## Itens da Requisição

| Item | Grupo do Mat. | Material | Quant. Solic. | Unid. de Medida | Situação |
|---|---|---|---|---|---|
| 1 | 52000 | SWITCH | 3.0000 | Unidade | ENC. PARA COMPRA |
| Item Apoiado: Equipamentos para viabilizar fornecimento do serviço de conectividade às empresas associadas ao METRÓPOLE PARQUE | | | | | |
| Especificação Complementar: SWITCH METROETHERNET 24 PORTAS SFP Deve ser compatível com rack de 19” e deve consistir de um único chassi de tamanho máximo de 1 U; Deve ser do fabricante Huawei; Deve acompanhar kit completo de instalação em rack (kits de fixação, cabos, acessórios); Deve ser do fabricante Huawei; Deve possuir fontes de alimentação 110V/220V (AC) redundantes, internas ou externas, com respectivos cabos no padrão brasileiro de 3 pinos. Deve ser possível alimentar o equipamento em sua máxima capacidade somente com uma das fontes; Deve possuir, no mínimo, 20 portas GE SFP e, no mínimo, 4 portas 10GE, e 6 portas 40GE QSFP+ (auto-sensing); Deve ser hot-swappable para inserção e retirada de módulos de interfaces e fontes de alimentação; Deve fornecer informações DDMI ou DOM para os transceivers ópticos; Deve possuir arquitetura non-blocking, wire-speed, para todos os módulos instalados, com tamanho mínimo de MTU de 1500 bytes; A memória interna do equipamento deve suportar, no mínimo, 2 (duas) imagens do sistema operacional simultaneamente, em sua versão mais atualizada; A capacidade de transmissão agregada do backplane deve suportar o tráfego máximo das interfaces instaladas sem perda de desempenho; Mínimo de 4000 VLANs suportadas; Mínimo de 128.000 endereços MAC suportados; Deve suportar jumbo frame (mínimo de 9000 bytes); Deve suportar, no mínimo, 192.000 rotas IPv4 e 80.000 rotas IPv6 em FIB, com encaminhamento por hardware; Roteamento entre VLANs para IPv4 e IPv6, encaminhamento de pacotes IPv4 e IPv6 em hardware; Roteamento estático para IPv4 e IPv6; Deve implementar protocolos de roteamento dinâmico OSPFv2, OSPFv3, IS-IS, BGP4 (MP-BGP) para IPv4 e IPv6; Deve ter suporte a PBR (policy based routing) para IPv4 e IPv6; Suporte a VLAN (802.1Q); Suporte a link aggregation (802.3ad) com, no mínimo, 8 grupos de agregação com LACP; Suporte a QinQ convencional (802.1ad) e QinQ seletivo; Suporte a RSTP (802.1w), MSTP (802.1s) e ERPS ou compatível; Suporte a LDP MPLS-TE; Deve permitir a criação de circuitos virtuais do tipo L2VPN e VPLS e L3VPN; Deve possuir mecanismos de classificação, marcação, priorização de tráfego aplicáveis em interfaces físicas e lógicas, sem impacto no encaminhamento de pacotes; Suporte a diffserv; Deve implementar mecanismos de limitação de tráfego (rate-limit) aplicáveis em interfaces físicas e lógicas, sem impacto no encaminhamento de pacotes; Deve suportar SNMPv2, SNMPv3; Suporte a OAM CFM e EFM; Deve ser possível o espelhamento de portas (port mirroring); Deve suportar a exportação de fluxos através de sFlow; Deve implementar o protocolo LLDP; Deve implementar definição de usuários/grupos com diferentes privilégios locais; Deve possuir suporte a NETCONF; Deve possuir porta para gerenciamento através de terminal RS-232 ou RJ45; Todas as funcionalidades e protocolos acima descritos devem estar contidos no software e hardware oferecido, não sendo necessária a aquisição de licenças ou componentes adicionais, inclusive a licença para ativação das portas 40G; Deve ser fornecida garantia de 3 anos, contados a partir da entrega do equipamento ao cliente, para substituição de componentes e peças (hardware) que apresentem defeito de funcionamento; Durante este mesmo período (3 anos) deve ser fornecida atualização de software para o equipamento bem como suporte e resolução de bugs de software; Deve ser entregue o equipamento com esta especificação ou superior. Modelo de referência: Huawei S5732-H24S6Q; | | | | | |
| 2 | 52000 | INTERFACES ÓPTICA BIDIRECIONAL SFP-10G-BXU1 E BXD1 (PAR) 10KM (MATERIAL NÃO CADASTRADO NO CATÁLOGO) | 4.0000 | Unidade | ENC. PARA COMPRA |
| Item Apoiado: Equipamentos para viabilizar fornecimento do serviço de conectividade às empresas associadas ao METRÓPOLE PARQUE | | | | | |
| Especificação Complementar: INTERFACES ÓPTICA BIDIRECIONAL SFP-10G-BXU1 e BXD1 (PAR) 10KM Deve ser do padrão de aplicação 10GBASE-BX; Possuir taxa de transmissão de 10 Gbit/s; Por trabalham em pares este item contempla duas interfaces , sendo uma BXU1 e a outra BXD1; Para interface BXU1 deve possuir comprimento de onda central em (Rx) de 1330nm e Possuir comprimento de onda central em (Tx) de 1270 nm; Para interface BXD1 deve possuir comprimento de onda central em (Rx) de 1270nm e possuir comprimento de onda central em (Tx) de 1330 nm ; Possuir distância de transmissão de 10km em fibra tipo Monomodo; Deve suportar fator de forma SFP+; Deve suportar conector do tipo LC; Deve suportar tipo de fibra óptica SMF; Deve possuir potência de transmissão óptica máxima Tx de 0dBm; Deve possuir potência de transmissão óptica mínima Tx de -5dBm; Deve possuir uma sensibilidade na recepção Rx de -14dBm; Deve possuir uma potência mínima de overload de 0dBm; Deve suportar a função bidirecional; Deve ser compatível com os equipamentos do fabricante Huawei; Deve ser entregue o equipamento com esta especificação ou superior; Deve possuir garantia de no mínimo 1 ano. | | | | | |
| 3 | 52000 | INTERFACES ÓPTICA BIDIRECIONAL SFP-1G-BXD1 E BXU1 (PAR) 10KM (MATERIAL NÃO CADASTRADO NO CATÁLOGO) | 6.0000 | Unidade | ENC. PARA COMPRA |
| Item Apoiado: Equipamentos para viabilizar fornecimento do serviço de conectividade às empresas associadas ao METRÓPOLE PARQUE | | | | | |
| Especificação Complementar: INTERFACES ÓPTICA BIDIRECIONAL SFP-1G-BXD1 e BXU1 (PAR) 10KM Deve ser do padrão de aplicação 1GBASE-BX; Possuir taxa de transmissão de 1 Gbit/s; ; Por trabalham em pares este item contempla duas interfaces , sendo uma BXU1 e a outra BXD1; Para interface BXD1 deve possuir comprimento de onda central em (Rx) | | | | | |

| Item | Grupo do Mat. | Material | Quant. Solic. | Unid. de Medida | Situação |
|---|---|---|---|---|---|
| de 1310nm e Possuir comprimento de onda central em (Tx) de 1490nm; Para interface BXU1 deve possuir comprimento de onda central em (Rx) de 1490nm e possuir comprimento de onda central em (Tx) de 1310 nm; Possuir distância de transmissão de 10km em fibra tipo Monomodo; Deve suportar fator de forma SFP+; Deve suportar conector do tipo LC; Deve suportar tipo de fibra óptica SMF; Deve possuir potência de transmissão óptica máxima Tx de -3 dBm; Deve possuir potência de transmissão óptica mínima Tx de -9,5dBm; Deve possuir uma sensibilidade na recepção Rx de -22dBm; Deve possuir uma potência mínima de overload de -3dBm; Deve suportar a função bidirecional; Deve ser compatível com os equipamentos do fabricante Huawei; Deve ser entregue o equipamento com esta especificação ou superior; Deve possuir garantia de no mínimo 1 ano. | | | | | |
| 4 | 52000 | TERMINAL DE REDE ÓPTICA (ONT) GPON (MATERIAL NÃO CADASTRADO NO CATÁLOGO) | 10.0000 | Unidade | ENC. PARA COMPRA |
| Item Apoiado: Equipamentos para viabilizar fornecimento do serviço de conectividade às empresas associadas ao METRÓPOLE PARQUE | | | | | |
| Especificação Complementar: TERMINAL DE REDE ÓPTICA (ONT) GPON ONT com 1 interface GPON, 4 interfaces GE/FE e interfaces WLAN (Wi-fi) 2.4GHz e 5GHz; O equipamento deve ser homologado pela Anatel; Operar nos modos Router e Brigde; Suporte aos endereçamentos IPv4 e IPv6; As ONTs ofertadas deverão ser totalmente compatíveis com as OLTs SmartAX MA5608T, e todas as funcionalidades do sistema de gerência, provisionamento e monitoramento iManager U2000; OS DIFERENTES MODELOS DE ONTS OFERTADOS DEVERÃO SUPORTAR OS SEGUINTES PADRÕES INTERNACIONAIS: TU-T G.983.3, ITU-T G.983.3 Amendment 1, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2 Amendment 1 (2.488 Gbit/s downstream 1.244 Gbit/s upstream G-PON), ITU-T G.984.3, ITU-T G.984.4; IEEE 802.1p VLAN prioritization; IEEE 802.1Q VLAN tagging; IEEE 802.1ad VLAN QinQ; IETF RFC 2516: PPPoE; IETF RFC 1334: PPP Authentication Protocols; IETF RFC 2131: DHCP; IETF RFC 2236: Internet Group Management Protocol, Version 2; IETF RFC 4604: IGMPv3; IETF RFC2663: IP NAT Terminology and Considerations; IEEE 802.3u 100 Mbps Fast Ethernet; IEEE 802.3ab 1000BASE-T Gigabit Ethernet; Desejável que a ONT atenda aos requisitos básicos do protocolo IPv6 definidos na RFC6204 "Requisitos Básicos para Roteadores IPv6 de Borda para Clientes" (Basic Requirements for IPv6 Customer Edge Routers); A ONT deve possuir indicação de LED de modo a indicar o estado do equipamento, status da porta PON e das portas de serviço; A ONT deve ter fonte AC (auto range) de 90-240V e frequência de 60HZ; A ONT deverá utilizar NRZ para realizar a codificação e embaralhamento (scrambling) em ambas direções; Conector óptico do tipo SC/APC; Comprimento de ondas de 1310 nm para Upstream e 1490 nm para Downstream; Para o tráfego de upstream e downstream a ONT deverá suportar a Classe B+, de acordo com o padrão ITU-T G.984.2; Sensibilidade do receptor de – 27 dBm; A ONT deverá suportar o envio de frames de acordo com a alocação estática provisionada pela OLT como: A ONT deverá ser capaz de prover as informações para a função do DBA da OLT de modo a otimizar a alocação de banda entre ambas sempre que necessário; A ONT deverá suportar os modos de Non-status Reporting e Status Reporting de acordo com o padrão ITU-T G.984.3; A ONT deverá suportar DBRu modo 0 de acordo com o padrão ITU-T G.984.3; A ONT deverá implementar o princípio de T-CONT (identificado pelo Allocid) como uma unidade de controle básico para o tráfego de upstream de acordo com a especificação ITU-T G. 984.3; A ONT deverá suportar até 8 T-CONT por ONT, e 128 GEM-Ports (port-id); A ONT deverá suportar a ativação via Discovered e Configured SN (Serial Number) de acordo com o padrão ITU-T G. 984.3; Deverá suportar o sistema de criptografia AES-128 e o mecanismo de troca de chaves de acordo com o padrão ITU-T G. 984.3; A ONT deverá implementar o "embedded OAM channel", "PLOAM channel" e "OMCI channel" em conformidade com a norma ITU-T G.984.4; A ONT deve suportar a monitoração do módulo óptico; As ONT deve atender ao padrão IEEE 802.3ab, 1000BASE-T, com conectorização RJ45; A interface Gigabit Ethernet deverá suportar auto negociação da velocidade; Permitir a configuração manual de velocidade em 10,100 ou 1000Mbps; As interfaces Gigabit Ethernet deverão suportar a auto negociação da velocidade; Este modelo de ONT deverá ter 4 (quatro) portas do tipo 1000BASE-T; Conexão wileress 2.4GHz e 5GHz simultâneos; Implementar os padrões IEEE 802.11 b/g/n (2.4GHz); Implementar os padrões IEEE 802.11 a/n/ac (5GHz); Implementar MIMO do tipo 2 x 2 ou superior (2.4GHz e 5GHz); Antenas omnidirecionais, com ganho mínimo de 5 dBi; Possibilitar o provisionamento de multiplos SSIDs; Throughput das interfaces wileress de 300 Mbps para 2.4GHz e 867 mbps para 5GHz; Modos de autenticação WAP, WPA2 e WPA2 Enterprise; Autenticação via Radius; Modos de encriptação AES, TKIP e TKIP&AES; Poderá ser entregue o equipamento com esta especificação ou superior; Deve ser entregue o equipamento com esta especificação ou superior. Modelo de Referência: EG8245W5-6T | | | | | |
| 5 | 52000 | FIREWALL APPLIANCE NGFW (MATERIAL NÃO CADASTRADO NO CATÁLOGO) | 2.0000 | Unidade | ENC. PARA COMPRA |
| Item Apoiado: Equipamentos para viabilizar fornecimento do serviço de conectividade às empresas associadas ao METRÓPOLE PARQUE | | | | | |
| Especificação Complementar: FIREWALL APPLIANCE NGFW O equipamento deve se encaixar no perfil de Next Generation Firewall (NGFW) - Firewall de próxima geração; Taxa de transferência de Firewall (Para qualquer tamanho de pacote UDP): 20Gbps; Taxa de transferência de IPSec VPN (Com pacotes de 512Bytes): 11Gbps Conexões simultâneas (milhões): 1.5; Novas sessões (TCP) por segundo: 56.000; Capacidade de inspeção SSL – HTTPS: 1Gbps; Capacidade para proteção combinada contra ameaças: 1Gbps; Deve estar com as funcionalidades habilitadas simultaneamente e devidamente atuantes: Controle de Aplicação, IDS/IPS e Controle de Malware (Antivírus), medidas com parâmetros de Throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais; Quantidade mínima de interfaces 1Gbps com conectores RJ-45, considerando conexão LAN, WAN, DMZ e Gerência: 22 (vinte e duas); Quantidade mínima de slots SFP+ | | | | | |

| Item | Grupo do Mat. | Material | Quant. Solic. | Unid. de Medida | Situação |
|---|---|---|---|---|---|
| | | para transceptores 10GbE: 02 (Duas); Deve possuir disco rígido interno para gravação de logs, com tamanho mínimo de 400GB (quatrocentos gigabytes). Deve conter duas fontes de alimentação redundantes; Deve ter tecnologia de firewall do tipo stateful; Deve realizar VLANs com tags padrão 802.1q; Deve possuir suporte a agregação de links 802.3ad e LACP; Deve realizar roteamento multicast (PIM-SM e PIM-DM); Deve realizar DHCP relay e DHCP server; Deve possuir suporte a sub-interfaces Ethernet lógicas; Deve suportar NAT64 e NAT46; Deve realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); Deve realizar, para IPv6, roteamento estático e dinâmico (OSPFv3); Deve suportar OSPF graceful restart; Deve suportar modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede; Deve suportar configuração de alta disponibilidade ativo/passivo ou ativo/ativo; Deve implementar no mínimo 05 (cinco) sistemas virtuais; Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente; Deve realizar controles por zona de segurança; Deve realizar controles de políticas por porta e protocolo; Deve realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; Deve realizar controle de políticas por código de país (por exemplo: br, usa, uk, rus); Deve realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (inbound) e saída (outbound); Deve realizar offload de certificado em inspeção de conexões SSL de entrada (inbound); Deve implementar objetos e regras IPv6; Deve implementar objetos e regras multicast; Deve realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente. Requisitos mínimos para solução de filtro de conteúdo; Deve possibilitar a criação de categorias personalizadas; Deve possibilitar a monitoração do tráfego internet sem bloqueio de acesso aos usuários; Deve possibilitar a categorização e reclassificação de sites web, tanto por URL quanto por endereço IP; Deve possibilitar a criação de listas de URL específicas para serem bloqueadas ou liberadas; Deve possibilitar, nas listas de URL personalizadas, a inserção de novas listas por expressão regular, permitindo adicionar domínios, subdomínios ou caminhos completos de sites; Deve possibilitar o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual; Deve possibilitar a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem; Deve ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP; Deve possibilitar proxy transparente; Deve possuir integração com serviços de diretório LDAP e Microsoft Active Directory para autenticação de usuários; Deve possibilitar a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory; Deve possibilitar a criação de quotas de utilização ou limite de banda por usuários e grupos de usuários por aplicação (Facebook, Youtube, etc.); Deve ter a capacidade de exibir mensagens de bloqueio customizável pelos administradores para resposta aos usuários; Deve realizar o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual; Deve possibilitar e forçar pesquisas seguras em sistemas de buscas, contemplando no mínimo: Google, Bing e Yahoo!. Requisitos mínimos para solução de controle de aplicações: Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo; Deve realizar a liberação e bloqueio somente de aplicações, sem a necessidade de liberação de portas e protocolos; Deve reconhecer, no mínimo, 1.800 (mil e oitocentas) aplicações diferentes; Deve identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da Deep Web (ex.: rede tor); Deve de-criptografar, para tráfego criptografado SSL, pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; Deve atualizar a base de assinaturas de aplicações automaticamente; Deve limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/MS AD; Deve possibilitar a solicitação de inclusão de aplicações na base de assinaturas de aplicações; Deve possibilitar a configuração de alertas quando uma aplicação for bloqueada; Deve garantir o funcionamento com módulos de IPS, antivírus e anti-spyware integrados no próprio appliance de firewall; Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (antivírus e anti-spyware); Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, anti-spyware e antivírus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo; Deve permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração; Deve possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança; Deve permitir o uso de exceções por IP de origem ou de destino nas regras e assinatura; Deve permitir o bloqueio de vulnerabilidades; Deve permitir o bloqueio de programas exploradores de vulnerabilidades (exploits) conhecidos; Deve incluir proteção contra-ataques de negação de serviços (DoS); Deve possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS) e negação de serviço distribuído (DDoS); Deve detectar e bloquear a origem de programas de varredura de portas (port scans); Deve bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; Deve possuir assinaturas para bloqueio de ataques de buffer overflow; Deve permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações; Deve permitir o bloqueio de vírus e spywares em, pelo menos, 02 (dois) dos seguintes protocolos: FTP, SMB, SMTP e POP3 e obrigatoriamente em HTTP; Deve identificar, alertar e bloquear comunicação com botnets; Deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; Deve identificar nos eventos, o país de onde partiu a ameaça; Deve criar políticas de QoS e Traffic Shaping por endereço de origem e destino; Deve criar políticas de QoS e Traffic Shaping por endereço de destino; Deve realizar a criação de políticas de QoS e Traffic Shaping por porta; Deve realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade; Deve realizar QoS (Traffic Shaping) em interfaces agregadas ou redundantes; Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos; Deve identificar arquivos criptografados e aplicar políticas sobre esses tipos de arquivos; Deve criar políticas por geolocalização, permitindo que o tráfego de determinado pais/países seja(m) bloqueados; Deve realizar a visualização dos países de origem e destino nos logs dos | | | | |

| Item | Grupo do Mat. | Material | Quant. Solic. | Unid. de Medida | Situação |
|---|---|---|---|---|---|
| | | acessos; Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular; Deve criar políticas por geolocalização, permitindo que o tráfego de determinado pais/países seja(m) bloqueados; Deve realizar a visualização dos países de origem e destino nos logs dos acessos; Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas; A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN A solução deve ser capaz de medir o Status de Saúde com Suporte a múltiplos servidores. A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links; A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 a 50) do seu valor de Saúde melhor que o link atual; A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema; A solução deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em Número de Sessões, Volume de Tráfego, IP de Origem e Destino e Transbordo de Link (Spillover), Requisitos mínimos de redes virtuais privadas (VPNs), Deve criar VPN dos tipos: site-to-site e client-to-site; Deve suportar e criar IPsec VPN e SSL VPN; Deve suportar nativamente a criação de VPN IPsec utilizando Triple Data Encryption Standard (3DES); Deve suportar nativamente a criação de VPN IPsec utilizando Advanced Encryption Standard (AES) 128, 192 ou 256 bits; Deve suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1; Deve suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-Hellman, grupos: 1, 2, 5 e 14; Deve suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKE) v1 e v2; Garantia conforme ESPECIFICAÇÃO PADRÃO DOS SERVIÇOS DE GARANTIA DO FABRICANTE DO FIREWALL, COM COBERTURA DE ATENDIMENTO 24X7; Serviço de gestão conforme ESPECIFICAÇÃO PADRÃO DOS SERVIÇOS DE ASSISTÊNCIA TÉCNICA; Todos produtos devem incluir Garantia do Fabricante dos produtos, incluindo os serviços e SLA especificados abaixo: As garantias dos itens acessórios e componentes internos como transceptores devem acompanhar a garantia ofertada do equipamento principal onde serão instalados; Recursos online: Acesso a um portal personalizado que inclua fóruns de suporte; envio de chamados de suporte; download de drivers, updates de software e firmware; gerenciamento de patches; principais problemas e soluções guiadas; detalhes de garantia; atualizações de software; acesso à base de conhecimento; ferramentas de diagnóstico; chat para envio de perguntas; Os equipamentos de NGFW devem incluir subscrição para licenças de uso para atualização de firmware e softwares, bem como a subscrição para atualização das bases de dados de Application Control, Internet Service, Client ID, IP Geography, Malicious URL, URL Whitelist, Botnet domain, IP Reputation, Antivírus e IPS, deve incluir também serviços remotos na nuvem do fabricante de Sandbox, Content Disarm & Reconstruct, Virus Outbreak Protection Query, Web Filtering Query, Secure DNS Query e AntiSpam Query; Central de Atendimento: Central com atendimento em português através de ligação local ou gratuita; Recursos Reativos: Atividades sob demanda, sem limite de quantidade de atendimentos, que deve incluir especialistas técnicos, gestores de eventos críticos Suporte técnico remoto para a solução ofertada incluindo hardware e softwares fornecidos; Período de cobertura: 24x7 (vinte quatro horas por dia, sete dias por semana); Registro de chamado: através da Central de Atendimento e portal na web; a Central deverá confirmar o recebimento do chamado informando um identificador para acompanhamento Níveis de Gravidade: (1) paralisação crítica: ex.: ambiente de produção ou sistema paralisado ou com risco grave de paralisação ou de perda de dados; (2) degradação crítica: ex.: ambiente de produção ou sistema seriamente prejudicado, parcialmente interrompido ou comprometido, risco de recorrência; (3) normal: ex.: ambiente não de produção ou sistema fora do ar ou degradado; (4) baixa: ex.: nenhum impacto sobre os sistemas ou usuários; Tempo de Atendimento: em até 1h (uma hora) após registro do chamado para início do atendimento por um especialista técnico para chamados classificados com nível de gravidade (1), e até 2h (duas horas) para os demais; Peças: O Serviço de Suporte deve incluir sem custos adicionais para o cliente, a substituição avançada de módulos ou do equipamento completo quando diagnosticado defeito. Isso significa que quando for diagnosticado defeito do equipamento pelo fabricante, o fabricante deve remeter módulo ou equipamento completo para substituição, e efetuar o recolhimento do módulo ou equipamento completo defeituoso. Gerenciamento de escalação: Para situações de gravidade 1 em que o atendimento precise ser escalado, deverá ser alocado de um gestor de eventos críticos para monitorar e coordenar todo o processo, do chamado até a resolução final, e assegurar o envolvimento imediato e efetivo dos recursos para agilizar a solução do incidente; Resolução remota dos chamados: Mediante autorização prévia do cliente, o fabricante poderá utilizar as ferramentas de software instaladas para monitoramento ou outras para realizar o diagnóstico, isolar e resolver o problema. Garantia de 5 Anos On-site 24x7 e licenciamento pelo mesmo período. Modelo de referência: FortiGate-101F | | | |