ADEQUAÇÃO ESCOPO TÉCNICO
INFOVIA 3.0

ENCARTE TÉCNICO I
REDE IP GOVERNO

SUGESTÃO 01

ENCARTE TÉCNICO I - O ITEM 4.1 – pág 07 – define o seguinte:

> *"4. ESPECIFICAÇÕES BÁSICAS DA REDE IP MPLS e SD-WAN*
> *4.1. A Rede IP MPLS ou SD-WAN a ser contratada através do PRODERJ deverá permitir a riação de múltiplas redes virtuais (VRFs), sendo que a cada VRF deverá ser logicamente do tipo "Full Mesh", permitindo que os sites pertencentes a uma mesma VRF, se comuniquem entre si, sem a necessidade de comutação através de um nó central;"*

Justificativa: Considerando que características como "VRFs" e comunicação "Full Mesh" são atributos intrínsecos de uma solução MPLS e que estes atributos não se aplicam a uma solução SD-WAN, onde as remotas remotas se comunicam com a concentradora através de túneis, tendo assim uma comunicação Hub and Spoke, sugerimos a redação abaixo:

Sugestão: *"4. ESPECIFICAÇÕES BÁSICAS DA REDE IP MPLS e SD-WAN*
4.1. A Rede IP MPLS a ser contratada através do PRODERJ deverá permitir a criação de múltiplas redes virtuais (VRFs), sendo que a cada VRF deverá ser logicamente do tipo "Full Mesh", permitindo que os sites pertencentes a uma mesma VRF, se comuniquem entre si, sem a necessidade de comutação através de um nó central;"

SUGESTÃO 02

ENCARTE TÉCNICO I - ITEM 4.4 – pág 07 e o ITEM 22.1 – pág 65 – solicitam o seguinte:

> *"4.4. Os meios de acessos para conexão dos sites à rede, última milha, deverão dar-se preferencialmente através de fibra ótica e par metálico. Será permitida a utilização de enlaces de rede em tecnologias alternativas desde que obedecendo aos critérios de desempenho estabelecidos neste projeto, principalmente o especificado no item 22 e todos os seus subitens;"*

> *"22.1. Será permitida a utilização de links de tecnologias alternativas, como, por exemplo, radiofrequência, satélite, links dedicados (ponto-a-ponto, L2VPN), ADSL, 4G, WiMax. Desde que sejam devidamente integrados à Rede IP Governo, preservando todos os requisitos de desempenho, disponibilidade e segurança definidos no Termo de Referência e este Encarte Técnico;"*

Justificativa: Ao se avaliar os meios de acessos WiMax, 4G e WiFi constata-se que para uma solução de integração entre sites e para interoperabilidade de solução de rede WAN para Governo do Rio de janeiro, é um meio de acesso fragilizado, ou seja, suscetíveis a interferências dado que nestas topologias, cada canal é utilizado por mais de um assinante (pessoa física e jurídica), sendo assim a frequência de transmissão é compartilhada por mais de um sinal. Soluções como estas também estão suscetíveis a interferências físicas e climáticas. Além dos itens citados, temos também uma assimetria na transmissão dos dados, não tendo o cliente final uma banda garantida mediante ao escopo final contratado.

Sendo assim sugerimos a redação abaixo:

Sugestão: *"4.4. Os meios de acessos para conexão dos sites à rede, última milha, deverão dar-se preferencialmente através de fibra ótica e par metálico. Será permitida a utilização de enlaces de rede em tecnologias alternativas desde que obedecendo aos critérios de desempenho estabelecidos neste projeto, principalmente o especificado no item 22 e todos os seus subitens;"*

Sugestão: *"22.1. Será permitida a utilização de links de tecnologias alternativas, como, por exemplo, Radiofrequência licenciada, satélite, links dedicados (ponto-a-ponto, L2VPN) e ADSL. Desde que sejam devidamente integrados à Rede IP Governo, preservando todos os requisitos de desempenho, disponibilidade e segurança definidos no Termo de Referência e este Encarte Técnico;"*

SUGESTÃO 03

ENCARTE TÉCNICO I - O ITEM 4.6 – pág 08, ITEM 8.1 – pág 11 e ITEM 9.1.12 – pág 20 – informam o seguinte:

> *""4.6. O hardware dos roteadores fornecidos (CPEs e Centrais) deverá suportar o funcionamento tanto na Rede IP MPLS como na Rede SD-WAN. Caso necessário será permitida apenas a atualização do software dos mesmos para funcionamento em cada uma das Redes;;"*
>
> *"8.1. Atenderem totalmente aos recursos solicitados, apresentando total compatibilidade e interoperabilidade, evitando-se problemas futuros na Rede do Governo, deste modo devendo ser do mesmo fabricante;"*
>
> *"9.1.12. Desempenho – Rede SD-WAN:*
> *9.1.12.1. Deve ser fornecido com capacidade de no mínimo 10 (dez) Gbps de criptografia;"*

Justificativa: Levando-se em conta o Princípio da Isonomia das licitações e por conseguinte buscar uma solução mais vantajosa para a administração pública do Governo do RJ, sugerimos que os equipamentos que estejam na solução MPLS, não necessariamente deverão ter uma solução de SD-WAN embarcada, possibilitando assim um investimento desnecessário que implicará maiores custos no certame. Seguindo o mesmo princípio para que tenhamos uma maior competitividade no certame, sugerimos retirar a obrigação da utilização de um mesmo fabricante para os CPEs do Datacenter e das remotas, segue sugestão de redação:

Sugestão: *Retirar o item 4.6, item 9.1.12 e item 9.1.12.1*

Sugestão: *"8.1. Atenderem totalmente aos recursos solicitados, apresentando total compatibilidade e interoperabilidade, evitando-se problemas futuros na Rede do Governo"*
";"

""9.1.12. Desempenho – Rede SD-WAN:
9.1.12.1. Deve ser fornecido com capacidade de no mínimo 10 (dez) Gbps de criptografia;;;"

SUGESTÃO 04

ENCARTE TÉCNICO I - O ITEM 10 – pág 36:

Justificativa: Visando uma maior competitividade no certame, sugerimos a redação abaixo com especificação técnica mínima para os roteadores da solução MPLS:

Sugestão:
TIPO I: circuitos com velocidades de até 20Mbps.
TIPO II: circuitos com velocidade de até 50Mbps.
TIPO III: circuitos com velocidade de até 300Mbps.
TIPO IV: circuitos com velocidade de até 4Gbps.

10.1. TIPO I
- *Deve possuir, no mínimo, 2 (duas) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.*
- *Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.*
- *Deve ter uma performance mínima de 280.000 pps com pacotes de 64 bytes.*
- *Deve implementar a opção local de carga do sistema do equipamento via memória Flash.*
- *Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.*
- *Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.*
- *Como uma opção de acesso alternativo, todos os CPE's devem suportar a adição de módulo que permita a conexão de dados através de rede celular 3G com as seguintes características:*
  - *Deve suportar as seguintes tecnologias e faixas de freqüência:*

HSPA: 850, 1900 e 2100 MHz
UMTS: 850, 1900 e 2100 MHz
EDGE: 850, 900, 1800 e 1900 MHz
GPRS: 850, 900, 1800 e 1900 MHz

CDMA 1xEV-DO Rev A: 800 e 1900 MHz
CDMA 1xEV-DO Rel 0
CDMA 1xRTT

  - *Deve permitir o uso de antenas externas ao módulo que possam ser instaladas distantes do CPE.*
  - *Deve permitir a monitoração de informações de rádio freqüência, da operação da interface e do tráfego através do protocolo.*
- *Caso o Fabricante possua mais de uma versão de uma mesma placa para atendimento a esta especificação, deverá ser fornecida a versão mais recente e estável da mesma.*
- *Deve suportar o protocolo HDLC (High-Level Data Link Control).*
- *Deve suportar o protocolo Frame Relay.*
- *Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame-Relay e PPP sobre Ethernet).*

- *Deve suportar, no mínimo, os padrões do Frame Relay Forum abaixo especificados ou superiores:*
- *FRF.16 – Multilink Frame Relay UNI/NNI Implementation Agreement.*
- *FRF.12 – Frame Relay Fragmentation Implementation Agreement.*
- *Deve suportar o protocolo roteável IP;*
- *Deve permitir a configuração de roteamento estático;*
- *Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:*
  - *RFC 1587 – The OSPF Not-So-Stubby Area (NSSA) Option;*
  - *RFC 1745 – BGP4/IDRP for IP --- OSPF Interaction;*
  - *RFC 1253 ou 1850 – OSPF Version 2 Management Information Base;*
  - *RFCs 2328 ou 2178 – OSPF Version 2;*
  - *RFC 2370 – The OSPF Opaque LSA Option;*
- *Deve suportar o protocolo de roteamento BGP versão 4, conforme os padrões RFCs especificados abaixo:*
  - *RFCs 1771 ou 1654 – A Border Gateway Protocol (BGP-4);*
  - *RFC 2796 – Autonomous System Confederation for BGP;*
  - *RFC 1997 – BGP Communities Attribute;*
  - *RFCs 2283 ou 2858 – Multi-Protocol Extensions for BGP-4;*
  - *RFC 2439 – BGP Route Flap Damping;*
  - *RFC 2842 – Capabilities Advertisement with BGP-4;*
  - *RFC 2918 – Route Refresh Capability for BGP-4;*
- *Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.*
- *Deve possuir suporte ao modo de operação full-duplex em todas as interfaces Ethernet.*
- *Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.*
- *Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 – The IP Network Address Translator (NAT) ou RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).*
- *Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT).*
- *Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338.*
- *Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode).*
- *Deve possuir suporte a implementação das funcionalidades de DHCP Relay.*
- *Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer 4.*
- *Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ).*
- *Deve suportar a funcionalidade de Policy-Based Routing (PBR).*
- *Deve possuir suporte a túneis de roteamento.*
- *Deve possuir suporte a Traffic Shapping.*
- *Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 2030 ou 4330 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, ou o protocolo NTP (Network Time Protocol).*
- *Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819 - Remote Network Monitoring Management Information Base.*
- *Deve implementar facilidades de syslog.*
- *Deve possuir suporte a autenticação de usuário através de RADIUS, em conformidade com, no mínimo, o padrão RFC 2865.*
- *Deve possuir suporte a autenticação de usuário através de TACACS em conformidade com, no mínimo, o padrão RFC 1492.*
- *Deve possuir suporte a protocolo de redirecionamento para cache de Web.*
- *Deve possuir suporte ao protocolo de gerenciamento SNMP e a MIB-II, em conformidade com as RFCs 1157 e 1213, respectivamente.*
- *Deve possuir suporte ao protocolo SNMPv2c.*
- *Deve possuir suporte ao protocolo SNMPv3.*

- *Deve implementar segurança baseada em, no mínimo, 2 (dois) níveis de acesso para a administração do equipamento.*
- *Deve fornecer suporte para prevenir fluxo de dados de entrada não autorizados através da configuração de filtros baseados em parâmetros de Layer 3 e Layer 4 do protocolo IP.*
- *Deve suportar a configuração de métodos de priorização de tráfego por tipo de protocolo e por serviços da pilha TCP/IP.*
- *Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol).*
- *Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508.*
- *Deve permitir administração e configuração através de interface de linha de comando (CLI).*
- *Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas.*
- *Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador.*
- *Deve ter a capacidade de atualização de software via FTP ou via TFTP, em conformidade com as RFCs 0783 ou 1350 – The TFTP Protocol (Revision 2).*
- *Deverá possuir suporte a técnicas de gerenciamento inteligente de energia, podendo desligar portas e módulos quando não utilizados para conservar energia.*
- *Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:*

o Digital Encryption Standard (DES) e Triple DES (3DES);

o Advanced Encryption Standard (AES) 128, 192, e 256 ;

o Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5_hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1_hmac ;

- *O equipamento deverá suportar, via licença adicional ou upgrade de software, no mínimo as seguintes funcionalidades:*

o Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol);

o Deve suportar a criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCS 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409;

o Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC;

o Deve suportar a criação de túneis VPN dinamicamente para criar uma rede VPN totalmente ligada.

10.2. TIPO II

- *Deve possuir, no mínimo, 3 (três) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.*
- *Deve suportar a inserção de interfaces analógicas (FXS ou FXO) e digitais de voz (E1).*
- *Deve suportar no mínimo 4 interfaces de Voz analógicas FXO.*
- *Deve suportar no mínimo dois slot(s) internos para a inserção de DSPs (Digital Signal Processor).*
- *Deve suportar os CODEC's (G.711, G.723.1, G.728, G.729 ou G.729b).*
- *Deve ter a possibilidade de ser inserido em redes com serviços de Voz sobre IP (VoIP), Voz sobre Frame Relay (VoFR) e Voz sobre ATM (VoATM).*
- *Deve suportar mecanismo de controle de chamadas IP sem a necessidade de um controlador central.*
- *Deve suportar mecanismo que permita a continuidade do controle de chamadas IP mesmo após a perda de comunicação com o controlador de chamadas central.*
- *Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.*
- *Deve ter uma performance mínima de 350.000 pps com pacotes de 64 bytes.*
- *Deve implementar a opção local de carga do sistema do equipamento via memória Flash.*
- *Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.*
- *Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.*
- *Como uma opção de acesso alternativo, deve suportar a adição de módulo que permita a conexão de dados através de rede celular 3G com as seguintes características:*

o Deve suportar as seguintes tecnologias e faixas de freqüência:

HSPA: 850, 1900 e 2100 MHz
UMTS: 850, 1900 e 2100 MHz
EDGE: 850, 900, 1800 e 1900 MHz
GPRS: 850, 900, 1800 e 1900 MHz

CDMA 1xEV-DO Rev A: 800 e 1900 MHz
CDMA 1xEV-DO Rel 0
CDMA 1xRTT
o Deve permitir o uso de antenas externas ao módulo que possam ser instaladas distantes do CPE.
o Deve permitir a monitoração de informações de rádio freqüência, da operação da interface e do tráfego através do protocolo.
• Deve suportar o protocolo HDLC (High-Level Data Link Control).
• Deve suportar o protocolo Frame Relay.
• Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame-Relay e PPP sobre Ethernet).
• Deve suportar, no mínimo, os padrões do Frame Relay Forum abaixo especificados ou superiores:
o FRF.16 – Multilink Frame Relay UNI/NNI Implementation Agreement;
o FRF.12 – Frame Relay Fragmentation Implementation Agreement;
• Deve suportar o protocolo roteável IP.
• Deve permitir a configuração de roteamento estático.
• Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:
o RFC 1587 – The OSPF Not-So-Stubby Area (NSSA) Option;
o RFC 1745 – BGP4/IDRP for IP --- OSPF Interaction;
o RFC 1253 ou 1850 – OSPF Version 2 Management Information Base;
o RFCs 2328 ou 2178 – OSPF Version 2;
o RFC 2370 – The OSPF Opaque LSA Option ;
• Deve suportar o protocolo de roteamento BGP versão 4, conforme os padrões RFCs especificados abaixo:
o RFCs 1771 ou 1654 – A Border Gateway Protocol (BGP-4);
o RFC 2796 – Autonomous System Confederation for BGP;
o RFC 1997 – BGP Communities Attribute;
o RFCs 2283 ou 2858 – Multi-Protocol Extensions for BGP-4;
o RFC 2439 – BGP Route Flap Damping;
o RFC 2842 – Capabilities Advertisement with BGP-4;
o RFC 2918 – Route Refresh Capability for BGP-4;
• Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.
• Deve possuir suporte ao modo de operação full-duplex em todas as interfaces Ethernet.
• Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.
• Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 – The IP Network Address Translator (NAT) ou RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).
• Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT).
• Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338.
• Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode).
• Deve possuir suporte a implementação das funcionalidades de DHCP Relay.
• Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer 4.
• Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ).
• Deve suportar a funcionalidade de Policy-Based Routing (PBR).
• Deve possuir suporte a túneis de roteamento.
• Deve possuir suporte a Traffic Shapping.

- *Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 2030 ou 4330 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, ou o protocolo NTP (Network Time Protocol).*
- *Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819 - Remote Network Monitoring Management Information Base.*
- *Deve implementar facilidades de syslog.*
- *Deve possuir suporte a autenticação de usuário através de RADIUS, em conformidade com, no mínimo, o padrão RFC 2865.*
- *Deve possuir suporte a autenticação de usuário através de TACACS em conformidade com, no mínimo, o padrão RFC 1492.*
- *Deve possuir suporte a protocolo de redirecionamento para cache de Web.*
- *Deve possuir suporte ao protocolo de gerenciamento SNMP e a MIB-II, em conformidade com as RFCs 1157 e 1213, respectivamente.*
- *Deve possuir suporte ao protocolo SNMPv2c.*
- *Deve possuir suporte ao protocolo SNMPv3.*
- *Deve implementar segurança baseada em, no mínimo, 2 (dois) níveis de acesso para a administração do equipamento.*
- *Deve fornecer suporte para prevenir fluxo de dados de entrada não autorizados através da configuração de filtros baseados em parâmetros de Layer 3 e Layer 4 do protocolo IP.*
- *Deve suportar a configuração de métodos de priorização de tráfego por tipo de protocolo e por serviços da pilha TCP/IP.*
- *Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol).*
- *Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508.*
- *Deve permitir administração e configuração através de interface de linha de comando (CLI).*
- *Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas.*
- *Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador.*
- *Deve ter a capacidade de atualização de software via FTP ou via TFTP, em conformidade com as RFCs 0783 ou 1350 – The TFTP Protocol (Revision 2).*
- *Deverá possuir suporte a técnicas de gerenciamento inteligente de energia, podendo desligar portas e módulos quando não utilizados para conservar energia.*
- *Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:*

o *Digital Encryption Standard (DES) e Triple DES (3DES);*

o *Advanced Encryption Standard (AES) 128, 192, e 256;*

o *Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5 hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1 hmac.*

- *O equipamento deverá suportar, via licença adicional ou upgrade de software, no mínimo as seguintes funcionalidades:*

o *Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol).*

o *Deve suportar a criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCS 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.*

o *Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC.*

o *Deve suportar a criação de túneis VPN dinamicamente para criar uma rede VPN totalmente ligada.*

o *Deve suportar a concentração de VPNs (IPSEC) para acessos remotos.*

o *Deve suportar a concentração de SSL-VPNs para acessos remotos.*

o *O equipamento fornecido suportar terminar simultaneamente conexões IPSEC do tipo "site-to-site","client-to-site" (VPNs de acesso remoto) e "clienteless" VPN (SSL VPN) . Nas conexões do tipo "client-to-site" (acesso remoto) o equipamento deve ser capaz de passar parâmetros tais como endereço IP, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name para o cliente VPN que está solicitando a conexão. Suporte a certificados digitais para autenticação das conexões IKE e IKEv2.*

o *Implementar/suportar mecanismo de automatização do processo de enrollment na autoridade certificadora para no mínimo as seguintes CAs de mercado: Baltimore, Entrust, Verisign, Microsoft e RSA.*

o *Deve suportar a autenticação e autorização de usuários para acesso VPN.*

o Deve suportar a operação como "Stateful Firewall" sem necessidade de adição de modulo específico para esta função, com no mínimo as seguintes características:

- Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP (e UDP), status dos flags "ACK", "SYN" e "FIN".
- Implementar filtragem "stateful" para pelo menos os seguintes protocolos de aplicação: HTTP, HTTPS, FTP, CIFS, SMTP, ESMTP, IMAP, POP3.
- Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "peer-to-peer": Kazaa, Morpheus, Gnutella, Edonkey, Bittorrent.
- Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "Instant Messaging": Yahoo messenger, AOL IM, ICQ, MSN.

- Bloquear "applets" Java . Deve ser possível efetuar tal bloqueio de forma geral ou para "applets" oriundos de endereços IP previamente especificados de endereços IP previamente especificados.
- Suportar operação como Firewall Transparente.
- Suportar a filtragem de pacotes Ipv4 e Ipv6.
- Prover proteção distribuída para diversos tipos de ataques, worms, exploits, vírus e vulnerabilidades de sistemas operacionais e aplicações.

o Deve suportar Intrusion Prevention System (IPS) com assinaturas de ataques, sem necessidade de adição de modulo especifico para esta função.

- Eliminar a necessidade de equipamentos isolados de IPS espalhados por diversos pontos da rede.
- Prover a inspeção do tráfego de rede através de várias combinações de interfaces de redes locais e redes WAN, em ambos os sentidos.
- Proteção para vulnerabilidades de aplicações Microsoft SMB e vulnerabilidades de protocolos MSRPC.
- A solução deve trabalhar com escala de risco para os alarmes de IPS baseado em severidade, fidelidade.
- Prover identificação multivetor de ameaças, através de inspeção pormenorizada das camadas de rede 2-7. Proteger a rede de violações as políticas de vulnerabilidade e atividades anômolas.
- Prover tecnologia acurada de prevenção, através de avaliação de risco e meta de evento gerador, para fornecer ações preventivas sobre um vasto leque de ameaças.

• Deverá possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento.

• Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9.

• Deverá possuir console com porta USB.

• Deve possuir uma porta auxiliar com velocidade de até 115.2Kbps, serial assíncrona, com conector RJ-45.

• Deverá permitir a acomodação em rack padrão 19" e ter no maximo 2 unidades racks (2RU).

• Deverá operar entre as temperaturas de 10°C e 40ºC.

• Deverá ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação) e suportar temperatura ambiente de armazenamento entre 0°C e 50°C.

• Deve operar com alimentação elétrica de 110/220 V, 60 Hz, com seleção automática de voltagem.

10.3. TIPO III

• Deve possuir, no mínimo, 3 (três) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.

• Deve possuir no mínimo 1 (uma) interface ATM OC-3/STM-1.

• Deve suportar a inserção de interfaces analogicas (FXS ou FXO) e digitais de voz (E1).

• Deve suportar no mínimo 4 (quatro) interfaces de Voz digitais E1.

• Deve suportar no mínimo dois slot(s) internos para a inserção de DSPs (Digital Signal Processor).

• Deve suportar os CODEC's (G.711, G.723.1, G.728, G.729 ou G.729b).

• *Deve ter a possibilidade de ser inserido em redes com serviços de Voz sobre IP (VoIP), Voz sobre Frame Relay (VoFR) e Voz sobre ATM (VoATM).*
• *Deve suportar mecanismo de controle de chamadas IP sem a necessidade de um controlador central.*
• *Deve suportar mecanismo que permita a continuidade do controle de chamadas IP mesmo após a perda de comunicação com o controlador de chamadas central.*
• *Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.*
• *Deve ter uma performance mínima de 980.000 pps com pacotes de 64 bytes.*
• *Deve implementar a opção local de carga do sistema do equipamento via memória Flash.*
• *Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.*
• *Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.*
• *Como uma opção de acesso alternativo, deve suportar a adição de módulo que permita a conexão de dados através de rede celular 3G com as seguintes características:*
o Deve suportar as seguintes tecnologias e faixas de freqüência:
HSPA: 850, 1900 e 2100 MHz
UMTS: 850, 1900 e 2100 MHz
EDGE: 850, 900, 1800 e 1900 MHz
GPRS: 850, 900, 1800 e 1900 MHz

CDMA 1xEV-DO Rev A: 800 e 1900 MHz
CDMA 1xEV-DO Rel 0
CDMA 1xRTT

o Deve permitir o uso de antenas externas ao módulo que possam ser instaladas distantes do CPE.
o Deve permitir a monitoração de informações de rádio freqüência, da operação da interface e do tráfego através do protocolo.
• *Deve suportar o protocolo HDLC (High-Level Data Link Control).*
• *Deve suportar o protocolo Frame Relay.*
• *Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame-Relay e PPP sobre Ethernet).*
• *Deve suportar, no mínimo, os padrões do Frame Relay Forum abaixo especificados ou superiores:*
o FRF.16 – Multilink Frame Relay UNI/NNI Implementation Agreement;
o FRF.12 – Frame Relay Fragmentation Implementation Agreement;
• *Deve suportar o protocolo roteável IP.*
• *Deve permitir a configuração de roteamento estático.*

• *Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:*
o RFC 1587 – The OSPF Not-So-Stubby Area (NSSA) Option;
o RFC 1745 – BGP4/IDRP for IP --- OSPF Interaction;
o RFC 1253 ou 1850 – OSPF Version 2 Management Information Base;
o RFCs 2328 ou 2178 – OSPF Version 2;
o RFC 2370 – The OSPF Opaque LSA Option ;
• *Deve suportar o protocolo de roteamento BGP versão 4, conforme os padrões RFCs especificados abaixo:*
o RFCs 1771 ou 1654 – A Border Gateway Protocol (BGP-4);
o RFC 2796 – Autonomous System Confederation for BGP;
o RFC 1997 – BGP Communities Attribute;
o RFCs 2283 ou 2858 – Multi-Protocol Extensions for BGP-4;
o RFC 2439 – BGP Route Flap Damping;
o RFC 2842 – Capabilities Advertisement with BGP-4;

o RFC 2918 – Route Refresh Capability for BGP-4;

- *Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.*
- *Deve possuir suporte ao modo de operação full-duplex em todas as interfaces Ethernet.*
- *Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.*
- *Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 – The IP Network Address Translator (NAT) ou RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).*
- *Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT).*
- *Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338.*
- *Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode).*
- *Deve possuir suporte a implementação das funcionalidades de DHCP Relay.*
- *Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer 4.*
- *Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ).*
- *Deve suportar a funcionalidade de Policy-Based Routing (PBR).*
- *Deve possuir suporte a túneis de roteamento.*
- *Deve possuir suporte a Traffic Shapping.*

- *Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 2030 ou 4330 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, ou o protocolo NTP (Network Time Protocol).*
- *Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819 - Remote Network Monitoring Management Information Base.*
- *Deve implementar facilidades de syslog.*
- *Deve possuir suporte a autenticação de usuário através de RADIUS, em conformidade com, no mínimo, o padrão RFC 2865.*
- *Deve possuir suporte a autenticação de usuário através de TACACS em conformidade com, no mínimo, o padrão RFC 1492.*
- *Deve possuir suporte a protocolo de redirecionamento para cache de Web.*
- *Deve possuir suporte ao protocolo de gerenciamento SNMP e a MIB-II, em conformidade com as RFCs 1157 e 1213, respectivamente.*
- *Deve possuir suporte ao protocolo SNMPv2c.*
- *Deve possuir suporte ao protocolo SNMPv3.*
- *Deve implementar segurança baseada em, no mínimo, 2 (dois) níveis de acesso para a administração do equipamento.*
- *Deve fornecer suporte para prevenir fluxo de dados de entrada não autorizados através da configuração de filtros baseados em parâmetros de Layer 3 e Layer 4 do protocolo IP.*
- *Deve suportar a configuração de métodos de priorização de tráfego por tipo de protocolo e por serviços da pilha TCP/IP.*
- *Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol).*
- *Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508.*
- *Deve permitir administração e configuração através de interface de linha de comando (CLI).*
- *Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas.*
- *Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador.*
- *Deve ter a capacidade de atualização de software via FTP ou via TFTP, em conformidade com as RFCs 0783 ou 1350 – The TFTP Protocol (Revision 2).*
- *Deverá possuir suporte a técnicas de gerenciamento inteligente de energia, podendo desligar portas e módulos quando não utilizados para conservar energia.*
- *Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:*

o Digital Encryption Standard (DES) e Triple DES (3DES)

o Advanced Encryption Standard (AES) 128, 192, e 256

o Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5_hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1_hmac

• O equipamento deverá suportar, via licença adicional ou upgrade de software, no mínimo as seguintes funcionalidades:

o Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol).

o Deve suportar a criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCS 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.

o Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC.

o Deve suportar a criação de túneis VPN dinamicamente para criar uma rede VPN totalmente ligada.

o Deve suportar a concentração de VPNs (IPSEC) para acessos remotos.

o Deve suportar a concentração de SSL-VPNs para acessos remotos.

o O equipamento fornecido suportar terminar simultaneamente conexões IPSEC do tipo "site-to-site","client-to-site" (VPNs de acesso remoto) e "clienteless" VPN (SSL VPN) . Nas conexões do tipo "client-to-site" (acesso remoto) o equipamento deve ser capaz de passar parâmetros tais como endereço IP, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name para o cliente VPN que está solicitando a conexão. Suporte a certificados digitais para autenticação das conexões IKE e IKEv2.

o Implementar/suportar mecanismo de automatização do processo de enrollment na autoridade certificadora para no mínimo as seguintes CAs de mercado: Baltimore, Entrust, Verisign, Microsoft e RSA.

o Deve suportar a autenticação e autorização de usuários para acesso VPN.

o Deve suportar a operação como "Stateful Firewall" sem necessidade de adição de módulo especifico para esta função, com no mínimo as seguintes características:

Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP (e UDP), status dos flags "ACK", "SYN" e "FIN".

Implementar filtragem "stateful" para pelo menos os seguintes protocolos de aplicação: HTTP, HTTPS, FTP, CIFS, SMTP, ESMTP, IMAP, POP3.

Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "peer-to-peer": Kazaa, Morpheus, Gnutella, Edonkey, Bittorrent.

Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "Instant Messaging": Yahoo messenger, AOL IM, ICQ, MSN.

Bloquear "applets" Java . Deve ser possível efetuar tal bloqueio de forma geral ou para "applets" oriundos de endereços IP previamente especificados de endereços IP previamente especificados.

Suportar operação como Firewall Transparente.

Suportar a filtragem de pacotes Ipv4 e Ipv6.

Prover proteção distribuída para diversos tipos de ataques, worms, exploits, vírus e vulnerabilidades de sistemas operacionais e aplicações.

o Deve suportar Intrusion Prevention System (IPS) com assinaturas de ataques, sem necessidade de adição de modulo especifico para esta função.

Eliminar a necessidade de equipamentos isolados de IPS espalhados por diversos pontos da rede.

Prover a inspeção do tráfego de rede através de várias combinações de interfaces de redes locais e redes WAN, em ambos os sentidos.

Proteção para vulnerabilidades de aplicações Microsoft SMB e vulnerabilidades de protocolos MSRPC.

A solução deve trabalhar com escala de risco para os alarmes de IPS baseado em severidade, fidelidade.

Prover identificação multivetor de ameaças, através de inspeção pormenorizada das camadas de rede 2-7. Proteger a rede de violações as políticas de vulnerabilidade e atividades anômolas.

Prover tecnologia acurada de prevenção, através de avaliação de risco e meta de evento gerador, para fornecer ações preventivas sobre um vasto leque de ameaças.

- *Deverá possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento.*
- *Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9.*
- *Deverá possuir console com porta USB.*
- *Deve possuir uma porta auxiliar com velocidade de até 115.2Kbps, serial assíncrona, com conector RJ-45.*
- *Deverá permitir acomodação em rack padrão 19" e ter no máximo 3 unidades racks (3RU).*
- *Deverá operar entre as temperaturas de 10°C e 40oC.*
- *Deverá ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação) e suportar temperatura ambiente de armazenamento entre 0°C e 50°C.*
- *Deve operar com alimentação elétrica de 110/220 V, 60 Hz, com seleção automática de voltagem.*

10.4. TIPO IV

- *Possuir, no mínimo, 1 slot para a inserção de módulos.*
- *Possuir 6 (seis) interfaces Ethernet 1000Base-X para inserção de conectores SFP.*
- *Possuir capacidade de associação das portas 1000Base-X, no mínimo, em grupo de 4 (quatro) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.*
- *Suportar módulos com portas do tipo 10GBASE-X, E3 e OC-48.*
- *Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.*
- *Implementar VLANs por porta.*
- *Implementar VLANs compatíveis com o padrão IEEE 802.1q.*
- *Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas nesta especificação.*
- *Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.*
- *Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.*
- *Suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com a solução.*
- *Possuir fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e freqüência (de 50/60 Hz).*
- *Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.*
- *Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.*
- *Possuir LEDs para a indicação do status das portas e atividade.*
- *Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.*
- *Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:*
  - *Sem autenticação e sem privacidade (noAuthNoPriv);*
  - *Com autenticação e sem privacidade (authNoPriv);*
  - *Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES.*
- *Suportar SNMP sobre IPv6.*
- *Possuir suporte a MIB II, conforme RFC 1213.*
- *Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.*
- *Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.*
- *Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.*
- *Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.*
- *Permitir o gerenciamento via CLI e Web, utilizando SSH e HTTPS.*
- *Implementar nativamente 2 grupos RMON (Alarms e Events) conforme RFC 1757.*

- *O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede.*
- *Possibilidade de criação de versões de configuração e suporte a "rollback" da configuração para versões anteriores.*
- *Implementar Telnet para acesso à interface de linha de comando.*
- *Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.*
- *Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.*
- *Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.*
- *Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).*
- *Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.*
- *Permitir que a sua configuração seja feita através de terminal assíncrono.*
- *Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.*
- *Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.*
- *Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.*
- *Suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.*
- *Deve suportar IPv6.*
- *Implementar NAT (Network Address Translation).*
- *Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações:*
  - *IP de origem/destino;*
  - *Parâmetro "protocol type" do cabeçalho IP;*
  - *Porta TCP/UDP de origem/ destino;*
  - *Interface de entrada do tráfego;*
- *Deve ser possível especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída (e também para ambos os sentidos simultaneamente) em uma dada interface do roteador.*
- *A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado.*
- *Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:*
  - *ICMP echo;*
  - *TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);*
  - *UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);*
  - *O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.*
- *Implementar o protocolo NTPv3 (Network Time Protocol, versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições da RFC 1305.*
- *Implementar DHCP Relay e DHCP Server.*
- *Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway. Suportar mecanismo de autenticação MD5 entre os peers VRRP.*
- *Implementar roteamento estático.*
- *Implementar roteamento dinâmico RIPv2 (RFC 2453 e 2082).*
- *Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101, 3137, 3623 e 2370).*
- *Implementar protocolo de roteamento BGPv4 (RFC 4271, 3065, 4456, 1997, 1965, 1966, 4897, 2858 e 2385).*
- *Permitir o roteamento nível 3 entre VLANs.*

- *Implementar, no mínimo, 100 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente.*
- *Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.*
- *Suporte ao protocolo de Tunelamento GRE (General Routing Encapsulation - RFCs 2784), contemplando, no mínimo, os seguintes recursos:*
  - *Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica, definida pelo administrador do equipamento;*
  - *Operação em modo multiponto ("multipoint GRE");*
  - *Possibilidade de configuração de " Keepalive" nos túneis;*
  - *Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.*
- *Implementar roteamento baseado em origem, com a possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.*
- *Suportar roteamento estático para IPv6.*
- *Implementar roteamento dinâmico RIPng.*
- *Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.*
- *Implementar protocolo de roteamento Multiprotocol BGP com suporte a IPv6.*
- *Implementar , no mínimo, 4000 vlans simultaneamente.*

- *Implementar, no mínimo, 4000 interfaces vlans simultaneamente, para roteamento nível 3 entre as vlans configuradas.*
- *Possuir backplane de, no mínimo 2,5 (dois vírgula cinco) Gbps.*
- *Suportar pelo menos 1 (um) Gbps de throughput com todas as funcionalidades de roteamento e segurança ativas simultaneamente.*
- *Possuir uma taxa de comutação de pacotes de no mínimo 3 (três) milhões pacotes por segundo (Mpps)*
- *Possuir no mínimo 8 (oito) GB de memória DRAM.*
- *Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.*
- *Implementar filtragem de pacotes (ACL - Access Control List), para IPv4 e IPv6.*
- *Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.*
- *Proteger a interface de comando do equipamento através de senha.*
- *Implementar o protocolo SSH V2 para acesso à interface de linha de comando.*
- *Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.*
- *Permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Tuneis IPSEC.*
- *Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.*
- *Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.*
- *Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede.*
- *Suportar serviços de VPN baseados no padrão IPSec (IP Security Protocol)*
- *Suportar serviços de VPN baseados no padrão IKE(Internet Key Exchange)*
- *Suportar pelo menos 4000 (quatro mil) túneis IPSec VPN Site- to- Site.*
- *Suportar uma taxa de estabelecimento de túneis VPN de no mínimo 80 (oitenta) túneis por segundo.*
- *Suportar algorítmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões com VPN IPSec.*
- *Suportar a transparência de conexões IPSEC a NAT(NAT-T) através do encapsulamento dos pacotes IPSEC com UDP.*
- *Reagrupar pacotes de sessão fragmentados para análise e entrega no destino.*
- *Permitir a criação de VPNS IPSEC baseada em políticas de segurança.*

- *Suportar criação de VPNs de acordo com o conjunto de padrões IPSEC em modo túnel.*
- *Devem ser implementados os modos de operação "tunnel mode" e "transport mode". Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.*
- *Suportar as funcionalidades de gerenciamento de chaves para VPN.*
- *Suportar a utilização de clientes baseados em IPSEC.*
- *Implementar a criptografia dos pacotes de forma totalmente transparente e automática, sem a alteração dos cabeçalhos incluindo endereços IP de origem e destino, e portas de origem e destino.*
- *Implementando uma rede VPN totalmente ligada com criptografia entre sites (full-mesh), sem a necessidade de túneis ponto a ponto conforme RFC 3547.*
- *Suportar o tráfego protocolo GRE sobre IPSEC.*
- *Suportar o tráfego de IP multicast sobre IPSEC.*
- *Implementar padrão IEEE 802.1q (Vlan Frame Tagging).*
- *Implementar padrão IEEE 802.1p (Class of Service) para cada porta.*
- *Implementar padrão IEEE 802.3ad.*
- *Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).*
- *Implementar mecanismo de controle de multicast através de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).*
- *Implementar roteamento multicast PIM (Protocol Independent Multicast) nos modos "sparse-mode" (RFC 2362) e "dense-mode". Deve ser suportada, por interface, a operação simultânea nos modos "sparse-mode" e "dense mode".*
- *Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.*
- *Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).*
- *Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.*
- *Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).*
- *Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".*
- *Deve ser possível a especificação de banda por classe de serviço.*
- *Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.*
- *Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection).*
- *Implementar LFI (Link Fragmentation e Interleaving), tanto em interfaces seriais com encapsulamento Frame Relay, quanto em interfaces seriais configuradas com encapsulamento PPP.*
- *Implementar RTP (Real-Time Transport Protocol) e a compressão do cabeçalho dos pacotes RTP (IP RTP Header Compression).*
- *Implementar priorização nível 2 IEEE 802.1p e priorização nível 3 dos tipos "IP precedence" e DSCP (Differentiated Services Code Point).*
  - *O roteador deve suportar o mapeamento das prioridades nível 2 (IEEE 802.1p) em prioridades nível 3 (IP Precedence e DSCP) e vice-versa.*
- *Implementar política de enfileiramento nas linhas seriais (priorização de tráfego por tipo de protocolo trafegado).*
  - *Devem ser suportadas pelo menos as seguintes técnicas de enfileiramento: Priority Queuing, Custom Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing e Low Latency Queuing.*
- *Implementar RSVP (Resource Reservation Protocol).*
- *Implementar IPv6.*
- *Permitir a configuração de endereços IPv6 para gerenciamento.*
- *Permitir consultas de DNS com resolução de nomes em endereços IPv6.*
- *Implementar ICMPv6 com as seguintes funcionalidades:*
  - *ICMP request;*
  - *ICMP Reply;*
  - *ICMP Neighbor Discovery Protocol (NDP);*
  - *ICMP MTU Discovery.*

- *Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, SNMP, SYSLOG e DNS sobre IPv6.*
- *Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6."*

SUGESTÃO 05

ENCARTE TÉCNICO I - O ITEM 14.4 – pág 51 – solicita que:

> *"14.4. A CONTRATADA deverá implementar e fornecer, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de pelo menos 5 (cinco) classes de serviços:"*

Justificativa: A marcação de QoS é uma característica intrínseca de uma solução MPLS, onde são dimensionas CoS (classes de serviço) por modalidade e aplicação do cliente. Em uma solução SD-WAN ocorre a priorização de tráfego (traffic shaping) em tuneis IPSEC, não fazendo sentido uma marcação de QoS em uma rede IP. Segue sugestão da redação

Sugestão: *14.4. A CONTRATADA deverá implementar e fornecer na solução MPLS, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de pelo menos 5 (cinco) classes de serviços"*

SUGESTÃO 06

ENCARTE TÉCNICO I - O ITEM 16.4 – pág 54 – define que:

> *"16.4. A Solução de Gerência da Rede deverá ter como base a plataforma Open-Source, sem qualquer necessidade de licenciamento para seu pleno funcionamento, e poderá usar como painel de controle ou backend a ferramenta de monitoramento nativa da CONTRATANTE;*
> *16.5. A Solução de Gerência da Rede não deverá demandar licenciamento para o seu funcionamento pleno e ao final da vigência contratual será entregue integralmente à CONTRATADA devidamente operacional;."*
>
> *"16.11. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto não serão aceitas soluções que possuem acessos segmentados aos módulos;"*

Justificativa: A solução de gerência da CONTRATADA possui softwares intrínsecos a solução e desenvolvidos/adquiridos pela mesma, sendo assim os mesmos não pode ser fornecidos como uma venda de ativo/licença ao fim do contrato, lembrando que a licitação engloba prestação de serviços SCM. Segue sugestão de redação:

Sugestão: *Retirar os itens 16.5 e 16.11*

SUGESTÃO 07

ENCARTE TÉCNICO I - O ITEM 16.9 – pág 54 – define que:

> *"16.9. A solução de Gerência da Rede da CONTRADA deverá enviar os alertas de incidentes também via e-mail e SMS;."*

Justificativa: Sugerimos a flexibilização das notificações onde os alertas poderão ser enviados via e-mail OU sms. Segue sugestão de redação:

Sugestão: *"16.9. A solução de Gerência da Rede da CONTRADA deverá enviar os alertas de incidentes também via e-mail ou SMS;."*

SUGESTÃO 08

ENCARTE TÉCNICO I - O ITEM 17.10 – pág 58 – solicita os seguinte SLA

Nível	RTT	Sítios
N1	≤ 100ms	Fibra Ótica, Rádio Terrestre e Par Metálico
N2	≤ 600ms	Acesso Satélite

Tabela 3 – Tempo de Retardo (RTT)

Justificativa/Sugestão: Sugerimos alterar a latência do acesso SAT para até 1000ms.

SUGESTÃO 09

ENCARTE TÉCNICO I - O ITEM 23.5 – pág 68 – solicita o seguinte:

> *"23.5. Não serão aceitas redes híbridas de forma segregada, ou seja, um equipamento concentrador SDWAN e um equipamento concentrador MPLS conectados para formar uma rede híbrida. A solução deverá ser única, seja uma rede puramente MPLS ou uma rede puramente SD-WAN, contendo apenas um hardware;*

Justificativa: Considerando o princípio da competitividade neste certame, sugerimos uma igualdade de condições para os principais licitantes, deliberando a utilização de uma solução hibrida em tecnologias (SD-WAN + MPLS), onde poderá também ser utilizado em um mesmo ambiente equipamentos segregados, ou seja, equipamentos MPLS e SD-WAN. Retirando-se também restrição de apenas um hardware para suportar SD-WAN + MPLS. Segue sugestão da redação:

Sugestão: *"23.5. Serão aceitas redes híbridas agregadas ou segregadas, ou seja, um equipamento concentrador SDWAN e um equipamento concentrador MPLS conectados para formar uma rede híbrida. A solução não necessariamente deverá ser uma rede puramente MPLS ou uma rede puramente SD-WAN, contendo apenas um hardware;*

SUGESTÃO 10

15. SERVIÇO DE SEGURANÇA GERENCIADA (MSS), página 59.

> *"15.9. O Serviço de Segurança Gerenciada deve contemplar a monitoração proativa do (s) dispositivo (s) de segurança ofertado (s), pela CONTRATADA, sendo esses uma solução de segurança cujo fabricante é avaliado pelo Gartner Group, mencionado em seu quadrante mágico;"*

Justificativa: Exigir que o fabricante de segurança seja avaliado pelo Gartnet Group restringe a competitividade do certame. Avaliações não podem ser exigidas como itens indispensáveis a serem provados por licitantes, pois falta expressa autorização legal para tanto. Como é sabido, a Administração Pública está vinculada ao princípio da legalidade, e nesta esfera o conteúdo jurídico do princípio da legalidade implica que o agente público somente pode fazer o que a lei expressamente autoriza. Apenas seria válido solicitar que o fabricante seja avaliado pelo Gartner em geral somente podem ser utilizadas como elementos de pontuação, nunca como itens de cumprimento obrigatório, a não ser as avaliações expressamente impostas pela lei, tais como as certificações ANATEL, INMETRO, ANVISA, Certics, etc. e somente para os produtos indicados nas respectivas normas.

Sugestão: *Sugerimos a retirada item 15.9.*

SUGESTÃO 12

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 22.

> *"9.2.2.5. Deve possuir 1 (uma) interface de rede Gigabit dedicada para gerenciamento;"*

Justificativa: Visando a competitividade no certame e sem perda de requisito funcional, limitar a oferta de produtos que apenas permitem que uma das interfaces ser utilizada para gerenciamento restringe a ampla participação de diversos fornecedores de segurança. Na questão técnica, ter apenas uma interface de gerenciamento coloca em risco perder a administração caso a interface apresente defeito.

Sugestão: *Baseado no exposto acima sugerimos a remoção do item.*

SUGESTÃO 13

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 25.

> *"9.2.4.3. Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;"*

Justificativa: A classificação dinâmica utiliza recurso de verificação de comportamento para classificar a aplicação. Esse método retorna muitos erros de classificação e permite ao usuário acessar uma aplicação que deveria ser bloqueada. Sugerimos reescrita do item conforme sugestão abaixo:

> **Sugestão:** *"9.2.4.3. Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações e categorias de aplicações;"*

SUGESTÃO 14

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 25 e 26

> *9.2.5.Controle de Aplicações:*
> *9.2.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independentemente de porta e protocolo, com as seguintes funcionalidades: "*
> ▪ *Deve permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do ambiente do CONTRATANTE;*
> ▪ *A criação de assinaturas personalizadas deve permitir o uso de expressões regulares e contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de, pelo menos, os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL; "*

Justificativa: Permitir que o usuário escreva as próprias assinaturas irá abrir a possibilidade de escrita de uma regra errada e assim causar o bloqueio do tráfego ou até mesmo não fazer tratamento nenhum. O mais grave para o mundo da segurança é o usuário acreditar que está protegido, ou seja, a falsa sensação que estar seguro. Somente o fabricante da solução é capaz de produzir assinaturas eficientes.

Sugestão: *Sugerimos a remoção do item.*

SUGESTÃO 15

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 27

> *9.2.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;"*

Justificativa: O tipo de controle que fazemos é bloquear o tráfego efetuando o drop da conexão, ou seja, o pacote é descartado sem o envio do tcp-reset. Esse controle é muito mais relevante para o ambiente protegido, pois assim o atacante não sabe que existe um

equipamento de segurança identificando o ataque. O hacker a partir do tcp-reset pode promover um ataque direcionado colocando assim em risco o ambiente. Sugerimos a remoção do trecho “enviar tcp-reset;”

> **Sugestão:** *9.2.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo;”*

SUGESTÃO 16

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 28

> *“9.2.6.7. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens:*
> *Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;”*

Justificativa: O protocolo SMB nada mais é que uma rede Microsoft. Efetuar o bloqueio de vírus no tráfego SMB já é executado pelos produtos de antivírus e ATP instalados nos SO Windows. A solução de Firewall quando analisa o protocolo SMB decai seu processamento, colocando assim a rede indisponível.
Sugestão: *Sugerimos a remoção do trecho “SMB”*

ENCARTE TÉCNICO II
REDE IP INTERNET SIMÉTRICA

SUGESTÃO 1

ENCARTE TÉCNICO II - O ITEM 3.21 – pág 07 – solicita o seguinte:

> *"3.21. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 25ms;*

Justificativa: Sugerimos alterar a latência para até 80ms. Segue sugestão de redação:

Sugestão *: ""3.21. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 80ms;;*

SUGESTÃO 2

ENCARTE TÉCNICO II - O ITEM 6.156– pág 23 – solicita o seguinte:

> *"6.156. A solução deverá ser totalmente apartada dos roteadores, sendo do tipo appliance e compatível para instalação no Datacenter da CONTRATANTE, não sendo permitida a utilização de módulos acoplados;;*

Justificativa Visando uma maior competitividade no certame, sugerimos flexibilizar o atendimento com a solução de Firewall embarcada nos roteadores ou a utilização de um appliance apartado. Segue sugestão de redação:

Sugestão *: "6.156. A solução poderá ser totalmente apartada dos roteadores ou embarcada nos equipamentos, sendo compatível com a instalação no Datacenter da CONTRATANTE, não sendo permitida a utilização de módulos acoplados;*

SUGESTÃO 3

ENCARTE TÉCNICO II - O ITEM 6.157– pág 23 – solicita o seguinte:

> *"6.157. A solução deverá atender, inclusive, aos circuitos de redundância, caso existam, independente da operadora contratada, quando os mesmos assumirem a posição de link principal;*

Justificativa: O TR em nenhum momento cita que terão links de contingência de operadoras distintas neste lote, sugerimos retirar este item.

SUGESTÃO 4

ENCARTE TÉCNICO II - O ITEM 6.158– pág 23 – define que:

> *"6.158. A solução deverá se integrar com o SNOC, e ferramentas de segurança fornecido pela CONTRATADA vencedora do Lote I e/ou do PRODERJ, sem que isto retire as suas responsabilidades*
> *conforme Termo de Referência e este Encarte Técnico.;*

Justificativa Fica-se inviável analisar uma integração entre sistemas de gestão e segurança de empresas e fornecedores distintos sem uma análise prévia dos part numbers e plataformas que as empresas irão utilizar. Sugerimos retirar este item, dado que é grande a chance de insucesso.

Sugestão *: Sugerimos remover o iten 6.158 ou que esteja explicito no item mecionado, que a integração será efetuada pela PRODERJ, onde as contratadas somente enviariam os MIBs dos equipamentos gerenciados para este respectivo órgão.*

SUGESTÃO 5

ENCARTE TÉCNICO II - O ITEM 10.6 – pág 23 – define que:

> *"10.6. A ativação dos enlaces referentes ao backbone da Rede IP Simétrica deverá ser feita numa*
> *única fase, que terá duração máxima de até 30 (trinta) dias, incluindo instalação e ativação dos circuitos, a contar da data de aprovação do Projeto Executivo;.;*

Justificativa: Dado o quantitativo de links simétricos que estão sendo licitados, é inviável tecnicamente para a contratada e também para a contratante que todos os 358 links sejam ativados em até 30 dias. Sugerimos alterar o prazo de uma ativação total de 120 dias para todo o projeto. Segue sugestão de redação:

Sugestão: *"10.6. A ativação dos enlaces referentes ao backbone da Rede IP Simétrica poderá ser efetuada em fases, porém respeitando um prazo máximo de até 120 (cento e vinte dias) para ativação de todo o projeto, incluindo instalação e configuração dos circuitos, a contar da data de aprovação do Projeto Executivo;.;*

SUGESTÃO 6

ENCARTE TÉCNICO II - O ITEM 12.6.2 – pág 32 – demonstra a seguinte tabela:

Nível	IDM	Serviços
N1	≥ 99,99%	Serviços de Acesso à Internet do Datacenter PRODERJ
N2	≥ 99,8%	Serviços de Acesso à Internet demais órgãos e secretarias – região metropolitana
N3	≥ 99,7%	Serviços de Acesso à Internet demais órgãos e secretarias – região não metropolitana

Tabela 1 – Índice de Disponibilidade Mensal (IDM)

Justificativa/Sugestão: Dado que para o lote 2 não foi contemplada nenhuma contingência de meio físico ou SD-WAN e que os endereços abrangem quase todo os municípios do estão do Rio de Janeiro, sugerimos alterar os IDMs N2 e N3 para o mesmo percentual dos IDMs do lote 1.

SUGESTÃO 7

ENCARTE TÉCNICO II - O ITEM 12.9 – pág 33 – demonstra a seguinte tabela:

Nível	RTT	Serviços
N1	≤ 20ms	Serviços de Acesso à Internet

Tabela 3 – Tempo de Retardo

Justificativa/Sugestão Sugerimos alterar a latência para até 80ms.

SUGESTÃO 8

ENCARTE TÉCNICO II - O ITEM 12.10 – pág 33 – demonstra a seguinte tabela:

Nível	PR	Serviços
N1	≤ 2 horas	Serviços de Acesso à Internet

Tabela 4 – Prazo de Reparo (PR)

Justificativa/Sugestão: Considerando que a distribuição dos links IP ocorrem em quase todos os municípios do estado do RJ, sugerimos alterar o tempo de reparo conforme os prazos de reparo do lote 1, lembrando que temos uma semelhança nessa distribuição geográfica.

SUGESTÃO 9

ENCARTE TÉCNICO II - O ITEM 12.10 – pág 33 – demonstra a seguinte tabela:

Nível	PAC	Serviços
N1	≤ 30 dias	Serviços de Acesso à Internet

Tabela 5 – Prazo de Alteração de Transmissão (PAT)

Justificativa/Sugestão: Dado o quantitativo de links simétricos que estão sendo licitados, é inviável tecnicamente para a contratada e também para a contratante que todos os 358 links sejam ativados em até 30 dias. Sugerimos alterar o prazo de uma ativação total de 120 dias para todo o projeto.

SUGESTÃO 10

ENCARTE TÉCNICO II - O ITEM 6.3 e ITEM 6.4 – pág 09 – solicitam o seguinte:

> *"6.3. Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de sequência dos pacotes TCP, status dos flags "ACK", "SYN" e "FIN";*
>
> *6.4. Deve permitir a "randomização" do número de sequência TCP, ou seja, funcionar como um "proxy" de número de sequência TCP de modo a garantir que um host situado em uma interface considerada "externa" (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;"*

Justificativa: Os itens citados acima permitem a participação de apenas 1 único fabricante nesta solução, encarecendo dessa maneira o preço final da oferta.

Sugestão: *Para manter a ampla participação é necessário remover os itens citados.*

SUGESTÃO 11

ENCARTE TÉCNICO II - O ITEM 6.6 – pág 09 – solicitam o seguinte:

> *"6.6. Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços. Deve ser possível verificar a utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;"*

Justificativa: A solicitação de hit counts também pode ser atendida se o produto indicar a quantidade de tráfego por regra. Sugerimos que adicione no texto que pode ser *hit counts ou quantidade de tráfego de cada regra de filtragem individualmente.*

SUGESTÃO 12

ENCARTE TÉCNICO II - OS ITENS 6.15, 6.16, 6.17 e 6.18 – pág 10 – solicitam o seguinte:

"6.15. Deve possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H.323 (v1, v2, v3, v4), SIP (Session Initiation Protocol), MGCP e SCCP;

6.16. A partir da inspeção dos protocolos de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones
envolvidos;

6.17. Deve ser suportada à inspeção do protocolo SIP (SIP over TLS) em ambientes com voz criptografada;

6.18. A partir da inspeção do protocolo de sinalização, devem ser criadas as conexões pertinentes para o tráfego SRTP (Secure RTP);"

Justificativa/Sugestão: As soluções padrões de mercado, atuam no protocolo de comunicação SIP/H323 priorizando o tráfico sobre outros protocolos de rede, garantindo desta fora a qualidade da comunicação VOIP. Desta forma solicita sugerimos a remoção dos itens acima.

SUGESTÃO 13

ENCARTE TÉCNICO II - OS ITENS 6.24, 6.25, 6.26, 6.27, 6.28 e 6.29 – pág 10 – solicitam o seguinte:

"6.24. Deve possuir suporte a tecnologia de Firewall Virtual, com instâncias totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas;

6.25. Dentro de cada instância de Firewall deve ser possível alocar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;

6.26. Dentro de cada instância de Firewall deve ser possível limitar (promover "rate limiting") os seguintes recursos: taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog;

6.27. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter Influência sobre a operação das demais instâncias;

6.28. Deve ser possível selecionar o modo de operação de cada instância de Firewall (seleção, por instância, de modo transparente ou roteado);

6.29. Deve ser suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias solicitado;"

Justificativa: A virtualização do firewall implica em consumo computacional relacionado a processamento e memória para suportar múltiplas instâncias virtuais. O objeto do lote 2 é para a aquisição de uma rede IP de baixo desempenho e para exclusivo acesso de internet. Essa solução acarreta alto custo para o certame de forma desnecessária e por conseguinte baixa economicidade para o órgão.

Sugestão: Sugerimos retirar esse item.

SUGESTÃO 13

ENCARTE TÉCNICO II - O ITEM 6.38 – pág 11 – solicitam o seguinte:

> *"6.38. Deve suporte à integração com servidores RADIUS, LDAP, Microsoft AD e Kerberos, para tarefas de autenticação, autorização e accounting (AAA) dos usuários VPN;"*

Justificativa/Sugestão: A solicitação de suporte a integração com servidores Kerberos apenas limita a participação de alguns fabricante, pois trata-se de protocolo descontinuado e suas funções são plenamente atendidas com a requisição de suporte a Microsoft AD. Sugerimos a remoção do texto "kerberos".

SUGESTÃO 14

ENCARTE TÉCNICO II - OS ITENS 6.40, 6.41, 6.51 e 6.55 – páginas 11 e 12– solicitam o seguinte:

> *"6.40. Deve ser capaz de configurar nos VPN clients uma lista de acesso de "split tunneling", de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta*
> *(sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo "all tunneling", em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;*
>
> *6.41. Deve permitir a criação de "banners" personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa;*
>
> *6.51. Deve permitir a terminação de conexões no modo IPSEC over TCP;*
>
> *6.55. Deve ser possível definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES, AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração ("lifetime") da conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN cliente;*

Justificativa/Sugestão: Os itens citados acima são referentes ao estabelecimento de comunicação VPN e fogem do padrão mínimos exigido para que ocorra a perfeita comunicação entre duas unidades remotas. Os itens apenas restringem a ampla participação do mercado. Sugerimos a remoção dos itens.

SUGESTÃO 15

ENCARTE TÉCNICO II - O ITEM 6.62 – pág 13 – solicita o seguinte:

> *"6.62. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;"*

Justificativa/Sugestão: O protocolo Telnet é inseguro e passível de captura dos dados, pois não ocorre de modo criptografado. Sugerimos por questões de segurança a remoção dos itens.

SUGESTÃO 16

ENCARTE TÉCNICO II - O ITEM 6.88– pág 14 – solicita o seguinte:

"6.88. Deve permitir a customização de regras de detecção de novas aplicações;"

Justificativa/Sugestão: A customização de regras pode ocorrer exclusivamente pelo fabricante, pois assim garante maior confiabilidade e elimina o erro de indisponibilidade do sistema se ocorrer a escrita errada da regra. Por motivos de segurança da sugerimos a remoção do item.

SUGESTÃO 17

ENCARTE TÉCNICO II - O ITEM 6.89 – pág 14 – solicita o seguinte:

"6.89. Deverá suportar a funcionalidades de filtragem de URL, através de licenciamento opcional e atendendo no mínimo as seguintes características:
Deve possibilitar o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo);"

Justificativa/Sugestão: A solicitação apenas restringe a ampla participação. Sugerimos a exclusão do item.

SUGESTÃO 18

ENCARTE TÉCNICO II - OS ITENS 6.116, 6.118, 6.120, 6.121 e 6.122 – páginas 18 e 19 – solicitam o seguinte:

"6.116. Deve permitir a inclusão de informações de vulnerabilidades oriundas de ferramentas de varredura externa;

6.118. Deve permitir a análise do comportamento da rede, com o intuito de detectar ameaças com origem/destino a segmentos monitorados pelo IPS. Isto inclui a capacidade de estabelecer padrões "normais" de tráfego através de técnicas de análise de fluxo (por exemplo, Netflow) e a capacidade de detectar desvios dos padrões considerados normais;

6.120. Deve permitir coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo(s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas:

- *Sistema operacional do Host;*
- *Serviços existentes no Host;*
- *Portas em uso no Host;*
- *Aplicações em uso no Host;*
- *Vulnerabilidades existentes no Host;*

- *Smart phones e tablets;*
- *Network flow;*
- *Anomalias de redes;*
- *Identidades de usuários;*
- *Tipo de arquivo e protocolo;*
- *Conexões maliciosas.*

6.121. Deve permitir criar uma lista com o "ambiente ideal esperado" e a cada mudança nesse
ambiente, o sensor deverá no mínimo alertar a console de gerencia sobre a mudança identificada.
Entendemos como "ambiente ideal esperado" o conjunto de informações pré-configuradas na gerencia
dos sensores de IPS a respeito dos atributos dos hosts participantes desse segmento, deve ser configurado no mínimo os seguintes atributos:

- *Sistema Operacional;*
- *Serviços vigentes nos hosts;*
- *Aplicações autorizadas a serem executadas nos hosts;*
- *Aplicações não autorizadas a serem executadas nos hosts.*

6.122. Deve permitir criar ou importar regras no padrão OpenSource (SNORT), essas regras, devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não deve haver limite da quantidade de regras a serem criadas ou importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;"

Justificativa/Sugestão: Os itens descritos tem como missão atender a soluções de segurança de concentradores/Datacentes que expõem aplicações para acesso externo, desta forma os itens acima aumentam a complexidade das soluções, consequentemente elevando os custos do certame e restringindo a ampla participação. Sugerimos a exclusão dos itens.

SUGESTÃO 19

ENCARTE TÉCNICO II - O ITEM 6.124 – pág 19 – solicita o seguinte:

"6.124. Deve possuir capacidade de criar assinaturas definidas pelo usuário com uso de Expressões regulares;"

Justificativa/Sugestão: A customização de regras pode ocorrer exclusivamente pelo fabricante, pois assim garante maior confiabilidade e elimina o erro de indisponibilidade do sistema se ocorrer a escrita errada da regra. Sugerimos a remoção do item.

SUGESTÃO 20

ENCARTE TÉCNICO II - OS ITENS 6.133, 6.134, 6.136 e 6.141 – pág 20 – solicitam o seguinte:

"6.133. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de
30 Gbps (Vinte) para pacotes TCP multiprotocolo;

6.134. Deve suportar um throughput de, no mínimo, 20 Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;

6.136. Deve possuir desempenho de, no mínimo, 10Gbps (Cinco Gbps) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;
6.141. Deve possuir mais de 280 Milhões de URL categorizadas;"

Justificativa/Sugestão: Os valores acima são números além da necessidade do órgão baseado no levantamento dos links de internet e apenas limitam a ampla participação do mercado. Sugerimos a mudança para os valores abaixo descritos:

"6.133. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de
10 Gbps (Vinte) para pacotes TCP multiprotocolo;

6.134. Deve suportar um throughput de, no mínimo, 5 Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;

6.136. Deve possuir desempenho de, no mínimo, 4 Gbps (quatro Gbps) para tratamento de
conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;

6.141. Deve possuir mais de 40 Milhões de URL categorizadas;"

SUGESTÃO 21

ENCARTE TÉCNICO II - OS ITENS 6.116, 6.118, 6.120, 6.121 e 6.122 – páginas 18 e 19 – solicitam o seguinte:

"6.128. Deve ser fornecido com pelo menos 8 (oito) interfaces 1 Gigabit Ethernet;
6.129. Deve ser fornecido com pelo menos 4 (quatro) interfaces 10 Gigabit;
6.130. Deve suportar pelo menos 50.000.000 (cinquenta milhões) conexões simultâneas em sua tabela de estados de Stateful Firewall;
6.131. Deve suportar a criação de pelo menos 350.000 (trezentos e cinquenta mil) novas conexões
TCP por segundo para a funcionalidade de Stateful Firewall;
6.132. Deve suportar funcionalidade de Stateful Firewall com des empenho mínimo de 40 Gbps (Quarenta Gbps) para pacotes UDP;
6.133. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 30 Gbps (Vinte) para pacotes TCP multiprotocolo;
6.134. Deve suportar um throughput de, no mínimo, 20 Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;
6.135. Deve suportar a terminação de pelo menos 20.000 túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;
6.136. Deve possuir desempenho de, no mínimo, 10Gbps (Cinco Gbps) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;"

Justificativa/Sugestão: Os itens acima remetem a um equipamento de grande capacidade computacional por link contratado, equipamentos este com um alto valor de mercado independendo de fornecedores, sendo sugerimos a especificação técnica mínima, segmentando por velocidade de links, segue abaixo sugestão:

6.1. Características do Hardware para link até 30 Mbps
- Possuir throughput mínimo de 490 Mbps para tráfego UDP;
- Suportar no mínimo 45.000 (quarenta e cinco mil) conexões simultâneas;
- Suportar no mínimo 5.000 (cinco mil) novas conexões por segundo;
- Possuir throughput mínimo de 90 Mbps para tráfego HTTP/ HTTPS via Proxy;
- Possuir throughput mínimo de 35 Mbps para tráfego HTTP/ HTTPS com

inspeção SSL via Proxy;

- Possuir throughput mínimo de 92 Mbps para tráfego IPS;
- Possuir throughput mínimo de 140 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput mínimo de 92 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;

6.2. Características do Hardware para link até 100 Mbps

- Possuir throughput de no mínimo 4000 Mbps para tráfego UDP;
- Suportar no mínimo 500.000 (quinhentas mil) conexões simultâneas;
- Suportar no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;
- Possuir throughput de no mínimo 720 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 280 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 369 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 584 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 485 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

6.3. Características do Hardware para link até 500 Mbps

- Possuir throughput de no mínimo 9.000 Mbps para tráfego UDP;
- Suportar no mínimo 1.300.000 (hum milhão e trezentas mil) conexões simultâneas;
- Suportar no mínimo 75.000 (setenta e cinco mil) novas conexões por segundo;
- Possuir throughput de no mínimo 1.700 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 820 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 1.320 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 1.420 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 1.298 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Permitir expandir para 4 LANs 10GbE SFP+
- Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão

SSD;

6.4. Características do Hardware para link até 2 Gbps
- Possuir throughput de no mínimo 38.000 Mbps para tráfego UDP;
- Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;
- Suportar no mínimo 195.000 (cento e noventa e cinco mil) novas conexões por segundo;
- Possuir throughput de no mínimo 9.500 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 2.300 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 3.200 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 4.000 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 6.500 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Permitir expandir no mínimo 24 interfaces GbE RJ45 ou 12 LANs 10GbE SFP+
- Possuir dispositivo de armazenamento interno de no mínimo 480 GB padrão SSD;

ENCARTE TÉCNICO III
REDE IP INTERNET ASSIMÉTRICA

SUGESTÃO 1

ENCARTE TÉCNICO III - O ITEM 3.7 – pág 04 – informa o seguinte:

> *"3.7. A CONTRATADA será responsável pela configuração do acesso à internet (modem / roteador / ONT / Firewall e demais dispositivos) e das configurações dos equipamentos;.;*

Justificativa/Sugestão: Este item especificamente cita uma possível solução de firewall para este lote, porém em nenhum momento está descrito que deverá ser fornecido firewall, ou como appliance apartado dos roteadores ou como uma solução embarcada nos equipamentos. Sugerimos que a contratação de Firewall seja opcional neste lote e tenha uma tabela com o valor apartado da dos lins IPs assimétricos, podendo desta maneira o cliente final agregar até 6 (seis) links IP assimétrico em apenas um único Firewall. Segue abaixo redação com a especificação mínima dos firewalls:

"xxx. São definidos os seguintes Tipos de Solução de Segurança Gerenciada, em função da velocidade do circuito.
FIREWALL TIPO I: Serviço de Segurança Gerenciada
FIREWALL TIPO II: Serviço de Segurança Gerenciada
FIREWALL TIPO III: Serviço de Segurança Gerenciada;.;

3.1. ESPECIFICAÇÕES TÉCNICAS DO FIREWALL UTM

6.5. *FIREWALL TIPO I: Características do Hardware para link até 15 Mbps*

- *Possuir throughput mínimo de 490 Mbps para tráfego UDP;*
- *Suportar no mínimo 45.000 (quarenta e cinco mil) conexões simultâneas;*
- *Suportar no mínimo 5.000 (cinco mil) novas conexões por segundo;*
- *Possuir throughput mínimo de 90 Mbps para tráfego HTTP/ HTTPS via Proxy;*
- *Possuir throughput mínimo de 35 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;*
- *Possuir throughput mínimo de 92 Mbps para tráfego IPS;*
- *Possuir throughput mínimo de 140 Mbps para tráfego VPN IPSEC com criptografia (AES-128);*
- *Possuir throughput mínimo de 92 Mbps para tráfego VPN SSL com criptografia (AES-128);*
- *Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;*
- *Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;*

6.6. *FIREWALL TIPO II: Características do Hardware para link até 25 Mbps*

- *Possuir throughput mínimo de 2000 Mbps para tráfego UDP;*
- *Suportar no mínimo 250.000 (duzentas e cinquenta mil) conexões simultâneas;*
- *Suportar no mínimo 15.000 (quinze mil) novas conexões por segundo;*
- *Possuir throughput mínimo de 430 Mbps para tráfego HTTP/ HTTPS via Proxy;*
- *Possuir throughput mínimo de 162 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;*
- *Possuir throughput mínimo de 254 Mbps para tráfego IPS;*
- *Possuir throughput mínimo de 325 Mbps para tráfego VPN IPSEC com criptografia (AES-128);*
- *Possuir throughput mínimo de 205 Mbps para tráfego VPN SSL com criptografia (AES-128);*
- *Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;*
- *Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;*

6.7. *FIREWALL TIPO III: Características do Hardware para link até 50 Mbps*

- *Possuir throughput de no mínimo 4000 Mbps para tráfego UDP;*
- *Suportar no mínimo 500.000 (quinhentas mil) conexões simultâneas;*
- *Suportar no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;*
- *Possuir throughput de no mínimo 720 Mbps para tráfego HTTP/ HTTPS via proxy;*

- *Possuir throughput de no mínimo 280 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;*
- *Possuir throughput de no mínimo 369 Mbps para tráfego IPS;*
- *Possuir throughput de no mínimo 584 Mbps para tráfego VPN IPSEC com criptografia (AES-128);*
- *Possuir throughput de no mínimo 485 Mbps para tráfego VPN SSL com criptografia (AES-128);*
- *Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;*
- *Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;*

6.8. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM PARA OS FIREWALL´S TIPO I, II, III

6.4.1. FUNÇÕES BÁSICAS

- *Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;*
- *VPN SSL, VPN IPSec (Client-to-site e Site-to-site);*
- *Controle de Aplicações;*
- *Proxy Web e Filtro de Conteúdo Web (URL Filtering);*
- *Detecção e prevenção de intrusos – IPS;*
- *Qualidade de serviço – QOS;*
- *Anti-Malware;*
- *Cluster.*

6.4.2. CARACTERÍSTICAS GERAIS

- *A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;*
- *Interface em português e inglês;*
- *O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;*
- *O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.*
- *Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.*
- *Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.*
- *A Solução deverá prover inspeção SSL:*

- *A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.*
- *Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;*
- *Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;*
- *Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:*
  - *Endereço do servidor;*
  - *Porta do servidor;*
  - *Usuário;*
  - *Senha;*
- *Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:*
  - *Desempenho total (throughput);*
  - *Conexões simultâneas;*
  - *Usuários autenticados;*
  - *Serviços habilitados ou desabilitados;*
  - *Quantidade de endereços distribuídos pelo DHCP.*

6.4.3. DAS FUNCIONALIDADES DO FIREWALL:

- *Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;*
- *Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;*
- *Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;*
- *Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.*
- *Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;*
- *O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.*

- *As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;*
- *O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;*
- *Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;*
- *Deve permitir habilitar ou desabilitar o registro de log por política de firewall.*
- *Possuir controle de acesso à internet por endereço IP de origem e destino;*
- *Possuir controle de acesso à internet por sub-rede;*
- *Possuir suporte a tags de VLAN (802.1q);*
- *Suportar agregação de links, segundo padrão IEEE 802.3ad;*
- *Possuir ferramenta de diagnóstico do tipo tcpdump;*
- *Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;*
- *Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);*
- *Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.*
- *Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;*
- *Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;*
- *Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.*
- *Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;*
- *Possuir funcionalidades de DHCP Cliente, Servidor e Relay;*
- *Deverá suportar aplicações multimídia como: H.323, SIP;*
- *Possuir tecnologia de firewall do tipo Stateful;*
- *Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;*
- *Permitir o funcionamento em modo transparente tipo "bridge";*

- *Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;*
- *Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);*
- *Deverá suportar forwarding de multicast;*
- *Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;*
- *Permitir o agrupamento de serviços;*
- *Permitir o filtro de pacotes sem a utilização de NAT;*
- *Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;*
- *Possuir mecanismo de anti-spoofing;*
- *Permitir criação de regras definidas pelo usuário;*
- *Permitir o serviço de autenticação para HTTP e FTP;*
- *Possuir a funcionalidade de balanceamento e contingência de links;*
- *Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.*

6.4.4. IDENTIFICAÇÃO DE USUÁRIO

- *Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;*
- *Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;*
- *Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;*
- *Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);*
- *A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;*
- *Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;*

- *A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;*
- *A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;*

6.4.5. DAS FUNCIONALIDADES DA VPN:

- *VPN baseada em appliance;*
- *Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;*
- *Suporte a certificados PKI X.509 para construção de VPNs;*
- *Possuir suporte a VPNs IPSec site-to-site:*
  - *Criptografia, 3DES, AES128, AES256, AES-GCM-128*
  - *Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;*
  - *Algoritmo Internet Key Exchange (IKE) versões I e II;*
  - *AES 128 e 256 (Advanced Encryption Standard);*
  - *Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;*
- *Possuir suporte a VPN SSL;*
- *Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;*
- *Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:*
  - *RDP;*
  - *VNC;*
  - *SSH;*
  - *WEB;*
  - *SMB.*
- *Deve permitir a arquitetura de vpn hub and spoke;*
- *Suporte a VPNs IPSec client-to-site;*
  - *Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.*
- *Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);*
- *Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;*

- *A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:*
    - *Site-to-Site;*
    - *Full-Mesh;*
    - *Star.*

6.4.6. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:

- *A Detecção de Intrusão deverá ser baseada em appliance:*
- *Capacidade de detecção de mais de 22.000 ataques;*
- *O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;*
- *Possuir tecnologia de detecção baseada em assinatura;*
- *Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;*
- *Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;*
- *O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;*
- *Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.*
- *Possuir capacidade de remontagem de pacotes para identificação de ataques;*
- *Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;*
- *Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;*
- *Mecanismos de detecção/proteção de ataques;*
- *Reconhecimento de padrões;*
- *Análise de protocolos;*
- *Detecção de anomalias;*
- *Detecção de ataques de RPC (Remote procedure call);*
- *Proteção contra ataques de Windows ou NetBios;*
- *Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);*

- *Proteção contra ataques DNS (Domain Name System);*
- *Proteção contra ataques a FTP, SSH , Telnet e rlogin;*
- *Proteção contra ataques de ICMP (Internet Control Message Protocol);*
- *Alarmes na console de administração;*
- *Alertas via correio eletrônico;*
- *Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;*
- *Capacidade de resposta/logs ativa a ataques;*
- *Terminação de sessões via TCP resets;*
- *Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;*
- *O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;*
- *Possuir filtros de ataques por anomalias;*
- *Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;*
- *Permitir filtros de anomalias de protocolos;*
- *Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;*
- *Suportar verificação de ataque nas camadas de aplicação;*

6.4.7. DAS FUNCIONALIDADES DE QOS

- *Adotar solução de Qualidade de Serviço baseada em appliance;*
- *Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;*
- *Permitir modificação de valores DSCP para o DiffServ;*
- *Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;*
- *Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;*
- *Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;*

- *Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;*
- *Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;*
- *Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;*

6.4.8. DAS FUNCIONALIDADES DO ANTIVÍRUS

- *Possuir funções de Antivírus, Anti-spyware;*
- *Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;*
- *Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)*
- *Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;*
- *Permitir o bloqueio de download de arquivos por tamanho.*

6.4.9. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB

- *Possuir solução de filtro de conteúdo web integrado a solução de segurança*
- *Possuir pelo menos 75 categorias para classificação de sites web*
- *Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;*
- *Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:*
  - *Webmail;*
  - *Instituições de Saúde;*
  - *Notícias;*
  - *Pornografia;*
  - *Restaurante;*
  - *Mídias Sociais;*
  - *Esporte;*
  - *Educação;*
  - *Games;*
  - *Compras;*
- *Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;*
- *Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;*

- *Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;*
- *Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;*
- *Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;*
- *Possibilitar a integração com servidores de cache WEB externos;*
- *Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®, Youtube®, MSN Vídeos®, Facebook®, Google Maps®;*
- *Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;*
- *Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;*
- *Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;*
- *Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;*
- *Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;*
- *Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;*
- *Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;*
- *Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;*
- *Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;*
- *Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;*
- *Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;*
- *Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;*

- *Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;*
- *Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;*
- *Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;*
- *Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;*
- *Deverá permitir configurar a porta do Proxy Explícito.*

6.4.10. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES

- *As funcionalidades abaixo devem ser baseadas em appliance:*
- *Deverá reconhecer no mínimo 700 aplicações;*
- *Deverá possuir pelo menos 10 categorias para classificação de aplicações;*
- *Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:*
  - *P2P;*
  - *Web;*
  - *Transferência de arquivos;*
  - *Chat;*
  - *Social;*
- *Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;*
- *Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;*
- *Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;*
- *Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;*
- *Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;*
- *Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;*
- *Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;*

- *Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.*

6.4.11. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS - ATP

- *Possuir sistema de proteção avançada contra ameaças (ATP) nativo;*
- *O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.*
- *Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;*
- *A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;*
- *Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;*
- *Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;*
- *Deve permitir a atualização automática das assinaturas por meio de agendamento diário;*
- *Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;*
- *Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;*

- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;*
- *Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;*
- *Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;*
- *Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";*
- *Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";*
- *Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";*
- *Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;*

SUGESTÃO 2

ENCARTE TÉCNICO III - O ITEM 3.12.4 – pág 04 – informa o seguinte:

> *"3.12.4. Tempo máximo total de latência para resposta à internet de 80 milissegundos (latência considerando os links de acesso e o link de saída à internet).;*

Justificativa/Sugestão: Tecnicamente as operadoras não garantem uma baixa latência em soluções de internet em ADSL. Sugerimos alterar a latência para até 200ms. Segue sugestão de redação:

"3.12.4. Tempo máximo total de latência para resposta à internet de até 200 milissegundos (latência considerando os links de acesso e o link de saída à internet).;

SUGESTÃO 3

ENCARTE TÉCNICO III - O ITENS 7.11.6, 7.11.7 e 8.10 – pág 11 – informa o seguinte: $$$$$$

> *"7.11.6. Este Portal WEB deve estar disponível em 30 dias corridos após assinatura do primeiro contrato;*
>
> *7.11.7. Enquanto o portal WEB não estiver disponível a CONTRATADA deverá disponibilizar um*

endereço de e-mail para registro das solicitações de serviços;."

"8.10. Abertura e fechamento de chamados serão efetuados através de Portal Web, providenciado pela CONTRATADA. O Portal WEB deverá estar disponível 24 horas por dia, 7 dias por semana, com geração de número de protocolo de atendimento, o qual só poderá ser fechado após confirmação com o responsável pela abertura;;"

Justificativa/ugestão: O fornecimento de um portal WEB implicará também no fornecimento de roteadores nas pontas que no final elevam o custo final da solução de IP Assimétrico, deve-se levar em conta também que serão necessárias customizações e integrações da plataforma que suportará o portal. Sugerimos retirar esses itens.

SUGESTÃO 4

ENCARTE TÉCNICO III - O ITENS 7.11.8 – demonstra a seguinte tabela:

Nível	PR	Serviços
N1	≤ 4 horas	Serviços de Acesso à Internet Assimétrica

Tabela 1 – Prazo de Reparo (PR)

Justificativa/Sugestão: Dado que os locais de instalação dos links IP deste lote abrangem quase todo os municípios do estão do Rio de Janeiro, sugerimos alterar o tempo de reparo para 5 horas na região metropolitana e 7 horas no interior.

ADEQUAÇÃO ESCOPO TÉCNICO
INFOVIA 3.0

ENCARTE TÉCNICO I
REDE IP GOVERNO

SUGESTÃO 01

ENCARTE TÉCNICO I - O ITEM 4.1 – pág 07 – define o seguinte:

> *"4. ESPECIFICAÇÕES BÁSICAS DA REDE IP MPLS e SD-WAN*
> *4.1. A Rede IP MPLS ou SD-WAN a ser contratada através do PRODERJ deverá permitir a riação de múltiplas redes virtuais (VRFs), sendo que a cada VRF deverá ser logicamente do tipo "Full Mesh", permitindo que os sites pertencentes a uma mesma VRF, se comuniquem entre si, sem a necessidade de comutação através de um nó central;"*

Justificativa: Considerando que características como "VRFs" e comunicação "Full Mesh" são atributos intrínsecos de uma solução MPLS e que estes atributos não se aplicam a uma solução SD-WAN, onde as remotas remotas se comunicam com a concentradora através de túneis, tendo assim uma comunicação Hub and Spoke, sugerimos a redação abaixo:

Sugestão: *"4. ESPECIFICAÇÕES BÁSICAS DA REDE IP MPLS e SD-WAN*
4.1. A Rede IP MPLS a ser contratada através do PRODERJ deverá permitir a criação de múltiplas redes virtuais (VRFs), sendo que a cada VRF deverá ser logicamente do tipo "Full Mesh", permitindo que os sites pertencentes a uma mesma VRF, se comuniquem entre si, sem a necessidade de comutação através de um nó central;"

RESPOSTA: Serão permitidas redes hibridas com equipamentos que fazem a função SD-WAN distintos do equipamento que gerencia os links MPLS, desde que integrados entre si, sem prejuízos aos requisitos técnicos especificados. O texto será ajustado para contemplar a sugestão.

SUGESTÃO 02

ENCARTE TÉCNICO I - ITEM 4.4 – pág 07 e o ITEM 22.1 – pág 65 – solicitam o seguinte:

> *"4.4. Os meios de acessos para conexão dos sites à rede, última milha, deverão dar-se preferencialmente através de fibra ótica e par metálico. Será permitida a utilização de enlaces de rede em tecnologias alternativas desde que obedecendo aos critérios de desempenho estabelecidos neste projeto, principalmente o especificado no item 22 e todos os seus subitens;"*

> *"22.1. Será permitida a utilização de links de tecnologias alternativas, como, por exemplo, radiofrequência, satélite, links dedicados (ponto-a-ponto, L2VPN), ADSL, 4G, WiMax. Desde que sejam devidamente integrados à Rede IP Governo, preservando todos os requisitos de desempenho, disponibilidade e segurança definidos no Termo de Referência e este Encarte Técnico;"*

Justificativa: Ao se avaliar os meios de acessos WiMax, 4G e WiFi constata-se que para uma solução de integração entre sites e para interoperabilidade de solução de rede WAN para Governo do Rio de janeiro, é um meio de acesso fragilizado, ou seja, suscetíveis a interferências dado que nestas topologias, cada canal é utilizado por mais de um assinante (pessoa física e jurídica), sendo assim a frequência de transmissão é compartilhada por mais de

um sinal. Soluções como estas também estão suscetíveis a interferências físicas e climáticas. Além dos itens citados, temos também uma assimetria na transmissão dos dados, não tendo o cliente final uma banda garantida mediante ao escopo final contratado.

Sendo assim sugerimos a redação abaixo:

Sugestão: *"4.4. Os meios de acessos para conexão dos sites à rede, última milha, deverão dar-se preferencialmente através de fibra ótica e par metálico. Será permitida a utilização de enlaces de rede em tecnologias alternativas desde que obedecendo aos critérios de desempenho estabelecidos neste projeto, principalmente o especificado no item 22 e todos os seus subitens;"*

Sugestão: *"22.1. Será permitida a utilização de links de tecnologias alternativas, como, por exemplo, Radiofrequência licenciada, satélite, links dedicados (ponto-a-ponto, L2VPN) e ADSL. Desde que sejam devidamente integrados à Rede IP Governo, preservando todos os requisitos de desempenho, disponibilidade e segurança definidos no Termo de Referência e este Encarte Técnico;"*

RESPOSTA: Serão permitidos os meios de acesso listados no item 2.21, entre outras tecnologias que por ventura não tenham sido listadas, visando ampliar os tipos de meios de transporte de dados e não limitá-los. A disponibilidade será cobrada conforme tabela estabelecida no item 17.7.3 do encarte técnico I. A garantia de banda para o lote 1 é de 100%, portanto o fornecedor deverá utilizar quantos meios de transmissão sejam necessários para garantir as entregas. Com relação à utilização de 4G, modificaremos os requisitos indicando que somente poderá ser utilizado meio de acesso 4G para fins de instalação do link novo, com prazo máximo de 90 dias, quando deverá ser modificado para fibra ótica, par metálico ou outras tecnologias alternativas.

SUGESTÃO 03

ENCARTE TÉCNICO I - O ITEM 4.6 – pág 08, ITEM 8.1 – pág 11 e ITEM 9.1.12 – pág 20 – informam o seguinte:

> *""4.6. O hardware dos roteadores fornecidos (CPEs e Centrais) deverá suportar o funcionamento tanto na Rede IP MPLS como na Rede SD-WAN. Caso necessário será permitida apenas a atualização do software dos mesmos para funcionamento em cada uma das Redes;;"*
>
> *"8.1. Atenderem totalmente aos recursos solicitados, apresentando total compatibilidade e interoperabilidade, evitando-se problemas futuros na Rede do Governo, deste modo devendo ser do mesmo fabricante;"*
>
> *"9.1.12. Desempenho – Rede SD-WAN:*
> *9.1.12.1. Deve ser fornecido com capacidade de no mínimo 10 (dez) Gbps de criptografia;"*

Justificativa: Levando-se em conta o Princípio da Isonomia das licitações e por conseguinte buscar uma solução mais vantajosa para a administração pública do Governo do RJ, sugerimos que os equipamentos que estejam na solução MPLS, não necessariamente deverão ter uma solução de SD-WAN embarcada, possibilitando assim um investimento desnecessário que implicará maiores custos no certame. Seguindo o mesmo princípio para que tenhamos uma maior competitividade no certame, sugerimos retirar a obrigação da utilização de um mesmo fabricante para os CPEs do Datacenter e das remotas, segue sugestão de redação:

Sugestão: *Retirar o item 4.6, item 9.1.12 e item 9.1.12.1*

Sugestão: *"8.1. Atenderem totalmente aos recursos solicitados, apresentando total compatibilidade e interoperabilidade, evitando-se problemas futuros na Rede do Governo"*
";"

RESPOSTA: Serão acatadas as sugestões para permitir diferentes fabricantes dos roteadores visando a competitividade do certame.

""9.1.12. Desempenho – Rede SD-WAN:
9.1.12.1. Deve ser fornecido com capacidade de no mínimo 10 (dez) Gbps de criptografia;;;"

RESPOSTA: Será avaliado se a retirada prejudica o projeto.

SUGESTÃO 04

ENCARTE TÉCNICO I - O ITEM 10 – pág 36:

Justificativa: Visando uma maior competitividade no certame, sugerimos a redação abaixo com especificação técnica mínima para os roteadores da solução MPLS:

Sugestão:
TIPO I: circuitos com velocidades de até 20Mbps.
TIPO II: circuitos com velocidade de até 50Mbps.
TIPO III: circuitos com velocidade de até 300Mbps.
TIPO IV: circuitos com velocidade de até 4Gbps.

10.1. TIPO I
- *Deve possuir, no mínimo, 2 (duas) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.*
- *Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.*
- *Deve ter uma performance mínima de 280.000 pps com pacotes de 64 bytes.*
- *Deve implementar a opção local de carga do sistema do equipamento via memória Flash.*
- *Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.*
- *Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.*
- *Como uma opção de acesso alternativo, todos os CPE's devem suportar a adição de módulo que permita a conexão de dados através de rede celular 3G com as seguintes características:*
  - *Deve suportar as seguintes tecnologias e faixas de freqüência:*

HSPA: 850, 1900 e 2100 MHz
UMTS: 850, 1900 e 2100 MHz
EDGE: 850, 900, 1800 e 1900 MHz
GPRS: 850, 900, 1800 e 1900 MHz

CDMA 1xEV-DO Rev A: 800 e 1900 MHz
CDMA 1xEV-DO Rel 0
CDMA 1xRTT

  - *Deve permitir o uso de antenas externas ao módulo que possam ser instaladas distantes do CPE.*
  - *Deve permitir a monitoração de informações de rádio freqüência, da operação da interface e do tráfego através do protocolo.*
- *Caso o Fabricante possua mais de uma versão de uma mesma placa para atendimento a esta especificação, deverá ser fornecida a versão mais recente e estável da mesma.*

- *Deve suportar o protocolo HDLC (High-Level Data Link Control).*
- *Deve suportar o protocolo Frame Relay.*
- *Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame-Relay e PPP sobre Ethernet).*
- *Deve suportar, no mínimo, os padrões do Frame Relay Forum abaixo especificados ou superiores:*
- *FRF.16 – Multilink Frame Relay UNI/NNI Implementation Agreement.*
- *FRF.12 – Frame Relay Fragmentation Implementation Agreement.*
- *Deve suportar o protocolo roteável IP;*
- *Deve permitir a configuração de roteamento estático;*
- *Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:*
  - *RFC 1587 – The OSPF Not-So-Stubby Area (NSSA) Option;*
  - *RFC 1745 – BGP4/IDRP for IP --- OSPF Interaction;*
  - *RFC 1253 ou 1850 – OSPF Version 2 Management Information Base;*
  - *RFCs 2328 ou 2178 – OSPF Version 2;*
  - *RFC 2370 – The OSPF Opaque LSA Option;*
- *Deve suportar o protocolo de roteamento BGP versão 4, conforme os padrões RFCs especificados abaixo:*
  - *RFCs 1771 ou 1654 – A Border Gateway Protocol (BGP-4);*
  - *RFC 2796 – Autonomous System Confederation for BGP;*
  - *RFC 1997 – BGP Communities Attribute;*
  - *RFCs 2283 ou 2858 – Multi-Protocol Extensions for BGP-4;*
  - *RFC 2439 – BGP Route Flap Damping;*
  - *RFC 2842 – Capabilities Advertisement with BGP-4;*
  - *RFC 2918 – Route Refresh Capability for BGP-4;*
- *Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.*
- *Deve possuir suporte ao modo de operação full-duplex em todas as interfaces Ethernet.*
- *Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.*
- *Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 – The IP Network Address Translator (NAT) ou RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).*
- *Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT).*
- *Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338.*
- *Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode).*
- *Deve possuir suporte a implementação das funcionalidades de DHCP Relay.*
- *Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer 4.*
- *Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ).*
- *Deve suportar a funcionalidade de Policy-Based Routing (PBR).*
- *Deve possuir suporte a túneis de roteamento.*
- *Deve possuir suporte a Traffic Shapping.*
- *Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 2030 ou 4330 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, ou o protocolo NTP (Network Time Protocol).*
- *Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819 - Remote Network Monitoring Management Information Base.*
- *Deve implementar facilidades de syslog.*
- *Deve possuir suporte a autenticação de usuário através de RADIUS, em conformidade com, no mínimo, o padrão RFC 2865.*
- *Deve possuir suporte a autenticação de usuário através de TACACS em conformidade com, no mínimo, o padrão RFC 1492.*
- *Deve possuir suporte a protocolo de redirecionamento para cache de Web.*

• Deve possuir suporte ao protocolo de gerenciamento SNMP e a MIB-II, em conformidade com as RFCs 1157 e 1213, respectivamente.

• Deve possuir suporte ao protocolo SNMPv2c.

• Deve possuir suporte ao protocolo SNMPv3.

• Deve implementar segurança baseada em, no mínimo, 2 (dois) níveis de acesso para a administração do equipamento.

• Deve fornecer suporte para prevenir fluxo de dados de entrada não autorizados através da configuração de filtros baseados em parâmetros de Layer 3 e Layer 4 do protocolo IP.

• Deve suportar a configuração de métodos de priorização de tráfego por tipo de protocolo e por serviços da pilha TCP/IP.

• Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol).

• Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508.

• Deve permitir administração e configuração através de interface de linha de comando (CLI).

• Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas.

• Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador.

• Deve ter a capacidade de atualização de software via FTP ou via TFTP, em conformidade com as RFCs 0783 ou 1350 – The TFTP Protocol (Revision 2).

• Deverá possuir suporte a técnicas de gerenciamento inteligente de energia, podendo desligar portas e módulos quando não utilizados para conservar energia.

• Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:

o Digital Encryption Standard (DES) e Triple DES (3DES);

o Advanced Encryption Standard (AES) 128, 192, e 256 ;

o Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5 hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1 hmac ;

• O equipamento deverá suportar, via licença adicional ou upgrade de software, no mínimo as seguintes funcionalidades:

o Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol);

o Deve suportar a criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCS 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409;

o Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC;

o Deve suportar a criação de túneis VPN dinamicamente para criar uma rede VPN totalmente ligada.

10.2. TIPO II

• Deve possuir, no mínimo, 3 (três) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.

• Deve suportar a inserção de interfaces analógicas (FXS ou FXO) e digitais de voz (E1).

• Deve suportar no mínimo 4 interfaces de Voz analógicas FXO.

• Deve suportar no mínimo dois slot(s) internos para a inserção de DSPs (Digital Signal Processor).

• Deve suportar os CODEC's (G.711, G.723.1, G.728, G.729 ou G.729b).

• Deve ter a possibilidade de ser inserido em redes com serviços de Voz sobre IP (VoIP), Voz sobre Frame Relay (VoFR) e Voz sobre ATM (VoATM).

• Deve suportar mecanismo de controle de chamadas IP sem a necessidade de um controlador central.

• Deve suportar mecanismo que permita a continuidade do controle de chamadas IP mesmo após a perda de comunicação com o controlador de chamadas central.

• Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.

• Deve ter uma performance mínima de 350.000 pps com pacotes de 64 bytes.

• Deve implementar a opção local de carga do sistema do equipamento via memória Flash.

• Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.

• *Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.*

• *Como uma opção de acesso alternativo, deve suportar a adição de módulo que permita a conexão de dados através de rede celular 3G com as seguintes características:*

o *Deve suportar as seguintes tecnologias e faixas de freqüência:*

HSPA: 850, 1900 e 2100 MHz

UMTS: 850, 1900 e 2100 MHz

EDGE: 850, 900, 1800 e 1900 MHz

GPRS: 850, 900, 1800 e 1900 MHz

CDMA 1xEV-DO Rev A: 800 e 1900 MHz

CDMA 1xEV-DO Rel 0

CDMA 1xRTT

o *Deve permitir o uso de antenas externas ao módulo que possam ser instaladas distantes do CPE.*

o *Deve permitir a monitoração de informações de rádio freqüência, da operação da interface e do tráfego através do protocolo.*

• *Deve suportar o protocolo HDLC (High-Level Data Link Control).*

• *Deve suportar o protocolo Frame Relay.*

• *Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame-Relay e PPP sobre Ethernet).*

• *Deve suportar, no mínimo, os padrões do Frame Relay Forum abaixo especificados ou superiores:*

o *FRF.16 – Multilink Frame Relay UNI/NNI Implementation Agreement;*

o *FRF.12 – Frame Relay Fragmentation Implementation Agreement;*

• *Deve suportar o protocolo roteável IP.*

• *Deve permitir a configuração de roteamento estático.*

• *Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:*

o *RFC 1587 – The OSPF Not-So-Stubby Area (NSSA) Option;*

o *RFC 1745 – BGP4/IDRP for IP --- OSPF Interaction;*

o *RFC 1253 ou 1850 – OSPF Version 2 Management Information Base;*

o *RFCs 2328 ou 2178 – OSPF Version 2;*

o *RFC 2370 – The OSPF Opaque LSA Option ;*

• *Deve suportar o protocolo de roteamento BGP versão 4, conforme os padrões RFCs especificados abaixo:*

o *RFCs 1771 ou 1654 – A Border Gateway Protocol (BGP-4);*

o *RFC 2796 – Autonomous System Confederation for BGP;*

o *RFC 1997 – BGP Communities Attribute;*

o *RFCs 2283 ou 2858 – Multi-Protocol Extensions for BGP-4;*

o *RFC 2439 – BGP Route Flap Damping;*

o *RFC 2842 – Capabilities Advertisement with BGP-4;*

o *RFC 2918 – Route Refresh Capability for BGP-4;*

• *Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.*

• *Deve possuir suporte ao modo de operação full-duplex em todas as interfaces Ethernet.*

• *Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.*

• *Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 – The IP Network Address Translator (NAT) ou RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).*

• *Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT).*

• *Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338.*

• *Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode).*

• *Deve possuir suporte a implementação das funcionalidades de DHCP Relay.*

• *Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer 4.*

- *Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ).*
- *Deve suportar a funcionalidade de Policy-Based Routing (PBR).*
- *Deve possuir suporte a túneis de roteamento.*
- *Deve possuir suporte a Traffic Shapping.*
- *Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 2030 ou 4330 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, ou o protocolo NTP (Network Time Protocol).*
- *Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819 - Remote Network Monitoring Management Information Base.*
- *Deve implementar facilidades de syslog.*
- *Deve possuir suporte a autenticação de usuário através de RADIUS, em conformidade com, no mínimo, o padrão RFC 2865.*
- *Deve possuir suporte a autenticação de usuário através de TACACS em conformidade com, no mínimo, o padrão RFC 1492.*
- *Deve possuir suporte a protocolo de redirecionamento para cache de Web.*
- *Deve possuir suporte ao protocolo de gerenciamento SNMP e a MIB-II, em conformidade com as RFCs 1157 e 1213, respectivamente.*
- *Deve possuir suporte ao protocolo SNMPv2c.*
- *Deve possuir suporte ao protocolo SNMPv3.*
- *Deve implementar segurança baseada em, no mínimo, 2 (dois) níveis de acesso para a administração do equipamento.*
- *Deve fornecer suporte para prevenir fluxo de dados de entrada não autorizados através da configuração de filtros baseados em parâmetros de Layer 3 e Layer 4 do protocolo IP.*
- *Deve suportar a configuração de métodos de priorização de tráfego por tipo de protocolo e por serviços da pilha TCP/IP.*
- *Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol).*
- *Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508.*
- *Deve permitir administração e configuração através de interface de linha de comando (CLI).*
- *Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas.*
- *Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador.*
- *Deve ter a capacidade de atualização de software via FTP ou via TFTP, em conformidade com as RFCs 0783 ou 1350 – The TFTP Protocol (Revision 2).*
- *Deverá possuir suporte a técnicas de gerenciamento inteligente de energia, podendo desligar portas e módulos quando não utilizados para conservar energia.*
- *Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:*
  - *Digital Encryption Standard (DES) e Triple DES (3DES);*
  - *Advanced Encryption Standard (AES) 128, 192, e 256;*
  - *Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5_hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1_hmac.*
- *O equipamento deverá suportar, via licença adicional ou upgrade de software, no mínimo as seguintes funcionalidades:*
  - *Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol).*
  - *Deve suportar a criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCS 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.*
  - *Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC.*
  - *Deve suportar a criação de túneis VPN dinamicamente para criar uma rede VPN totalmente ligada.*
  - *Deve suportar a concentração de VPNs (IPSEC) para acessos remotos.*
  - *Deve suportar a concentração de SSL-VPNs para acessos remotos.*
  - *O equipamento fornecido suportar terminar simultaneamente conexões IPSEC do tipo "site-to-site","client-to-site" (VPNs de acesso remoto) e "clienteless" VPN (SSL VPN) . Nas conexões do tipo "client-to-site" (acesso remoto) o equipamento deve ser capaz de passar parâmetros tais como endereço IP, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name para o cliente VPN*

que está solicitando a conexão. Suporte a certificados digitais para autenticação das conexões IKE e IKEv2.

- *Implementar/suportar mecanismo de automatização do processo de enrollment na autoridade certificadora para no mínimo as seguintes CAs de mercado: Baltimore, Entrust, Verisign, Microsoft e RSA.*
- *Deve suportar a autenticação e autorização de usuários para acesso VPN.*
- *Deve suportar a operação como "Stateful Firewall" sem necessidade de adição de modulo específico para esta função, com no mínimo as seguintes características:*

- *Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP (e UDP), status dos flags "ACK", "SYN" e "FIN".*
- *Implementar filtragem "stateful" para pelo menos os seguintes protocolos de aplicação: HTTP, HTTPS, FTP, CIFS, SMTP, ESMTP, IMAP, POP3.*
- *Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "peer-to-peer": Kazaa, Morpheus, Gnutella, Edonkey, Bittorrent.*
- *Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "Instant Messaging": Yahoo messenger, AOL IM, ICQ, MSN.*

- *Bloquear "applets" Java . Deve ser possível efetuar tal bloqueio de forma geral ou para "applets" oriundos de endereços IP previamente especificados de endereços IP previamente especificados.*
- *Suportar operação como Firewall Transparente.*
- *Suportar a filtragem de pacotes Ipv4 e Ipv6.*
- *Prover proteção distribuída para diversos tipos de ataques, worms, exploits, vírus e vulnerabilidades de sistemas operacionais e aplicações.*
- *Deve suportar Intrusion Prevention System (IPS) com assinaturas de ataques, sem necessidade de adição de modulo especifico para esta função.*
- *Eliminar a necessidade de equipamentos isolados de IPS espalhados por diversos pontos da rede.*
- *Prover a inspeção do tráfego de rede através de várias combinações de interfaces de redes locais e redes WAN, em ambos os sentidos.*
- *Proteção para vulnerabilidades de aplicações Microsoft SMB e vulnerabilidades de protocolos MSRPC.*
- *A solução deve trabalhar com escala de risco para os alarmes de IPS baseado em severidade, fidelidade.*
- *Prover identificação multivetor de ameaças, através de inspeção pormenorizada das camadas de rede 2-7. Proteger a rede de violações as políticas de vulnerabilidade e atividades anômolas.*
- *Prover tecnologia acurada de prevenção, através de avaliação de risco e meta de evento gerador, para fornecer ações preventivas sobre um vasto leque de ameaças.*

- *Deverá possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento.*
- *Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9.*
- *Deverá possuir console com porta USB.*
- *Deve possuir uma porta auxiliar com velocidade de até 115.2Kbps, serial assíncrona, com conector RJ-45.*
- *Deverá permitir a acomodação em rack padrão 19" e ter no maximo 2 unidades racks (2RU).*
- *Deverá operar entre as temperaturas de 10°C e 40ºC.*
- *Deverá ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação) e suportar temperatura ambiente de armazenamento entre 0°C e 50°C.*
- *Deve operar com alimentação elétrica de 110/220 V, 60 Hz, com seleção automática de voltagem.*

10.3. TIPO III

- *Deve possuir, no mínimo, 3 (três) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.*

- *Deve possuir no mínimo 1 (uma) interface ATM OC-3/STM-1.*
- *Deve suportar a inserção de interfaces analogicas (FXS ou FXO) e digitais de voz (E1).*
- *Deve suportar no mínimo 4 (quatro) interfaces de Voz digitais E1.*
- *Deve suportar no mínimo dois slot(s) internos para a inserção de DSPs (Digital Signal Processor).*
- *Deve suportar os CODEC's (G.711, G.723.1, G.728, G.729 ou G.729b).*
- *Deve ter a possibilidade de ser inserido em redes com serviços de Voz sobre IP (VoIP), Voz sobre Frame Relay (VoFR) e Voz sobre ATM (VoATM).*
- *Deve suportar mecanismo de controle de chamadas IP sem a necessidade de um controlador central.*
- *Deve suportar mecanismo que permita a continuidade do controle de chamadas IP mesmo após a perda de comunicação com o controlador de chamadas central.*
- *Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.*
- *Deve ter uma performance mínima de 980.000 pps com pacotes de 64 bytes.*
- *Deve implementar a opção local de carga do sistema do equipamento via memória Flash.*
- *Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.*
- *Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.*
- *Como uma opção de acesso alternativo, deve suportar a adição de módulo que permita a conexão de dados através de rede celular 3G com as seguintes características:*

o *Deve suportar as seguintes tecnologias e faixas de freqüência:*

HSPA: 850, 1900 e 2100 MHz
UMTS: 850, 1900 e 2100 MHz
EDGE: 850, 900, 1800 e 1900 MHz
GPRS: 850, 900, 1800 e 1900 MHz

CDMA 1xEV-DO Rev A: 800 e 1900 MHz
CDMA 1xEV-DO Rel 0
CDMA 1xRTT

o *Deve permitir o uso de antenas externas ao módulo que possam ser instaladas distantes do CPE.*
o *Deve permitir a monitoração de informações de rádio freqüência, da operação da interface e do tráfego através do protocolo.*

- *Deve suportar o protocolo HDLC (High-Level Data Link Control).*
- *Deve suportar o protocolo Frame Relay.*
- *Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame-Relay e PPP sobre Ethernet).*
- *Deve suportar, no mínimo, os padrões do Frame Relay Forum abaixo especificados ou superiores:*

o *FRF.16 – Multilink Frame Relay UNI/NNI Implementation Agreement;*
o *FRF.12 – Frame Relay Fragmentation Implementation Agreement;*

- *Deve suportar o protocolo roteável IP.*
- *Deve permitir a configuração de roteamento estático.*

- *Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:*

o *RFC 1587 – The OSPF Not-So-Stubby Area (NSSA) Option;*
o *RFC 1745 – BGP4/IDRP for IP --- OSPF Interaction;*
o *RFC 1253 ou 1850 – OSPF Version 2 Management Information Base;*
o *RFCs 2328 ou 2178 – OSPF Version 2;*
o *RFC 2370 – The OSPF Opaque LSA Option ;*

- *Deve suportar o protocolo de roteamento BGP versão 4, conforme os padrões RFCs especificados abaixo:*

o *RFCs 1771 ou 1654 – A Border Gateway Protocol (BGP-4);*

o RFC 2796 – Autonomous System Confederation for BGP;
o RFC 1997 – BGP Communities Attribute;
o RFCs 2283 ou 2858 – Multi-Protocol Extensions for BGP-4;
o RFC 2439 – BGP Route Flap Damping;
o RFC 2842 – Capabilities Advertisement with BGP-4;
o RFC 2918 – Route Refresh Capability for BGP-4;
• Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.
• Deve possuir suporte ao modo de operação full-duplex em todas as interfaces Ethernet.
• Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.
• Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 – The IP Network Address Translator (NAT) ou RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).
• Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT).
• Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338.
• Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode).
• Deve possuir suporte a implementação das funcionalidades de DHCP Relay.
• Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer 4.
• Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ).
• Deve suportar a funcionalidade de Policy-Based Routing (PBR).
• Deve possuir suporte a túneis de roteamento.
• Deve possuir suporte a Traffic Shapping.

• Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 2030 ou 4330 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, ou o protocolo NTP (Network Time Protocol).
• Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819 - Remote Network Monitoring Management Information Base.
• Deve implementar facilidades de syslog.
• Deve possuir suporte a autenticação de usuário através de RADIUS, em conformidade com, no mínimo, o padrão RFC 2865.
• Deve possuir suporte a autenticação de usuário através de TACACS em conformidade com, no mínimo, o padrão RFC 1492.
• Deve possuir suporte a protocolo de redirecionamento para cache de Web.
• Deve possuir suporte ao protocolo de gerenciamento SNMP e a MIB-II, em conformidade com as RFCs 1157 e 1213, respectivamente.
• Deve possuir suporte ao protocolo SNMPv2c.
• Deve possuir suporte ao protocolo SNMPv3.
• Deve implementar segurança baseada em, no mínimo, 2 (dois) níveis de acesso para a administração do equipamento.
• Deve fornecer suporte para prevenir fluxo de dados de entrada não autorizados através da configuração de filtros baseados em parâmetros de Layer 3 e Layer 4 do protocolo IP.
• Deve suportar a configuração de métodos de priorização de tráfego por tipo de protocolo e por serviços da pilha TCP/IP.
• Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol).
• Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508.
• Deve permitir administração e configuração através de interface de linha de comando (CLI).
• Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas.
• Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador.
• Deve ter a capacidade de atualização de software via FTP ou via TFTP, em conformidade com as RFCs 0783 ou 1350 – The TFTP Protocol (Revision 2).

- *Deverá possuir suporte a técnicas de gerenciamento inteligente de energia, podendo desligar portas e módulos quando não utilizados para conservar energia.*
- *Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:*
  - *Digital Encryption Standard (DES) e Triple DES (3DES)*
  - *Advanced Encryption Standard (AES) 128, 192, e 256*
  - *Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5_hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1_hmac*
- *O equipamento deverá suportar, via licença adicional ou upgrade de software, no mínimo as seguintes funcionalidades:*
  - *Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol).*
  - *Deve suportar a criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCS 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.*
  - *Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC.*
  - *Deve suportar a criação de túneis VPN dinamicamente para criar uma rede VPN totalmente ligada.*
  - *Deve suportar a concentração de VPNs (IPSEC) para acessos remotos.*
  - *Deve suportar a concentração de SSL-VPNs para acessos remotos.*
  - *O equipamento fornecido suportar terminar simultaneamente conexões IPSEC do tipo "site-to-site","client-to-site" (VPNs de acesso remoto) e "clienteless" VPN (SSL VPN) . Nas conexões do tipo "client-to-site" (acesso remoto) o equipamento deve ser capaz de passar parâmetros tais como endereço IP, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name para o cliente VPN que está solicitando a conexão. Suporte a certificados digitais para autenticação das conexões IKE e IKEv2.*
  - *Implementar/suportar mecanismo de automatização do processo de enrollment na autoridade certificadora para no mínimo as seguintes CAs de mercado: Baltimore, Entrust, Verisign, Microsoft e RSA.*
  - *Deve suportar a autenticação e autorização de usuários para acesso VPN.*
  - *Deve suportar a operação como "Stateful Firewall" sem necessidade de adição de módulo especifico para esta função, com no mínimo as seguintes características:*
    - *Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP (e UDP), status dos flags "ACK", "SYN" e "FIN".*
    - *Implementar filtragem "stateful" para pelo menos os seguintes protocolos de aplicação: HTTP, HTTPS, FTP, CIFS, SMTP, ESMTP, IMAP, POP3.*
    - *Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "peer-to-peer": Kazaa, Morpheus, Gnutella, Edonkey, Bittorrent.*
    - *Detectar e bloquear atividade de pelo menos os seguintes protocolos do tipo "Instant Messaging": Yahoo messenger, AOL IM, ICQ, MSN.*
    - *Bloquear "applets" Java . Deve ser possível efetuar tal bloqueio de forma geral ou para "applets" oriundos de endereços IP previamente especificados de endereços IP previamente especificados.*
    - *Suportar operação como Firewall Transparente.*
    - *Suportar a filtragem de pacotes Ipv4 e Ipv6.*
    - *Prover proteção distribuída para diversos tipos de ataques, worms, exploits, vírus e vulnerabilidades de sistemas operacionais e aplicações.*
  - *Deve suportar Intrusion Prevention System (IPS) com assinaturas de ataques, sem necessidade de adição de modulo especifico para esta função.*
    - *Eliminar a necessidade de equipamentos isolados de IPS espalhados por diversos pontos da rede.*
    - *Prover a inspeção do tráfego de rede através de várias combinações de interfaces de redes locais e redes WAN, em ambos os sentidos.*
    - *Proteção para vulnerabilidades de aplicações Microsoft SMB e vulnerabilidades de protocolos MSRPC.*
    - *A solução deve trabalhar com escala de risco para os alarmes de IPS baseado em severidade, fidelidade.*

- *Prover identificação multivetor de ameaças, através de inspeção pormenorizada das camadas de rede 2-7. Proteger a rede de violações as políticas de vulnerabilidade e atividades anômolas.*
- *Prover tecnologia acurada de prevenção, através de avaliação de risco e meta de evento gerador, para fornecer ações preventivas sobre um vasto leque de ameaças.*
- *Deverá possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento.*
- *Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9.*
- *Deverá possuir console com porta USB.*
- *Deve possuir uma porta auxiliar com velocidade de até 115.2Kbps, serial assíncrona, com conector RJ-45.*
- *Deverá permitir acomodação em rack padrão 19" e ter no máximo 3 unidades racks (3RU).*
- *Deverá operar entre as temperaturas de 10°C e 40oC.*
- *Deverá ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação) e suportar temperatura ambiente de armazenamento entre 0°C e 50°C.*
- *Deve operar com alimentação elétrica de 110/220 V, 60 Hz, com seleção automática de voltagem.*

10.4. TIPO IV

- *Possuir, no mínimo, 1 slot para a inserção de módulos.*
- *Possuir 6 (seis) interfaces Ethernet 1000Base-X para inserção de conectores SFP.*
- *Possuir capacidade de associação das portas 1000Base-X, no mínimo, em grupo de 4 (quatro) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.*
- *Suportar módulos com portas do tipo 10GBASE-X, E3 e OC-48.*
- *Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.*
- *Implementar VLANs por porta.*
- *Implementar VLANs compatíveis com o padrão IEEE 802.1q.*
- *Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas nesta especificação.*
- *Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.*
- *Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.*
- *Suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com a solução.*
- *Possuir fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e freqüência (de 50/60 Hz).*
- *Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.*
- *Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.*
- *Possuir LEDs para a indicação do status das portas e atividade.*
- *Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.*
- *Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:*
  - *Sem autenticação e sem privacidade (noAuthNoPriv);*
  - *Com autenticação e sem privacidade (authNoPriv);*
  - *Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES.*
- *Suportar SNMP sobre IPv6.*
- *Possuir suporte a MIB II, conforme RFC 1213.*
- *Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.*
- *Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.*
- *Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.*

- *Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.*
- *Permitir o gerenciamento via CLI e Web, utilizando SSH e HTTPS.*
- *Implementar nativamente 2 grupos RMON (Alarms e Events) conforme RFC 1757.*
- *O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede.*
- *Possibilidade de criação de versões de configuração e suporte a "rollback" da configuração para versões anteriores.*
- *Implementar Telnet para acesso à interface de linha de comando.*
- *Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.*
- *Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.*
- *Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.*
- *Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).*
- *Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.*
- *Permitir que a sua configuração seja feita através de terminal assíncrono.*
- *Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.*
- *Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.*
- *Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.*
- *Suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.*
- *Deve suportar IPv6.*
- *Implementar NAT (Network Address Translation).*
- *Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações:*
  - *IP de origem/destino;*
  - *Parâmetro "protocol type" do cabeçalho IP;*
  - *Porta TCP/UDP de origem/ destino;*
  - *Interface de entrada do tráfego;*
- *Deve ser possível especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída (e também para ambos os sentidos simultaneamente) em uma dada interface do roteador.*
- *A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado.*
- *Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:*
  - *ICMP echo;*
  - *TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);*
  - *UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);*
  - *O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.*
- *Implementar o protocolo NTPv3 (Network Time Protocol, versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições da RFC 1305.*
- *Implementar DHCP Relay e DHCP Server.*
- *Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway. Suportar mecanismo de autenticação MD5 entre os peers VRRP.*
- *Implementar roteamento estático.*
- *Implementar roteamento dinâmico RIPv2 (RFC 2453 e 2082).*
- *Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101, 3137, 3623 e 2370).*

- *Implementar protocolo de roteamento BGPv4 (RFC 4271, 3065, 4456, 1997, 1965, 1966, 4897, 2858 e 2385).*
- *Permitir o roteamento nível 3 entre VLANs.*
- *Implementar, no mínimo, 100 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente.*
- *Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.*
- *Suporte ao protocolo de Tunelamento GRE (General Routing Encapsulation - RFCs 2784), contemplando, no mínimo, os seguintes recursos:*
  - *Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica, definida pelo administrador do equipamento;*
  - *Operação em modo multiponto ("multipoint GRE");*
  - *Possibilidade de configuração de " Keepalive" nos túneis;*
  - *Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.*
- *Implementar roteamento baseado em origem, com a possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.*
- *Suportar roteamento estático para IPv6.*
- *Implementar roteamento dinâmico RIPng.*
- *Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.*
- *Implementar protocolo de roteamento Multiprotocol BGP com suporte a IPv6.*
- *Implementar , no mínimo, 4000 vlans simultaneamente.*

- *Implementar, no mínimo, 4000 interfaces vlans simultaneamente, para roteamento nível 3 entre as vlans configuradas.*
- *Possuir backplane de, no mínimo 2,5 (dois vírgula cinco) Gbps.*
- *Suportar pelo menos 1 (um) Gbps de throughput com todas as funcionalidades de roteamento e segurança ativas simultaneamente.*
- *Possuir uma taxa de comutação de pacotes de no mínimo 3 (três) milhões pacotes por segundo (Mpps)*
- *Possuir no mínimo 8 (oito) GB de memória DRAM.*
- *Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.*
- *Implementar filtragem de pacotes (ACL - Access Control List), para IPv4 e IPv6.*
- *Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.*
- *Proteger a interface de comando do equipamento através de senha.*
- *Implementar o protocolo SSH V2 para acesso à interface de linha de comando.*
- *Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.*
- *Permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Tuneis IPSEC.*
- *Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.*
- *Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.*
- *Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede.*
- *Suportar serviços de VPN baseados no padrão IPSec (IP Security Protocol)*
- *Suportar serviços de VPN baseados no padrão IKE(Internet Key Exchange)*
- *Suportar pelo menos 4000 (quatro mil) túneis IPSec VPN Site- to- Site.*
- *Suportar uma taxa de estabelecimento de túneis VPN de no mínimo 80 (oitenta) túneis por segundo.*
- *Suportar algorítmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões com VPN IPSec.*

- *Suportar a transparência de conexões IPSEC a NAT(NAT-T) através do encapsulamento dos pacotes IPSEC com UDP.*
- *Reagrupar pacotes de sessão fragmentados para análise e entrega no destino.*
- *Permitir a criação de VPNS IPSEC baseada em políticas de segurança.*
- *Suportar criação de VPNs de acordo com o conjunto de padrões IPSEC em modo túnel.*
- *Devem ser implementados os modos de operação "tunnel mode" e "transport mode". Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.*
- *Suportar as funcionalidades de gerenciamento de chaves para VPN.*
- *Suportar a utilização de clientes baseados em IPSEC.*
- *Implementar a criptografia dos pacotes de forma totalmente transparente e automática, sem a alteração dos cabeçalhos incluindo endereços IP de origem e destino, e portas de origem e destino.*
- *Implementando uma rede VPN totalmente ligada com criptografia entre sites (full-mesh), sem a necessidade de túneis ponto a ponto conforme RFC 3547.*
- *Suportar o tráfego protocolo GRE sobre IPSEC.*
- *Suportar o tráfego de IP multicast sobre IPSEC.*
- *Implementar padrão IEEE 802.1q (Vlan Frame Tagging).*
- *Implementar padrão IEEE 802.1p (Class of Service) para cada porta.*
- *Implementar padrão IEEE 802.3ad.*
- *Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).*
- *Implementar mecanismo de controle de multicast através de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).*
- *Implementar roteamento multicast PIM (Protocol Independent Multicast) nos modos "sparse-mode" (RFC 2362) e "dense-mode". Deve ser suportada, por interface, a operação simultânea nos modos "sparse-mode" e "dense mode".*
- *Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.*
- *Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).*
- *Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.*
- *Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).*
- *Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".*
- *Deve ser possível a especificação de banda por classe de serviço.*
- *Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.*
- *Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection).*
- *Implementar LFI (Link Fragmentation e Interleaving), tanto em interfaces seriais com encapsulamento Frame Relay, quanto em interfaces seriais configuradas com encapsulamento PPP.*
- *Implementar RTP (Real-Time Transport Protocol) e a compressão do cabeçalho dos pacotes RTP (IP RTP Header Compression).*
- *Implementar priorização nível 2 IEEE 802.1p e priorização nível 3 dos tipos "IP precedence" e DSCP (Differentiated Services Code Point).*
  - *O roteador deve suportar o mapeamento das prioridades nível 2 (IEEE 802.1p) em prioridades nível 3 (IP Precedence e DSCP) e vice-versa.*
- *Implementar política de enfileiramento nas linhas seriais (priorização de tráfego por tipo de protocolo trafegado).*
  - *Devem ser suportadas pelo menos as seguintes técnicas de enfileiramento: Priority Queuing, Custom Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing e Low Latency Queuing.*
- *Implementar RSVP (Resource Reservation Protocol).*
- *Implementar IPv6.*
- *Permitir a configuração de endereços IPv6 para gerenciamento.*
- *Permitir consultas de DNS com resolução de nomes em endereços IPv6.*
- *Implementar ICMPv6 com as seguintes funcionalidades:*

o ICMP request;
o ICMP Reply;
o ICMP Neighbor Discovery Protocol (NDP);
o ICMP MTU Discovery.
• Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, SNMP, SYSLOG e DNS sobre IPv6.
• Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6."

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 05

ENCARTE TÉCNICO I - O ITEM 14.4 – pág 51 – solicita que:

> *"14.4. A CONTRATADA deverá implementar e fornecer, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de pelo menos 5 (cinco) classes de serviços:"*

Justificativa: A marcação de QoS é uma característica intrínseca de uma solução MPLS, onde são dimensionas CoS (classes de serviço) por modalidade e aplicação do cliente. Em uma solução SD-WAN ocorre a priorização de tráfego (traffic shaping) em tuneis IPSEC, não fazendo sentido uma marcação de QoS em uma rede IP. Segue sugestão da redação

Sugestão: *14.4. A CONTRATADA deverá implementar e fornecer na solução MPLS, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de pelo menos 5 (cinco) classes de serviços"*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 06

ENCARTE TÉCNICO I - O ITEM 16.4 – pág 54 – define que:

> *"16.4. A Solução de Gerência da Rede deverá ter como base a plataforma Open-Source, sem qualquer necessidade de licenciamento para seu pleno funcionamento, e poderá usar como painel de controle ou backend a ferramenta de monitoramento nativa da CONTRATANTE;*
> *16.5. A Solução de Gerência da Rede não deverá demandar licenciamento para o seu funcionamento pleno e ao final da vigência contratual será entregue integralmente à CONTRATADA devidamente operacional;."*
>
> *"16.11. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto não serão aceitas soluções que possuem acessos segmentados aos módulos;"*

Justificativa: A solução de gerência da CONTRATADA possui softwares intrínsecos a solução e desenvolvidos/adquiridos pela mesma, sendo assim os mesmos não pode ser fornecidos como uma venda de ativo/licença ao fim do contrato, lembrando que a licitação engloba prestação de serviços SCM. Segue sugestão de redação:

Sugestão: *Retirar os itens 16.5 e 16.11*

RESPOSTA: Acataremos a sugestão de retirada do item 16.5.

SUGESTÃO 07

ENCARTE TÉCNICO I - O ITEM 16.9 – pág 54 – define que:

> *"16.9. A solução de Gerência da Rede da CONTRADA deverá enviar os alertas de incidentes também via e-mail e SMS;."*

Justificativa: Sugerimos a flexibilização das notificações onde os alertas poderão ser enviados via e-mail OU sms. Segue sugestão de redação:

Sugestão: *"16.9. A solução de Gerência da Rede da CONTRADA deverá enviar os alertas de incidentes também via e-mail ou SMS;."*

RESPOSTA: Acataremos a sugestão especificando que o alerta de e-mail é obrigatório e o SMS será opcional.

SUGESTÃO 08

ENCARTE TÉCNICO I - O ITEM 17.10 – pág 58 – solicita os seguinte SLA

Nível	RTT	Sítios
N1	≤ 100ms	Fibra Ótica, Rádio Terrestre e Par Metálico
N2	≤ 600ms	Acesso Satélite

Tabela 3 – Tempo de Retardo (RTT)

Justificativa/Sugestão: Sugerimos alterar a latência do acesso SAT para até 1000ms.

RESPOSTA: Acataremos a sugestão de latência para até 1000ms.

SUGESTÃO 09

ENCARTE TÉCNICO I - O ITEM 23.5 – pág 68 – solicita o seguinte:

> *"23.5. Não serão aceitas redes híbridas de forma segregada, ou seja, um equipamento concentrador SDWAN e um equipamento concentrador MPLS conectados para formar uma rede híbrida. A solução deverá ser única, seja uma rede puramente MPLS ou uma rede puramente SD-WAN, contendo apenas um hardware;*

Justificativa: Considerando o princípio da competitividade neste certame, sugerimos uma igualdade de condições para os principais licitantes, deliberando a utilização de uma solução hibrida em tecnologias (SD-WAN + MPLS), onde poderá também ser utilizado em um mesmo ambiente equipamentos segregados, ou seja, equipamentos MPLS e SD-WAN. Retirando-se

também restrição de apenas um hardware para suportar SD-WAN + MPLS. Segue sugestão da redação:

Sugestão: *"23.5. Serão aceitas redes híbridas agregadas ou segregadas, ou seja, um equipamento concentrador SDWAN e um equipamento concentrador MPLS conectados para formar uma rede híbrida. A solução não necessariamente deverá ser uma rede puramente MPLS ou uma rede puramente SD-WAN, contendo apenas um hardware;*

RESPOSTA: Será alterado o texto permitindo redes hibridas, desde que em um equipamento único, ou módulos independentes mas que façam parte do mesmo "chassis", de um equipamento único.

SUGESTÃO 10

15. SERVIÇO DE SEGURANÇA GERENCIADA (MSS), página 59.

> *"15.9. O Serviço de Segurança Gerenciada deve contemplar a monitoração proativa do (s) dispositivo (s) de segurança ofertado (s), pela CONTRATADA, sendo esses uma solução de segurança cujo fabricante é avaliado pelo Gartner Group, mencionado em seu quadrante mágico;"*

Justificativa: Exigir que o fabricante de segurança seja avaliado pelo Gartnet Group restringe a competitividade do certame. Avaliações não podem ser exigidas como itens indispensáveis a serem provados por licitantes, pois falta expressa autorização legal para tanto. Como é sabido, a Administração Pública está vinculada ao princípio da legalidade, e nesta esfera o conteúdo jurídico do princípio da legalidade implica que o agente público somente pode fazer o que a lei expressamente autoriza. Apenas seria válido solicitar que o fabricante seja avaliado pelo Gartner em geral somente podem ser utilizadas como elementos de pontuação, nunca como itens de cumprimento obrigatório, a não ser as avaliações expressamente impostas pela lei, tais como as certificações ANATEL, INMETRO, ANVISA, Certics, etc. e somente para os produtos indicados nas respectivas normas.

Sugestão: *Sugerimos a retirada item 15.9.*

RESPOSTA: A necessidade de o fabricante estar listado no quadrante mágico do Gartner nos garante que o fabricante é mundialmente reconhecido e possui qualidade de produto e suporte adequados à nossa necessidade.

SUGESTÃO 12

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 22.

> *"9.2.2.5. Deve possuir 1 (uma) interface de rede Gigabit dedicada para gerenciamento;"*

Justificativa: Visando a competitividade no certame e sem perda de requisito funcional, limitar a oferta de produtos que apenas permitem que uma das interfaces ser utilizada para gerenciamento restringe a ampla participação de diversos fornecedores de segurança. Na questão técnica, ter apenas uma interface de gerenciamento coloca em risco perder a administração caso a interface apresente defeito.

Sugestão: *Baseado no exposto acima sugerimos a remoção do item.*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 13

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 25.

> *"9.2.4.3. Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;"*

Justificativa: A classificação dinâmica utiliza recurso de verificação de comportamento para classificar a aplicação. Esse método retorna muitos erros de classificação e permite ao usuário acessar uma aplicação que deveria ser bloqueada. Sugerimos reescrita do item conforme sugestão abaixo:

> **Sugestão:** *"9.2.4.3. Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações e categorias de aplicações;"*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 14

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 25 e 26

> *9.2.5.Controle de Aplicações:*
> *9.2.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independentemente de porta e protocolo, com as seguintes funcionalidades: "*
> ▪ *Deve permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do ambiente do CONTRATANTE;*
> ▪ *A criação de assinaturas personalizadas deve permitir o uso de expressões regulares e contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de, pelo menos, os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL; "*

Justificativa: Permitir que o usuário escreva as próprias assinaturas irá abrir a possibilidade de escrita de uma regra errada e assim causar o bloqueio do tráfego ou até mesmo não fazer tratamento nenhum. O mais grave para o mundo da segurança é o usuário acreditar que está protegido, ou seja, a falsa sensação que estar seguro. Somente o fabricante da solução é capaz de produzir assinaturas eficientes.

Sugestão: *Sugerimos a remoção do item.*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 15

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 27

> *9.2.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;"*

Justificativa: O tipo de controle que fazemos é bloquear o tráfego efetuando o drop da conexão, ou seja, o pacote é descartado sem o envio do tcp-reset. Esse controle é muito mais relevante para o ambiente protegido, pois assim o atacante não sabe que existe um equipamento de segurança identificando o ataque. O hacker a partir do tcp-reset pode promover um ataque direcionado colocando assim em risco o ambiente. Sugerimos a remoção do trecho "enviar tcp-reset;"

> **Sugestão:** *9.2.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo;"*

RESPOSTA: Acataremos a sugestão tendo em vista que não impacta negativamente na qualidade do projeto.

SUGESTÃO 16

Item 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ, página 28

> *"9.2.6.7. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens:*
> *Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;"*

Justificativa: O protocolo SMB nada mais é que uma rede Microsoft. Efetuar o bloqueio de vírus no tráfego SMB já é executado pelos produtos de antivírus e ATP instalados nos SO Windows. A solução de Firewall quando analisa o protocolo SMB decai seu processamento, colocando assim a rede indisponível.
Sugestão: *Sugerimos a remoção do trecho "SMB"*

RESPOSTA: Acataremos a sugestão tendo em vista que não impacta negativamente na qualidade do projeto.

ENCARTE TÉCNICO II
REDE IP INTERNET SIMÉTRICA

SUGESTÃO 1

ENCARTE TÉCNICO II - O ITEM 3.21 – pág 07 – solicita o seguinte:

> *"3.21. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 25ms;*

Justificativa: Sugerimos alterar a latência para até 80ms. Segue sugestão de redação:

Sugestão *: ""3.21. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 80ms;;*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 2

ENCARTE TÉCNICO II - O ITEM 6.156– pág 23 – solicita o seguinte:

> *"6.156. A solução deverá ser totalmente apartada dos roteadores, sendo do tipo appliance e compatível para instalação no Datacenter da CONTRATANTE, não sendo permitida a utilização de módulos acoplados;;*

Justificativa Visando uma maior competitividade no certame, sugerimos flexibilizar o atendimento com a solução de Firewall embarcada nos roteadores ou a utilização de um appliance apartado. Segue sugestão de redação:

Sugestão *: "6.156. A solução poderá ser totalmente apartada dos roteadores ou embarcada nos equipamentos, sendo compatível com a instalação no Datacenter da CONTRATANTE, não sendo permitida a utilização de módulos acoplados;*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 3

ENCARTE TÉCNICO II - O ITEM 6.157– pág 23 – solicita o seguinte:

> *"6.157. A solução deverá atender, inclusive, aos circuitos de redundância, caso existam, independente da operadora contratada, quando os mesmos assumirem a posição de link principal;*

Justificativa: O TR em nenhum momento cita que terão links de contingência de operadoras distintas neste lote, sugerimos retirar este item.

RESPOSTA: Acataremos a sugestão tendo em vista que não impacta negativamente na qualidade do projeto.

SUGESTÃO 4

ENCARTE TÉCNICO II - O ITEM 6.158– pág 23 – define que:

> *"6.158. A solução deverá se integrar com o SNOC, e ferramentas de segurança fornecido pela CONTRATADA vencedora do Lote I e/ou do PRODERJ, sem que isto retire as suas responsabilidades*
> *conforme Termo de Referência e este Encarte Técnico.;*

Justificativa Fica-se inviável analisar uma integração entre sistemas de gestão e segurança de empresas e fornecedores distintos sem uma análise prévia dos part numbers e plataformas que as empresas irão utilizar. Sugerimos retirar este item, dado que é grande a chance de insucesso.

Sugestão *: Sugerimos remover o iten 6.158 ou que esteja explicito no item mecionado, que a integração será efetuada pela PRODERJ, onde as contratadas somente enviariam os MIBs dos equipamentos gerenciados para este respectivo órgão.*

RESPOSTA: Para a CONTRATADA do Lote II, este item se refere tão somente ao envio do tráfego para o SNOC realizar a análise e gerar os alertas no âmbito da prestação dos serviços do Lote I. Não entendemos isto como algo complexo.

SUGESTÃO 5

ENCARTE TÉCNICO II - O ITEM 10.6 – pág 23 – define que:

> *"10.6. A ativação dos enlaces referentes ao backbone da Rede IP Simétrica deverá ser feita numa*
> *única fase, que terá duração máxima de até 30 (trinta) dias, incluindo instalação e ativação dos circuitos, a contar da data de aprovação do Projeto Executivo;.;*

Justificativa: Dado o quantitativo de links simétricos que estão sendo licitados, é inviável tecnicamente para a contratada e também para a contratante que todos os 358 links sejam ativados em até 30 dias. Sugerimos alterar o prazo de uma ativação total de 120 dias para todo o projeto. Segue sugestão de redação:

Sugestão: *"10.6. A ativação dos enlaces referentes ao backbone da Rede IP Simétrica poderá ser efetuada em fases, porém respeitando um prazo máximo de até 120 (cento e vinte dias) para ativação de todo o projeto, incluindo instalação e configuração dos circuitos, a contar da data de aprovação do Projeto Executivo;.;*

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 6

ENCARTE TÉCNICO II - O ITEM 12.6.2 – pág 32 – demonstra a seguinte tabela:

Nível	IDM	Serviços
N1	≥ 99,99%	Serviços de Acesso à Internet do Datacenter PRODERJ
N2	≥ 99,8%	Serviços de Acesso à Internet demais órgãos e secretarias – região metropolitana
N3	≥ 99,7%	Serviços de Acesso à Internet demais órgãos e secretarias – região não metropolitana

Tabela 1 – Índice de Disponibilidade Mensal (IDM)

Justificativa/Sugestão: Dado que para o lote 2 não foi contemplada nenhuma contingência de meio físico ou SD-WAN e que os endereços abrangem quase todo os municípios do estão do Rio de Janeiro, sugerimos alterar os IDMs N2 e N3 para o mesmo percentual dos IDMs do lote 1.

RESPOSTA: Os IDMs N2 e N3 são para órgãos que hoje possuem serviços críticos publicados na Internet (Ex. Secretaria de Fazenda), não cabendo um IDM diferente dos que foram definidos.

SUGESTÃO 7

ENCARTE TÉCNICO II - O ITEM 12.9 – pág 33 – demonstra a seguinte tabela:

Nível	RTT	Serviços
N1	≤ 20ms	Serviços de Acesso à Internet

Tabela 3 – Tempo de Retardo

Justificativa/Sugestão Sugerimos alterar a latência para até 80ms.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 8

ENCARTE TÉCNICO II - O ITEM 12.10 – pág 33 – demonstra a seguinte tabela:

Nível	PR	Serviços
N1	≤ 2 horas	Serviços de Acesso à Internet

Tabela 4 – Prazo de Reparo (PR)

Justificativa/Sugestão: Considerando que a distribuição dos links IP ocorrem em quase todos os municípios do estado do RJ, sugerimos alterar o tempo de reparo conforme os prazos de reparo do lote 1, lembrando que temos uma semelhança nessa distribuição geográfica.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 9

ENCARTE TÉCNICO II - O ITEM 12.10 – pág 33 – demonstra a seguinte tabela:

Nível	PAC	Serviços
N1	≤ 30 dias	Serviços de Acesso à Internet

Tabela 5 – Prazo de Alteração de Transmissão (PAT)

Justificativa/Sugestão: Dado o quantitativo de links simétricos que estão sendo licitados, é inviável tecnicamente para a contratada e também para a contratante que todos os 358 links sejam ativados em até 30 dias. Sugerimos alterar o prazo de uma ativação total de 120 dias para todo o projeto.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 10

ENCARTE TÉCNICO II - O ITEM 6.3 e ITEM 6.4 – pág 09 – solicitam o seguinte:

> *"6.3. Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de sequência dos pacotes TCP, status dos flags "ACK", "SYN" e "FIN";*
>
> *6.4. Deve permitir a "randomização" do número de sequência TCP, ou seja, funcionar como um "proxy" de número de sequência TCP de modo a garantir que um host situado em uma interface considerada "externa" (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;"*

Justificativa: Os itens citados acima permitem a participação de apenas 1 único fabricante nesta solução, encarecendo dessa maneira o preço final da oferta.

Sugestão: *Para manter a ampla participação é necessário remover os itens citados.*

RESPOSTA: Os itens serão removidos tendo em vista que não impactam significativamente na qualidade do projeto.

SUGESTÃO 11

ENCARTE TÉCNICO II - O ITEM 6.6 – pág 09 – solicitam o seguinte:

> *"6.6. Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços. Deve ser possível verificar a utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;"*

Justificativa: A solicitação de hit counts também pode ser atendida se o produto indicar a quantidade de tráfego por regra. Sugerimos que adicione no texto que pode ser *hit counts ou quantidade de tráfego de cada regra de filtragem individualmente.*

RESPOSTA: Acataremos a sugestão tendo em vista que não impacta negativamente na qualidade do projeto.

SUGESTÃO 12

ENCARTE TÉCNICO II - OS ITENS 6.15, 6.16, 6.17 e 6.18 – pág 10 – solicitam o seguinte:

> *"6.15. Deve possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H.323 (v1, v2, v3, v4), SIP (Session Initiation Protocol), MGCP e SCCP;*
>
> *6.16. A partir da inspeção dos protocolos de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos;*
>
> *6.17. Deve ser suportada à inspeção do protocolo SIP (SIP over TLS) em ambientes com voz criptografada;*
>
> *6.18. A partir da inspeção do protocolo de sinalização, devem ser criadas as conexões pertinentes para o tráfego SRTP (Secure RTP);"*

Justificativa/Sugestão: As soluções padrões de mercado, atuam no protocolo de comunicação SIP/H323 priorizando o tráfico sobre outros protocolos de rede, garantindo desta fora a qualidade da comunicação VOIP. Desta forma solicita sugerimos a remoção dos itens acima.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 13

ENCARTE TÉCNICO II - OS ITENS 6.24, 6.25, 6.26, 6.27, 6.28 e 6.29 – pág 10 – solicitam o seguinte:

> *"6.24. Deve possuir suporte a tecnologia de Firewall Virtual, com instâncias totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas;*
>
> *6.25. Dentro de cada instância de Firewall deve ser possível alocar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;*
>
> *6.26. Dentro de cada instância de Firewall deve ser possível limitar (promover "rate limiting") os seguintes recursos: taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog;*
>
> *6.27. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter Influência sobre a operação das demais instâncias;*
>
> *6.28. Deve ser possível selecionar o modo de operação de cada instância de Firewall*

(seleção, por instância, de modo transparente ou roteado);

6.29. Deve ser suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias solicitado;"

Justificativa: A virtualização do firewall implica em consumo computacional relacionado a processamento e memória para suportar múltiplas instâncias virtuais. O objeto do lote 2 é para a aquisição de uma rede IP de baixo desempenho e para exclusivo acesso de internet. Essa solução acarreta alto custo para o certame de forma desnecessária e por conseguinte baixa economicidade para o órgão.

Sugestão: Sugerimos retirar esse item.

RESPOSTA: O objeto do lote 2 não é para aquisição de rede IP de baixo desempenho, é para rede IP Internet de alto desempenho e resiliência. Desta forma deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 13

ENCARTE TÉCNICO II - O ITEM 6.38 – pág 11 – solicitam o seguinte:

"6.38. Deve suporte à integração com servidores RADIUS, LDAP, Microsoft AD e Kerberos, para tarefas de autenticação, autorização e accounting (AAA) dos usuários VPN;"

Justificativa/Sugestão: A solicitação de suporte a integração com servidores Kerberos apenas limita a participação de alguns fabricante, pois trata-se de protocolo descontinuado e suas funções são plenamente atendidas com a requisição de suporte a Microsoft AD. Sugerimos a remoção do texto "kerberos".

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 14

ENCARTE TÉCNICO II - OS ITENS 6.40, 6.41, 6.51 e 6.55 – páginas 11 e 12– solicitam o seguinte:

"6.40. Deve ser capaz de configurar nos VPN clients uma lista de acesso de "split tunneling", de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta
(sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo "all tunneling", em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;

6.41. Deve permitir a criação de "banners" personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa;

6.51. Deve permitir a terminação de conexões no modo IPSEC over TCP;

6.55. Deve ser possível definir vários templates de conexão no cliente VPN antes que seja

enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES, AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração ("lifetime") da conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN cliente;

Justificativa/Sugestão: Os itens citados acima são referentes ao estabelecimento de comunicação VPN e fogem do padrão mínimos exigido para que ocorra a perfeita comunicação entre duas unidades remotas. Os itens apenas restringem a ampla participação do mercado. Sugerimos a remoção dos itens.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 15

ENCARTE TÉCNICO II - O ITEM 6.62 – pág 13 – solicita o seguinte:

"6.62. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;"

Justificativa/Sugestão: O protocolo Telnet é inseguro e passível de captura dos dados, pois não ocorre de modo criptografado. Sugerimos por questões de segurança a remoção dos itens.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 16

ENCARTE TÉCNICO II - O ITEM 6.88– pág 14 – solicita o seguinte:

"6.88. Deve permitir a customização de regras de detecção de novas aplicações;"

Justificativa/Sugestão: A customização de regras pode ocorrer exclusivamente pelo fabricante, pois assim garante maior confiabilidade e elimina o erro de indisponibilidade do sistema se ocorrer a escrita errada da regra. Por motivos de segurança da sugerimos a remoção do item.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 17

ENCARTE TÉCNICO II - O ITEM 6.89 – pág 14 – solicita o seguinte:

"6.89. Deverá suportar a funcionalidades de filtragem de URL, através de licenciamento opcional e atendendo no mínimo as seguintes características:
Deve possibilitar o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo);"

Justificativa/Sugestão: A solicitação apenas restringe a ampla participação. Sugerimos a exclusão do item.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 18

ENCARTE TÉCNICO II - OS ITENS 6.116, 6.118, 6.120, 6.121 e 6.122 – páginas 18 e 19 – solicitam o seguinte:

> *"6.116. Deve permitir a inclusão de informações de vulnerabilidades oriundas de ferramentas de varredura externa;*
>
> *6.118. Deve permitir a análise do comportamento da rede, com o intuito de detectar ameaças com origem/destino a segmentos monitorados pelo IPS. Isto inclui a capacidade de estabelecer padrões "normais" de tráfego através de técnicas de análise de fluxo (por exemplo, Netflow) e a capacidade de detectar desvios dos padrões considerados normais;*
>
> *6.120. Deve permitir coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo(s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas:*
> - *Sistema operacional do Host;*
> - *Serviços existentes no Host;*
> - *Portas em uso no Host;*
> - *Aplicações em uso no Host;*
> - *Vulnerabilidades existentes no Host;*
> - *Smart phones e tablets;*
> - *Network flow;*
> - *Anomalias de redes;*
> - *Identidades de usuários;*
> - *Tipo de arquivo e protocolo;*
> - *Conexões maliciosas.*
>
> *6.121. Deve permitir criar uma lista com o "ambiente ideal esperado" e a cada mudança nesse ambiente, o sensor deverá no mínimo alertar a console de gerencia sobre a mudança identificada.*
> *Entendemos como "ambiente ideal esperado" o conjunto de informações pré-configuradas na gerencia dos sensores de IPS a respeito dos atributos dos hosts participantes desse segmento, deve ser configurado no mínimo os seguintes atributos:*
> - *Sistema Operacional;*
> - *Serviços vigentes nos hosts;*
> - *Aplicações autorizadas a serem executadas nos hosts;*
> - *Aplicações não autorizadas a serem executadas nos hosts.*
>
> *6.122. Deve permitir criar ou importar regras no padrão OpenSource (SNORT), essas regras, devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não deve haver limite da quantidade de regras a serem criadas ou importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;"*

Justificativa/Sugestão: Os itens descritos tem como missão atender a soluções de segurança de concentradores/Datacentes que expõem aplicações para acesso externo, desta forma os

itens acima aumentam a complexidade das soluções, consequentemente elevando os custos do certame e restringindo a ampla participação. Sugerimos a exclusão dos itens.

RESPOSTA: O objeto do Lote II é exatamente prover uma rede IP para clientes que possuem aplicações para acesso externo, desta forma, deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 19

ENCARTE TÉCNICO II - O ITEM 6.124 – pág 19 – solicita o seguinte:

> *"6.124. Deve possuir capacidade de criar assinaturas definidas pelo usuário com uso de Expressões regulares;"*

Justificativa/Sugestão: A customização de regras pode ocorrer exclusivamente pelo fabricante, pois assim garante maior confiabilidade e elimina o erro de indisponibilidade do sistema se ocorrer a escrita errada da regra. Sugerimos a remoção do item.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 20

ENCARTE TÉCNICO II - OS ITENS 6.133, 6.134, 6.136 e 6.141 – pág 20 – solicitam o seguinte:

> *"6.133. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de*
> *30 Gbps (Vinte) para pacotes TCP multiprotocolo;*
>
> *6.134. Deve suportar um throughput de, no mínimo, 20 Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;*
>
> *6.136. Deve possuir desempenho de, no mínimo, 10Gbps (Cinco Gbps) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;*
> *6.141. Deve possuir mais de 280 Milhões de URL categorizadas;"*

Justificativa/Sugestão: Os valores acima são números além da necessidade do órgão baseado no levantamento dos links de internet e apenas limitam a ampla participação do mercado. Sugerimos a mudança para os valores abaixo descritos:

> "6.133. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de
> 10 Gbps (Vinte) para pacotes TCP multiprotocolo;
>
> 6.134. Deve suportar um throughput de, no mínimo, 5 Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;
>
> 6.136. Deve possuir desempenho de, no mínimo, 4 Gbps (quatro Gbps) para tratamento de
> conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;
>
> 6.141. Deve possuir mais de 40 Milhões de URL categorizadas;"

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

SUGESTÃO 21

ENCARTE TÉCNICO II - OS ITENS 6.116, 6.118, 6.120, 6.121 e 6.122 – páginas 18 e 19 – solicitam o seguinte:

> *"6.128. Deve ser fornecido com pelo menos 8 (oito) interfaces 1 Gigabit Ethernet;*
> *6.129. Deve ser fornecido com pelo menos 4 (quatro) interfaces 10 Gigabit;*
> *6.130. Deve suportar pelo menos 50.000.000 (cinquenta milhões) conexões simultâneas em sua tabela de estados de Stateful Firewall;*
> *6.131. Deve suportar a criação de pelo menos 350.000 (trezentos e cinquenta mil) novas conexões*
> *TCP por segundo para a funcionalidade de Stateful Firewall;*
> *6.132. Deve suportar funcionalidade de Stateful Firewall com des empenho mínimo de 40 Gbps (Quarenta Gbps) para pacotes UDP;*
> *6.133. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 30 Gbps (Vinte) para pacotes TCP multiprotocolo;*
> *6.134. Deve suportar um throughput de, no mínimo, 20 Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;*
> *6.135. Deve suportar a terminação de pelo menos 20.000 túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;*
> *6.136. Deve possuir desempenho de, no mínimo, 10Gbps (Cinco Gbps) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;"*

Justificativa/Sugestão: Os itens acima remetem a um equipamento de grande capacidade computacional por link contratado, equipamentos este com um alto valor de mercado independendo de fornecedores, sendo sugerimos a especificação técnica mínima, segmentando por velocidade de links, segue abaixo sugestão:

6.1. Características do Hardware para link até 30 Mbps
- Possuir throughput mínimo de 490 Mbps para tráfego UDP;
- Suportar no mínimo 45.000 (quarenta e cinco mil) conexões simultâneas;
- Suportar no mínimo 5.000 (cinco mil) novas conexões por segundo;
- Possuir throughput mínimo de 90 Mbps para tráfego HTTP/ HTTPS via Proxy;
- Possuir throughput mínimo de 35 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;
- Possuir throughput mínimo de 92 Mbps para tráfego IPS;
- Possuir throughput mínimo de 140 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput mínimo de 92 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;

6.2. Características do Hardware para link até 100 Mbps
- Possuir throughput de no mínimo 4000 Mbps para tráfego UDP;
- Suportar no mínimo 500.000 (quinhentas mil) conexões simultâneas;
- Suportar no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;

- Possuir throughput de no mínimo 720 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 280 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 369 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 584 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 485 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

6.3. Características do Hardware para link até 500 Mbps

- Possuir throughput de no mínimo 9.000 Mbps para tráfego UDP;
- Suportar no mínimo 1.300.000 (hum milhão e trezentas mil) conexões simultâneas;
- Suportar no mínimo 75.000 (setenta e cinco mil) novas conexões por segundo;
- Possuir throughput de no mínimo 1.700 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 820 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 1.320 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 1.420 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 1.298 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Permitir expandir para 4 LANs 10GbE SFP+
- Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;

6.4. Características do Hardware para link até 2 Gbps

- Possuir throughput de no mínimo 38.000 Mbps para tráfego UDP;
- Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;
- Suportar no mínimo 195.000 (cento e noventa e cinco mil) novas conexões por segundo;
- Possuir throughput de no mínimo 9.500 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 2.300 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 3.200 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 4.000 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 6.500 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser

roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

- Permitir expandir no mínimo 24 interfaces GbE RJ45 ou 12 LANs 10GbE SFP+
- Possuir dispositivo de armazenamento interno de no mínimo 480 GB padrão SSD;

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

ENCARTE TÉCNICO III
REDE IP INTERNET ASSIMÉTRICA

SUGESTÃO 1

ENCARTE TÉCNICO III - O ITEM 3.7 – pág 04 – informa o seguinte:

> *"3.7. A CONTRATADA será responsável pela configuração do acesso à internet (modem / roteador / ONT / Firewall e demais dispositivos) e das configurações dos equipamentos;.;*

Justificativa/Sugestão: Este item especificamente cita uma possível solução de firewall para este lote, porém em nenhum momento está descrito que deverá ser fornecido firewall, ou como appliance apartado dos roteadores ou como uma solução embarcada nos equipamentos. Sugerimos que a contratação de Firewall seja opcional neste lote e tenha uma tabela com o valor apartado da dos lins IPs assimétricos, podendo desta maneira o cliente final agregar até 6 (seis) links IP assimétrico em apenas um único Firewall. Segue abaixo redação com a especificação mínima dos firewalls:

"xxx. São definidos os seguintes Tipos de Solução de Segurança Gerenciada, em função da velocidade do circuito.
FIREWALL TIPO I: Serviço de Segurança Gerenciada
FIREWALL TIPO II: Serviço de Segurança Gerenciada
FIREWALL TIPO III: Serviço de Segurança Gerenciada;.;

3.1. ESPECIFICAÇÕES TÉCNICAS DO FIREWALL UTM

6.5. FIREWALL TIPO I: Características do Hardware para link até 15 Mbps

- *Possuir throughput mínimo de 490 Mbps para tráfego UDP;*
- *Suportar no mínimo 45.000 (quarenta e cinco mil) conexões simultâneas;*
- *Suportar no mínimo 5.000 (cinco mil) novas conexões por segundo;*
- *Possuir throughput mínimo de 90 Mbps para tráfego HTTP/ HTTPS via Proxy;*
- *Possuir throughput mínimo de 35 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;*
- *Possuir throughput mínimo de 92 Mbps para tráfego IPS;*
- *Possuir throughput mínimo de 140 Mbps para tráfego VPN IPSEC com criptografia (AES-128);*
- *Possuir throughput mínimo de 92 Mbps para tráfego VPN SSL com criptografia (AES-128);*
- *Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet*

10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

- *Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;*

6.6. FIREWALL TIPO II: Características do Hardware para link até 25 Mbps

- *Possuir throughput mínimo de 2000 Mbps para tráfego UDP;*
- *Suportar no mínimo 250.000 (duzentas e cinquenta mil) conexões simultâneas;*
- *Suportar no mínimo 15.000 (quinze mil) novas conexões por segundo;*
- *Possuir throughput mínimo de 430 Mbps para tráfego HTTP/ HTTPS via Proxy;*
- *Possuir throughput mínimo de 162 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;*
- *Possuir throughput mínimo de 254 Mbps para tráfego IPS;*
- *Possuir throughput mínimo de 325 Mbps para tráfego VPN IPSEC com criptografia (AES-128);*
- *Possuir throughput mínimo de 205 Mbps para tráfego VPN SSL com criptografia (AES-128);*
- *Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;*
- *Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;*

6.7. FIREWALL TIPO III: Características do Hardware para link até 50 Mbps

- *Possuir throughput de no mínimo 4000 Mbps para tráfego UDP;*
- *Suportar no mínimo 500.000 (quinhentas mil) conexões simultâneas;*
- *Suportar no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;*
- *Possuir throughput de no mínimo 720 Mbps para tráfego HTTP/ HTTPS via proxy;*
- *Possuir throughput de no mínimo 280 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;*
- *Possuir throughput de no mínimo 369 Mbps para tráfego IPS;*
- *Possuir throughput de no mínimo 584 Mbps para tráfego VPN IPSEC com criptografia (AES-128);*
- *Possuir throughput de no mínimo 485 Mbps para tráfego VPN SSL com criptografia (AES-128);*
- *Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;*
- *Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;*

6.8. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM PARA OS FIREWALL´S TIPO I, II,

III

6.4.1. FUNÇÕES BÁSICAS

- *Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;*
- *VPN SSL, VPN IPSec (Client-to-site e Site-to-site);*
- *Controle de Aplicações;*
- *Proxy Web e Filtro de Conteúdo Web (URL Filtering);*
- *Detecção e prevenção de intrusos – IPS;*
- *Qualidade de serviço – QOS;*
- *Anti-Malware;*
- *Cluster.*

6.4.2. CARACTERÍSTICAS GERAIS

- *A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;*
- *Interface em português e inglês;*
- *O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;*
- *O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.*
- *Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.*
- *Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.*
- *A Solução deverá prover inspeção SSL:*
- *A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.*
- *Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;*
- *Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;*
- *Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:*
  - *Endereço do servidor;*
  - *Porta do servidor;*
  - *Usuário;*

- *Senha;*

- *Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:*
  - *Desempenho total (throughput);*
  - *Conexões simultâneas;*
  - *Usuários autenticados;*
  - *Serviços habilitados ou desabilitados;*
  - *Quantidade de endereços distribuídos pelo DHCP.*

6.4.3. DAS FUNCIONALIDADES DO FIREWALL:

- *Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;*
- *Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;*
- *Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;*
- *Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.*
- *Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;*
- *O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.*
- *As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;*
- *O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;*
- *Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;*
- *Deve permitir habilitar ou desabilitar o registro de log por política de firewall.*
- *Possuir controle de acesso à internet por endereço IP de origem e destino;*
- *Possuir controle de acesso à internet por sub-rede;*

- *Possuir suporte a tags de VLAN (802.1q);*
- *Suportar agregação de links, segundo padrão IEEE 802.3ad;*
- *Possuir ferramenta de diagnóstico do tipo tcpdump;*
- *Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;*
- *Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);*
- *Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.*
- *Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;*
- *Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;*
- *Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.*
- *Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;*
- *Possuir funcionalidades de DHCP Cliente, Servidor e Relay;*
- *Deverá suportar aplicações multimídia como: H.323, SIP;*
- *Possuir tecnologia de firewall do tipo Stateful;*
- *Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;*
- *Permitir o funcionamento em modo transparente tipo "bridge";*
- *Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;*
- *Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);*
- *Deverá suportar forwarding de multicast;*
- *Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;*
- *Permitir o agrupamento de serviços;*
- *Permitir o filtro de pacotes sem a utilização de NAT;*
- *Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;*
- *Possuir mecanismo de anti-spoofing;*
- *Permitir criação de regras definidas pelo usuário;*

- *Permitir o serviço de autenticação para HTTP e FTP;*
- *Possuir a funcionalidade de balanceamento e contingência de links;*
- *Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.*

6.4.4. IDENTIFICAÇÃO DE USUÁRIO

- *Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;*
- *Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;*
- *Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;*
- *Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);*
- *A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;*
- *Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;*
- *A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;*
- *A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;*

6.4.5. DAS FUNCIONALIDADES DA VPN:

- *VPN baseada em appliance;*
- *Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;*
- *Suporte a certificados PKI X.509 para construção de VPNs;*
- *Possuir suporte a VPNs IPSec site-to-site:*
  - *Criptografia, 3DES, AES128, AES256, AES-GCM-128*
  - *Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;*
  - *Algoritmo Internet Key Exchange (IKE) versões I e II;*

- *AES 128 e 256 (Advanced Encryption Standard);*
- *Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;*

- *Possuir suporte a VPN SSL;*
- *Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;*
- *Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:*
  - *RDP;*
  - *VNC;*
  - *SSH;*
  - *WEB;*
  - *SMB.*
- *Deve permitir a arquitetura de vpn hub and spoke;*
- *Suporte a VPNs IPSec client-to-site;*
  - *Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.*
- *Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);*
- *Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;*
- *A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:*
  - *Site-to-Site;*
  - *Full-Mesh;*
  - *Star.*

6.4.6. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:

- *A Detecção de Intrusão deverá ser baseada em appliance:*
- *Capacidade de detecção de mais de 22.000 ataques;*
- *O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;*
- *Possuir tecnologia de detecção baseada em assinatura;*
- *Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;*
- *Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;*

- *O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;*
- *Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.*
- *Possuir capacidade de remontagem de pacotes para identificação de ataques;*
- *Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;*
- *Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;*
- *Mecanismos de detecção/proteção de ataques;*
- *Reconhecimento de padrões;*
- *Análise de protocolos;*
- *Detecção de anomalias;*
- *Detecção de ataques de RPC (Remote procedure call);*
- *Proteção contra ataques de Windows ou NetBios;*
- *Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);*
- *Proteção contra ataques DNS (Domain Name System);*
- *Proteção contra ataques a FTP, SSH , Telnet e rlogin;*
- *Proteção contra ataques de ICMP (Internet Control Message Protocol);*
- *Alarmes na console de administração;*
- *Alertas via correio eletrônico;*
- *Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;*
- *Capacidade de resposta/logs ativa a ataques;*
- *Terminação de sessões via TCP resets;*
- *Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;*
- *O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;*

- *Possuir filtros de ataques por anomalias;*
- *Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;*
- *Permitir filtros de anomalias de protocolos;*
- *Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;*
- *Suportar verificação de ataque nas camadas de aplicação;*

6.4.7. DAS FUNCIONALIDADES DE QOS

- *Adotar solução de Qualidade de Serviço baseada em appliance;*
- *Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;*
- *Permitir modificação de valores DSCP para o DiffServ;*
- *Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;*
- *Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;*
- *Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;*
- *Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;*
- *Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;*
- *Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;*

6.4.8. DAS FUNCIONALIDADES DO ANTIVÍRUS

- *Possuir funções de Antivírus, Anti-spyware;*
- *Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;*
- *Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)*
- *Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;*

- *Permitir o bloqueio de download de arquivos por tamanho.*

6.4.9. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB

- *Possuir solução de filtro de conteúdo web integrado a solução de segurança*
- *Possuir pelo menos 75 categorias para classificação de sites web*
- *Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;*
- *Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:*
  - *Webmail;*
  - *Instituições de Saúde;*
  - *Notícias;*
  - *Pornografia;*
  - *Restaurante;*
  - *Mídias Sociais;*
  - *Esporte;*
  - *Educação;*
  - *Games;*
  - *Compras;*
- *Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;*
- *Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;*
- *Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;*
- *Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;*
- *Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;*
- *Possibilitar a integração com servidores de cache WEB externos;*
- *Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®, Youtube®, MSN Vídeos®, Facebook®, Google Maps®;*
- *Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;*
- *Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;*
- *Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;*

- *Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;*
- *Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;*
- *Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;*
- *Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;*
- *Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;*
- *Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;*
- *Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;*
- *Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;*
- *Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;*
- *Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;*
- *Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;*
- *Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;*
- *Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;*
- *Deverá permitir configurar a porta do Proxy Explícito.*

6.4.10. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES

- *As funcionalidades abaixo devem ser baseadas em appliance:*
- *Deverá reconhecer no mínimo 700 aplicações;*
- *Deverá possuir pelo menos 10 categorias para classificação de aplicações;*
- *Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:*

- *P2P;*
- *Web;*
- *Transferência de arquivos;*
- *Chat;*
- *Social;*

- *Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;*
- *Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;*
- *Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;*
- *Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;*
- *Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;*
- *Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;*
- *Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;*
- *Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.*

6.4.11. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS - ATP

- *Possuir sistema de proteção avançada contra ameaças (ATP) nativo;*
- *O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.*
- *Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;*
- *A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;*
- *Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;*
- *Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;*
- *Deve permitir a atualização automática das assinaturas por meio de agendamento diário;*

- *Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;*
- *Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;*
- *Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;*
- *Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;*
- *Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;*
- *Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";*
- *Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";*
- *Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";*
- *Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;*

RESPOSTA: Não haverá opção ou obrigação de inclusão de Firewall no Lote III, o texto será alterado para reforçar esta definição. Trata-se apenas de prestação de serviços de acesso à Internet assimétrico sem segurança, que ficará a cargo do cliente.

SUGESTÃO 2

ENCARTE TÉCNICO III - O ITEM 3.12.4 – pág 04 – informa o seguinte:

> *"3.12.4. Tempo máximo total de latência para resposta à internet de 80 milissegundos (latência considerando os links de acesso e o link de saída à internet).;*

Justificativa/Sugestão: Tecnicamente as operadoras não garantem uma baixa latência em soluções de internet em ADSL. Sugerimos alterar a latência para até 200ms. Segue sugestão de redação:

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.

"3.12.4. Tempo máximo total de latência para resposta à internet de até 200 milissegundos (latência considerando os links de acesso e o link de saída à internet).;

SUGESTÃO 3

ENCARTE TÉCNICO III - O ITENS 7.11.6, 7.11.7 e 8.10 – pág 11 – informa o seguinte: $$$$$$

> *"7.11.6. Este Portal WEB deve estar disponível em 30 dias corridos após assinatura do primeiro contrato;*
>
> *7.11.7. Enquanto o portal WEB não estiver disponível a CONTRATADA deverá disponibilizar um endereço de e-mail para registro das solicitações de serviços;."*
>
> *"8.10. Abertura e fechamento de chamados serão efetuados através de Portal Web, providenciado pela CONTRATADA. O Portal WEB deverá estar disponível 24 horas por dia, 7 dias por semana, com geração de número de protocolo de atendimento, o qual só poderá ser fechado após confirmação com o responsável pela abertura;;"*

Justificativa/ugestão: O fornecimento de um portal WEB implicará também no fornecimento de roteadores nas pontas que no final elevam o custo final da solução de IP Assimétrico, deve-se levar em conta também que serão necessárias customizações e integrações da plataforma que suportará o portal. Sugerimos retirar esses itens.

RESPOSTA: Trata-se de um portar de abertura e acompanhamento de chamados, não sendo necessária qualquer integração física ou lógica com os links fornecidos.

SUGESTÃO 4

ENCARTE TÉCNICO III - O ITENS 7.11.8 – demonstra a seguinte tabela:

Nível	PR	Serviços
N1	≤ 4 horas	Serviços de Acesso à Internet Assimétrica

Tabela 1 – Prazo de Reparo (PR)

Justificativa/Sugestão: Dado que os locais de instalação dos links IP deste lote abrangem quase todo os municípios do estão do Rio de Janeiro, sugerimos alterar o tempo de reparo para 5 horas na região metropolitana e 7 horas no interior.

RESPOSTA: Deverá ser atendido o Termo de Referência, Encartes Técnicos e Anexos.