aplicações automaticamente, durante o período de suporte/garantia contratado
3.9. O fabricante deve permitir a solicitação de inclusão de aplicações na base padrão de assinaturas.
3.10. Deve alertar o usuário quando uma aplicação for bloqueada.
3.11. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.
3.12. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos.
3.13. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, YIM, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos.
3.14. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o chat e bloquear a transferência de arquivos.
3.15. Deve possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos.
3.16. Deve 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, Edirectory e base de dados local.
3.17. Deve incluir a capacidade de criação de políticas baseadas no controle por aplicação, categoria de aplicação, subcategoria, tecnologia e fator de risco.
3.18. Deve incluir a capacidade de criação de políticas baseadas no controle por usuário, grupos de usuários ou endereço IP.
3.19. Deve incluir a capacidade de criação de políticas baseadas em "traffic shaping" por aplicação, usuário, origem, destino, túnel vpnipsec- ssl.
3.20. 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 firewall (Captive Portal).
3.21. Deve suportar autenticação Kerberos.
3.22. Deve possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

A4. Prevenção de ameaças.
4.1. IPS / IDS
4.1.1. Para proteção do ambiente contra ataques, deve ser incluído modulo de IPS e IDS integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.
4.1.2. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
4.1.3. Deve possibilitar a criação de diferentes perfis de IPS a serem aplicados por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
4.1.4. Deve permitir o bloqueio de vulnerabilidades.
4.1.5. Deve permitir o bloqueio de exploits conhecidos.
4.1.6. Deve incluir proteção contra-ataques de negação de serviços.

4.1.7. Deve possuir os seguintes mecanismos de inspeção de IPS:
4.1.7.1. Análise de padrões de estado de conexões
4.1.7.2. Análise de decodificação de protocolo
4.1.7.3. Análise para detecção de anomalias de protocolo
4.1.7.4. Análise heurística
4.1.7.5. IP Defragmentation
4.1.7.6. Remontagem de pacotes de TCP
4.1.7.7. Bloqueio de pacotes malformados
4.1.8. Deve possuir assinaturas para bloqueio de ataques "buffer overflow".
4.1.9. Deve possuir assinaturas para o bloqueio de ataques DoS/DDoS e SandBox.
4.1.10. Deve suportar o reconhecimento de ataques em trafego IPv6.
4.1.11. Deve possuir assinaturas e mecanismos de detecção de anomalias prontas.
4.1.12. Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
4.1.13. Deve ser possível a criação de exceções/exclusões por hosts para determinadas assinaturas.
4.1.14. Deve suportar referência cruzada com CVE (Common Vulnerabilities and Exposures).
4.1.15. Deve possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente.
4.1.16. Deve suportar atualização automática das assinaturas através de conexão segura.
4.1.17. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.
4.1.18. Deve suportar várias técnicas de prevenção, incluindo Drop e TCP-RST (Cliente, Servidor e ambos).
4.1.19. Deve suportar ações por assinaturas.
4.1.20. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.
4.2. Antivírus / Anti-Spyware
4.2.1. Para proteção do ambiente contra malware conhecido, deve ser incluído modulo de antivírus e antispyware de gateway integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.
4.2.2. Deve permitir o bloqueio de malwares e spywares.
4.2.3. Deve ser possível a inspeção de antivírus para no mínimo nos seguintes tipos de tráfegos: HTTP, SMTP, POP3, IMAP e SMB.
4.2.4. Deve incluir proteção contra vírus, spyware e worms em conteúdo HTML e javascript;
4.2.5. Proteção contra downloads involuntários de arquivos executáveis maliciosos usando HTTP.
4.2.6. Rastreamento de vírus em arquivos pdf.
4.2.7. Deve realizar a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
4.2.8. Deve suportar bloqueio de arquivos por tipo (no mínimo 50 tipos).
4.2.9. A atualização de assinaturas deverá ser diária, semanal e de emergência.
4.2.10. Deve suportar atualização automática das assinaturas através de conexão segura, até no mínimo o limite do suporte/garantia contratado.
4.2.11. As atualizações de ameaças, antivírus e antispyware não devem depender de reboot do equipamento para efetivação.
4.2.12. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.
4.2.13. Suportar notificações e alertas via email, SNMP traps e log de pacotes.
4.3. Análise de Malware "In Cloud"
4.3.1. 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

www.patrocinio.mg.gov.br – (34) 3839-1800 – Praça Olímpio Garcia Brandão 1.452, Cidade Jardim CEP 38747-050

ofertada dever possuir funcionalidades para análise de malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.
4.3.2. Para ameaças/malwares não conhecidos, o produto deve ser capaz de enviar o arquivo para analise automática "In Cloud" ou analisá-lo localmente. Onde o arquivo será executado e simulado em ambiente controlado.
4.3.3. Esse sistema automático de analise "In Cloud" deve prover:
4.3.3.1. Informações sobre as ações do malware na máquina infectada.
4.3.3.2. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção.
4.3.3.3. Detectar aplicações não confiáveis utilizadas pelo malware.
4.3.3.4. Gerar assinaturas de antivírus e antispyware automaticamente.
4.3.3.5. Definir URLs não confiáveis utilizadas pelo novo malware.
4.3.3.6. Entre outros provendo uma maior segurança para a rede do cliente.

A5. Filtro de URL
5.1. Para maior controle e visibilidades dos acessos dos usuários do ambiente, deve ser incluído modulo de filtro de URL integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.
5.2. Deve ser possível a criação de políticas por usuário, grupos de usuários, endereços IP, redes e zonas de segurança.
5.3. Deve ser possível definir horários para o funcionamento da política.
5.4. Deve 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, Edirectory e base de dados local.
5.5. Deve incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
5.6. 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 firewall (Captive Portal).
5.7. Deve possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.
5.8. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs.
5.9. Deve possibilitar a criação de categorias de URLs customizadas.
5.10. Deve possibilitar a exclusão de URLs do bloqueio por categoria.
5.11. Deve possibilitar a customização da página de bloqueio.
5.12. Deve possibilitar o bloqueio e continuação, possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site.
5.13. Os logs do produto devem incluir informações das atividades dos usuários.
5.14.A atualização da base de dados deve ser automática com a opção de ser feita manualmente via TFTP.

A6. Filtro de Dados
6.1. Deve ser possível a criação de filtros para arquivos e dados pré-definidos.
6.2. Os arquivos devem ser identificados por extensão e assinaturas.

6.3. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (ex. MS Office, PDF,etc) identificados sobre aplicações (Ex. P2P, IM, SMB,etc).
6.4. Deve ser possível a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
6.5. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de informações sensíveis (Ex. Número de cartão de credito, etc) possibilitando a criação de novos tipos de dados via expressão regular.
6.6. Listar o número de aplicações suportadas para controle de dados.
6.7. Listar o numero de tipos de arquivos suportados para controle de dados.

A7. QoS
7.1. Deve permitir o controle através de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o consumo da largura de banda que cada aplicação ou usuário utiliza.
7.2. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, ustream, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicação, deva ter a capacidade de controlá-las por políticas de consumo máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
7.3. Suportar a criação de políticas de QoS por:
7.3.1. Endereço de origem
7.3.2. Endereço de destino
7.3.3. Por usuário ou grupo do AD.
7.3.4. Por aplicações (como por exemplo: Skype, Bittorrent, YouTube, Azureus)
7.3.5. Por aplicações estaticamente ou grupos dinamicamente (como por exemplo Instant Messaging ou grupo de aplicações P2P) 7.3.6. Por porta
7.4. O QoS deve possibilitar a definição de classes por:
7.4.1. Banda Garantida
7.4.2. Banda Máxima
7.4.3. Fila de Prioridade.
7.5. Suportar priorização em tempo real de
protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
7.6. Suportar marcação de pacotes Diffserv
7.7. Disponibilizar estatísticas em tempo real para as classes de QoS.
7.8. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

A8. Deciframento SSL/SSH
8.1. Deve identificar, decifrar e analisar o trafego SSL em conexões de saída (Outbound)
8.2. Deve identificar, decifrar e analisar o trafego SSL em conexões de entrada (Inbound)
8.3. Deve identificar, decifrar e analisar o trafego SSH em conexões de saída (Outbound)
8.4. Deve identificar, decifrar e analisar o trafego SSH em conexões de entrada (Inbound)
8.5. A inspeção de SSL deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc) e tráfegos não pessoais.
8.6. Deve decifrar o trafego em todos os tipos de implantação suportadas pelo firewall, como:
8.6.1. Tap mode ou Mirror/Monitor mode
8.6.2. Modo Transparente/Bridge
8.6.3. Layer 2

8.6.4. Layer 3

A9. Identificação de Usuários.

9.1. Deve suportar no mínimo os seguintes serviços de autenticação para identificação de usuários:
9.1.1. Active Directory
9.1.2. LDAP
9.1.3. eDirectory
9.1.4. RADIUS
9.1.5. Kerberos
9.1.6. Client Certificate
9.2. Deve suportar a criação de políticas baseado em Grupos e Usuários do Active Directory adicionalmente a IP Origem / Destino.
9.3. Deve possibilitar a identificação de usuários sem a necessidade de instalação de agente individualmente em cada equipamento da rede.
9.4. Deve suportar a identificação de usuários em ambientes Citrix e Terminal Server, assim como a utilização dos mesmos nas políticas de acesso.
9.5. Deve popular todos os logs de trafego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários.
9.6. Os logs de identificação de usuários deverão ser feitos em tempo real.
9.7. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
9.8. Deve possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
9.9. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

A10. Funcionalidades de Rede

10.1. Suportar funcionamento em Tap Mode (Via porta espelhada, Tap ou SPAN port).
10.2. Suportar funcionamento em modo transparente (Bridge ou similar).
10.3. Suportar funcionamento em Layer 2
10.4. Suportar funcionamento em Layer 3
10.5. Suportar a implementação simultânea em todos os modos descritos acima (Tap, Transparente, Layer2 e Layer3) no mesmo equipamento.
10.6. Deve suportar Vlan Tagging (802.1Q) em todos os cenários de implementação acima (Transparente, Layer2 e Layer3) .
10.7. Deve suportar controle de aplicações em IPV6 em todos os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3).
10.8. Suportar sub-interfaces ethernet lógicas.

A11. NAT

11.1. Deve suportar:
11.1.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many).
11.1.2. IP Nat dinâmico (Many-to-Many).
11.1.3. IP Nat estático (1-to-1, Many-to- Many).
11.1.4. Nat estático bidirecional 1-to-1.
11.2. IP Virtual (VIP)

11.3. Tradução de porta (PAT).
11.4. NAT de Origem
11.5. NAT de Destino
11.6. Suportar NAT de origem e NAT de destino simultaneamente.
11.7. Prover capacidade de NAT Traversal, suportando aplicações e serviços VoIP.

A12. VPN
12.1. Suportar VPN Site-to-Site e Cliente-to-Site.
12.2. Suportar IPSec VPN
12.3. Suportar SSL VPN
12.4. Suportar atribuição de endereço IP nos clientes remotos de VPN.
12.5. Suportar atribuição de DNS nos clientes remotos de VPN.
12.6. Deve estar licenciada para clientes de VPN simultâneos.
12.7. IPSec VPN deve suportar:
12.7.1. 3DES, AES (chaves de 128, 192 e 256 bits);
12.7.2. Autenticação MD5 e SHA 1;
12.7.3. Diffie Hellman Group 1 , Group 2 e Group 5;
12.7.4. Algoritimo Internet Key Exchange (IKE)
12.8. Deve possuir interoperabilidade com os seguintes fabricantes:
12.8.1. Cisco
12.8.2. Checkpoint
12.8.3. Juniper
12.8.4. Palo Alto Networks
12.8.5. Fortinet
12.8.6. Sonic Wall
12.9.O módulo de VPN IPSec deve suportar no mínimo 245 túneis e ter performance de no mínimo 148 Mbps de throughput.
12.10. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
12.11. Deve contar com um software cliente de VPN-SSL para os sistemas operacionais Windows XP, Vista (32 e 64 bits) e Windows 7 (32 e 64 bits).
12.12. Deve permitir criar políticas para tráfego VPN-SSL.
12.13. SSL VPN com suporte a proxy arp e uso de interfaces PPPOE.
12.14. Deve suportar usuários simultâneos via SSL VPN.
12.15. Suporte para autenticação de VPNs SSL, LDAP, Secure id e base de dados própria.

A13. Roteamento
13.1. Deve suportar as seguintes funcionalidades de roteamento:
13.1.1. Estático e Dinâmico.
13.1.2. RIP v2
13.1.3. OSPF
13.1.4. BGP v4
13.2. Suporte a roteamento IPv6.
13.3. Suporte a roteadores virtuais (Virtual Routers).
13.4. Suporte a "Policy Based Fowarding" por:
13.4.1. Zona de segurança

13.4.2. Endereço de origem e destino
13.4.3. Porta de origem e destino
13.4.4. Aplicação
13.4.5. Usuários e/ou Grupos da base AD/LDAP
13.4.6. Combinação de todos acima.

A14. Alta Disponibilidade
14.1. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
14.1.1. Em modo Transparente.
14.1.2. Em layer 2
14.1.3. Em layer 3
14.2. O sistema de alta disponibilidade deve sincronizar:
14.2.1. Todas as sessões.
14.2.2. Certificados decifrados
14.2.3. Todas associações de segurança das VPNs
14.2.4. Todas as assinaturas de antivírus, antispyware e aplicações.
14.2.5. Todas as configurações
14.2.6. Tabelas FIB.
14.3. O sistema de alta disponibilidade deve possibilitar o rastreamento (tracking) de IP.
14.4. Monitoração de falha de link.

A15. Suporte à Segurança nos equipamentos host da instituição
15.1. Deve suportar um agente que quando instalado nos equipamentos desktop ou laptop da instituição, transportem as políticas e todas as características de segurança do Firewall a tal equipamento.
15.2. O agente de software a ser instalado nos equipamentos desktop e laptops, deverá ser capaz de ser distribuído de maneira automática via SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no Firewall.
15.3. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário.
15.4. Deve manter uma conexão segura com o portal durante a sessão.
15.5. Determinar o perfil de host com base em: Sistema Operacional e seus níveis de instalação de patches, versão de antimalware no host, versão de firewall no host, criptografia do disco, chaves de registros e processos ativos.
15.6. Deve ser possível a criação de perfis customizados com base em Sistema Operacional e seus níveis de instalação de patches, versão de antimalware no host, versão de firewall no host, criptografia do disco, chaves de registros e processos ativos.
15.7.O portal deverá enviar ao agente a lista de portais trabalhando como gateways ativos, os quais serão administrados centralmente e deverá trabalhar com os certificados de autenticação correspondentes a cad. usuário. O cliente poderá encontrar a melhor rota com base nos gateways disponíveis e a localização do host, determinando a rota com o tempo de resposta mais rápido.
15.8. Em conformidade com o perfil de segurança detectado, se o dispositivo de conexão VPN não for suficientemente seguro, serão determinadas políticas de segurança novas com base no seu perfil. Estas políticas estarão baseadas em: Sistema Operacional e seus níveis de instalação de patches, versão de antimalware no host, versão de firewall no host, criptografia do disco, chaves de registros e processos ativos.

www.patrocinio.mg.gov.br – (34) 3839-1800 – Praça Olímpio Garcia Brandão 1.452, Cidade Jardim CEP 38747-050

15.9. Deve estabelecer um túnel VPN-SSL do cliente ao Gateway, fornecendo uma solução de single sign-on (SSO) aos usuários, integrando-se com as ferramentas de Windows login.
15.10. Deve ter suporte para os sistemas operacionais Windows XP, Vista (32 e 64 bits), Windows 7 (32 e 64 bits), Windows 8 (64 bits) e Windows 10 / 11 (64 bits).

A16. Requerimentos de hardware e desempenho (capacidades e quantidades).
A plataforma de segurança deve possuir as capacidades e as características mínimas abaixo, por equipamento:

1. O equipamento deve possuir interfaces 10/100/1000 Ethernet base-TX.
2. O equipamento deve possuir interface "Out-Of-Band" dedicada para gerenciamento.
3. Suportar no mínimo 1,5 Gbps de throughput para controle de aplicações.
4. Suportar no mínimo 2,6 Gbps de throughput de IPS.
5. Suportar throughput necessário para as funcionalidades de firewall, controle de aplicações, IPS, antivírus e antispyware habilitados simultaneamente.
6. Estar licenciado para, ou suportar sem o uso de licença, no mínimo 300 (trezentos) clientes de VPN SSL simultâneos;
7. Atender a demanda de no mínimo 600 (seiscentos) usuários de Internet.
8. IPS: 2.6 Gbps, NGFW: 1.6 Gbps, Threat Protection: 1 Gbps
9. Interfaces: Multiple GE RJ45, GE SFP and 10 GE SFP+ slots
10. Portas GE RJ45 aceleradas por hardware: 12
11. GE RJ45 acelerado por hardware: 1 / 2 / 1
12. Gerenciamento/ HA/ Portas DMZ: 4
13. Slots GE SFP acelerados por hardware: 2
14. Hardware acelerado 10 GE SFP+: 2, Portas WAN GE RJ45: 2
15. Portas compartilhadas GE RJ45 ou SFP *: 4, Porta USB: 1, Porta do console: 1
16. Taxa de transferência do firewall (pacotes UDP de 1518/512/64 bytes): 20 / 18 / 10 Gbps
17. Latência do firewall (pacotes UDP de 64 bytes): 4,97 µs
18. Taxa de transferência do firewall (pacote por segundo): 15 Mpps
19. Sessões simultâneas (TCP): 1,5 milhões
20. Novas Sessões/Segunda (TCP): 56.000
21. Políticas de Firewall: 10.000
22. Taxa de transferência de VPN IPsec (512 bytes): 11,5 Gbps
23. Túneis VPN IPsec de gateway para gateway: 2.000
24. Túneis VPN IPsec cliente-para-gateway: 16.000
25. Taxa de transferência SSL-VPN: 1 Gbps
26. Usuários simultâneos de SSL-VPN (máximo recomendado, modo túnel): 500
27. Taxa de transferência de inspeção SSL (IPS, HTTPS médio): 1 Gbps
28. Inspeção SSL CPS (IPS, HTTPS médio): 1.800
29. Sessão simultânea de inspeção SSL (IPS, HTTPS médio): 135.000
30. Taxa de transferência de controle de aplicativo (HTTP 64K): 2,2 Gbps
31. Taxa de transferência CAPWAP (HTTP 64K): 15 Gbps
32. Domínios virtuais (padrão/máximo): 10 / 10
33. Número máximo de APs (Total / Túnel): 128 / 64
34. Número máximo de Tokens: 5.000
35. Número máximo de Clients vpn registrados: 600

36. Configurações de alta disponibilidade: Ativo / Ativo, Ativo / Passivo, Clustering

37. Tecnologias "Core Features" possíveis de serem utilizadas: Advanced Routing, IPv6, Switch Controller, VPN, WiFi Controller.

38. Tecnologias "Security Features" possíveis de serem utilizadas: *AntiVirus, *Application Control, Data Leak Prevention, *DNS Filter, *Email Filter, Explicit Proxy, File Filter, *Intrusion Prevention, *Video Filter, Web Application Firewall, *Web Filter, Zero Trust Network Access.

39. Tecnologias adicionais possíveis de serem utilizadas: Advanced Wireless Features, Allow Unnamed Policies, Application Detection-Based SD-WAN, Certificates, DNS Database, DoS Policy, Email Collection, Cloud Sandbox, ICAP, Implicit, Firewall Policies, Load Balance, Local In Policy, Local Out Routing, Multicast Policy, Multiple Interface Policies, Operational Technology (OT), Policy Advanced Options, Policy Disclaimer, Policy-based IPsec VPN, Replacement Message Groups, SD-WAN Interface, SSL-VPN Personal Bookmark, SSL-VPN Realms, Threat Weight Tracking, Traffic Shaping, VoIP, Wireless Open Security, Workflow Management.

40. As licenças dos serviços necessários, a serem fornecidos juntamente com o firewall serão relacionados no item A21;

A17. Gerenciamento

17.1. Deve ser suportado o gerenciamento por:

17.1.1. CLI via SSH

17.1.2. WebUI via HTTPS

17.1.3. Console

17.1.4. API Aberta

17.2. O gerenciamento local do equipamento deve permitir/Possuir:

17.2.1. Criação e administração de políticas

17.2.2. Administração de políticas de IPS, antivírus e antispyware

17.2.3. Política de filtro de dados e filtro de URLs.

17.2.4. Monitoração de logs.

17.2.5. Ferramentas de investigação de logs

17.2.6. Debugging

17.2.7. Captura de pacotes.

17.3.A solução ofertada deverá suportar gerenciamento centralizado através de solução do mesmo fabricante, possibilitando o gerenciamento de diversos equipamentos.

17.4. Deve possuir relatórios de utilização dos recursos por aplicações, URL e ameaças.

17.5. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução.

17.6. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em tempo real.

17.7. Deve ser possível identificar o usuário que fez determinado acesso nas opções de "DrillPODER Down".

17.8. Deve ser possível exportar os logs para formato CSV.

17.9. Deve ser possível acessar o equipamento e aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem totalmente utilizadas.

17.10. Deve ser possível capturar as URLs acessadas para todas as sessões HTTP.

17.11. Deve possibilitar a criação de diferentes perfis de administração separando no mínimo: leitura, alterações, relatórios e monitoração.

17.12. Deve ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações.

17.13. Deve ser possível administrar o firewall localmente ou remotamente sem causar problemas de

sincronismo de configurações. Disponibilizar usuário com permissões administrativas e completas ao firewall para o Administrador local da Contratante;
17.14. Deve possuir interface ethernet "Outof-Band" para gerenciamento via SSH e HTTPS
17.15. Deve gerar alertas automáticos via email, SNMP e Syslog
17.16. Deve suportar o upgrade de software via SCP, TFTP e Web-UI.
17.17. Devera suportar "rollback" de configuração para a ultima configuração salva.
17.18. Deve suportar "rollback" de Sistema Operacional para a ultima versão local.
17.19. Deve suportar a validação de regras antes da aplicação.
17.20. Deve possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando houver mais de um administrador executando alterações simultaneamente.
17.21. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.
17.22. Deve possibilitar a integração com outras soluções de SIEM (Security Information and Event Management) de mercado.
17.23. Deve suportar autenticação de administradores usando base de dados local e RADIUS.
17.24. Deve suportar a geração de relatórios de atividades do usuário.
17.25. Deve suportar objetos e políticas compartilhadas.
17.26. Deve suportar relatórios predefinidos e relatórios projetados pelo usuário (custom), sendo que todos os relatórios deverão poder ser exportados em formatos CSV e PDF.

A18. Autenticação
18.1. Para autenticação dos administradores da solução deve ser suportado:
18.1.1. LDAP
18.1.2. RADIUS
18.1.3. Soluções Baseadas em Token (i.e. Secure-ID)
18.1.4. Kerberos
18.2. Para autenticação de VPN SSL deve ser suportado:
18.2.1. LDAP
18.2.2. RADIUS
18.2.3. Soluções Baseadas em Token (i.e. Secure-ID)
18.2.4. Kerberos

A19. Captura de pacotes.
19.1. Deve ser possível a captura de pacotes por:
19.1.1. Endereço de Origem
19.1.2. Endereço de destino
19.1.3. Aplicações
19.1.4. Aplicações desconhecidas
19.1.5. Portas
19.1.6. IPS
19.1.7. Antivírus
19.1.8. Antispyware
19.1.9. Filtro de dados
19.1.10. Usuário
19.1.11. Qualquer combinação acima

A20. Relatórios

20.1. Deve incluir a capacidade de proporcionar um resumo gráfico de aplicações utilizadas e ameaças encontradas diariamente.

20.2. Deve permitir o controle de transferência de dados não autorizados com ferramenta para realizar padrões definidos por usuário.

20.3. Deve contar com a funcionalidade para exportação de logs, captura de tráfego URL e ameaças.

20.4. Deve permitir a criação de relatórios personalizáveis.

20.5. Deve contar com ferramenta para criar filtros de monitoramento das sessões históricas no firewall seja por aplicação, endereço IP de origem e de destino.

20.6. Deve 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 de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.

20.7. O equipamento deverá proporcionar os seguintes conjuntos de relatórios:

20.7.1. Utilização de largura de banda de entrada e saída por aplicação (TOP 10)

20.7.2. Número de sessões por aplicação (TOP 10)

20.7.3. Comparativo semanal de aplicações utilizadas na rede que possam induzir latência. (TOP 10)

20.7.4. Taxa de transferência (em bytes) por aplicação (TOP 10).

20.7.5. Origem e destino do tráfego por aplicação – Usuário (TOP 10)

20.7.6. Sessões e E-mail público

20.7.7. Utilização de navegação

20.7.8. Eventos / Ataques por: origem, categoria, ameaça, protocolo. (TOP 10)

20.7.9. Nível de risco da rede

20.7.10. Principais protocolos e aplicações que circulam pelo firewall (TOP 25).

20.7.11. Principais endereços de IP destino por protocolo (TOP 25).

20.7.12. Os principais endereços IP para cada um dos protocolos e aplicações principais (TOP 50)

A21. Licenciamento (licenças a serem fornecidas):

21.1. Application Detection

21.2. IPS

21.3. Antivírus

21.4. Antispyware

21.5. Botnet detection

21.6. URL-Filtering Web Filtering

21.7. Data Content Filtering

21.8. IPSec VPN – SSL VPN

21.9. Care Support (NOC / SOC)

21.10. Clientes de VPN

21.11. High Availability

21.12. QoS (marking and/or traffic shaping)

21.13. SSL / SSH Decryption

21.14. Firewall Policy

21.15. Cloud Manager Analyzer

A22 - Serviço de instalação do Firewall

www.patrocinio.mg.gov.br - (34) 3839-1800 – Praça Olímpio Garcia Brandão 1.452, Cidade Jardim CEP 38747-050

22.1. A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante / licitante, com acompanhamento e apresentação ao gestor local, contemplando os itens a seguir:
22.1.1. Análise da topologia e arquitetura da rede da contratante, considerando os roteadores e switches de backbone instalados, acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários da contratante, serviços externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema relevante na segurança do perímetro, sendo então feitas as configurações gerais do sistema de firewall de acordo com a configuração atual.
22.1.2. Para as regras específicas de usuários e aplicações deverá ser repassado o modo de criação do modelo destas regras, ficando a cargo deste órgão o desenvolvimento conforme suas políticas.
22.1.3. Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar o firewall (instalação assistida). Esta demonstração deverá ser no formato treinamento hands-on com no mínimo 08(oito) horas de duração, contemplando os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.
22.1.4. Todo o processo de instalação e configuração do sistema deverá ser documentado pela contratada sob a forma de relatório ou roteiro, de forma que os técnicos da contratante possam reproduzir a instalação do firewall quando necessário consultando a documentação.

2. DA DEFINIÇÃO DOS MÉTODOS E ESTRATÉGIAS DE EXECUÇÃO

2.1. Condições de Execução e Métodos:
2.1.1 - Da instalação física
2.1.1 – A instalação deverá ser realizada por profissional da Contratada que detenha todas as condições técnicas (teóricas e práticas) necessárias.
2.1.2 – A instalação deverá ser precedida da elaboração de projeto de instalação e configuração dos componentes fornecidos, com avaliação e aprovação do gestor do contrato.
2.1.3 – A instalação deverá contemplar a verificação da infraestrutura elétrica e lógica existentes no local de instalação, sendo necessário o registro de toda alteração realizada no ambiente.
2.1.4 – A instalação dos equipamentos e componentes da solução deverá levar em consideração o ambiente e instalações existentes (espaço físico, sistema de refrigeração e de fornecimento de energia elétrica, dutos, eletrocalhas, entre outros elementos). Os componentes fornecidos em comodato (equipamentos e acessórios) deverão proporcionar condições ideais de funcionamento no que diz respeito à disposição física, evitando problemas de refrigeração, falta de energia (nobreak) e também de acesso físico aos equipamentos.
2.1.5 – As instalações de cabeamento de dados deverão atender às normas TIA/EIA 568 e 569 aplicáveis.
2.1.6 – As instalações elétricas deverão atender às normas NBR aplicáveis.
2.1.7 – Todas as partes metálicas deverão ser corretamente aterradas.
2.1.8 – Após a instalação dos equipamentos, alimentação elétrica e conexões com a rede de dados, não poderá haver cabos sem proteção mecânica, soltos, por cima do piso elevado ou que obstruam a frente ou visibilidade dos equipamentos instalados.
2.1.9 – Cabos de dados e de energia não poderão passar juntos, devendo existir uma distância ou separação física entre eles, conforme boas práticas de instalação.

2.2. Dos testes

2.2.1. Os testes deverão ser acompanhados por profissionais da Contratante de forma a certificar a correta instalação da solução.

2.2.2. Após a realização de todos os testes, deverá ser apresentado um relatório com o detalhamento de todos os testes realizados, bem como os resultados obtidos.

2.2.3. Para efeito de contrato, os circuitos SOMENTE serão considerados ACEITOS (implantados e ativados), quando os testes de conectividade entre os equipamentos de cada localidade ocorrerem dentro dos parâmetros de desempenho aceitáveis pela CONTRATANTE.

2.3. Local e horário da prestação do serviço:

Local de Instalação física: Prefeitura Municipal de Patrocínio

Horário: como agendamento com o Departamento de TI.

A prestação de serviços será composta pela instalação dos equipamentos necessários e o fornecimento dos serviços solicitados (LINKS e FIREWALL);

2.4. Rotinas a serem cumpridas:

2.4.1. Autorização de Fornecimento pela CONTRATANTE;

2.4.2. Agendamento do dia e horário pela CONTRATADA junto a CONTRATANTE;

2.4.3. Instalação física dos equipamentos no local especificado conforme agendamento;

2.4.4. Testes de conformidade e aprovação junto ao fornecedor;

2.4.5. Aprovação e início da prestação de serviços de link e firewall;

2.4.6. Prestação dos serviços conforme descritivos deste termo.

2.5. Condições de aceite:

2.5.1 – Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturas ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas. Este órgão poderá efetuar consulta do número de série do equipamento, junto ao fabricante, informando data de compra e empresa adquirente, confirmando a procedência legal dos equipamentos.

2.5.2 – Este órgão também poderá efetuar consulta junto aos órgãos competentes para certificar a legalidade do processo de importação.

2.5.3 – O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica.

2.5.4 – Para comprovação de pleno atendimento aos requisitos deste edital, serão consultados folhetos, prospectos, manuais e toda documentação pública disponível diretamente do site do fabricante do equipamento. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 3 (três) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão.

2.5.5 – No valor proposto deverão estar inclusos todos os custos envolvidos para a perfeita execução dos serviços, tais como: fornecimento do produto, quando o caso, impostos, tarifas, taxas, salários, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe etc.;

2.5.6 – Será considerada vencedora, a empresa que ofertar o menor valor em cada lote, sendo que

cada lote deverá ser adjudicado e homologado a empresas diferentes, ou seja, cada lote deverá conter um fornecedor diferente, conforme justificado, visando a contratação do link de contingência / backup.

2.6. Dos prazos e duração do contrato

2.6.1 – O prazo máximo de entrega e instalação do objeto licitado é de, no máximo, 15 (quinze) dias corridos para o link, contados a partir da data da assinatura do contrato.

2.6.2 – O prazo de configuração e testes será de até 3 (três) dias corridos após instalação.

2.6.3 – O prazo de duração do contrato será de **12 (doze) meses** podendo ser prorrogado de acordo com a legislação em vigor.

2.7. Do acordo de nível de serviço (SLA)

2.7.1 – A Contratada deverá garantir o tempo de indisponibilidade mensal máximo de até 4 (quatro) horas, sendo contados todos os momentos de indisponibilidade, sejam parciais ou totais, incluindo, quando for o caso, indisponibilidade do equipamento fornecido.

2.7.2 - Qualquer interrupção dos serviços de link deverá ser restabelecida em no máximo 30 (trinta) minutos, salvo situações em que houver necessidade de troca de equipamentos devidamente comunicadas ao gestor.

2.7.3 – Considera-se o serviço indisponível quando o mesmo estiver inoperante ou quando for constatada taxa de erros de bits (BER) no circuito igual ou superior a 10^{-8} (dez elevado à potência de menos oito) erros, em um período contínuo mínimo de 30 (trinta) minutos.

2.7.4 – O momento inicial de indisponibilidade do serviço não estará vinculado apenas à abertura de um chamado técnico pela Contratada ou pela Contratante, pois este poderá estar sendo registrado pelos sistemas de monitoramento da Contratada bem como pelos sistemas da Contratante.

2.7.5 – Será computado como indisponibilidade todo o tempo decorrido entre o início da interrupção do serviço e sua total recuperação.

2.7.6 – No caso de indisponibilidade reincidente num período de 3 (três) horas, contado a partir do restabelecimento do serviço, considerar-se-á como tempo de indisponibilidade o início da primeira indisponibilidade até o final da última indisponibilidade, quando o serviço estiver totalmente operacional.

2.7.7 – Mensalmente, a Contratada apurará os tempos de indisponibilidade do serviço, considerando as ocorrências desde a zero hora do primeiro dia até as 24h (vinte e quatro horas) do último dia do mês anterior ao da apuração e calculará o total do desconto a ser concedido. O valor do desconto será calculado pela fórmula a seguir e ressarcido à Contratante na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração. Sob o acompanhamento do gestor do contrato.

2.7.8 – Fórmula de cálculo dos descontos: total de horas de indisponibilidade multiplicado pelo valor mensal do contrato e dividido por 720, que representa a quantidade de horas do mês (30 x 24). Eventual fração de hora resultante do somatório de tempos de indisponibilidade deverá ser convertida em hora.

2.7.9 – Relatório com as informações apuradas deverá ser enviado, por correio postal, eletrônico ou disponibilizado na internet, informando, inclusive, a identificação do circuito e do chamado, data e hora da ocorrência, data e hora de restabelecimento do serviço, causas da indisponibilidade e solução adotada para sua total recuperação.

2.7.10 – A CONTRATANTE manterá registro das ocorrências para fins de apuração paralela dos tempos de indisponibilidade.

2.7.11 – A Contratada deverá manter monitoramento do serviço 24 (vinte e quatro) horas por dia, 7

(sete) dias por semana, todos os dias do ano, devendo agir pró-ativamente em caso de falhas ou degradação de performance e comunicar, de imediato, a Contratante os problemas detectados.
2.7.12 – Qualquer evento que cause degradação ou indisponibilidade dos serviços, seja parcial ou total, deve ser informado a Contratante, por telefone ou e-mail, no máximo em 20 (vinte) minutos após sua ocorrência.
2.7.13 – Ao final do mês será computado o tempo total de indisponibilidade do serviço, sendo cobrada uma multa de 3% (três por cento) do valor mensal dos serviços por hora ou fração que exceder a 4 (quatro) horas mensais. Caso o tempo total computado seja superior a 24 (vinte e quatro) horas, será aplicada, adicionalmente, multa de 10% (dez por cento) do valor mensal dos serviços.
2.7.14 – Não serão consideradas como indisponibilidade de serviço as interrupções programadas para manutenções preventivas, desde que efetuadas no período compreendido entre 00h00min (zero hora) e 06h00min (seis) horas de sábado, horário de Brasília, e comunicadas a Contratante com antecedência mínima de 03 (três) dias.

2.8. Do suporte técnico
2.8.1 – A Central de Assistência Técnica da Contratada deverá estar à disposição para interação com a Contratante durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, todos os dias do ano com profissionais dedicados para este propósito.
2.8.2 - A Contratada deverá fornecer e manter contato específico, como consultor de relacionamento e ou manutenção, para suporte técnico específico em problemas ou configurações necessárias ao bom funcionamento dos serviços licitados.

2.9 - Da fiscalização
2.9.1 – O acompanhamento e a fiscalização do objeto desta Licitação serão exercidos por meio de um representante (denominado Gestor) e um substituto, designados pela CONTRATANTE, aos quais compete acompanhar, fiscalizar, conferir e avaliar a execução do objeto, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, e os quais de tudo darão ciência à CONTRATADA, conforme determina artigos da Lei nº 14.133/2021, e suas alterações.
2.9.2 – Não obstante ser a CONTRATADA a única e exclusiva responsável pela execução do objeto, a CONTRATANTE reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização.
2.9.3 – Cabe à CONTRATADA atender prontamente e dentro do prazo estipulado quaisquer exigências do Fiscal ou do substituto inerentes ao objeto desta licitação, sem que disso decorra qualquer ônus extra para a CONTRATANTE, não implicando essa atividade de acompanhamento e fiscalização qualquer exclusão ou redução da responsabilidade da CONTRATADA, que é total e irrestrita em relação ao objeto executado, inclusive perante terceiros, respondendo a mesma por qualquer falta, falha, problema, irregularidade ou desconformidade observada na execução do ajuste.
2.9.4 – A atividade de fiscalização não resultará, tampouco, e em nenhuma hipótese, em co-responsabilidade da CONTRATANTE ou de seus agentes, prepostos e/ou assistentes.
2.9.5 – O objeto do presente Edital deverá estar rigorosamente dentro das normas vigentes e das especificações estabelecidas pelos órgãos competentes e pela CONTRATANTE, sendo que a inobservância desta condição implicará a recusa do mesmo, bem como o seu devido refazimento e/ou substituição, sem que caiba à CONTRATADA qualquer tipo de reclamação ou indenização.
2.9.6 – As decisões e providências que ultrapassem a competência do Gestor do Contrato serão encaminhadas à autoridade competente da CONTRATANTE para adoção das medidas convenientes,

consoante aos artigos da Lei nº 14.133/2021, e suas alterações.

2.10. Das sanções administrativas

2.10.1 – Em virtude da inexecução parcial ou total das condições pactuadas, erro ou mora na execução, à contratada poderão ser aplicadas as seguintes sanções, sem prejuízo de outras previstas na legislação vigente e neste edital, garantida a prévia defesa:

(a) Advertência formal; (b) Multa de até 2% (dois por cento), calculada sobre o valor total do contrato; (c) Suspensão temporária, pelo período de até 02 (dois) anos, de participação em licitação e contratação com a contratante; (d) Suspensão temporária do direito de participar de licitação e contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos, nos termos do art. 7º, caput, da Lei nº 10.520/2002 e suas alterações.

2.10.2 – Na ocorrência de falhas ou irregularidades, a contratante poderá aplicar à contratada sanções listadas neste Projeto Básico/Termo de Referência, consideradas a natureza e a gravidade da infração cometida, sem prejuízo da responsabilidade civil e criminal que seus atos ensejarem;

2.10.3 – Em caso de rescisão contratual, a critério da Administração, e considerando a gravidade da conduta do contratado, poderão ser aplicadas alternativamente as sanções previstas legalmente;

2.10.4 – As multas previstas, caso sejam aplicadas, serão descontadas por ocasião de pagamentos futuros ou serão pagas por meio de Guia de Recolhimento, no prazo fixado, ou serão descontadas da garantia contratual;

2.10.5 – As sanções fixadas nesta cláusula serão aplicadas nos autos do processo, no qual será assegurado à contratada o contraditório e a ampla defesa.

2.11. Das Garantias:

2.11.1 – Garantia para equipamentos de no mínimo 36 (trinta e seis) meses com atendimento "on site" em até 2 horas a partir da abertura do chamado, podendo o atendimento ser feito remotamente, quando possível e reposição de peças e equipamento em até 24 (vinte quatro) horas. Durante este período, deve ser garantida a atualização de firmware e contato de suporte com telefone com o próprio fabricante/fornecedor do equipamento, em português, durante todo o período de garantia, durante o horário comercial.

2.11.2 – Os produtos fornecidos e em comodato, deverão estar cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento, pelo período mínimo especificado, a contar da data do recebimento definitivo dos produtos.

2.11.3 – Os serviços de garantia aos produtos, ou troca imediata, deverão ser prestados por empresa credenciada pelo fabricante ou pelo próprio licitante ou fabricante dos produtos fornecidos.

2.11.2 – O fabricante/fornecedor deve possuir estrutura de suporte com atendimento em português do Brasil via chamada telefônica, a cobrar ou 0800;

2.11.3 – A solução ofertada deverá ser constituída dos equipamentos e serviços relacionados nos itens e necessários a prestação dos serviços.

2.11.4 – A empresa deve indicar, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos equipamentos ou diretamente com o fabricante dos equipamentos.

2.11.5 – A empresa deve possuir, no fornecimento e prestação de serviço, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade.

2.11.6 – A empresa contratada deverá disponibilizar um portal web 24x7 com sistema de help-desk

para abertura de chamados de suporte técnico. Mediante login e senha de acesso ao sistema, os membros da equipe técnica da contratante poderão abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico.
2.11.7 – Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk.
2.11.8 – A contratante poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware.

2.12. Das Condições de Entrega dos equipamentos e serviços
2.12.1 – Prazo de entrega: no máximo 20 (vinte) dias corridos para o firewall, a partir da data de assinatura do contrato, pelo contratado.
2.12.2 – A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.
2.12.3 – Para itens de software, estes devem ser fornecidos com ou sem mídia de instalação. No caso de não fornecimento de mídia, deve ser indicado local para download da instalação.
2.12.4 – Para itens de software, deve ser apresentada chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que se trata de uma ferramenta devidamente licenciada.

2.13. Dos produtos ofertados e da proposta
2.13.1 – A proposta comercial deverá ser apresentada em formulário oficial da licitante, em uma via, redigida em português, sem emendas, rasuras, ressalvas ou entrelinhas, assinada e carimbada na última folha e rubricada nas demais pelo seu representante legal. Deve conter: I) Todas as comprovações, declarações e especificações técnicas solicitadas no presente documento; II) Preço unitário e total de todos os componentes, expressos em algarismos e o total também por extenso, em moeda nacional, a ser cobrado pelo objeto da presente licitação;
2.13.2 – O licitante deverá fornecer em sua proposta todos os produtos ou serviços referidos no item a que está concorrendo, neste termo, sob pena de desclassificação;
2.13.3 – A proposta de cada licitante deve conter tabela comprobatória das características solicitadas, independente da sua descrição, através de documentos cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator), ou por meio de declarações do fabricante. As comprovações devem ser claras, com indicação de página na proposta. Serão aceitos documentos em português ou inglês para comprovações técnicas. A não comprovação de alguma característica exigida, quando solicitada pela Prefeitura Municipal, levará à desclassificação da proposta;
2.13.4 – Deverão ser listados todos os componentes da solução proposta com seus respectivos part numbers, além de descrição e quantidades;
2.13.5 – O prazo de validade da proposta, deverá constar nela e deverá ser, de no mínimo, 90 (noventa) dias consecutivos da data da sessão de abertura desta licitação;

3. DA EXIGÊNCIA DE LAUDOS E/OU CERTIFICAÇÕES COMO REQUISITO TÉCNICO

3.1. Comprovação de aptidão para prestação de serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado.
3.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as características mínimas de capacidade técnica conforme objeto e especificações do termo de referência e deste projeto básico.
3.3. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados.
3.4. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

4. DAS OBRIGAÇÕES ESPECÍFICAS DAS PARTES NO PROJETO

4.1. Das obrigações e responsabilidades da CONTRATADA
4.1.1. Cumprir todas as obrigações constantes deste instrumento e seus anexos, nas quantidades, prazos e condições pactuadas. Cumprir todas as obrigações de manutenção específicas de cada fabricante para a marca e modelo do equipamento objeto de manutenção;
4.1.2. Efetuar a prestação do serviço conforme fixado em todos os itens do contrato, do edital e de todos os termos que o compõem;
4.1.3. Providenciar a imediata correção das irregularidades apontadas pelo Contratante, quanto à prestação do serviço;
4.1.4. Garantir a boa qualidade do serviço prestado;
4.1.5. Executar todas as intervenções nos equipamentos de acordo com as especificações obrigatórias e necessárias apontadas pelo fabricante dos equipamentos;
4.1.6. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para a habilitação na licitação em cumprimento ao disposto no Inciso XVI do artigo 92 da Lei nº 14.133, de 2021.
4.1.7. Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que vier causar ao Contratante ou a terceiros, por sua culpa ou dolo, na pessoa de preposto ou terceiros a seu serviço, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Contratante.
4.1.8. Responsabilizar-se pelos salários, encargos sociais, previdenciários, securitários, taxas, impostos e quaisquer outros que incidam ou venham a incidir sobre seu pessoal necessário à execução deste contrato.
4.1.9. Apresentar sempre que solicitado pelo Contratante, comprovação de cumprimento das obrigações tributárias e sociais, legalmente exigíveis.
4.1.10. Submeter-se às normas e determinações do Contratante no que se referem à execução deste contrato:
4.1.10.1 – Executar os serviços a que se propõe o objeto desse Termo de Referência com qualidade, eficiência e celeridade.
4.1.10.2 – Fornecer equipamentos essenciais ao funcionamento do objeto deste Termo de Referência instalados e configurados.
4.1.10.3 – O circuito deverá ser fornecido por meio de fibra ótica fim a fim, não será aceito enlace de rádio ou outras tecnologias em qualquer pedaço da rede.

4.1.10.4 – Disponibilizar profissionais devidamente capacitados para realização dos serviços.
4.1.10.5 – É vedada à empresa a ser contratada, a transferência dos serviços a serem executados, no todo ou em parte, sem a prévia anuência da CONTRATANTE.
4.1.10.6 – Prestar todos os esclarecimentos que forem solicitados pela CONTRATANTE
4.1.10.7 – Disponibilizar contatos e telefones para abertura de chamados 24 horas x 7 dias por semana.
4.1.10.8 – Assumir a responsabilidade por todos os encargos e obrigações sociais previstos na legislação trabalhista em vigor, bem como a responsabilidade por todas as providencias e obrigações estabelecidas na legislação especifica de acidentes de trabalho quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços aqui discriminados ou em conexão com eles, ainda que ocorridos nas dependências da CONTRATANTE.
4.1.10.9 – Responder por quaisquer danos pessoais ou materiais, ocasionados por seus empregados, ao patrimônio da Contratante ou de terceiros, originados direta ou indiretamente da execução dos serviços, inclusive, por culpa ou dolo não servindo como excludente ou redutor dessa responsabilidade o fato de haver acompanhamento e fiscalização por parte da CONTRATANTE.
4.1.10.10 – Manter a situação de regularidade relativa aos seguintes documentos: "Certidão Negativa de Débitos (INSS/CND)", "Certidão de Regularidade do FGTS (CEF/CRF)", "Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União (SRF/PFN)" e "Certidão Negativa de Débitos Trabalhistas (CNDT).
4.1.10.11 – Guardar, garantir e responsabilizar-se pelo sigilo de seus funcionários sobre a estrutura de rede e de qualquer dado a que tenha acesso em virtude da instalação ou configuração dos equipamentos.
4.1.10.12 – Assegurar todos os princípios da segurança da informação, conforme normativas LGPD, relativo à solução, levada em consideração a informação de necessidade de sigilo dos dados que trafegarão pelas redes integrantes da solução de conexão.
4.1.10.13 – Apresentar, ao Fiscal do Contrato, por ocasião do início da execução dos serviços, documento que comprove que a licitante é autorizada pela ANATEL (Agência Nacional de Telecomunicações) para prestar os serviços compatíveis com o objeto deste termo de referência.
4.1.10.14 – Submeter à CONTRATANTE a relação de empregados credenciados a prestar os serviços, devendo promover, de imediato, a substituição daqueles que não forem aceitos pela CONTRATANTE;
4.1.10.15 – Deve apresentar, quando da celebração do contrato e da execução de serviço, indicação do(s) profissional(ais) habilitados juntamente com seus comprovantes de certificação, expedidos pelo fabricante ou por instituição acreditada/referendada pelo mesmo, e com prazo de validade não vencido, bem como fornecer aos técnicos a identificação pertinente, bem como todas as ferramentas, materiais e produtos necessários à execução dos serviços;
4.1.10.16 – Não serão admitidas pela administração a cobrança de juros, multa ou qualquer outra denominação similar a título de encargo, ressalvando as atualizações financeiras por atraso de pagamento, expressamente previstas no edital, no contrato e/ou nesse Termo de Referência;
4.1.10.17 – As notas fiscais devem conter a discriminação detalhada dos PRODUTOS ENTREGUES ou dos serviços executados;
4.1.10.18 – Responsabilizar-se por todas as despesas diretas ou indiretas, vinculadas ao contrato, tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no desempenho dos serviços objeto do contrato, ficando a CONTRATANTE isenta de qualquer vínculo empregatício com os mesmos;

4.1.10.19 – Conforme especificações da LGPD, a Contratada deverá garantir o sigilo e a inviolabilidade das informações da contratante, que eventualmente, seus empregados ou prepostos, tenham acesso, durante os procedimentos de instalação e manutenção dos softwares, bem como durante a operação, respondendo pelos danos que eventual vazamento de informação, decorrentes de ação dolosa, negligência, imperícia ou imprudência, venha ocasionar à contratante ou a terceiros;

4.2. Das obrigações e responsabilidades da CONTRATANTE

4.2.1. Acompanhar e fiscalizar toda a execução da prestação do serviço contratado, por meio do fiscal do contrato, conforme especificações contidas no edital;

4.2.2. Fiscalizar a manutenção pelo Contratado, das condições de habilitação exigidas neste Termo de Referência, durante toda a execução do contrato, em cumprimento ao disposto no Inciso XVI do artigo 92 da Lei nº 14.133, de 2021.

4.2.3. Pagar no vencimento a fatura apresentada pelo Contratado correspondente ao serviço prestado;

4.2.4. Notificar o Contratado, por escrito, fixando-lhe prazo para corrigir defeitos ou irregularidades encontradas na execução do serviço;

4.2.5. Todas as demais obrigações apresentadas no Termo de Referência;

4.2.5.1 – Fornecer à empresa a ser contratada bem como aos empregados responsáveis pela execução dos serviços todas as informações e esclarecimentos que forem solicitados relacionados ao objeto deste Termo de Referência.

4.2.5.2 – Efetuar o pagamento de acordo comas condições de preço e prazo estabelecidas entre a contratada e a CONTRATANTE.

4.2.5.3 – Notificar, por escrito, à empresa a ser contratada, toda e qualquer irregularidade constatada na execução dos serviços.

4.2.5.4 – Promover, por meio de servidor a ser designado pela Administração, o acompanhamento e a fiscalização da prestação do serviço.

4.2.5.5 – Não exigir da empresa serviços estranhos às atividades especificadas neste termo de referência.

4.2.5.6 – Observar para que, durante a vigência contratual, sejam mantidas todas as condições de habilitação e qualificação exigidas para contratação, bem como sua compatibilidade com as obrigações assumidas;

4.2.5.7 – Dar providências às recomendações da CONTRATADA, concernentes ao objeto do contrato;

5. DA VIGÊNCIA E ASSINATURA DO CONTRATO

5.1. A vigência contratual será de 12 (doze) meses conforme legislação, podendo ser prorrogado para igual período se comprovadas condições vantajosas para a contratação;

6. DO PAGAMENTO

6.1. O pagamento será efetuado em até 30 (trinta) dias, conforme termo de referência, após todas as aprovações pelos requisitantes dos serviços e pelo fiscal do contrato. Conforme aprovação de todos os serviços fornecidos pela CONTRATADA, de acordo com os requisitos desse Projeto Básico e os outros termos;
6.2. Todos os pagamentos somente serão efetuados após apresentação de documento fiscal contendo a descrição dos serviços e período de atendimento;

7. ENCAMINHAMENTO DO INTEGRANTE REQUISITANTE:

Em conformidade com a legislação que rege o tema, encaminhe-se à autoridade competente para análise de conveniência e oportunidade para a contratação e demais providências cabíveis.

Data: Patrocínio / MG, 19 de março de 2025.

Junior Cesar Ferreira
Departamento de TI

8. IDENTIFICAÇÃO E AUTORIZAÇÃO DO ADMINISTRATIVO:

Por este instrumento declaro ter ciência das competências e certifico que a formalização da demanda acima identificada se faz necessária, pelos motivos expostos no presente documento e que se encaminhe ao setor competente que deverá realizar o prosseguimento da contratação.

Data: Patrocínio / MG, 19 de março de 2025.

Aldo Candido Roriz Júnior
Secretaria Municipal de Administração

www.patrocinio.mg.gov.br – (34) 3839-1800 – Praça Olímpio Garcia Brandão 1.452, Cidade Jardim CEP 38747-050