## ANEXO I DO TERMO DE REFERÊNCIA

## ESPECIFICAÇÃO TÉCNICA

**Observações:**

 1) Todos os requisitos especificados, independentemente do verbo utilizado, deverão estar habilitados e completamente funcionais, exceto quando explicitamente mencionado o contrário;

2) A licitante deverá apresentar, para cada um dos requisitos especificados, uma comprovação de que a solução proposta atende ao requisito. Esta comprovação deverá ser feita por meio da indicação do documento público (eletrônico ou impresso) e da numeração da página (ou localização no texto) onde a equipe técnica da CGU possa confirmar tais argumentos. Na Tabela 1 deverá ser especificado o documento, e na coluna **COMPROVAÇÃO** das especificações deverá ser especificado o **ÍNDICE** do documento na Tabela 1 e a **NUMERAÇÃO DA PÁGINA** (ou localização no texto do documento) para comprovação;

3) A CGU reserva-se o direito de diligenciar, após apresentação da proposta, o fornecedor e/ou fabricante para comprovação das informações prestadas na proposta e nas tabelas.

 4) A documentação de comprovação de atendimentos aos requisitos poderá ser apresentada em língua inglesa.

**Tabela 1**

|  |  |
| --- | --- |
| **ÍNDICE** | **DOCUMENTO (anexo impresso ou sítio da internet)** |
| A |  |
| B |  |
| C |  |
| D |  |
| E |  |
| F |  |
| G |  |
| H |  |
| I |  |
| J |  |

A solução ofertada deve atender a todos os requisitos técnicos descritos abaixo:

|  |  |
| --- | --- |
| **Termo** | **Significado** |
| ACL | Access Control List |
| AS (plural ASes) | Autonomous System |
| BGP | Border Gateway Protocol |
| CoS | Class of Service |
| CPE | Customer Premises Equipment |
| CDN | Content Deliveryt Network |
| DIO | Distribuidor Interno Óptico |
| DSCP | Differentiated Services Code Point |
| IKE | Internet Key Exchange |
| FIB | Forwarding Information Base |
| HUB-AND-SPOKE | Topologia em estrela, em que o nó central é chamado de HUB e as extremidades são chamadas de SPOKES |
| IPS | Intrusion Prevention System |
| IXP | Internet Exchange Point |
| MP-BGP | Multiprotocol Border Gateway Protocol |
| NAT | Network Address Translation |
| NTP | Network Time Protocol |
| PE | Provider Equipment |
| PIM | Protocol Independent Multicast |
| POD | Point of Delivery |
| POP | Point of Presence |
| QoS | Quality of Service |
| RSSO | Radius Single Sign-On |
| SSL | Secure Socket Layer |
| UTP | Unshielded Twisted Pair  |
| VPN | Virtual Private Network |
| VRF | Virtual Routing and Forwarding |
| WRED | Weighted Random Early Detection |

|  |  |  |
| --- | --- | --- |
| **ITEM / SUBITEM** | **ESPECIFICAÇÃO** | **COMPROVAÇÃO****(ÍNDICE E PÁGINA)** |
|  | **Características gerais e premissas aplicáveis a todos os itens** | **-** |
|  | **Funcionamento geral da solução** | - |
|  | * A CONTRATANTE pretende implementar uma solução de comunicação entre suas unidades, bem como de suas unidades com a rede mundial de computadores (Internet).
 | - |
|  | * A sede da CONTRATANTE está localizada em Brasília, enquanto as unidades regionais estão nas capitais de todos os estados brasileiros.
 | - |
|  | * O objetivo é que exista uma rede MPLS para a comunicação entre todas as unidades. Adicionalmente, cada localidade deve ter conexão direta com a Internet.
 | - |
|  | * Em situações normais, os tráfegos de sistemas e serviços corporativos, além dos tráfegos multimídia de telefonia IP e videoconferência devem ser encaminhados exclusivamente pela rede MPLS. Por outro lado, os serviços que estiverem publicados na Internet devem ser acessados diretamente sem a necessidade de utilização da rede MPLS.
 | - |
|  | * Em situações de falha da rede MPLS, alternativamente os tráfegos corporativos devem ser encaminhados entre as regionais da CONTRATANTE e a sede utilizando túneis VPN IPSEC que devem ser estabelecidos pela Internet. Os túneis VPN devem utilizar a topologia hub-and-spoke, com centralização nos equipamentos da sede.
 | - |
|  | * Em situações de falha dos Links de internet das unidades regionais, o tráfego deve ser encaminhado pela rede MPLS até a sede em Brasília para que então possa ser enviado para a Internet.
 | - |
|  | * A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita preferencialmente com a correta configuração do protocolo de roteamento OSPF, embora seja permitida a utilização de tecnologias SDN-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas (situação em que a topologia poderá ser revista). Também será permitida a redistribuição de rotas entre o OSPF e outros protocolos de roteamento. O OSPF deve ser utilizado para efetuar a troca de informações de roteamento com o equipamento denominado “Firewall existente na CONTRATANTE”.
 | - |
|  | * Objetivando redundância e independência das conexões à Internet e dos serviços de proteção, os lotes 1 e 2 deverão ser arrematados por fornecedores distintos, sendo vedado o compartilhamento de serviços ou de infraestrutura em qualquer nível.
 | - |
|  | **Características gerais dos links MPLS e Internet** | - |
|  | * As unidades regionais da CONTRATANTE farão acesso à Internet, mas não haverá nenhum serviço publicado externamente. Em função do exposto, basta que seja fornecido pela CONTRATADA 1 (um) IPv4 válido para os links internet dessas localidades. Será permitida a utilização da RFC 3021 (utilização de prefixos /31 IPv4 em links ponto-a-ponto) nesses casos.
 | - |
|  | * Devem transportar pacotes IPv4 e IPv6 com 1500 (mil e quinhentos) bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.
 | - |
|  | * Os links devem suportar IPv6, não sendo necessário o fornecimento de endereçamento para as redes internas da CONTRATANTE.
 | - |
|  | * A velocidade de todos os Links deverá ser simétrica e disponível de forma simultânea, ou seja, mesma velocidade de entrada e de saída (Links full-duplex).
 | - |
|  | * Todos os canais deverão ser entregues e mantidos sem nenhum mecanismo de restrição a qualquer volume de tráfego.
 | - |
|  | * Para as unidades regionais, a CONTRATADA poderá entregar os links MPLS e Internet diretamente nos appliances de Firewall/Filtro de Conteúdo ou poderá opcionalmente utilizar roteadores específicos para interconectar cada um dos links. Caso seja feita opção por utilizar roteadores, não poderá haver custo adicional para tais equipamentos e todos os demais requisitos para a utilização da solução devem ser mantidos e respeitados.
 | - |
|  | **Regime de operação dos serviços** | - |
|  | * Regime de operação de todos os serviços deverá ser de 24 (vinte e quatro) horas por dia, durante os 7 (sete) dias da semana.
 | - |
|  | * Eventuais manutenções preventivas dos serviços deverão ser agendadas com antecedência mínima de 5 (cinco) dias corridos.
 | - |
|  | **Última milha** | - |
|  | * A última milha caracteriza-se como o meio de comunicação utilizado para interligar cada unidade da CONTRATANTE ao backbone da CONTRATADA.
 | - |
|  | * Deverão ser utilizados Links de comunicação terrestre confeccionados com fibra óptica. Apenas será permitida a conversão do meio óptico para UTP para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances de firewall/filtro de conteúdo.
 | - |
|  | * A CONTRATADA se responsabilizará pela implantação, nas unidades da CONTRATANTE, de toda a infraestrutura necessária à configuração dos canais de comunicação. Dentre os itens de infraestrutura a serem fornecidos pela CONTRATADA, caso seja necessário, estão: construção/reforma de caixas de passagem, instalação de dutos entre a caixa de passagem e a unidade da CGU, lançamento de cabos, e recomposição de calçada quando for necessário. Não estão incluídas neste item obras internas nas unidades da CGU, como lançamento de canaletas e recomposição de gesso.
 | - |
|  | **Dupla abordagem:** | - |
|  | * Para as unidades regionais da CONTRATANTE, o link MPLS e o link internet deverão ser entregues com dupla abordagem em fibra óptica. O mesmo requisito deve ser respeitado para os dois links MPLS da sede. Nas duas situações descritas acima, os links poderão ser atendidos pelo mesmo POP da CONTRATADA.
 | - |
|  | * Os circuitos com dupla abordagem não poderão ser instalados no mesmo PE. O circuito do item 61 também não poderá compartilhar o PE com nenhum dos dois circuitos do item 27.
 | - |
|  | * Os links com dupla abordagem, em fibra óptica, que devem ser estabelecidas por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação. Por ponto de falha comum entende-se:
 | - |
|  | * + Utilização compartilhada dos mesmos equipamentos no ambiente da CONTRATADA ou em ambientes públicos: roteadores, multiplexadores, switches, conversores ópticos e outros. Para os links das unidades regionais da CONTRATANTE (não se aplica aos links da sede) será permitido o compartilhamento de equipamentos dentro das instalações da CONTRATANTE apenas;
 | - |
|  | * + Utilização compartilhada de Links físicos ou lógicos no ambiente da CONTRATADA ou em ambientes públicos, como: utilização dos mesmos encaminhamentos, dutos, caixas de passagem, DIOs e outros. Para os links das unidades regionais da CONTRATANTE (não se aplica aos links da sede) será permitido o compartilhamento da caixa de passagem (na calçada do prédio da CONTRATANTE) e dos dutos da caixa de passagem até o rack dentro das instalações da CONTRATANTE apenas.
 | - |
|  | **Fornecimento de energia e disponibilização de espaço** | - |
|  | * Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação, se necessário. Caso seja necessário devem ser fornecidos adaptadores para racks ou bandejas.
 | - |
|  | * A CONTRATANTE disponibilizará circuitos elétricos e até 8 Us (oito unidades de rack) em bastidor de 19” para acomodar os equipamentos da CONTRADADA em suas unidades regionais.
 | - |
|  | * A CONTRATANTE disponibilizará circuitos elétricos redundantes e a CONTRATADA deverá providenciar 1 (um) rack de 19” com dimensões adequadas para acomodar os equipamentos na sede em Brasília.
 | - |
|  | **Características comuns aos equipamentos e gerência** | - |
|  | * Os equipamentos deverão ser dimensionados, fornecidos, instalados e configurados, pela CONTRATADA, garantindo-se o desempenho e os níveis de serviços contratados.
 | - |
|  | * A CONTRATANTE deverá ter acesso do tipo leitura nos equipamentos “roteador internet” e “roteador MPLS” da sede e das regionais (caso sejam instalados).
 | - |
|  | * A CONTRATANTE deverá ter acesso do tipo escrita nos equipamentos denominados “appliance de firewall/filtro de conteúdo”. A CONTRATANTE isentará a CONTRADATA de incidentes causados por erros de configuração causados pela própria CONTRATANTE. A CONTRATADA poderá ter acesso do tipo leitura nos referidos equipamentos.
 | - |
|  | * A qualquer momento durante a execução do contrato, a CONTRATANTE poderá optar por solicitar o acesso do tipo escrita para os equipamentos “roteador internet” da sede, por utilizarem o ASN e o bloco de endereços da CGU. Nesta situação, a CONTRATADA poderá ter acesso do tipo leitura nos referidos equipamentos.
 | - |
|  | * Por acesso entende-se permissão de ingresso utilizando interface web utilizando https, linha de comando utilizando ssh, possibilidade de obtenção de dados via SNMP e syslog.
 |  |
|  | * Mesmo para as situações em que a CONTRATANTE possuir acesso de escrita, a CONTRATADA não estará isenta de oferecer suporte para qualquer necessidade em que seja necessário acionar o fabricante, bem como em casos de indisponibilidade, substituição do hardware ou partes dos hardwares, atualização do firmware entre outras possíveis situações. A CONTRATANTE não acionará a CONTRATADA para configurações básicas e rotineiras, como: configurações de interfaces, regras de firewalls e controle de aplicações, ACLs, NATs, SNMP, NTP, VPN client do site, entre outras possíveis situações.
 | - |
|  | * Todos os equipamentos e links devem suportar tanto IPv4 quanto IPv6, sendo que este último deve estar implementado de forma nativa em pilha dupla.
 | - |
|  | * Deverão suportar o respectivo tráfego da banda completamente ocupada sem degradação do desempenho, atendendo aos níveis de serviço pretendidos. Para isso deverão apresentar configuração de memória, de CPU e capacidade de vazão compatíveis (de forma qualitativa e quantitativa) com as características e componentes desta especificação.
 | - |
|  | * Deverão possuir fonte de alimentação com chaveamento automático de tensão de entrada 110/220 VAC a 60 Hz.
 | - |
|  | * Os appliances de firewall/filtro de conteúdo da sede e de todas as regionais devem ser do mesmo fabricante para que a solução de gerência seja única e as configurações possam ser aplicadas em todos os dispositivos de forma unificada.
 | - |
|  | **Topologia da solução** | - |
|  | * As regionais da CONTRATANTE foram divididas em 3 tipos conforme a quantidade de pessoas e a capacidade de seus links. Esses parâmetros serão utilizados para detalhar as capacidades dos appliances de firewall/filtro de conteúdo. Apenas para referência, as unidades regionais tipo 1 possuem até 70 (setenta) usuários simultâneos, as unidades regionais tipo 2 possuem até 100 (cem) usuários simultâneos, as unidades tipo 3 possuem até 150 (cento e cinquenta) usuários simultâneos e a sede possui até 2.000 (dois mil) usuários simultâneos.
 | - |
|  | * Foi elaborada uma topologia lógica da solução. O diagrama também detalha a distribuição dos itens em função dos lotes. Para simplificar o diagrama foram demonstradas apenas 3 unidades regionais da CONTRATANTE (uma de cada tipo).
 | - |
|  | Q:\DF\Grupos\DSI\DSI_Gab\Proj_contratacoes\2017\Rede WAN\3 - Especificação Técnica\Projeto nova rede CGU-1.jpg | - |
|  | * A CONTRATANTE poderá desativar o cluster de equipamentos denominado “Firewall existente na CONTRATANTE” e migrar todas as conexões e regras para os equipamentos denominados “appliances de firewall/filtro de conteúdo da sede”. Para isso as especificações do referido item irão prever interfaces e throughput adequados. Neste caso a topologia lógica da solução será modificada para a forma como está descrita no diagrama abaixo. Para simplificar o desenho há alguns segmentos não representados na topologia (em especial nos firewalls da sede), mas a quantidade de portas do “appliances de firewall/filtro de conteúdo da sede” comporta os segmentos em questão.
 | - |
|  | Q:\DF\Grupos\DSI\DSI_Gab\Proj_contratacoes\2017\Rede WAN\3 - Especificação Técnica\Projeto nova rede CGU-2.jpg | - |
|  | * Não será necessário fornecer nenhum switch para o atendimento da solução proposta. Os barramentos ethernet representados nas topologias lógicas serão de responsabilidade da CONTRATANTE.
 | - |
|  | * A CONTRATANTE poderá utilizar os roteadores internet (itens 62 e 68) para interconexão a qualquer IXP.
 | - |
| 1.
 | **Características comuns dos itens 1 a 27 - Link MPLS** | - |
|  | **Backbone** | - |
|  | * Rede de dados com capacidade de encaminhar pacotes IPv4 e IPv6, composto por uma malha de canais de comunicação dedicados, que permitirá a conexão entre todas as unidades da CONTRATANTE sob uma topologia any-to any (full mesh).
 | - |
|  | * Deve permitir o isolamento total do tráfego e das tabelas de roteamento da CONTRATANTE e dos demais clientes da CONTRATADA utilizando tecnologia de VRFs criando uma VPN MPLS. Em função disso a CONTRATANTE poderá utilizar qualquer faixa de endereço privados IPv4 em sua estrutura de rede.
 | - |
|  | * Deverá possuir capacidade de tráfego em IP multicast para que aplicações de voz e vídeo que utilizem esta tecnologia possam ser implementadas independente de qualquer configuração no backbone. Não será permitido o estabelecimento de túneis entre os roteadores para que o tráfego multicast seja encaminhado.
 | - |
|  | * Não serão permitidos POPs atendidos de forma primária por Links de satélite.
 | - |
|  | * O backbone MPLS deve pertencer inteiramente a ASes do mesmo grupo econômico.
 | - |
|  | **Qualidade de Serviço** | - |
|  | * A solução da CONTRATADA deverá suportar a arquitetura Diffserv, incluindo Diffserv sobre redes MPLS.
 | - |
|  | * De acordo com as prioridades e níveis de serviços definidos, os diferentes tipos de tráfego que serão encaminhados pela Rede CONTRATANTE deverão ser classificados em 5 (cinco) classes de serviços (Diffserv) pela rede MPLS da CONTRATADA, conforme descrito a seguir:
 | - |
|  | * + **Voz:** aplicações de voz sensíveis a retardo (delay) e variações de retardo (jitter), que exijam priorização absoluta de tráfego e reserva de banda;
 | - |
|  | * + **Vídeo:** aplicações multimídia sensíveis a retardo (delay) e variações de retardo (jitter), que exijam priorização de tráfego e reserva de banda;
 | - |
|  | * + **Serviços críticos:** aplicações críticas para o negócio, que exigem entrega garantida, reserva de banda e tratamento prioritário;
 | - |
|  | * + **Serviços interativos:** aplicações interativas, que exigem entrega garantida, reserva de banda e tratamento prioritário. Esta classe deve acomodar o tráfego utilizado para medir o SLA;
 | - |
|  | * + **Serviços não prioritários:** aplicações com mensagens de tamanho muito variado e não imprescindíveis para o atendimento imediato aos clientes.
 | - |
|  | * A marcação da classe de serviço dos pacotes deve ser feita pela CONTRATADA utilizando o campo DSCP dos pacotes IP nos CPEs, ou seja, roteadores ou appliances de firewall/filtro de conteúdo.
 | - |
|  | * As classes podem ser remapeadas quando os pacotes forem encaminhados para o backbone MPLS.
 | - |
|  | * A CONTRADATA poderá implementar outras classes além das utilizadas pela CONTRATANTE para fins de operação dos protocolos de roteamento e/ou de gerência. As bandas das classes somadas poderão consumir até 2% (dois por cento) da capacidade do link. Caso haja sobreposição de tráfego entre as classes será feita a diferenciação das regras da CONTRATANTE em relação às da CONTRATADA com base em endereços IP de origem e/ou de destino.
 | - |
|  | * O mapeamento dos tráfegos e larguras de banda de cada classe será definido pela CONTRATANTE, respeitado os seguintes critérios:
 | - |
|  | * + A soma das bandas das classes da CONTRATANTE com as classes da CONTRATADA não excederão 97% (noventa e sete por cento) da capacidade do link.
 | - |
|  | * + A soma das bandas das classes de **voz** e **vídeo** somadas não excederão 50% (cinquenta por cento) da capacidade do link.
 | - |
|  | **Características específicas dos itens 1 a 16 - Link MPLS - Regionais Tipo 1** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 4 Mbps (quatro megabits por segundo);
 | **-** |
|  | * 6 Mbps (seis megabits por segundo);
 | **-** |
|  | * 8 Mbps (oito megabits por segundo);
 | **-** |
|  | * 10 Mbps (dez megabits por segundo);
 | **-** |
|  | * 12 Mbps (doze megabits por segundo);
 | **-** |
|  | **Características específicas dos itens 17 a 23 - Link MPLS - Regionais Tipo 2** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 6 Mbps (seis megabits por segundo);
 | **-** |
|  | * 8 Mbps (oito megabits por segundo);
 | **-** |
|  | * 10 Mbps (dez megabits por segundo);
 | **-** |
|  | * 12 Mbps (doze megabits por segundo);
 | **-** |
|  | * 14 Mbps (quatorze megabits por segundo);
 | **-** |
|  | **Características específicas dos itens 24 a 26 - Link MPLS - Regionais Tipo 3** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 8 Mbps (oito megabits por segundo);
 | **-** |
|  | * 10 Mbps (dez megabits por segundo);
 | **-** |
|  | * 12 Mbps (doze megabits por segundo);
 | **-** |
|  | * 14 Mbps (quatorze megabits por segundo);
 | **-** |
|  | * 16 Mbps (dezesseis megabits por segundo);
 | **-** |
|  | **Características específicas do item 27 - Link MPLS - Sede – DF** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 50 Mbps (cinquenta megabits por segundo);
 | **-** |
|  | * 100 Mbps (cem megabits por segundo);
 | **-** |
|  | * 150 Mbps (cento e cinquenta megabits por segundo);
 | **-** |
|  | * 200 Mbps (duzentos megabits por segundo);
 | **-** |
|  | * 250 Mbps (duzentos e cinquenta megabits por segundo).
 | **-** |
|  | **Item 28 - Roteador MPLS - Sede** | **-** |
|  | As características abaixo se referem a 1 (uma) unidade do roteador. | **-** |
|  | Além das interfaces utilizadas para o link MPLS e back-to-back (caso seja necessário) deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas na rede interna da CONTRATANTE. |  |
|  | Deve ter no mínimo 2 (duas) fontes de alimentação. |  |
|  | **Devem suportar os seguintes protocolos/funcionalidades:** | **-** |
|  | * O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;
 |  |
|  | * Priorização e conformação de tráfego com pelo menos os seguintes métodos: Traffic Policing, Traffic Shaping, Class Based Weighted Fair Queueing, Low-latency Queuing;
 |  |
|  | * WRED;
 |  |
|  | * Implementar classificação de tráfego com base em ACLs, no campo DSCP e no campo CoS;
 |  |
|  | * Implementar a marcação e priorização do tráfego previamente classificado com base no campo DSCP e no campo CoS;
 |  |
|  | * Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode;
 |  |
|  | * Implementar RFC 3768 VRRP.
 |  |
|  | * OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;
 |  |
|  | * Cliente NTP, contemplando suporte à autenticação entre os peers, conforme definido na RFC 1305. Deve possibilitar a especificação da interface de origem dos pacotes NTP;
 |  |
|  | * Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;
 |  |
|  | * Capacidade de geração e armazenamento de logs locais;
 |  |
|  | * Protocolo Syslog com a possibilidade de envio de timestamp baseado no relógio do roteador;
 |  |
|  | * Protocolo IP SLA ou similar, ou sejam deve ser capaz de responder a pacotes de simulação de tráfegos. Devem ser suportados, no mínimo, os protocolos ICMP, TCP e UDP. Os dados referentes aos tráfegos simulados devem ser disponibilizados via SNMP;
 |  |
|  | * Implementar ACLs com pelo menos os seguintes parâmetros;
 |  |
|  | * + Endereços IP de host ou rede, de pacotes IPv4 e IPv6 (tanto de origem quanto de destino);
 |  |
|  | * + Tipos de pacote ICMP;
 |  |
|  | * + Portas e faixas de portas dos protocolos TCP e UDP (tanto de origem quanto de destino);
 |  |
|  | * + Deve permitir criar regras com base em hora do dia e com base nos dias da semana;
 |  |
|  | * Protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, IPFIX ou similar, contemplando no mínimo as seguintes informações:
 |  |
|  | * + IP de origem/destino;
 |  |
|  | * + Parâmetro “protocol type” do cabeçalho IP;
 |  |
|  | * + Porta TCP/UDP de origem/destino;
 |  |
|  | * + Campo TOS ou DSCP do cabeçalho IP;
 |  |
|  | * + Interface do equipamento em que o tráfego foi identificado;
 |  |
|  | * + A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo padrão de mercado para este fim;
 |  |
|  | **Características comuns dos itens 29 a 54, 61 e 67 - Link Internet** | **-** |
|  | Acessos IP permanentes que possibilitem a interligação (IPv4 e IPv6) das unidades da CONTRATANTE à rede mundial de computadores, Internet. | **-** |
|  | O backbone da CONTRATADA deverá possuir conexão direta com pelo menos 1 (um) IXP para troca de trânsito. |  |
|  | O backbone da CONTRATADA deverá possuir pelo menos 2 (duas) saídas internacionais próprias, ou contratados para seu uso. |  |
|  | O backbone da CONTRATADA deverá possuir interligação direta através de canais próprios e dedicados, a pelo menos 3 (três) outros ASes (além das conexões descritas no item anterior), com peering BGP IPv4 e IPv6. As bandas de saída entre referidos ASes deverão somar pelo menos 10 Gbps (dez gigabits por segundo). |  |
|  | Disponibilizar serviço de DNS da CONTRATADA, capaz de resolver direta e reversa endereços IPv4 e IPv6 de internet. | **-** |
|  | Não será permitido o uso de tecnologias DSL, BLC Cable, 3G e 4G.  | **-** |
|  | Todos os links internet das regionais e o PE que atenderá o link internet (Item 61) devem necessariamente pertencer a ASes do mesmo grupo econômico para que a latência da VPN seja reduzida. Por esse motivo o referido item deve ser licitado em conjunto com os demais itens do lote 1. |  |
|  | **Características específicas dos itens 29 a 44 - Link Internet - Regionais Tipo 1** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 6 Mbps (seis megabits por segundo);
 | **-** |
|  | * 10 Mbps (dez megabits por segundo);
 | **-** |
|  | * 14 Mbps (quatorze megabits por segundo);
 | **-** |
|  | * 18 Mbps (dezoito megabits por segundo);
 | **-** |
|  | * 22 Mbps (vinte e dois megabits por segundo);
 | **-** |
|  | **Características específicas dos itens 45 a 51 - Link Internet - Regionais Tipo 2** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 8 Mbps (oito megabits por segundo);
 | **-** |
|  | * 12 Mbps (doze megabits por segundo);
 | **-** |
|  | * 16 Mbps (dezesseis megabits por segundo);
 | **-** |
|  | * 20 Mbps (vinte megabits por segundo);
 | **-** |
|  | * 24 Mbps (vinte e quatro megabits por segundo);
 | **-** |
|  | **Características específicas dos itens 52 a 54 - Link Internet - Regionais Tipo 3** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 10 Mbps (dez megabits por segundo);
 | **-** |
|  | * 14 Mbps (quatorze megabits por segundo);
 | **-** |
|  | * 18 Mbps (dezoito megabits por segundo);
 | **-** |
|  | * 22 Mbps (vinte e dois megabits por segundo);
 | **-** |
|  | * 26 Mbps (vinte e seis megabits por segundo);
 | **-** |
|  | **Características comuns dos itens 55 a 58 - Appliance de Firewall/Filtro de Conteúdo** | **-** |
|  | Aplliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW). Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. | **-** |
|  | A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7. |  |
|  | Deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. |  |
|  | Nos estados, caso a CONTRATADA opte por fornecer CPEs para o link MPLS e/ou para o link internet, as características do conjunto formado pelos três equipamentos devem atender aos requisitos deste item. |  |
|  | Deve implementar funcionalidade de anti-spoofing, configurável por segmento de rede de modo que seja possível: utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote. |  |
|  | Deve permitir a configuração de ISP (rota default estática) com a utilização de probe para verificar a disponibilidade do provedor. A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência). |  |
|  | As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas durante toda a vigência do contrato. |  |
|  | **Deve possuir pelo menos as seguintes funcionalidades:** | **-** |
|  | * Policy based routing ou policy based forwarding;
 |  |
|  | * Jumbo Frames;
 |  |
|  | * DHCP Relay;
 |  |
|  | * Suportar IGMP, v2 e v3;
 |  |
|  | * O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;
 |  |
|  | * Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode (não será exigida a implementação dos dois modos de forma simultânea);
 |  |
|  | * OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;
 |  |
|  | * Cliente NTP, contemplando suporte à autenticação entre os peers;
 |  |
|  | * Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;
 |  |
|  | * Protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, sFlow, IPFIX ou similar, contemplando no mínimo as seguintes informações:
 |  |
|  | * + IP de origem/destino;
 |  |
|  | * + Parâmetro “protocol type” do cabeçalho IP;
 |  |
|  | * + Porta TCP/UDP de origem/destino;
 |  |
|  | * + Interface do equipamento em que o tráfego foi identificado.
 |  |
|  | **Deve suportar os seguintes tipos de NAT:** | **-** |
|  | * NAT dinâmico (Many-to-1);
 |  |
|  | * NAT dinâmico (Many-to-Many);
 |  |
|  | * NAT estático (1-to-1);
 |  |
|  | * NAT estático (Many-to-Many);
 |  |
|  | * NAT estático bidirecional 1-to-1;
 |  |
|  | * Tradução de porta (PAT);
 |  |
|  | * NAT de origem;
 |  |
|  | * NAT de destino;
 |  |
|  | * NAT de origem e NAT de destino simultaneamente.
 |  |
|  | **Controle de política de firewall** | **-** |
|  | * Controles de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
 |  |
|  | * Controle, inspeção e decriptografia de SSL por política para trafego de entrada (inbound) e Saída (outbound);
 |  |
|  | * Deve suportar offload de certificado em inspeção de conexões SSL de entrada (inbound);
 |  |
|  | * Deve permitir bloquear, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg;
 |  |
|  | * Suporte a objetos e regras multicast;
 |  |
|  | * Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
 |  |
|  | * Suportar a criação de políticas com data de expiração.
 |  |
|  | **Controle de aplicações** | **-** |
|  | * Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
 |  |
|  | * Deve ser possível a liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;
 |  |
|  | * Reconhecer diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail;
 |  |
|  | * Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
 |  |
|  | * Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443;
 |  |
|  | * Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
 |  |
|  | * Deve ser possível a liberação e bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica;
 |  |
|  | * Atualizar a base de assinaturas de aplicações automaticamente;
 |  |
|  | * Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
 |  |
|  | * O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
 |  |
|  | * Deve alertar o usuário quando uma aplicação for bloqueada;
 |  |
|  | * Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao whatsapp mas bloquear a transferência de arquivos.
 |  |
|  | * Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos;
 |  |
|  | * Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
 |  |
|  | * Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);
 |  |
|  | * Nível de risco da aplicação;
 |  |
|  | * Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.
 |  |
|  | **Prevenção de ameaças** | **-** |
|  | * Deve possuir módulo de IPS integrado no próprio appliances,
 |  |
|  | * Deve incluir assinaturas de prevenção de intrusão (IPS);
 |  |
|  | * Deve-se sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo (quando aplicável);
 |  |
|  | * Deverá possuir os seguintes mecanismos de inspeção de IPS:
 | **-** |
|  | * + Análise de padrões de estado de conexões;
 |  |
|  | * + Análise de decodificação de protocolo;
 |  |
|  | * + Análise para detecção de anomalias de protocolo;
 |  |
|  | * + IP Defragmentation;
 |  |
|  | * + Remontagem de pacotes TCP;
 |  |
|  | * + Bloqueio de pacotes malformados;
 |  |
|  | * Ser capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
 |  |
|  | * Detectar e bloquear a origem de port scans;
 |  |
|  | * Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
 |  |
|  | * Possuir assinaturas para bloqueio de ataques de buffer overflow;
 |  |
|  | * Deverá possibilitar a criação de assinaturas customizadas;
 |  |
|  | * Suportar bloqueio de arquivos por tipo;
 |  |
|  | * Identificar e bloquear comunicação com botnets;
 |  |
|  | * Deve suportar várias técnicas de prevenção, incluindo Drop (Cliente, Servidor e ambos);
 |  |
|  | * Deve suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);
 |  |
|  | * Deve suportar a captura de pacotes (PCAP), por assinatura de IPS;
 |  |
|  | * Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
 |  |
|  | * Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis;
 |  |
|  | * Rastreamento de vírus em pdf;
 |  |
|  | * Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate, como: zip e gzip;
 |  |
|  | * Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
 |  |
|  | * Deve permitir a inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção.
 |  |
|  | **Identificação de usuários** | **-** |
|  | * Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local;
 |  |
|  | * Suporte a autenticação Kerberos;
 |  |
|  | * Deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
 |  |
|  | * Quando integrado ao Microsoft Active Directory, deve permitir identificar usuários dentro de grupos, mesmo que estejam em um uma hierarquia de grupo dentro de grupo.
 |  |
|  | * Deve possuir suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso;
 |  |
|  | * Deve permitir a atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos.
 |  |
|  | **QoS** | **-** |
|  | * Com a finalidade de controlar aplicações e tráfego, cujo consumo possa ser excessivo (como youtube, ustream, etc) e ter um alto consumo de largura de banda, a solução deve, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por aplicação, tanto de áudio como de vídeo streaming;
 |  |
|  | * Deve suportar a funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo;
 |  |
|  | * Suportar a criação de políticas de QoS por:
 | **-** |
|  | * + Por usuário e grupo do LDAP/AD;
 |  |
|  | * + Por aplicações (traffic shaping);
 |  |
|  | * + Por interface física ou lógica do equipamento;
 |  |
|  | * Suportar priorização de protocolos de voz e video como H.323, SIP, SCCP, MGCP e aplicações como Skype;
 |  |
|  | * Deve suportar conformação de tráfego com pelo menos os seguintes métodos: Traffic Policing e Traffic Shaping;
 |  |
|  | * Deve implementar classificação de tráfego com no campo DSCP;
 |  |
|  | * Implementar a marcação e priorização do tráfego previamente classificado com base no campo DSCP;
 |  |
|  | **VPN** | **-** |
|  | * Deve implementar VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke.
 |  |
|  | * Deve permitir o estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais.
 |  |
|  | * Deve implementar IKEv1 e IKEv2;
 |  |
|  | * Deve oferecer suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES-256;
 |  |
|  | * Deve oferecer suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512;
 |  |
|  | **Filtro de URLs** | **-** |
|  | * Deve implementar a funcionalidade de filtro de URL HTTP e HTTPS.
 |  |
|  | * Deve implementar a funcionalidade de filtro de conteúdo HTTP.
 |  |
|  | * Deve implementar a funcionalidade de SSL Scanner.
 |  |
|  | * Deve ter funcionalidade de proxy transparente HTTP/HTTPS (situação em que o cliente não precisa encaminhar o tráfego para o IP do proxy e não há instalação de cliente). No modo proxy transparente o cliente acreditar estar acessando diretamente o conteúdo desejado.
 |  |
|  | * Deve implementar a funcionalidade de cache de dados.
 |  |
|  | * Deve bloquear as tentativas de acesso proibidas pela política antes que ocorra o carregamento da página solicitada, exibindo mensagem customizada para o bloqueio.
 |  |
|  | * Deve garantir o monitoramento do tráfego internet independente de plataforma, sistema operacional ou aplicação utilizada pelos usuários.
 |  |
|  | * Não deve instalar nem executar agentes, módulos ou scripts nas estações de trabalho para prover qualquer serviço. Deve ser transparente ao usuário final.
 |  |
|  | * Controle de acesso à Internet
 | **-** |
|  | * + As regras de acesso à Internet devem se basear tanto na requisição quanto na resposta HTTP;
 |  |
|  | * + Deve permitir a criação de regras baseadas em horário do dia;
 |  |
|  | * + Deve possuir controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo;
 |  |
|  | * + Deve possuir controle de acesso à Internet por domínio, exemplo: gov.br, org.br;
 |  |
|  | * + Deve possuir controle de acesso à Internet por categorias de sites web;
 |  |
|  | * + Deve possuir controle de acesso à Internet por lista de sites web proibidos (blacklist) customizável;
 |  |
|  | * + Deve possuir controle de acesso à Internet por lista de sites web permitidos (whitelist) customizável;
 |  |
|  | * + Deve possuir mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos tipo malwares ou spywares;
 |  |
|  | * + O serviço deve possuir mecanismo automático para detecção de tráfego tunelado na porta 80;
 |  |
|  | * + Deve permitir que as páginas de erro e bloqueio sejam customizáveis;
 |  |
|  | * + Deve possuir compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca;
 |  |
|  | * + Deve permitir a definição e aplicação das regras por meio de expressões regulares;
 |  |
|  | * + Deve permitir a liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site www.facebook.com ou postagem no site www.twitter.com;
 |  |
|  | * Categorização de sites web
 | **-** |
|  | * + Deve conter base com no mínimo 15 (quinze) milhões de URL´s cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas;
 |  |
|  | * + Deve permitir a classificação/categorização de sites de acordo com o assunto;
 |  |
|  | * + Deve possuir no mínimo as seguintes categorias (ou similares): pornografia, nudez, sites maliciosos, webmail, blog/fotolog, jogos, hacking, racismo, comunidades virtuais, radio e tv, streaming, instant messaging, chat, sites de download, storage online, P2P, medias sociais, sites maliciosos e acesso remoto;
 |  |
|  | * + Deve possibilitar que URLs não cadastradas possam ser enviadas ao fabricante para a devida categorização;
 |  |
|  | * + Deve permitir à CONTRATANTE reclassificar, a seu critério, os registros de site web que julgar necessários.
 |  |
|  | * Atualização da base de sites
 | **-** |
|  | * + Durante o período de prestação do serviço a base de sites web deve ser atualizada automaticamente pela solução, via Internet. A periodicidade de atualização deve ser customizável. Essa atualização pode ser feita pela Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo;
 |  |
|  | * + A atualização da base de sites web deve transcorrer de forma transparente, sem comprometer a execução dos serviços;
 |  |
|  | * + A ausência de atualização da base de sites web, por qualquer motivo, não deve interromper nem comprometer funcionalidades da solução;
 |  |
|  | * + Durante o período de prestação do serviço, os sites web devem ser atualizados, sempre na categoria que reflita o seu conteúdo mais recente, ou seja, em caso de modificação, deve ser reclassificado para a categoria pertinente;
 |  |
|  | * + Durante o período de prestação do serviço, sites web de phishing, spyware ou que tenham sido usados para hospedar códigos maliciosos, devem retornar à categoria original depois de “descontaminados”;
 |  |
|  | **Características específicas do Item 55 - Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 1** | **-** |
|  | Além das interfaces utilizadas para o link MPLS e para o link internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas na rede interna da CONTRATANTE. |  |
|  | O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 70 Mbps (setenta megabits por segundo). |  |
|  | O throughtput de VPN, deve ser maior do que 70 Mbps (setenta megabits por segundo). |  |
|  | O throughtput de IPS, deve ser maior do que 70 Mbps (setenta megabits por segundo). |  |
|  | Deverá suportar no mínimo 50.000 (cinquenta mil) sessões de firewall simultâneas. |  |
|  | **Características específicas do item 56 - Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 2** | **-** |
|  | Além das interfaces utilizadas para o link MPLS e para o link internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas na rede interna da CONTRATANTE. |  |
|  | O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 90 Mbps (noventa megabits por segundo). |  |
|  | O throughtput de VPN, deve ser maior do que 90 Mbps (noventa megabits por segundo). |  |
|  | O throughtput de IPS, deve ser maior do que 90 Mbps (noventa megabits por segundo). |  |
|  | Deverá suportar no mínimo 60.000 (sessenta mil) sessões de firewall simultâneas. |  |
|  | **Características específicas do item 57 - Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 3** | **-** |
|  | Além das interfaces utilizadas para o link MPLS e para o link internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T), que serão utilizadas na rede interna da CONTRATANTE. |  |
|  | O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 150 Mbps (cento e cinquenta megabits por segundo). |  |
|  | O throughtput de VPN, deve ser maior do que 150 Mbps (cento e cinquenta megabits por segundo). |  |
|  | O throughtput de IPS, deve ser maior do que 150 Mbps (cento e cinquenta megabits por segundo). |  |
|  | Deverá suportar no mínimo 80.000 (oitenta mil) sessões de firewall simultâneas. |  |
|  | **Características específicas do item 58 - Appliance de Firewall/Filtro de Conteúdo - Sede** | **-** |
|  | As características abaixo se referem a 1 (uma) unidade do appliance. | **-** |
|  | Além das interfaces utilizadas para gerência e para funcionamento do cluster deve possuir pelo menos 8 (oito) interfaces GigabitEthernet (10/100/1000Base-T e 4 (quatro) interfaces 10GigabitEthernet 10Gbase-SR, que serão utilizadas na rede interna da CONTRATANTE. |  |
|  | Deve ter no mínimo 2 (duas) fontes de alimentação; |  |
|  | Deve suportar a configuração em alta disponibilidade ativo/passivo e ativo/ativo e em caso de falha em um dos nós, o remanescente deverá assumir o controle automaticamente, mantendo as sessões correntes ativas; |  |
|  | O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 5.8 Gbps (seis gigabits por segundo). |  |
|  | O throughtput de VPN, deve ser maior do que 6 Gbps (seis gigabits por segundo). |  |
|  | O throughtput de IPS, deve ser maior do que 6 Gbps (seis gigabits por segundo). |  |
|  | Deverá suportar no mínimo 2.000.000 (dois milhões) de sessões de firewall simultâneas. |  |
|  | **Prevenção de ameaças** | **-** |
|  | * Deve-se sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.
 |  |
|  | **Identificação de usuários** | **-** |
|  | * 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 (portal captivo);
 |  |
|  | * Deve implementar funcionalidade que possibilite analisar as informações de accounting do Microsoft NPS para permitir a identificação de usuários, como RSSO, Radius Accounting ou similar;
 |  |
|  | * Deve suportar a identificação de usuários via certificados digitais ICP-Brasil para conexões a serviços via SSL VPN.
 |  |
|  | **VPN** | **-** |
|  | * Suportar VPN client-to-site;
 |  |
|  | * Suportar IPSec VPN, com suporte a AES e autenticação via certificado IKE PKI;
 |  |
|  | * Suportar SSL VPN com as seguintes funcionalidades:
 | **-** |
|  | * + Que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
 |  |
|  | * + Que as funcionalidades de VPN SSL sejam atendidas sem o uso de cliente;
 |  |
|  | * + Atribuição de endereço IP nos clientes remotos de VPN;
 |  |
|  | * + Atribuição de DNS nos clientes remotos de VPN;
 |  |
|  | * + Criar políticas de controle de aplicações, IPS, para trafego dos clientes remotos conectados na VPN SSL;
 |  |
|  | * + Suportar autenticação via AD/LDAP, Secure id, certificado padrão ICP-Brasil e base de usuários local;
 |  |
|  | * + Permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
 |  |
|  | * + Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos tuneis SSL;
 |  |
|  | * + O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows Vista Windows 7, Windows 8 e Mac Osx;
 |  |
|  | * + A solução de segurança entregue deverá suportar e estar licenciada para pelo menos 2.000 (duas mil) conexões remotas simultaneas VPN SSL.
 |  |
|  | **Filtro de URLs** | **-** |
|  | * Deve permitir os segmentos de rede funcionem de maneira diferente, com pelo menos as seguintes possibilidades: proxy explicito, proxy transparente, portal captivo.
 |  |
|  | **Item 59 - Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo** | **-** |
|  | Deve centralizar a administração de regras, políticas e geração de relatórios dos appliances de firewall/filtro de conteúdo, usando uma única interface de gerenciamento. |  |
|  | Deve ser disponibilizado em hardware próprio ou em servidor x86 com a capacidade adequada. Será permitida a utilização de solução de virtualização. |  |
|  | Pode ser disponibilizada no ambiente da CONTRATADA, com acesso pela rede MPLS. |  |
|  | **Deve permitir/possuir** | **-** |
|  | * Acesso via cliente para Windows ou WEB (HTTPS);
 |  |
|  | * Autenticações integrada ao Microsoft Active Directory ou servidor Radius;
 |  |
|  | * Permitir a criação de grupos de dispositivos com a possibilidade de aplicar a mesma política em vários dispositivos de forma simultânea;
 |  |
|  | * Inspeção de logs com a possibilidade de exportar tais registros em formato CSV;
 |  |
|  | * Armazenamento de logs com capacidade de acesso instantâneo e capacidade de rotacionar tais registros;
 |  |
|  | * Busca de objetos como: regras, hosts, redes, aplicações;
 |  |
|  | * Definições de perfis de acesso a console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
 |  |
|  | * Localização de em quais regras um endereço IP, IP Range, rede ou objetos estão sendo utilizados;
 |  |
|  | * Contador ou gráfico de matchs das regras;
 |  |
|  | * Contador ou gráfico de volume trafegado por cada regra;
 |  |
|  | * Backup das configurações com versionamento e aplicação de rollback para uma versão anterior;
 |  |
|  | * A visualização e comparação das configurações atuais de um appliance com configurações anteriores;
 |  |
|  | * A atualização de sistema operacional dos appliances bem como o rollback em caso de falha;
 |  |
|  | * A integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
 |  |
|  | * 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;
 |  |
|  | * Relatórios de utilização dos recursos por aplicações, URL e ameaças;
 |  |
|  | * Visualização sumarizada de todas as aplicações, ameaças e URLs que trafegaram pelos appliances;
 |  |
|  | * Cliente NTP, contemplando suporte à autenticação entre os peers;
 |  |
|  | * Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;
 |  |
|  | **Exibição das seguintes informações, de forma histórica:** | **-** |
|  | * Situação dos appliances individuais e do cluster;
 |  |
|  | * Principais aplicações;
 |  |
|  | * Principais aplicações por risco;
 |  |
|  | * Administradores autenticados na gerencia da plataforma de segurança;
 |  |
|  | * Número de sessões simultâneas;
 |  |
|  | * Status das interfaces;
 |  |
|  | * Utilização das interfaces;
 |  |
|  | * Erros das interfaces;
 |  |
|  | * Uso de CPU;
 |  |
|  | * Memória RAM;
 |  |
|  | **Deve permitir visualizar as seguintes tabelas de informação (via dashboard ou linha de comando) para cada appliance e cluster** | **-** |
|  | * MAC;
 |  |
|  | * ARP;
 |  |
|  | * De roteamento unicast, informando como a rota foi aprendida bem como qual é o próximo salto;
 |  |
|  | * De roteamento multicast, informando a origem e o status de cada grupo bem como a quantidade de pacotes encaminhados;
 |  |
|  | * O status de um dado link de dados (para a funcionalidade de balanceamento de ISP).
 |  |
|  | **Registro de informações de filtro de URLs** | **-** |
|  | * Deverá manter os registros de conexão para o envio e recebimento de pacotes de dados com pelo menos os seguintes dados: data e hora de início e término, sua duração, usuário (quando houver identificação), o endereço IP de origem, URL de destino da requisição, categoria do site, tamanho do objeto solicitado (em bytes) e ação tomada pela solução (bloqueado, permitido);
 |  |
|  | * Deverá ser capaz de reter dados e logs nos modos on-line e off-line, em que:
 |  |
|  | * No modo on-line, os dados deverão ser mantidos disponíveis para consulta imediata por um período mínimo de 90 (noventa) dias;
 |  |
|  | * No modo off-line, os dados deverão ser arquivados na solução de backup da CONTRATANTE, sem acesso direto pela solução de gerência, e que precisam ser restaurados e reativados para consulta, disponíveis para consulta imediata por um período mínimo de 1 (um) ano;
 |  |
|  | **Geração de, no mínimo, os seguintes relatórios:** | **-** |
|  | * Resumo gráfico de aplicações utilizadas;
 |  |
|  | * Principais aplicações por utilização de largura de banda de entrada e saída;
 |  |
|  | * Principais aplicações por taxa de transferência de bytes;
 |  |
|  | * Principais hosts por número de ameaças identificadas;
 |  |
|  | * Atividades de um usuário especifico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças, de rede vinculadas a este tráfego.
 |  |
|  | * Relatórios de filtro de URLs
 | **-** |
|  | * + Deve disponibilizar ferramenta para geração de relatórios, fornecendo informações gerenciais a partir dos logs gerados, permitindo a extração de informações detalhadas sobre usuários, sites e categorias acessadas, rede de origem, IP de origem, grupos de usuários, protocolos e tempo de navegação;
 |  |
|  | * + Deve permitir a geração de relatório com a quantidade de acessos autorizados, bem como a quantidade de bytes trafegados, permitindo a visualização por usuário, grupo de usuário, IP de origem, aplicação e URL completa acessada;
 |  |
|  | * + Deve possuir templates com pelos menos os seguintes relatórios:
 |  |
|  | * + - Lista de usuários com maior número de acessos;
 |  |
|  | * + - Lista de usuários que geraram maior volume trafegado;
 |  |
|  | * + - Lista de sites com maior número de acessos, incluindo detalhamento por usuário dos 2 (dois) sites com maior número de acessos;
 |  |
|  | * + - Lista de sites que geraram maior volume trafegado, incluindo detalhamento por usuário dos 2 (dois) sites com maior volume trafegado;
 |  |
|  | * + - Lista de categorias com maior número de acessos;
 |  |
|  | * + - Lista de categorias que geraram maior volume trafegado;
 |  |
|  | * + - Lista de sites bloqueados com maior número de tentativa de acessos;
 |  |
|  | * + - Lista de sites maliciosos com maior número de tentativa de acessos;
 |  |
|  | * + Deve exportar relatórios para, no mínimo, os formatos PDF ou CSV;
 |  |
|  | * + Deve possibilitar a automatização no envio a usuários pré-definidos ou publicação de relatórios;
 |  |
|  | **Item 60 - Solução de Netflow** | **-** |
|  | Software e/ou ferramenta e/ou funcionalidade de gerenciamento capaz de receber e analisar tráfego dos roteadores e appliances de firewall/filtro de conteúdo utilizando Netflow, IPFIX ou similar. |  |
|  | A solução de netflow pode estar disponibilizada no ambiente da CONTRATADA, com acesso pela rede MPLS. |  |
|  | A solução deve ser dimensionada para suportar o tráfego de todos os links MPLS desta especificação técnica. |  |
|  | Deve ser capaz de agrupar os tráfegos em aplicações utilizando pelo menos os seguintes critérios, redes de origem/destino, protocolo da camada de transporte, lista de porta de origem/destino da camada de transporte. Deve ser possível visualizar gráficos de cada link separando o tráfego com base nas aplicações em cores diferentes. Deve ser possível atualizar o gráfico omitindo/mostrando cada uma das aplicações.  |  |
|  | Deve ser capaz de agrupar os tráfegos em classes de QoS. Deve ser possível visualizar gráficos de cada link separando o tráfego com base nas classes de Qos com em cores diferentes. Deve ser possível atualizar o gráfico omitindo/mostrando cada uma das classes de QoS. |  |
|  | Deve permitir o agrupamento de interfaces de hosts diferentes, formando uma interface agregada para fins de detalhamento de tráfego.  |  |
|  | Deve presentar em gráficos separados o tráfego de entrada e de saída de cada link. |  |
|  | Deve permitir a elaboração de relatórios dos fluxos de comunicação em que deve ser possível verificar IP de origem e destino, protocolo da camada de transporte, porta de origem e destino da camada de transporte.  |  |
|  | Deve ter capacidade suficiente para o armazenamento de histórico de pelo menos 1 (um) dos seguintes requisitos: 1 (um) TB de dados ou 6 (seis) meses de informações. |  |
|  | **Características específicas dos itens 61 e 67 - Link Internet – Sede** | **-** |
|  | **A taxa de transmissão deve variar conforme os valores abaixo descritos:** | **-** |
|  | * 150 Mbps (cento e cinquenta megabits por segundo);
 | **-** |
|  | * 200 Mbps (duzentos megabits por segundo);
 | **-** |
|  | * 250 Mbps (duzentos e cinquenta megabits por segundo);
 | **-** |
|  | * 300 Mbps (trezentos megabits por segundo);
 | **-** |
|  | * 350 Mbps (trezentos e cinquenta por segundo).
 | **-** |
|  | **Anti-DDOoS (Distributed Denial of Service)** | **-** |
|  | * Solução integrada ao backbone da CONTRATADA que deve proteger 100% (cem por cento) do tráfego de entrada do link internet;
 |  |
|  | * A proteção suportará Flash Crowd, ou seja, quando ocorrer o crescimento do volume de tráfego legítimo acima do esperado (perfil de tráfego/baseline), a solução será capaz de diferenciar o tráfego legítimo do malicioso, bloqueando apenas o tráfego proveniente de ataques;
 |  |
|  | * A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.
 |  |
|  | * A solução deve suportar a mitigação automática de ataques, incluindo, mas não se restringindo as seguintes técnicas:
 |  |
|  | * + Whitelists;
 |  |
|  | * + Blacklists;
 |  |
|  | * + Limitação de taxa;
 |  |
|  | * + Técnicas desafio-resposta;
 |  |
|  | * + Descarte de pacotes mal formados;
 |  |
|  | * + Técnicas de mitigação de ataques aos protocolos HTTP e DNS;
 |  |
|  | * + Bloqueio por localização geográfica de endereços IP;
 |  |
|  | * + Lista dinâmica de endereços bloqueados. Os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA devem ser removidos da referida lista.
 |  |
|  | * A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede para IPv4, incluindo, mas não se restringindo aos seguintes:
 |  |
|  | * + Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
 |  |
|  | * + Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
 |  |
|  | * + Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
 |  |
|  | * + Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);
 |  |
|  | * + Quanto a ataques à camada de aplicação, para os protocolos HTTP e DNS, a solução deve manter uma lista dinâmica de endereços IP bloqueados.
 |  |
|  | * A CONTRATADA deve possuir, no mínimo, 2 (dois) centros de limpeza, cada um com capacidade de mitigação de ataques. Dos centros de limpeza, pelo menos um deverá estar em território nacional e pelo um deverá estar no exterior. Para a mitigação dos ataques de origem no território brasileiro não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.
 |  |
|  | * A CONTRATADA deverá prover o serviço de mitigação sem limitação de duração, volume de tráfego, quantidade de pacotes, ataques nacionais ou internacionais, quantidade de eventos, requisições por segundo, intervalos entre os ataques.
 |  |
|  | * As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.
 |  |
|  | * Em momentos de ataques DoS e DDoS, todo trafego limpo deve ser reencaminhado para a CONTRATANTE.
 |  |
|  | * Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de bordas.
 |  |
|  | * A mitigação de ataques deve iniciar no prazo máximo de 15 (quinze) minutos após sua detecção.
 |  |
|  | **Topologia e roteamento** | **-** |
|  | * O serviço deverá ser fornecido com suporte a MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6.
 |  |
|  | * A rede de trânsito entre os roteadores internet e o cluster de appliances de firewall/filtro de conteúdo da sede utilizará endereçamento IPv4 e IPv6 pertencentes ao AS da CONTRATANTE.
 |  |
|  | * A CONTRATADA deverá divulgar o AS (16 bits) e os blocos de endereços IPv4 e IPv6 da CONTRATANTE que serão divulgados pelos CPEs. Deve permitir a divulgação de blocos IPv4 /22, /23 e /24 e blocos IPv6 /44 e /48.
 |  |
|  | * A CONTRATADA deverá disponibilizar o seguinte conjunto de endereços:
 | **-** |
|  | * + 1 (um) endereço IPv4 (/32) para a interface de Loopback do CPE;
 | **-** |
|  | * + 1 (um) endereço IPv6 (/128) para a interface de Loopback do CPE;
 | **-** |
|  | * + 1 (um) bloco IPv4 /30 (ou /31) para o Link ponto-a-ponto da interface WAN;
 | **-** |
|  | * + 1 (um) bloco IPv6 /64 ou /127 para o Link ponto-a-ponto da interface WAN.
 | **-** |
|  | * A vizinhança iBGP (IPv4 e IPv6) entre os dois CPEs bem como a vizinhança eBGP (IPv4 e IPv6) entre cada CPE e o PE da CONTRATADA devem ser estabelecidas utilizando os seguintes requisitos:
 |  |
|  | * + Interfaces de loopback;
 |  |
|  | * + TTL-Security habilitado;
 |  |
|  | * + Autenticação MD5;
 |  |
|  | * + Fornecimento de tabela parcial (partial routing) e tabela completa (full routing) para IPv4. A CONTRATANTE poderá optar pela tabela parcial ou tabela completa conforme solicitação. A tabela parcial deve incluir seleção definida pela CONTRATADA que inclua os ASes nacionais e internacionais com maior interesse de tráfego.
 |  |
|  | * + A tabela partial deve conter no mínimo os principais ASes dos seguintes serviços de CDN, nuvem e provedores de conteúdo: Akamai, Amazon, Facebook, IBM, Google, Microsoft, Oracle, Rackspace, SoftLayer, Youtube. Por principais ASes entende-se aqueles da Europa e América, não havendo necessidade de prever ASes da Africa, Ásia e Oceania.
 |  |
|  | * + Caso a tabela de parcial da CONTRATADA não forneça os ASes solicitados pela CONTRATANTE, será permitido o fornecimento da tabela completa (full routing) IPv4 desde que seja possível limitar as rotas a serem inseridas na tabela de roteamento com base no tamanho do AS Path a ser definido pela CONTRATANTE.
 |  |
|  | * + Fornecimento de tabela completa IPv6 (full routing).
 |  |
|  | * A CONTRATADA deverá disponibilizar à CONTRATANTE a possibilidade de “negação de tráfego” à CONTRATANTE através de uso de uma community BGP de “blackhole/sinkhole” (buraconegro/vertedouro) em anúncio BGP da CONTRATANTE.
 |  |
|  | * Deverão ser aceitos para o efeito de “blackhole”, em IPv4: prefixos com tamanhos /24 e /32.
 |  |
|  | * Deverão ser aceitos para o efeito de “blackhole”, em IPv6: prefixos com tamanhos /32, /48, /56, /64 e /128.
 |  |
|  | **Itens 62 e 68 - Roteador Internet - Sede** | **-** |
|  | As características abaixo se referem a 1 (uma) unidade do roteador. | **-** |
|  | Além da interface utilizada para o link Internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas pela CONTRATANTE. |  |
|  | Deve ter no mínimo 2 (duas) fontes de alimentação. |  |
|  | Possuir capacidade de comutação agregada igual ou superior à 2,5 Gbps (dois vírgula cinco gigabits por segundo) |  |
|  | Possuir capacidade de encaminhamento igual ou superior a 4 Mpps (quatro milhões de pacotes por segundo). |  |
|  | Possuir capacidade de memória RAM no processador central de no mínimo 1 GB (um gigabyte). |  |
|  | Possuir capacidade para 1.000.000 (um milhão) de prefixos IPv4 (FIB). |  |
|  | Possuir capacidade para 250.000 (duzentos e cinquenta mil) prefixos IPv6 (FIB). |  |
|  | **Devem suportar os seguintes protocolos/funcionalidades:** | **-** |
|  | * O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;
 |  |
|  | * Implementar RFC 3768 VRRP;
 |  |
|  | * OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;
 |  |
|  | * Cliente NTP, contemplando suporte à autenticação entre os peers, conforme definido na RFC 1305. Deve possibilitar a especificação da interface de origem dos pacotes NTP;
 |  |
|  | * Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;
 |  |
|  | * Capacidade de geração e armazenamento de logs locais;
 |  |
|  | * Protocolo Syslog com a possibilidade de envio de timestamp baseado no relógio do roteador;
 |  |
|  | * Protocolo IP SLA ou similar, ou sejam deve ser capaz de responder a pacotes de simulação de tráfegos. Devem ser suportados, no mínimo, os protocolos ICMP, TCP e UDP. Os dados referentes aos tráfegos simulados devem ser disponibilizados via SNMP;
 |  |
|  | * Implementar ACLs com pelo menos os seguintes parâmetros;
 | **-** |
|  | * + Endereços IP de host ou rede, de pacotes Ipv4 e Ipv6 (tanto de origem quanto de destino);
 |  |
|  | * + Tipos de pacote ICMP;
 |  |
|  | * + Portas e faixas de portas dos protocolos TCP e UDP (tanto de origem quanto de destino);
 |  |
|  | * + Deve permitir criar regras com base em hora do dia e com base nos dias da semana;
 |  |
|  | * Protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, IPFIX ou similar, contemplando no mínimo as seguintes informações:
 |  |
|  | * + IP de origem/destino;
 |  |
|  | * + Parâmetro “protocol type” do cabeçalho IP;
 |  |
|  | * + Porta TCP/UDP de origem/destino;
 |  |
|  | * + Campo TOS ou DSCP do cabeçalho IP;
 |  |
|  | * + Interface do equipamento em que o tráfego foi identificado;
 |  |
|  | * + A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo padrão de mercado para este fim;
 |  |
|  | * BGP
 | **-** |
|  | * + Implementar RFC 4271 BGPv4.
 |  |
|  | * + Implementar RFC 1997 Communities and Attributes.
 |  |
|  | * + Implementar RFC 4360 BGP Extended Communities Attribute.
 |  |
|  | * + Implementar RFC 2918 Route Refresh Capability.
 |  |
|  | * + Implementar RFC 2385 BGP Session Protection via TCP MD5.
 |  |
|  | * + Implementar Generalized TTL Security Mechanism (GTSM).
 |  |
|  | * + Implementar RFC 4893 BGP Support for Four-octet AS Number Space.
 |  |
|  | * + Implementar Outbound Route Filtering Capability for BGP-4.
 |  |
|  | * + Implementar RFC 2858 Multiprotocol Extensions for BGP-4.
 |  |
|  | * + Implementar RFC 4724 Graceful Restart Mechanism for BGP.
 |  |
|  | * + Implementar definição de políticas de controle dos anúncios BGP.
 |  |
|  | * + Implementar aplicação de expressões regulares para filtragem de anúncios
 |  |
|  | **Item 63 - Serviço de Mudança de Endereço** | **-** |
|  | Qualquer unidade poderá ter sua localização alterada, dentro dos limites de cada município. | **-** |
|  | A instalação física e lógica do canal de comunicação no novo endereço deverá ser realizada em até 60 (sessenta) dias corridos, a contar da emissão da ordem de serviço pela CONTRATANTE; | **-** |
|  | ­ Todas as ações de funcionários da CONTRATADA dentro das dependências das Unidades da CONTRATANTE deverão ser executadas na presença do responsável da CONTRATANTE ou representantes por ela estabelecidos. | **-** |
|  |  A CONTRATANTE informará à CONTRADA exata em que a mudança do circuito deve ser realizada com pelo menos 3 (três) dias úteis de antecedência.  | **-** |
|  | A mudança poderá ocorrer em dias não úteis sem que haja qualquer custo adicional para a CONTRATANTE.  | **-** |
|  | **Item 64 - Implantação solução - Lote 1** | **-** |
|  | Deverão ser apropriados neste contratado todos os custos para a implantação de infraestrutura dos itens 1 a 62 como: lançamento de fibras, construção de dutos, mão de obra para instalar e configurar os equipamentos, dentre outros custos existentes apenas na fase de instalação. | **-** |
|  | Não deverão ser apropriados neste item os custos referentes aos equipamentos utilizados exclusivamente no provimento do serviço e que serão discriminados nos itens 28, 55 a 60 e 62. | **-** |
|  | Não deverão ser apropriados neste item os custos referentes aos repasses de conhecimento e que serão discriminados nos itens 65 e 66. | **-** |
|  | **Item 65 - Repasse de Conhecimento - Solução Firewall/Filtro de Conteúdo** | **-** |
|  | A prestação do serviço de transferência de conhecimento deverá observar o disposto no Anexo III - ESPECIFICAÇÃO DOS SERVIÇOS DE TRANSFERENCIA DE CONHECIMENTO. | **-** |
|  | **Deve abordar pelo menos os seguintes tópicos:** | **-** |
|  | * Conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;
 | **-** |
|  | * Compreensão geral da filosofia de funcionamento e de operação da solução adotada;
 | **-** |
|  | * Criação de grupos de dispositivos para aplicação de configurações em lote;
 | **-** |
|  | * Criação/configuração e aplicação de regras com controle de aplicação;
 | **-** |
|  | * Criação/configuração e aplicação de regras com filtro de URL;
 | **-** |
|  | * Criação/configuração e aplicação de regras com SSL Inspection;
 | **-** |
|  | * Criação/configuração e aplicação de regras com NAT estático e dinâmico;
 | **-** |
|  | * Serviços de prevenção de ameaças;
 | **-** |
|  | * VPN site-to-site;
 | **-** |
|  | * SSL VPN;
 | **-** |
|  | * Verificação de logs;
 | **-** |
|  | * Backup e restauração de configuração;
 | **-** |
|  | * Geração de relatórios gerenciais.
 | **-** |
|  | **Itens 66 e 70 - Repasse de Conhecimento - Roteador Internet - Sede** | **-** |
|  | A prestação do serviço de transferência de conhecimento deverá observar o disposto no Anexo III - ESPECIFICAÇÃO DOS SERVIÇOS DE TRANSFERENCIA DE CONHECIMENTO. | **-** |
|  | **Deve abordar pelo menos os seguintes tópicos:** | **-** |
|  | * O Protocolo BGP e seus Pacotes;
 | **-** |
|  | * MP-BGP;
 | **-** |
|  | * Vizinhança BGP (IPv4/IPV6, autenticação, TTL e uso de loopback);
 | **-** |
|  | * iBGP e eBGP;
 | **-** |
|  | * Atributos do BGP (Origin, AS Path, Next Hop, MED, Local Preference, Weight, Aggregator e Community);
 | **-** |
|  | * Algoritmo para escolha do melhor caminho utilizado pelo BGP;
 | **-** |
|  | * Filtros de entrada e saída;
 | **-** |
|  | * Expressões regulares;
 | **-** |
|  | * Boas práticas de BGP para sistemas autônomos;
 | **-** |
|  | * Conectando a um IXP.
 | **-** |
|  | **Item 69 - Implantação solução - Lote 2** | **-** |
|  | Deverão ser apropriados neste contratado todos os custos para a implantação de infraestrutura do item 67 como: lançamento de fibras, construção de dutos, mão de obra para instalar e configurar os equipamentos, dentre outros custos existentes apenas na fase de instalação. | **-** |
|  | Não deverá ser apropriado neste item o custo referente ao equipamento utilizado no provimento do serviço e que será discriminado no item 68. | **-** |
|  | Não deverá ser apropriado neste item o custo referente ao repasse de conhecimento e que será discriminado no item 70. | **-** |