GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO - SECTI
CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO – PRODERJ

DIRETORIA DE INFRAESTRUTURA TECNOLÓGICA

ANEXO A

CATÁLAGO DE SERVIÇOS

INTRODUÇÃO

Neste documento são descritos todos os itens integrantes do catalogo de serviços do Rio Digital. Todos estes serviços devem ser geridos pelo serviço de Gestão Integrada conforme figura 1 do termo de referência deste edital.

A Gestão integrada é conforme descrita no item 3 do Termo de Referência, é um serviço composto de infraestrutura tecnológica, processual, sistema de gestão e recursos humanos qualificados.

Para cada um dos itens contratados do catalogo de serviço serão incluídos o Serviço de Gestão Integrada, que irá garantir uma gestão eficiente e eficaz de todos os itens contratados.

1. SERVIÇO DE REDE MPLS

1.1. A Rede MPLS a ser CONTRATADA através do PRODERJ deverá permitir a criação de múltiplas 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.

1.2. Os Órgãos e Secretarias de governo poderão constituir cada um sua própria VRF, contudo a interligação destas redes com o Backbone da Rede Governo localizado no PRODERJ deverá seguir as orientações e estrutura estipulada neste documento, tendo como premissas a segurança e padronização da Rede Governo.

1.3. 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 rádio em casos excepcionais, sendo que estes enlaces deverão utilizar frequências licenciadas pela Anatel, evitando-se problemas de interferências. A escolha dos meios deverá obedecer aos critérios de desempenho estabelecidos neste projeto.

1.4. Os roteadores CPE (Customer Premises Equipment) deverão ser fornecidos pela CONTRATADA de acordo com os requisitos previstos neste documento e adequados as especificações e velocidades dos circuitos a serem contratados.

1.5. A infraestrutura de rede da CONTRATADA deverá ser redimensionada e capaz de suportar serviços adicionais que possam ser solicitados pelo PRODERJ, como expansão ou redução de banda mínima de acesso garantida, ou alteração do endereço de um novo sítio, ou mesmo adição de um novo sítio não contemplado na relação de sítios. Em todos os casos, a CONTRATADA deve manter os níveis de

serviços de desempenho especificados.

1.6. O limite de atuação da CONTRATADA deverá ser a porta de rede local do roteador CPE.

1.7. A assessoria de TIC de cada Secretaria ou Órgão será responsável pelo fornecimento de cabo(s) de rede local certificado(s) no padrão RJ-45 para interligação do(s) roteador CPE com o switch(es)/firewall(s) de sua propriedade, os quais serão responsáveis pelo encaminhamento de pacotes e conexões aos ativos finais de comunicação.

1.8. A rede oferecida deve ser logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da internet.

1.9. A rede deverá ser flexível e escalável, permitindo acomodação instantânea do tráfego dos sítios em todo momento durante o período de vigência do contrato, permitindo a adaptação tempestiva a eventuais aumentos ou diminuição de demanda por tráfego, ou necessidade de provimento de novos serviços.

1.10. A rede MPLS CONTRATADA deverá respeitar o plano de endereçamento das Redes Locais atuais, permitindo o roteamento entre as redes conectadas. Os detalhes de endereçamento deverão ser definidos em conjunto com CONTRATADA.

1.11. O uso da tecnologia MPLS deverá permitir que a rede se beneficiasse das vantagens da adoção desse padrão, tais como: configuração de recursos de qualidade de serviço (QoS), flexibilidade na definição de topologia lógica, simplificação de roteamento, menor custo, implantação de parâmetros de segurança da informação, entre outros.

1.12. A rede MPLS da CONTRATADA deverá atender também aos seguintes requisitos:

- Ser de alta qualidade, disponibilidade e atualização tecnológica;
- Possibilitar o suporte à implantação de soluções de contingência e redundância;
- Suportar Qualidade de Serviço fim a fim, permitindo a priorização do tráfego de voz e videoconferência;
- Possuir Backbone IP com de tolerância a falhas em suas conexões, com baixos tempos de convergência em caso de falha de enlaces ou equipamentos;
- Seguir as melhores práticas de projeto e suporte e operação de redes.

1.13. A solução deverá ser ofertada prevendo o atendimento de várias VRFs independentes utilizando a tecnologia MPLS, sendo que o Núcleo da Rede localizado no PRODERJ deverá atender as condições de contingência entre sites distintos, considerando a topologia da rede atual da figura abaixo.

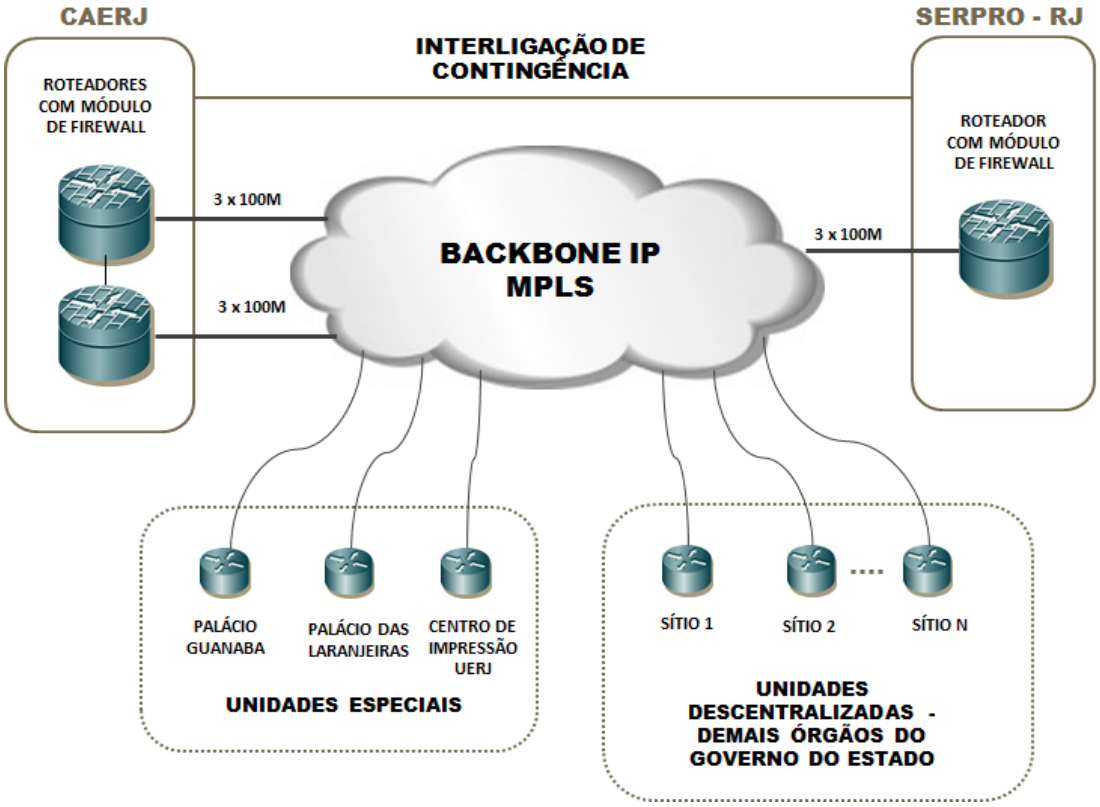


Figura 1 – Núcleo da Rede Governo.

1.14. DOS LOCAIS DE IMPLANTAÇÃO

1.14.1. Os endereços de instalação dos circuitos constantes foram levantados no momento da elaboração do Estudo Técnico, e pode haver alterações até a finalização do procedimento licitatório. Durante a implantação de cada circuito, a CONTRATADA deverá validar os endereços aos Órgãos e Secretarias do Governo com a anuência do PRODERJ.

1.14.2. Durante o decorrer da vigência do contrato de prestação poderá eventualmente haver mudança de endereços dos sites relacionados.

1.14.3. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios (unidades descentralizadas) e localizados no Estado do Rio de Janeiro durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão ou redução de bandas de comunicação, respeitados os limites legais e técnicos, bem como os prazos estipulados.

1.14.4. A CONTRATANTE poderá solicitar a desativação do serviço prestado de qualquer sítio ou, bem como mudança de local de prestação dos serviços ou mesmo adição de um novo sítio não contemplado na relação de sítios indicados.

A CONTRATANTE deverá comunicar essas alterações em tempo hábil antes do início da prestação do serviço.

1.14.5. Eventuais mudanças de local de prestação dos serviços poderão ser solicitadas, durante a vigência do contrato. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da mesma localidade.

1.15. PROJETO EXECUTIVO DA REDE MPLS

1.15.1. O Projeto Executivo para a Rede MPLS deverá contemplar os seguintes itens:

- Definição de topologias físicas e lógicas da rede.
- Cronograma da implantação dos serviços.
- Os Esquemas de redundância para os enlaces necessários.
- O Plano de Roteamento.
- Os parâmetros de qualidade de serviço.
- Dimensionamento de enlaces e interfaces de comunicação.
- Plano de endereçamento compatível com a atual rede corporativa do Governo do Estado do Rio de Janeiro, associando endereços IPs privados de modo a torná-los únicos dentro da nuvem MPLS.
- Definição do QoS e dos perfil de banda por Classe de Serviço.

1.16. DOS REQUISITOS DE INFRAESTRUTURA

1.16.1. Os equipamentos fornecidos pela CONTRATADA deverão ser capazes de operar com a alimentação elétrica de 110V ou 220V e frequência de 60Hz.

1.16.2. A CONTRATADA será responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os Equipamentos/recursos que forem necessários (roteadores, modems, estações de gerenciamento, meios de transmissão, cabeamento WAN, acessórios necessários, dentre outros) para o provimento dos serviços. Os Equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos.

1.16.3. A infraestrutura interna da rede da CONTRATADA (backbones, POPs, Equipamentos internos, dentre outros) deverá ser atendida por solução de alimentação e proteção elétrica de modo a manter todos os Equipamentos em operação por tempo indeterminado no caso de falta de energia.

1.16.4. A CONTRATADA será responsável pela interligação da rede entre o Distribuidor Geral (DG) de telefonia do prédio em cada um dos sítios e o local físico onde será

instalado o roteador CPE para os acessos por rede cabeada.

1.16.5. Para o caso de atendimento do sítio por meio de rede não-cabeada, por exemplo, enlace de rádio frequência terrestre ou satélite, quando a implantação implique a necessidade de execução de obras civis, estas ficarão a cargo da CONTRATANTE, e deverão constar do cronograma que faz parte do Projeto Executivo. Nestes casos, a CONTRATADA apresentará relatório de visita contendo as adequações e providências necessárias para a conclusão da instalação dos circuitos.

1.17. REQUISITOS GERAIS DOS CPEs

Os roteadores e equipamentos CPE, de propriedade da CONTRATADA, a serem disponibilizados em cada um dos endereços deverão satisfazer os seguintes requisitos.

1.17.1. 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.

1.17.2. Serem fornecidos com todos os componentes, módulos e acessórios necessários ao seu funcionamento atendendo aos requisitos deste documento.

1.17.3. Todos os roteadores CPE do Backbone PRODERJ, unidades especiais e dos sítios especificados deverão ser dimensionados, fornecidos, instalados, configurados, mantidos, gerenciados e operados de modo a garantir o desempenho e os níveis de serviços contratados.

1.17.4. Todos os roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), devem ser dimensionados de forma que tenham capacidade de encaminhamento de pacotes IPV4/IPV6, em pacotes por segundo, compatíveis com as velocidades dos enlaces WAN conectados.

1.17.5. Todos os roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), deverão ser dimensionados para operarem com utilização de CPU e memória de no máximo de 75% (setenta e cinco por cento), desde que satisfeita a condição de tráfego igual ou inferior à capacidade da soma dos enlaces WAN calculada a média de no mínimo 5 (cinco) minutos.

1.17.6. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para o Governo do Estado.

1.17.7. Todas as atualizações e correções (patches) de softwares, necessárias para o cumprimento dos requisitos exigidos neste documento técnico, deverão ser monitoradas e realizadas pela CONTRATADA sem ônus adicionais para o Governo do Estado, e comunicadas previamente, quando estas exigirem reinicialização de Equipamentos.

1.17.8. A CONTRATADA deverá habilitar nos roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), o protocolo SNMP, disponibilizando nestes uma comunidade SNMP com acesso de leitura e permitir a solicitação de configuração de traps específicos pelo PRODERJ.

1.17.9. A configuração lógica dos roteadores CPE, para cada nível de serviço, será definida pela CONTRATADA com a aprovação do PRODERJ, e apresentada no Projeto Executivo.

1.17.10. Todos os equipamentos fornecidos pela CONTRATADA deverão suportar os protocolos IPV4 e IPV6.

1.17.11. Os roteadores fornecidos deverão contemplar todas as interfaces necessárias para o fornecimento dos circuitos por parte da CONTRATADA e com as especificações adequadas.

1.17.12. Todos os roteadores deverão possuir no mínimo uma interface LAN de 1G padrão Ethernet para a conexão da Rede Local dos endereços, sendo que devem satisfazer também as necessidades específicas em termos de desempenho e interfaces, como por exemplo: no caso da necessidade de balanceamento de dois circuitos em um mesmo roteador.

1.18. ESPECIFICAÇÃO DOS EQUIPAMENTOS CONCENTRADORES DO DATACENTER DO PRODERJ

1.18.1. ROTEADORES CONCENTRADORES PRODERJ

Os roteadores a serem fornecidos devem ser novos e de primeiro uso.

Deverão ser fornecidos pela CONTRATADA um total de 3 (três) roteadores, 2 (dois) Principal e Backup para o Data Center principal e um para o Data Center secundário.

Estes equipamentos serão utilizados exclusivamente para o Núcleo da Rede Governo, situados nos Datacenter do PRODERJ.

1.18.1.1. Características de Hardware

- equipamento deve permitir ser montado em rack padrão de 19” (dezenove polegadas), sendo fornecido com todos os acessórios indispensáveis para sua instalação e funcionamento;
- Deve possuir altura máxima de 2 (duas) unidades rack (2RU) / 88.9mm;
- O equipamento deve suportar no mínimo 2 (duas) fontes de energia internas, para Corrente Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz), conforme abaixo:
    - As fontes de energia devem permitir utilização de circuitos

elétricos distintos;

- As fontes de energia devem ser do tipo substituível (hot-swap), permitindo instalação e/ou substituição sem a necessidade de remoção do equipamento;
- As fontes de energia devem ser suficientes para manter todas as operações do equipamento, mesmo no caso de falha de uma das fontes de energia, independentemente da quantidade de interfaces em uso ou funcionalidades habilitadas;
- As fontes de energia devem vir acompanhadas com cabos de energia com 1,80m (hum metro e oitenta centímetros) de comprimento mínimo;
- Os sistemas de fonte de alimentação devem ser o de maior capacidade oferecido pelo fabricante para o equipamento;

- Deve possuir memória não-volátil com capacidade suficiente para armazenar, no mínimo, uma nova versão de sistema operacional que tenha o tamanho de 2 (duas) vezes o sistema operacional na versão mais recente, atendendo simultaneamente a todas as funcionalidades exigidas nesta Especificação, em conformidade com as recomendações do Fabricante;
- Deve possuir configuração de CPU e memória RAM suficiente para a implementação de todas as funcionalidades descritas nesta especificação;
- Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9 ou uma porta de console com interface USB;
- Deve operar entre as temperaturas de 0°C e 40ºC;
- Deve ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação);
- Deve suportar temperatura ambiente de armazenamento entre -10ºC e 60ºC;
- O sistema operacional / firmware dos equipamentos fornecidos deve, dentro das características solicitadas, ser a versão atual mais estável no momento da instalação.
- O equipamento deve implementar, no momento da entrega, todas as características exigidas nesta Especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras;
- Suportar no mínimo 3 interfaces até 10 Gigabit Ethernet;
- Suportar módulos com portas do tipo, OC-192, OC-48, OC-12, OC-3, E3, E1 e V.35 serial.
- Deve permitir operar simultaneamente todas as interfaces, mantendo a mesma capacidade e as características descritas nesta especificação;

- Todas as interfaces deverão ser internas ao equipamento, não serão aceitos conversores externos para nenhum tipo de interfaces exigidas;
- Deve possuir pelo menos 6 (seis) interfaces Gigabit Ethernet com suporte a adaptadores padrão SFP
- Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo;
- Deve possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento;
- Deve possuir LEDs de diagnósticos que forneçam informações e atividades das portas;

1.18.1.2. Funcionalidades Gerais

- 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 possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 e RFC 3022;
- Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT);
- Deve suportar o protocolo de tunelamento GRE (Generic Routing Encapsulation) em conformidade com o padrão RFC 2784, contemplando, no mínimo, os seguintes recursos:
  - Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica;
  - Operação em modo multiponto (“multipoint GRE”);
  - Possibilidade de configuração de “Keepalive” nos túneis;
  - Suporte a QoS – deve ser possível preservar as marcações no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE;
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface Ethernet e serial;
- Deve permitir a criação de versões de configuração e suporte a “rollback” da configuração para versões anteriores;
- Deve ter a capacidade de atualização de software via FTP e via TFTP, em conformidade com as RFCs 783 e 1350;
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) e SFTP (Secure FTP);
- Deve implementar a opção local de carga do sistema do equipamento via memória Flash;

- Permitir que a sua configuração seja feita através de terminal assíncrono;
- Deve permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes syslog gerados pelo equipamento;
- Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;
- Deve implementar ICMPv6, em conformidade com a RFC 4443;
- Possuir ferramentas para depuração e gerenciamento em primeiro nível para IPv4 e IPv6, implementando ao menos, testes ICMP, debug, trace e 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;
- Permitir o espelhamento do tráfego total de uma porta e de um grupo de portas para outra porta localizada no mesmo equipamento;
- Suportar mecanismo de extensão de Layer 2 sobre redes IP sem a necessidade de extensão do domínio Spanning-Tree entre sites diferentes e com a supressão de broadcast de ARP-requests sobre a rede IP de transporte. Este mecanismo não deverá necessitar de uma rede MPLS de transporte;
- 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, Marcação de QoS, Portas 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 cada uma das interfaces do equipamento;
- A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo IPFIX padronizado, para no mínimo: Net Flow ou Sflow ou JFlow ou Hflow;
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deverão ser suportadas no mínimo as seguintes operações de teste: ICMP echo, estabelecimento de conexão TCP (em porta TCP configurável), UDP echo (em porta UDP configurável);
- Deve suportar o envio de traps SNMP em função do resultado dos testes ultrapassarem limiares pré-configurados ou no caso de falha.
- O equipamento deve suportar ao menos 2000 (dois mil) destas operações de testes simultaneamente;
- Deve implementar o protocolo NTPv3 (Network Time Protocol versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições

da RFC 1305;

- Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 4330 ou 5905;
- Deve suportar a implementação da funcionalidade de DHCP Relay e DHCP Server;
- Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Deve possibilitar a implementação de Lan Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q;
- Deve implementar, no mínimo, 4000 (quatro mil) VLANs simultaneamente;
- Deve permitir o roteamento nível 3 entre as VLANs;
- Deve implementar o protocolo de controle de agregação de enlace (LACP) conforme o padrão IEEE 802.3ad, permitindo agrupar, no mínimo, 4 (quatro) interfaces do mesmo tipo;
- Deve permitir o encaminhamento de “jumbo frames” (pacotes de 9016 bytes);
- Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338;
- Deve suportar mecanismo de autenticação MD5 entre os peers VRRP;
- Deve implementar, no mínimo, 100 grupos VRRP;

1.18.1.3. Roteamento

- Deve suportar a pilha de protocolos TCP/IP;
- Deve suportar o protocolo roteável IPv4;
- Deve suportar o protocolo roteável IPv6;
- Deve implementar mecanismo de pilha dupla (IPv4 e IPv6), para permitir o funcionamento simultâneo dos protocolos IPv4 e IPv6
- Deve permitir a configuração de rotas estáticas para IPv4 e IPv6;
- Deve implementar o protocolo de roteamento RIPv2, em conformidade com, no mínimo, os padrões RFC 2453 e 2082;
- Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões RFC 2328, 3101, 3137, 3623, 2370 e 4750;
- Deve implementar o protocolo de roteamento BGPv4, em conformidade com, no mínimo, os padrões RFC 1997, 2858, 2439, 2842, 2918, 4271, 3065, 4456, e 2385;
- Deve implementar mecanismo de controle de multicast conforme os protocolos: IGMPv1, IGMPv2 e IGMPv3. Deve implementar roteamento multicast PIM-SM (Protocol Independent Mode-Sparse Mode) e PIM-DM

(Protocol Independent Mode-Dense Mode), em conformidade com, no mínimo, os padrões RFC 1112, 1349, 1256, 2236, 3376 e 2362;

- Deve suportar o protocolo MPLS (Tag Distribution Protocol, Label Distribution Protocol, MPLS Virtual Private Network, MPLS QoS, MPLS Traffic Engineering), em conformidade com, no mínimo, os padrões RFC 4364, 2702, 3031, 3443, 3036, 3037, 3107, 3215 e 3270;
- Deve implementar roteamento dinâmico RIPng, em conformidade com o padrão RFC 2080;
- Deve suportar roteamento dinâmico OSPFv3 para IPv6, em conformidade com o padrão RFC 5340;
- Deve implementar Multiprotocol BGP (MP-BGP) com suporte a IPv6;
- Deve permitir a virtualização das tabelas de roteamento (camada 3). As tabelas de roteamento virtuais deverão ser completamente segmentadas;
- Deve suportar a criação de, no mínimo, 4000 tabelas de roteamento virtuais (VRF) p/ IPv4 e IPv6;
- Deve implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs.
- Deve permitir a possibilidade de alterações de roteamento automatizadas baseadas em métricas de desempenho dos enlaces, para no mínimo, perda de pacotes, atraso e jitter;

1.18.1.4. Segurança

- Deve implementar filtragem de pacotes (listas de controle de acesso) para IPv4 e IPv6;
- Deve 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;
- Deve permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao equipamento via Telnet, SSH e SNMP;
- Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um servidor de autenticação e autorização do tipo Radius ou TACACS+;
- Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- Deve permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir;
- Deve suportar serviços de Virtual Private Network (VPN) baseados no padrão IPSec (IP Security Protocol), compatível com IPv4 e IPv6;

- Deve suportar serviços de Virtual Private Network (VPN) baseados no padrão IKE (Internet Key Exchange);
- Deve suportar, no mínimo, 2000 (dois mil) túneis VPN IPSec Site-to-Site;
- Deve suportar uma taxa de estabelecimento de túneis VPN de no mínimo 30 (trinta) túneis por segundo;
- Deve suportar algoritmos de criptografia DES – 56 bits, 3DES – 168 bits, AES – 128 bits, AES – 256 bits para conexões de túneis VPN IPSec;
- Deve suportar a transparência de conexões IPSEC a NAT (NAT-T) através do encapsulamento dos pacotes IPSEC com UDP;
- Deve reagrupar pacotes de sessão de VPN fragmentados para análise e entrega no destino;
- Deve permitir a criação de VPNs IPSec baseada em politícas de segurança;
- Devem ser implementados túneis VPN nos modos de operação “tunnel mode” e “transport mode”. Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409;
- Deve suportar as funcionalidades de gerenciamento de chaves para VPN;
- Deve suportar a utilização de clientes baseados em IPSec;
- Suportar o tráfego do protocolo GRE sobre IPSec;
- Suportar o tráfego Multicast IP sobre IPSec;
- Deve suportar as funcionalidades de "Stateful Firewall", baseado em zonas de segurança, através da ativação de licença de software.

1.18.1.5. Gerenciamento

- 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;
- Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213;
- Deve suportar os protocolo 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 (no AuthNoPriv);
  - Com autenticação e sem privacidade (authNoPriv);
  - Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES;
- Suportar SNMP sobre IPv6;
- Implementar 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;
- Deve permitir ser configurável e gerenciável via interface gráfica (GUI), linha de comando (CLI), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 15 sessões simultâneas e independentes
- Deve permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC;
- 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;
- Deve permitir a configuração de endereços IPv6 para gerenciamento;
- Deve proteger a interface de gerência do equipamento através de senha;

1.18.1.6. Desempenho

- Deve suportar uma taxa de comutação de pacotes de no mínimo 10 Mpps (dez milhões de pacotes por segundo), considerando-se pacotes de 64 bytes;

1.18.1.7. Qualidade de Serviço

- Deve suportar o padrão IEEE 802.1p para cada porta;
- Deve possuir a facilidade de priorização de tráfego através do padrão IEEE 802.1p;
- Deve 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);
- Deve suportar a classificação de pacotes de dados (QoS), baseados em:
  - Protocolos da camada de rede (IPv4 e IPv6) do Modelo OSI (Endereços IP origem e destino);
  - Protocolos da camada de transporte do Modelo OSI (TCP e UDP);
  - Endereços MAC de origem e destino;
  - VLAN;
- Deve suportar a classificação, marcação e remarcação baseadas em CoS (“Class of Service”) para a camada de enlace;

- Deve suportar a classificação, marcação e remarcação baseados em "IP precedence" e "DSCP" ("Differentiated Services Code Point") para a camada de rede, em conformidade com os padrões RFC 3260;
- Deve permitir a marcação de tráfego baseado no campo ToS (Type of Service), conforme RFC 2474;
- Deve prover as funcionalidades de priorização de tráfego nas interfaces através da utilização de First In First Out (FIFO), Priority Queuing (PQ), Custom Queuing (CQ), Weighted Fair Queuing (WFQ), Class-Based Weighted Fair Queueing (CBWFQ) e Low Latency Queueing (LLQ);
- Deve suportar funcionalidades de QoS de "Traffic Shapping";
- Deve suportar funcionalidades de QoS de "Traffic Policing";
- Deve ser possível a especificação de garantia de banda por classe de serviço;
- Deve possuir mecanismos de descarte de pacotes que evitem o congestionamento nas filas do equipamento, tais como RED (Random Early Detection) ou WRED (Weighted Random Early Detection);
- Para os pacotes que excederem a especificação, deve ser possível configurar ações, para no mínimo: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP e descarte do pacote;
- O equipamento deve suportar o mapeamento das prioridades nível 2 (802.1p) em prioridades nível 3 (IP Precedence e DSCP) e vice-versa;
- Deve suportar a priorização do tráfego de rede, com no mínimo 10 (dez) filas por interface (processamento distribuido) ou 100.000 (cem mil) filas (processamneto centralizado), permitindo uma integração transparente de dados, voz e vídeo;
- Deve implementar RSVP (Resource Reservation Protocol) em conformidade com no mínimo, os padrões RFC 3209, RFC 2961, RFC 2747 e RFC 2205;
- Deve suportar o padrão IEEE 802.3x (Flow Control);

1.19. SOLUÇÃO DE FIREWALL/IPS DATA CENTER PRODERJ

Com o objetivo de permitir o controle e a gestão das conexões dos distintos Órgãos e Unidades a aplicações sitiadas no PRODERJ a CONTRATADA deverá provê solução de Firewall/IPS para o Núcleo da Rede.

A Solução de Firewall/IPS a ser fornecida deverá suportar os seguintes requisitos.

1.19.1. Deve suportar a definição de VLAN trunking conforme padrão IEEE 802.1q, a criação de interfaces lógicas associadas às VLANs e o estabelecimento de regras de filtragem (Stateful Firewall) entre elas.

1.19.2. Deve suportar agregação de portas, com a criação de grupos de pelo menos 08 (oito) portas. Deve ser suportado o padrão LACP (Link Aggregation Control Protocol).

1.19.3. 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”.

1.19.4. 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.

1.19.5. Deve possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas.

1.19.6. 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.

1.19.7. Deve possuir a funcionalidade de “proxy” de autenticação (“authentication proxy”), permitindo a criação de políticas de segurança de forma dinâmica, com autenticação e autorização do acesso aos serviços de rede sendo efetuadas por usuário. Deve ser possível obter as informações de usuário/senha por meio de pelo menos os seguintes protocolos: HTTP, HTTPS e Telnet. Deve ser possível ao Firewall exigir autenticação inclusive para uso de protocolos que não possuam nativamente recursos de autenticação.

1.19.8. Deve suportar autenticação usando base local de usuários (interna ao equipamento).

1.19.9. Deve permitir a integração do Firewall com a solução Microsoft Active Directory (MS-AD), permitindo a criação de políticas de filtragem baseados em usuários e grupos de usuários existentes na base MS AD.

1.19.10. Deve implementar listas de controle de acesso com no mínimo os seguintes campos: IP de Origem, Nome do Usuário/Grupo do AD, IP de Destino, Serviço de origem, Serviço de destino e Ação (permit/deny). O “nome de usuário” deverá ser identificado de forma automática e transparente para o usuário final através de consultas à base MS-AD.

1.19.11. Deve implementar políticas de controle de acesso baseadas em informações de horário (“time-based access control”).

1.19.12. Deve possibilitar a remontagem virtual de fragmentos (“Virtual Fragment Reassembly”) em conjunto com o processo de inspeção stateful. Deve ser possível estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem.

1.19.13. Deve possuir suporte a inspeção “stateful” para pelo menos os seguintes protocolos de aplicação: Oracle SQL*Net Access, Remote Shell, FTP, HTTP, SMTP, ILS (Internet Locator Service), LDAP, ESMTP, TFTP.

1.19.14. Deve suportar a tradução do endereço IP carregado em uma mensagem DNS Reply (NAT na camada de aplicação) juntamente com a tradução do endereço IP presente no cabeçalho L3.

1.19.15. 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.

1.19.16. 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.

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

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

1.19.19. Deve possuir capacidade de limitar o número de conexões TCP simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP).

1.19.20. Deve possuir capacidade de limitar o número de conexões TCP incompletas (‘half-open’) simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP).

1.19.21. Deve possuir capacidade de limitar o número de conexões TCP simultâneas para um endereço de destino especificado.

1.19.22. Deve possuir capacidade de limitar o número de conexões TCP incompletas (‘half-open’) simultâneas para um endereço de destino especificado.

1.19.23. Deve permitir simultaneamente com a implementação “Network Address Translation” a filtragem “stateful” de pelo menos as seguintes aplicações:

- H.323 (v1, v2, v3, v4), Real Time Streaming Protocol (RTSP), SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol).
- Microsoft Networking client and server communication (NetBIOS over IP).

- Oracle SQL*Net client and server communication.
- Domain Name System (DNS).
- SUN Remote Procedure Call (RPC).
- File Transfer Protocol (FTP) – modos “standard” e “passive”.

1.19.24. 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.

1.19.25. 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.

1.19.26. 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.

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

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

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

1.19.30. Deve suportar versões do cliente IPSEC VPN fornecido com a appliance para, no mínimo, os seguintes sistemas operacionais: Windows 8 e superior, Linux (Intel) Red Hat e MacOS.

1.19.31. Deve suportar a terminação túneis IPSEC do tipo “site-to-site” (LAN-to-LAN).

1.19.32. Deve suportar a terminação simultânea de conexões IPSEC VPN.

1.19.33. Deve suporte à criação de VPNs IPSEC com criptografia 168-bit 3DES, 128-bit AES e 256-bit AES.

1.19.34. Deve suportar alta disponibilidade das conexões IPSEC VPN, permitindo a utilização de uma segunda unidade em “standby”. Em caso de falha de uma das unidades, não deverá haver perda das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final.

1.19.35. Deve suportar negociação de túneis VPN IPSEC utilizando o protocolo IKE (Internet Key Exchange) nas versões 1 e 2, para garantir a geração segura das chaves de criptografia simétrica.

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

1.19.37. Deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente: endereço IP do cliente VPN, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name. A configuração do cliente VPN deve ser completamente automatizada, sendo exigida do usuário apenas a instalação do cliente VPN em seu PC.

1.19.38. 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.

1.19.39. 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.

1.19.40. Deve suportar o uso de certificados digitais emitidos pela autoridade certificadora ICP Brasil para autenticação das VPNs IPSec.

1.19.41. Deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento.

1.19.42. Deve permitir a criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento.

1.19.43. Deve suportar a integração com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes.

1.19.44. Deve permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema.

1.19.45. Deve ser possível a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN.

1.19.46. Deve permitir a definição dos horários do dia e os dias da semana em que um dado usuário pode requisitar uma conexão VPN.

1.19.47. Deve suportar NAT (Network Address Translation).

1.19.48. Deve suportar operação no modo transparente a NAT ("NAT-transparent mode"), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation).

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

1.19.50. Deve permitir a terminação de conexões no modo IPSEC over UDP.

1.19.51. Deve ser possível visualizar no concentrador o número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas.

1.19.52. Deve ser possível visualizar no cliente VPN o endereço privado adquirido durante a negociação da conexão IPSEC.

1.19.53. 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.

1.19.54. Deve suportar a utilização de certificados digitais padrão X.509 para a própria appliance VPN, possuindo integração com pelo menos as seguintes Certificate Authorities (CAs): Baltimore, Entrust, Verisign, Microsoft e RSA. Os clientes VPNs devem ter o mesmo suporte a certificados digitais. Deve ser suportado o protocolo SCEP para "enrollment" automático na autoridade certificadora (tanto para o concentrador como para os clientes IPSEC).

1.19.55. Deve suportar protocolo Syslog para geração de logs de sistema.

1.19.56. Deve implementar o protocolo DTLS (TLS over UDP) de acordo com a RFC 4748.

1.19.57. Deve permitir o mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS.

1.19.58. Deve implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers.

1.19.59. Deve ser gerenciável via SNMP, v2c e v3.

1.19.60. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS.

1.19.61. Deve ser fornecido com pelo menos uma interface 10/100/1000 dedicada ao gerenciamento (out-of-band). Esta interface não deverá ser contabilizada para o atendimento daquelas originalmente especificadas para a appliance firewall.

1.19.62. Deve possuir mecanismo interno de captura de pacotes. Deve ser possível selecionar através de guias de configuração ("wizards") quais os pacotes: IP de origem e destino, portas TCP/UDP de origem e destino e interfaces de entrada devem ser os pacotes capturados.

1.19.63. Deve permitir o armazenamento de pacotes capturados em formato tcpdump.

1.19.64. Deve possuir memória flash para armazenamento de imagem do sistema operacional e arquivos de configuração do equipamento.

1.19.65. Deve implementar completamente a porção cliente do protocolo TACACS+ para controle de acesso administrativo ao equipamento. Deve ser possível especificar conjuntos de comandos acessíveis a cada grupo de usuários administrativos e cada comando deve ser autorizado individualmente no servidor TACACS+. Todos os comandos executados bem como todas as tentativas não autorizadas de execução de comandos devem ser enviados ao servidor TACACS+.

1.19.66. Deve vir acompanhado de interface gráfica para gerenciamento das funcionalidades de VPN e Stateful Firewall relativas ao dispositivo.

1.19.67. Deve implementar, por interface, as funções de DHCP Server, Client e Relay.

1.19.68. Deve suportar a criação de rotas estáticas e pelo menos os seguintes protocolos de roteamento dinâmicos: RIP, RIPv2, OSPF, OSPFv3 e BGPv4. Deve suportar a utilização de pelo menos dois processos de roteamento simultâneos e independentes.

1.19.69. Deve implementar o protocolo PIM (Protocol Independent Multicast) em Sparse Mode.

1.19.70. Deve suportar a operação como IGMP Proxy Agent.

1.19.71. Deve suportar inspeção stateful de tráfego IPv6.

1.19.72. Deve suportar simultaneamente a criação de regras IPv4 e IPv6.

1.19.73. Deve suportar roteamento estático.

1.19.74. Deve implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv6.

1.19.75. Deve suportar anti-spoofing (sem uso de ACLs) para endereços IPv6.

1.19.76. Deve suportar gerenciamento sobre IPv6. Devem ser suportados pelo menos os seguintes protocolos de gerência: Telnet, SSH e HTTPS.

1.19.77. Deve suportar stateful failover de conexões IPv6.

1.19.78. Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

1.19.79. A solução deverá suportar alta disponibilidade em modo ativo-standby com todas as funcionalidades habilitadas.

1.19.80. Deverá suportar alta disponibilidade em modo cluster, com todas as unidades ativas simultaneamente. O modo cluster deve ser suportado com pelo menos as funcionalidades Stateful Firewall, VPN site-to-site e Next-Generation Firewall/IPS ativas simultaneamente.

1.19.81. Deve suportar a identificação e controle de aplicações através de inspeção profunda de pacotes (Deep Packet Inspection), independentemente das portas usadas pela aplicação.

1.19.82. As aplicações devem ser classificadas de acordo com categoria, tipo e nível de risco.

1.19.83. Deve permitir criar regras para monitoramento e controle das aplicações e serviços, sendo capaz de executar no mínimo as seguintes ações:

- Permitir o uso irrestrito de uma ou mais aplicações.
- Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução.
- Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução.
- Negar totalmente o uso de uma ou mais aplicações independentes do usuário.

1.19.84. Deve suportar o controle de aplicações Web 2.0, definindo quais são as operações permitidas para cada uma destas aplicações (deve ser possível, no mínimo, restringir operações de “Post”, bloquear transferência de arquivos, bloquear uso de “games”);

1.19.85. Deve ser possível controlar as micro-applicações que podem ser utilizadas por cada uma destas aplicações Web 2.0 (esse tipo de controle deve estar disponível, no mínimo, para as aplicações Facebook, Google+, Twitter e Skype);

1.19.86. Deve permitir a customização de regras de detecção de novas aplicações.

1.19.87. Deverá suportar a funcionalidades de filtragem de URL, através de licenciamento opcional e atendendo no mínimo as seguintes características:

- Deve permitir a criação de regras de controle de acesso com base em informação de reputação dos sites. Essa base deve ser atualizada dinamicamente.
- Deve permitir criar políticas de acesso baseadas em filtro de categorias de URL.
- Deve ser incluído módulo de filtro de URL integrado na própria ferramenta de Firewall.

- Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, MS Active Directory.
- Deverá possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e Grupos de usuários.
- Deverá possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
- Deverá incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação.
- Deve possibilitar base de URLs local no appliance, evitando delay de comunicação/validação da URLs.
- Deverá possuir pelo menos 50 (cinquenta) categorias de URLs.
- Deverá possibilitar a criação categorias de URLs customizadas.
- Deverá possibilitar a exclusão de URLs do bloqueio por categoria.
- Deve possibilitar a customização de página de bloqueio.
- 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).
- Os logs do produto devem incluir informações das atividades dos usuários.
- A atualização da base de dados deve ser automática com a opção de ser feita manualmente.

1.19.88. Deverá implementar as funcionalidades de IPS, com no mínimo as seguintes características:

- Deve permitir a configuração de regras de exceção de inspeção de tráfego por endereço IP origem/destino ou VLAN, por segmento, realizando apenas a comutação do tráfego sem executar inspeção.
- Deve realizar a monitoração de segmentos de rede em modo transparente sem endereço IP associado às interfaces de monitoração.
- Deve suportar integração com um sistema de gerenciamento centralizado, permitindo que as atualizações, configurações, geração de relatórios e monitoração do IPS seja realizada através de um único ponto.
- Deve ser transparente aos protocolos VRRP, OSPF e HSRP, não causando prejuízo ou modificações de arquitetura de redundância de redes.
- Deve possuir suporte a Jumbo Frame.
- Deve monitorar VLANs padrão 802.1q.
- Deve suportar o protocolo SNTP ou NTP.
- Deve permitir nativamente o uso do SNMP versão 3.
- Deve ser gerenciável via linha de comando através de acesso seguro utilizando o protocolo SSH.
- Deve ser capaz de realizar auditoria das atividades de cada usuário.

1.19.89. Deve ser capaz de visualizar no mínimo as seguintes informações:

- Incidentes de Intrusão.
- Políticas aplicadas.
- Atualizações instaladas.
- Login e logout na interface web de gerência.
- Requisições de aumento de privilégio.
- Inclusões e remoções de regras.
- Registro de sensores na console de gerenciamento.

1.19.90. Configurações relacionadas ao envio de informações detectadas pelos sensores de prevenção contra invasão, para dispositivo de armazenamento externo a solução de gerenciamento.

1.19.91. Deve permitir enviar os logs de auditoria das atividades de cada usuário, para um servidor de Syslogs.

1.19.92. Deve permitir armazenamento dos arquivos de configuração diretamente no appliance.

1.19.93. Deve permitir temporariamente, o armazenamento dos dados coletados e inspecionados em banco de dados local armazenado no sensor de IPS.

1.19.94. Deve permitir inspeção em IP versão 6 incluindo tunelamento IP versão 4 em IP versão 6, IP versão 6 em IP versão 4, IP versão 6 em IP versão 6, IP versão 6 com VLAN e label MPLS.

1.19.95. Deve permitir a inspeção em túneis GRE.

1.19.96. Deve permitir identificar/ restringir o acesso de hosts externos ao perímetro monitorado baseando-se em informações de reputação de domínios de e ranges de endereço IP.

1.19.97. Deve possuir capacidade de criar regras independentes para cada segmento monitorado.

1.19.98. Deve ser capaz de reconstruir e inspecionar fluxos de dados na camada de aplicação.

1.19.99. Deve possuir capacidade de remontagem de fluxo TCP e IP defragmentation;

1.19.100. Deve possuir capacidade a resistência às ferramentas de evasão.

1.19.101. Deve possuir a capacidade de identificação de protocolos que utilizam portas aleatórias.

1.19.102. Deve detectar e bloquear os ataques independente do sistema operacional alvo.

1.19.103. Deve permitir monitoração de sessões de pacotes na rede, atuando em modo “stateful inspection” (análise pacote a pacote e todo o seu estado), sendo capaz de bloquear ataques e tráfego não autorizado ou suspeito.

1.19.104. Deve possuir filtros de “PortScan”, protegendo a rede contra ataques do tipo “scan”.

1.19.105. Deve possuir filtros de proteção a equipamentos de rede, protegendo contra ataques a vulnerabilidades de equipamentos de rede (ex.: roteadores, switches, etc.).

1.19.106. Deve realizar análise e decodificação de fluxos de pacotes nas camadas 2 à 7 com no mínimo suporte aos seguintes protocolos e aplicações: IP, DNS, H.323, TCP, RPC, MPLS, SIP, ICMP, HTTP, FTP, P2P, ARP, Telnet, SMTP, IM, UDP, IMAP, SMB.

1.19.107. Deve possuir filtros de vulnerabilidades específicos dos protocolos de VoIP que bloqueiem: anomalias de protocolos, ataques de negação de serviço, vulnerabilidades específicas conhecidas, ferramentas de ataque e geradores de tráfego que causem degradação ou indisponibilidade de serviços.

1.19.108. Deve possuir no mínimo as seguintes proteções contra ataques a aplicações Web:

- Web Protection;
- Cross-Site Scripting;
- SQL Injection;
- Client-side attacks;
- Injection Attacks;
- Malicious Files Execution;
- Information Disclosure;
- Path Traversal;
- Authentication;
- Buffer Overflow;
- Brute Force;
- Directory Indexing.

1.19.109. Deve permitir criar regras para filtro com base em endereços de origem/destino, protocolo e VLAN ID.

1.19.110. Deve implementar proteção contra ataques DDoS através dos seguintes métodos:

- Controle (limite de quantidade) de conexões por origem;
- Controle (limite de quantidade) de conexões por destino;
- Controle (limite de quantidade) de requisições “SYN” por origem;
- Controle (limite de quantidade) de requisições “SYN” por destino;
- Controle (limite de quantidade) de conexões (origem e Destino) e Controle (limite de quantidade) de requisições “SYN”(Origem e Destino).

1.19.111. Deve possibilitar que os pacotes sejam capturados para análise.

1.19.112. Deve ser capaz de identificar e bloquear ataques baseados em análises de anomalias de tráfego, anomalias de protocolo (RFC Compliance, Protocol Decoders, Normalização), assinaturas e vulnerabilidades.

1.19.113. Deve ser fornecido com uma configuração de filtros recomendados pré-configurados.

1.19.114. Deve permitir a inclusão de informações de vulnerabilidades oriundas de ferramentas de varredura externa.

1.19.115. Deve permitir a identificação de anomalia de rede observando o tráfego ou informações do flow de ativos da rede de forma nativa.

1.19.116. 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.

1.19.117. Deve permitir a análise do comportamento da rede fornecendo visibilidade do uso do segmento monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, no mínimo as seguintes informações devem ser disponibilizadas:

- Fluxos de sessão dos hosts
- Hora de início/fim.
- Quantidade de dados trafegados.

1.19.118. 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.

1.19.119. 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.

1.19.120. 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.

1.19.121. Deve permitir criar regras para monitoramento e controle das aplicações e serviços nos segmentos monitorados, os sensores de IPS devem ser capazes de executar no mínimo as seguintes ações:

- Permitir o uso irrestrito de uma ou mais aplicações.
- Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução.
- Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução.
- Negar totalmente o uso de uma ou mais aplicações independente do usuário.

1.19.122. Deve possuir capacidade de criar assinaturas definidas pelo usuário com uso de expressões regulares.

1.19.123. Deve ter a capacidade de identificar o tipo de arquivo trafegado e permitir a criação de políticas de detecção e bloqueio de eventos baseados no tipo de arquivo.

1.19.124. A solução deverá detectar e bloquear as seguintes categorias de ataques e ameaças:

- Malwares.
- Port Scans.
- VoIP attacks.
- IPv6 attacks.
- DoS attacks.
- Buffer overflows.

- P2P attacks.
- Anomalias em protocolos e aplicações.
- Ameaças Zero-day.
- Pacotes malformados.
- Segmentação TCP e fragmentação IP.

1.19.125. Deve ser montável em rack de 19 polegadas (devem ser fornecidos os kits de fixação necessários). O equipamento fornecido deve ocupar no máximo 03 (Três) unidades de rack (03 RU).

1.19.126. Deve suportar pelo menos 8 (oito) interfaces 1 Gigabit Ethernet.

1.19.127. Deve suportar com pelo menos 4 (quatro) interfaces 10 Gigabit.

1.19.128. Deve suportar pelo menos 2.000.000 (2 milhões) de conexões simultâneas em sua tabela de estados de Stateful Firewall.

1.19.129. Deve suportar a criação de pelo menos 125.000 (cento e vinte e cinco mil) novas conexões TCP por segundo para a funcionalidade de Stateful Firewall.

1.19.130. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 10 (dez) Gbps para pacotes UDP.

1.19.131. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 5 (cinco) Gbps para pacotes TCP multiprotocolo.

1.19.132. Deve suportar a terminação de pelo menos 10.000 (dez mil) túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas.

1.19.133. Não deve haver restrição de número de usuários simultâneos através do equipamento para a licença de software fornecida para a funcionalidade de Stateful Firewall.

1.19.134. Deve ser possível criar pelo menos 30 (trinta) interfaces lógicas associadas a VLANs.

1.19.135. Deve reconhecer mais de 3000 (três mil) aplicações com atualizações automáticas.

1.19.136. Deve suportar pelo menos 80 categorias de URL.

1.19.137. Deve suportar um throughput de, no mínino, 3 (três) Gbps com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente.

1.19.138. Deve possuir desempenho de, no mínimo, 2 (dois) Gbps para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado.

1.19.139. Deve possuir mais de 280 Milhões de URL categorizadas.

1.19.140. Deverá suportar a funcionalidades de proteção contra Malware, através de licenciamento opcional e atendendo no mínimo as seguintes características:

- Deve prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de command & control, resolução e call-backs.
- Deve possui capacidade para monitoração em tempo real.
- Deve permitir diariamente, semanalmente ou mensalmente informações a respeito das tendências de ataque e riscos do ambiente.
- Deve permitir identificar tráfego de rede gerado por dispositivos conectados no segmento monitorado, incluindo tráfego malware e ataques associados.
- Deve oferecer capacidade nativa e sem necessidade de equipamentos tipo SIEM de correlacionar informações de alertas malwares com ataques detectados e condições de tráfego, para assim definir um tipo de alerta personalizado em tempo real.
- Deve permitir o controle em tempo real de arquivos.
- Deve permitir o bloqueio em tempo real de malwares.
- Deve permitir em tempo real o controle e bloqueio de aplicações (protocolos, clientes e web).
- Deve permitir o controle de acesso.
- Deve permitir o controle de URL's.
- Deve suportar em tempo real a detecção e prevenção (bloqueio imediato) de arquivos malwares e ataques para os protocolos HTTP (Inbound e Outbound), SMTP (Inbound e Outbound), FTP (Inbound e Outbound), POP3 (Inbound e Outbound), IMAP (Inbound e Outbound), NETBIOS-SSN (SMB, Inbound e Outbound) e adicionalmente permite em tempo real a detecção (Inbound ou outbound) e prevenção (bloqueio imediato, Inbound ou outbound) de ataques e tráfego malware do tipo: comunicações de comando e controle, identificação de backdoors, propagação de infecção, presença e uso de ferramentas malware, ataques de negação de serviço, comunicação e presença de keyloggers (troca de informações), identificar redirecionamentos, identificar a exploração de overflows.
- Deve implementar e identifica existência de Malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Command and Control.

- Deve implementar mecanismos de detecção e bloqueio de vazamento de informações sensíveis no ambiente, ao permitir a identificação de dados em: arquivos Microsoft Word (não criptografados) sendo enviados ou recebidos via protocolos FTP e HTTP, números de cartões de crédito para até 8 tipos de protocolos diferentes, endereços e-mail para até 8 tipos de protocolos diferentes e dados customizados pelo administrador para até 8 tipos de protocolos diferentes.
- Deve possuir capacidade de implementar detecção de ataques e malwares que utilizem mecanismo de exploit em arquivos PDF.
- Deve implementar capacidade para detecção de explorações diretas, uso suspeito ou malicioso das seguintes aplicações.
- Deve permitir que arquivos executáveis (MSEXE) identificados pelo sensor sejam automaticamente enviados para análise utilizando tecnologia de virtualização em nuvem.
- Deve manter um histórico dos resultados de avaliações prévias e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite.
- Deve permitir virtualização para análise sobre sistemas operacional Windows;
- Deve implementar rede de inteligência global em tempo real proprietária para cobrir ataques originados de qualquer localidade global, novas origens e destinos de comunicações e distribuição de malwares.
- Deve permitir modo de configuração in-line (em linha) totalmente transparente que permita em tempo real a detecção (inbound e/ou outbound) e a prevenção através de bloqueio (inbound e/ou outbound) de ataques malwares sejam estes no formato de arquivos maliciosos, comunicações ou explorações diretas, caso seja necessário a solução suporta a utilização de configurações de proxies.
- Deve possuir capacidade de automatica e periódicam para download e instalar atualizações de dados de reputação IP para identificação de tráfego associado a origens e destinos de malware, comando e controle, spam, bots, proxies abertos, relays abertos, phishing e TOR (the onion router).
- Deve implementar funcionalidade de bloqueio em tempo real de arquivos maliciosos (detectados como malwares) e comunicações malwares conhecidas no modo inline.

- Deve possuir um recurso de análise tipo “sandbox”, para no mínimo arquivos executáveis (MSEXE) de modo a permitir a análise completa do comportamento do Malware ou código malicioso.
- Deve possuir recursos que permitem o envio de informações de eventos de ataques e malwares para ferramentas de SIEM de fabricantes terceiros.
- Deve possuir recursos que permitem o envio de informações de eventos de ataques e malwares para servidores Syslog.

1.19.141. Deve implementar suporte a protocolo SNMP v1, v2 e v3 para atividades de gerenciamento.

1.19.142. Deve implementar atualização da base de dados da Rede de Inteligência de forma automático, permitindo o agendamento mínimo de 2 hora de intervalo.

1.19.143. Deve implementar via interface de gráfica de gerenciamento todas as opções de análise e tratamento eventos de ataques de rede, Malware, detecção de tráfego e notificação de eventos em tempo real, adicionalmente implementa automáticamente a capacidade de traçar uma visão cronológica de eventos de forma gráfica permitindo identificar em tempo-real a trajetória de acesso ou propagação de ameaças malware de forma lateral no ambiente, identificando o nome do arquivo, tipo e categoria do arquivo, nível de ameaça quando disponível, sha-256, tipo de evento, protocolo de aplicação utilizado, aplicação cliente utilizada para transferência, quantidade de visualizações, dia e hora, origem e destino do tráfego.

1.19.144. Deve realizar toda detecção e bloqueio de ataques de rede e malwares em tempo real, não sendo uma solução que necessita de ou é exclusivamente dependentes de tecnologia de virtualização tipo “sandboxing” para detecção de arquivos maliciosos e presenção de malware na rede monitorada.

1.19.145. Os processos de detecção e determinação de malwares, ataques e tráfego assim como os bloqueios preventivos inclusive para os arquivos sendo transferidos pela rede pelos protocolos suportados são realizados de forma automatizada e em tempo real.

1.19.146. O recurso de execução em ambiente de virtualização disponibilizado (sandbox), permite o envio de arquivos suportados pela solução de rede para este tipo de solicitação de análise dinâmica.

1.19.147. A solução implementa múltiplos motores (engines) para verificação de Malware e/ou códigos maliciosos, não dependendo somente da utilização de recursos de análise virtualizada (sandbox) como método de identificação de malwares em arquivos.

1.19.148. Deve permitir implementar mecanismo de definição de exceções do tipo whitelist de arquivos, endereços IP, aplicações.

1.19.149. Deve permitir criação de regras de detecção utilizando o padrão SNORT e permitir a criação de detecções de arquivos maliciosos utilizando amostra de arquivo, hash SHA-256 único e lista de hash SHA-256.

1.19.150. Deve permitir implementar mecanismo de whitelist e detecções customizadas de arquivos, permitindo definição de regras por VLAN, subrede, endereço IP para utilização das listas.

1.19.151. Deve implementar a identificação e capacidade de controle de acesso em tempo real para os seguintes tipos de arquivo:

- MSEXE,9XHIVE,DMG,DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN,BINARY_DATA,BINHEX, EICAR, ELF,ISHIELD_MSI, MACHO, RPM, TORRENT, AMR,FFMPEG,FLAC,FLIC,FLV,IVR,MIDI,MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WAV,WEBM,7Z, ARJ,BZ,CPIO_CRC,CPIO_NEWC,CPIO_ODC,,JAR,LHA,MSCAB,MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_ENC,ACCDB,HLP, MAIL,MDB,MDI,MNY,MSCHM,MSOLE2,MSWORD_MAC5,MWL, NEW_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS.

1.19.152. Deve implementar em tempo real a inspeção, detecção e bloqueio autónomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos:

- 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC.

1.20. EQUIPAMENTOS ROTEADORES

Com objetivo de atender as necessidades dos Órgãos e Unidades da Rede de Dados do Governo do estado do Rio de Janeiro, são especificados 4 (quatro) tipos de roteadores em função das velocidades e da demanda por funcionalidades e serviços. Assim, estima-se a sua utilização do seguinte modo, considerando também o limite de 75% de utilização da CPU.

TIPO I: circuitos com velocidades de até 15Mbps.

TIPO II: circuitos com velocidade de até 35Mbps.

TIPO III: circuitos com velocidade de até 100Mbps.

TIPO IV: circuitos com velocidade de até 250Mbps.

TIPO V: circuitos com veurançalocidade de até 2Gbps.

Todos os roteadores a serem fornecidos devem ser novos e de primeiro uso.

1.20.1. 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.
- 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 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;
- 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 autenticação de usuário através de TACACS+.
- Deve possuir suporte a protocolo de redirecionamento para cache de Web (WCCP).

- 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);
    - Implementar serviços de VPN baseados no padrão IKE(Internet Key Exchange).
    - Possuir capacidade de pelo menos 100 (cem) túneis IPSec VPN Site- to-Site.

- 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.
- Possuir mecanismo de automatização dos processos de “enrollment” e autenticação na autoridade certificadora (obtenção dos certificados digitais da CA e do certificado que ela gerou para o equipamento solicitante).
- Suportar IKEv1 e IKEv2.
- Suportar Suite B de criptografia conforme RFC 4869.
- Deve possuir capacidade de autenticação via Radius para estabelecimento de um VPN IPSec site-to-site.
- Suportar alta disponibilidade de túneis IPSec em cenários com 2 CPEs.
- Deve ser fornecido hardware específico (interno ao equipamento) dedicado às funções criptográficas.
- 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.
- Permitir a criação de VPNs de acordo com o conjunto de padrões IPSEC em modo túnel.
- Suportar os modos de operação “tunnel mode” e “transport mode”.
- Suportar as funcionalidades de gerenciamento de chaves para VPN.
- Implementar VPNs IPSec em IPv6.
- Implementar o transporte do protocolo IPv6 sobre VPNs IPSec.
- Implementar distribuição de chaves criptográficas e criação de IPSec “Security Associations” de acordo com o padrão GDOI (Group Domain of Interpretation), definido na RFC 3547.
- A distribuição de políticas de criptografia e chaves criptográficas, assim como a renovação de tais chaves, deve ser feita de forma centralizada em Unicast e Multicast. Deve ser possível autenticar as entidades que participam da VPN baseada no padrão GDOI através de chaves pré-compartilhadas e certificados digitais, utilizando-se o protocolo Internet Key Exchange (IKE, RFC 2409)
- Implementar, de forma transparente (sem alteração de endereços IP de origem e destino), a criptografia dos pacotes IP Multicast. O tráfego de multicast deve ser cifrado fim-a-fim (entre o roteador ao qual a fonte se conecta e os roteadores em que há receivers” conectados),

sem a necessidade de criação de túneis.

- 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.
- Devem ser preservadas para os pacotes cifrados todas as marcações de QoS (campo DSCP) feitas para os pacotes originais (antes do processo de criptografia).
- Deve implementar uma rede VPN totalmente ligada com criptografia entre sites (full-mesh), sem a necessidade de túneis ponto a ponto.
- A solução de VPN fornecida deve ser capaz de proteger, usando os serviços IPSec (confidencialidade, integridade e autenticação), tráfego real-time entre as localidades remotas. Deve ser possível estabelecer dinamicamente tais conexões spoke-to-spoke, de modo a evitar duplo processo de criptografia no elemento central, utilizando Túneis dinâmicos Ponto a Ponto, conforme RFC 2332.
- O equipamento fornecido deve ser capaz de terminar simultaneamente conexões IPSEC do tipo “site-to-site” e “client-to-site” (VPNs de acesso remoto). 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.
- Suportar o tráfego protocolo GRE sobre IPSEC.
- 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.

1.20.2. 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.
- 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.
- 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:
    - 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.

- 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 autenticação de usuário através de TACACS+.
- Deve possuir suporte a protocolo de redirecionamento para cache de Web (WCCP).

- 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.
- Suportar Suite B de criptografia conforme RFC 4869.
- 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.

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.

1.20.3. 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.
- 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.
- 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 883.000 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:
    - 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.

- 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 autenticação de usuário através de TACACS+.
- Deve possuir suporte a protocolo de redirecionamento para cache de Web (WCCP).
- 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.

- Suportar Suite B de criptografia conforme RFC 4869.
- 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.

1.20.4. TIPO IV

- Deve possuir, no mínimo, 4 (quatro) 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.
- 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.
- 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 1.845.000 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:
    - 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.
- 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 autenticação de usuário através de TACACS+.
- Deve possuir suporte a protocolo de redirecionamento para cache de Web (WCCP).
- 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.
    - Suportar Suite B de criptografia conforme RFC 4869.
    - 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.

1.20.5. TIPO V

- 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 frequência (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) e IKEv2.
- Suportar Suite B de criptografia conforme RFC 4869.
- 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.

1.21. DOS CIRCUITOS DE ACESSO DA REDE GOVERNO

1.21.1. CIRCUITOS DE ACESSO DO DATACENTER DO PRODERJ

Os circuitos de acessos do Backbone da Rede Governo conectados aos Datacenter do PRODERJ deverão atender aos seguintes requisitos.

1.21.1.1. Todos os circuitos deverão ser atendidos obrigatoriamente através de Fibra Ótica, sendo que os acessos redundantes deverão ser atendidos por cabos de fibra ótica por caminhos distintos.

1.21.1.2. A redundância dos enlaces e roteadores CPEs deverá ser implementada, de modo que cada enlace seja conectado a um CPE físico distinto, sendo que circuitos e roteadores deverão ser capazes de assumir todo o tráfego.

1.21.1.3. Cada enlace contratado, principal e de contingência deverão ser conectados a um PE (Provider Edge) físico distinto do backbone da CONATRATADA.

1.21.1.4. A CONTRATADA deverá elaborar o Projeto Físico e Lógico de Redundância, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados.

1.21.2. CIRCUITOS DE ACESSO DAS UNIDADES ESPECIAIS

1.21.2.1. Todos os circuitos deverão ser atendidos obrigatoriamente através de Fibra Ótica, sendo que os acessos redundantes deverão ser atendidos por cabos de fibra ótica por caminhos distintos ou por fibra ótica (principal) e rádio enlace de frequência licenciada.

1.21.2.2. A CONTRATADA deverá elaborar o Projeto Físico e Lógico de Redundância, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados.

1.21.2.3. Casos de exceções para atendimento as Redes dos Órgãos e Unidades

do Governo deverão ser tratadas com Órgãos com a anuência da Gerência de Redes e Telecomunicações do PRODERJ, durante validação do Projeto Executivo com os envolvidos.

1.21.2.4. A solução completa de contingência deverá ser testada pela CONTRATADA periodicamente ao longo da execução do contrato. A periodicidade deverá ser semestral e o horário da realização dos testes será definido em comum acordo com o PRODERJ que deverá ser notificado para acompanhar os testes.

1.21.2.5. A CONTRATADA deverá disponibilizar relatório com os resultados dos testes de Contingência.

1.21.2.6. O PRODERJ poderá solicitar a realização extraordinária dos testes com antecedência mínima de sete dias úteis.

1.22. DOS REQUISITOS DE ROTEAMENTO

1.22.1. O Plano de Roteamento deverá ser proposto pela prestadora vencedora em seu Projeto Executivo. Serão definidas as características dos protocolos de roteamento que serão instalados em cada um dos sítios, de forma a garantir a interconexão entre eles.

1.22.2. A CONTRATADA deverá prestar os serviços de comunicação de dados, conforme os seguintes padrões: RFC 1163 (BGP - Border Gateway Protocol), RFC 2283 (Multiprotocol Extensions for BGP-4) e RFC 2547 (BGP/MPLS/VPNs).

1.22.3. As premissas para a criação do Plano de Roteamento da rede são:

- Ser escalável.
- Realizar agregação de rotas para endereços contíguos.
- Manter o plano de roteamento atual das redes internas da Rede Governo.
- Permitir o acesso de qualquer ponto da rede às aplicações compartilhadas.

1.22.4. Devido ao porte da rede corporativa, a configuração do roteamento através de rotas estáticas pode não ser muito atrativa, pois a tarefa de gerenciamento de rotas principais e alternativas, para o caso de falhas, se torna uma tarefa muito trabalhosa e suscetível a erros.

1.22.5. Ficará a cargo da CONTRATADA a definição do protocolo de roteamento a ser utilizado entre os roteadores PE e CPE. Porém, recomenda-se o uso de um protocolo com baixo tempo de convergência, como o BGP em sua última versão. Nesse sentido, a solução de roteamento deverá permitir a convergência da rede em um tempo menor que 20 (vinte) segundos para o caso de mudança topológica da rede causada por falha(s) em enlace(s) ou equipamento(s).

1.22.6. A solução de roteamento deverá ser projetada e implantada de forma escalável permitindo a evolução e o crescimento da rede.

1.23. DOS REQUISITOS DE SEGURANÇA

1.23.1. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados.

1.23.2. A ação descrita no subitem anterior possui o intuito de prevenção de incidentes de segurança de forma a garantir níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do Governo do Estado do Rio de Janeiro.

1.23.3. Em relação aos aspectos técnicos de segurança da informação, a CONTRATADA deverá atender aos seguintes requisitos:

1.23.3.1. Prover uma rede logicamente independente e isolada de qualquer rede de terceiros, inclusive da internet. O isolamento deverá ser realizado em nível lógico do MPLS e em nível 2 (do modelo OSI) para o acesso. Esta garantia deverá ser implantada fim-a-fim e também se aplica às soluções de contingência.

1.23.3.2. Caso seja solicitado pelo PRODERJ, a CONTRATADA deverá aplicar nos roteadores CPEs fornecidos e em outros equipamentos, exclusivos para prestação de serviços, implementações de segurança tais como: autenticação do roteador CPE, controle de acesso aos dispositivos, listas de acesso e logging e outras configurações necessárias à segurança da Rede Governo.

1.23.3.3. Caso necessário deverá ser empregado esquema de autenticação no nível de protocolo de roteamento, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da Rede Governo.

1.23.3.4. Será responsabilidade da CONTRATADA, manter em seus quadros técnicos especialistas em segurança e prover serviços específicos de prevenção e reação aos incidentes de segurança em tecnologia da informação.

1.23.3.5. A CONTRATADA deverá configurar de maneira apropriada os elementos de rede para habilitar o registro dos eventos da Rede Governo, tais como conexões externas e registro de utilização de serviços (por exemplo, arquivos transferidos através de FTP e tentativas de login não autorizados). Os registros devem estar com o horário sincronizado via protocolo NTP e possuir detalhes suficientes para identificação do evento, seu autor, seu alvo/objeto e momento de ocorrência.

1.23.3.6. A CONTRATADA deverá possuir um sistema dedicado à coleta e ao armazenamento dos registros gerados pelos dispositivos da Rede Governo.

1.23.3.7. A CONTRATADA deverá aplicar e manter atualizados patches de segurança nos seus roteadores, incluindo os CPE dos sítios ou em outros equipamentos de suas redes, exclusivos para prestação de serviços ao Governo do Estado.

1.23.3.8. A CONTRATADA deverá informar ao PRODERJ os patches de segurança necessários para a atualização dos roteadores CPEs do backbone do PRODERJ, unidades especiais e dos sítios, exclusivos para prestação de serviços a Rede do Governo.

1.24. ESPECIFICAÇÕES DE QoS DA REDE MPLS

1.24.1. A rede MPLS da CONTRATADA deverá suportar Qualidade de Serviço (QoS), de acordo com condições estabelecidas nesse item, inclusive considerando a arquitetura DiffServ.

1.24.2. Deverá permitir a obtenção de escalabilidade e eficácia na diferenciação dos serviços através da implementação de mecanismos de classificação e condicionamento somente nos elementos de borda da rede e aplicação “per-hop behaviors” aos agregados de tráfego que forem marcados usando se o campo DS nos campos apropriados dos cabeçalhos de pacotes MPLS.

1.24.3. No escopo da conexão de cada cliente, há a necessidade de diferenciação de serviços, incluindo a alocação de banda e priorização de pacotes para redução de atrasos de certas classes de tráfego.

1.24.4. 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:

1.24.4.1. Supervisão de Rede: aplicações de monitoramento e controle da rede, que deverão ser priorizadas acima de todas as outras a fim de garantir a disponibilidade de recursos para as intervenções preventivas ou corretivas que se façam necessárias ao seu correto funcionamento, tais como, por exemplo: Telnet, SSH, SNMP, NTP, syslog e Radius.

1.24.4.2. Tempo Real – aplicações de Voz e Video sensíveis que são sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem priorização de pacotes limitadas a 50% da Banda.

1.24.4.3. Deverá a CONTRATADA disponibilizar duas classes de serviços distintas de Tempo Real, uma para Voz e outa para Víodeo.

1.24.4.4. Dados Críticos: aplicações críticas que exigem a entrega garantida e tratamento prioritário, tais como acesso HTTP e HTTPS a portais corporativos internos.

1.24.4.5. Dados Prioritários: aplicações que sejam menos críticas, mas que também necessitem de tratamento prioritário na rede da CONTRATADA.

1.24.4.6. Melhor Esforço – Best Effort: todo tráfego não explicitamente atribuído às classes Supervisão da Rede, Tempo Real, Dados Prioritários deverá ser alocado nesta classe. Sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como tráfegos importantes. Essa classe deverá permitir o fluxo de tráfego, se houver recursos disponíveis na rede, impedindo que esse tráfego afete negativamente as demais classes.

1.24.5. A definição das classes e percentuais de reserva de banda deverá discutida com a equipe técnica do PRODERJ para definição no Projeto Executivo da solução. A equipe de engenharia de tráfego da CONTRATADA deverá, sempre que possível, auxiliar acerca de tais aspectos de modo a otimizar a operação da rede. Ademais, o PRODERJ poderá solicitar a qualquer momento a modificação nas configurações das classes de serviço, de modo a adaptar à evolução de tráfego de suas aplicações.

2. SERVIÇO MPLS ATRAVÉS DE ACESSO SATÉLITE

O Serviço VPN IP MPS através de acesso satélite tem por objetivo ser uma alternativa para atendimento de localidades onde não existam facilidades de acesso terrestre convencional limitado a 10% do total de acessos.

Neste item são descritos requisitos para prestação do serviço MPLS através de acessos satélites VSAT.

2.1. Os satélites para acesso VSAT (Very Small Apaerture Terminal) estão em órbita geoestacionária e fazem o intermédio da transmissão dos dados entre as pequenas estações terrestres remotas (terminais VSAT) e a estação de terrestre mestre ou "HUB".

2.2. O serviço deverá ser prestado através da tecnologia VSAT com antenas remotas parabólicas terminais entre 75 cm e 1,2m de diâmetro.

2.3. Os acessos VSAT deverão possibilitar a interligação ao mesmo Backbone IP da CONTRATADA que compõe o serviço MPLS, isto é, o serviço MPLS SAT será um acesso, que mesmo possuindo características específicas, deve fazer parte da mesma rede MPLS terrestre contemplada neste edital.

2.4. A CONTRATADA deverá disponibilizar:

2.5. Características básicas do serviço a ser prestado:

- MPLS com acesso satélite, qualidade de serviço e perfil de tráfego.
- Dois perfis de tráfego: D (dados), DV (dados e voz).
- Quatro velocidades: 512 Kbps, 1 Mbps e 2 Mbps.
- Antenas de 1.2m.
- Cobertura Nacional.

- Operação em Banda Ku.
- Utilização da tecnologia VSAT (TDMA) banda larga bidirecional.

2.6. Definições:

- Taxa Nominal de Download: corresponde à velocidade de pico que poderá ser alcançada pelo usuário no sentido download da rede para o cliente. A velocidade de pico não é garantida e depende da carga de tráfego da rede.
- Velocidade Típica de Download: é a taxa tipicamente garantida no sentido de download.
- Taxa Nominal de Upload: corresponde à velocidade de pico que poderá ser alcançada pelo usuário no sentido upload do cliente para rede. A velocidade de pico não é garantida e depende da carga de tráfego da rede.
- Velocidade Típica de Upload: é a taxa tipicamente garantida no sentido de upload.

2.7. O serviço ofertado pela CONTRATADA deverá atender aos seguintes Perfis de Tráfego.

- Perfil D: 100% de tráfego de dados.
- Perfil DV: 70% de tráfego de dados e 30% de tráfego de voz. Podendo através ser disponibilizados até 2 canais de voz.

2.8. A CONTRATADA deverá fornecer antena VSAT e receptor satélite IDU (Indoor Unit), conjuntamente com os serviços de instalação e manutenção dos acessos VSAT.

2.9. A CONTRATADA também deverá disponibilizar o roteador adequado à prestação do serviço MPLS com acesso satélite.

2.10. Os Órgãos CONTRATANTES serão responsáveis por disponibilizar local, energia e aterramento e climatização adequada para instalação dos equipamentos, com deverá possuir sistema de para-raios em suas instalações, caso necessário para disponibilização dos serviços.

2.11. Opções de acordo com a velocidade e perfil de tráfego solicitado pela CONTRATANTE.

Opções	**Perfil**	**Velocidade de Download (bps)**		**Velocidade de Upload (bps)**	
		Nominal	**Típica**	**Nominal**	**Típica**
512K/256K/D	Dados	512K	256K	256K	128K
1M/512K/D	Dados	1M	512K	512K	256K

2M/1M/D	Dados	2M	1M	1M	512K
1M/512K/DV	Dados e Voz	1M	512K	1M	512K

3. SERVIÇO DE INTERLIGAÇÃO DATACENTER

Neste item são descritos os requisitos do serviço a ser prestado pela CONTRATADA para interligação dos dois Datacenters do PRODERJ.

3.1. Esta interligação deverá possuir baixa latência, tipicamente abaixo de 20ms, possibilitando a implementação de sistemas de replicação de bases de dados entre os dois Datacenter e soluções de Disaster Recovery.

3.2. A conectividade entre os Datacenters deverá ser no mínimo na velocidade de 1Gbps através de solução der transporte PTN ou DWDM.

3.3. A conectividade desta interligação deverá ser realizada com os Roteadores Concentradores do Núcleo da Rede Governo.

3.4. A CONTRATADA deverá quando da implantação o projeto Lógico de contingência envolvendo esta interligação, que deverá ser aprovado pelo PRODERJ para a sua implantação.

3.5. O PRODERJ será responsável pela configuração dos elementos de sua rede interna de forma que projeto aprovado possa ser implantado.

4. SERVIÇO DE SEGURANÇA DE REDE

O Serviço de Segurança de Rede tem por objetivo ofertar uma camada de segurança adicional para determinados sites críticos da Rede Privativa MPLS, sendo que sua contratação é opcional para cada circuito da Rede MPLS que atenda a determinado Sítio.

4.1. A solução de Segurança deverá ser baseada nos softwares dos roteadores (CPE) a serem instalados nos circuitos, através do fornecimento das licenças de Segurança, assinatura de IPS/IDS e licenças de Suporte de Assinatura e de Upgrade de Sistema Operacional.

4.2. Deverá ser realizado a configuração da solução de Firewall embarcada nos roteadores (CPE) dos circuitos da Rede MPLS, e o provimento das atualizações das licenças forma a minimizar os incidentes de Segurança.

4.3. Implementar novas regras nos equipamentos de segurança, em conformidade com o solicitado pela CONTRATANTE.

4.4. O serviço de Segurança de Rede deverá contemplar:

4.4.1. Criação e administração de políticas de firewall.

4.4.2. Criação e administração de políticas de IPS/IDS.

4.5. A Contratada deverá atuar para solucionar possíveis problemas e incidentes de segurança.

4.6. São definidas as seguintes opções Segurança de Rede em função do tipo de roteador definido no atendimento dos circuitos.

SEC-TIPO I: para o roteador TIPO I.

SEC-TIPO II: para o roteador TIPO II**.**

SEC-TIPO III: para o roteador TIPO III.

SEC-TIPO IV: para o roteador TIPO IV.

4.7. Sendo contratado um roteador com a funcionalidade do serviço de segurança incorporada o valor para este deverá contemplar ambas as funcionalidades de roteamento e segurança.

5. SERVIÇO CENTRALIZADO DE ACESSO À INTERNET

Este documento apresenta os requisitos e especificações técnicas para contratação do Serviço de Acesso à Internet para a Rede Governo do Estado do Rio de Janeiro.

5.1. Este encarte complementa o Termo de Referência, constituindo a documentação necessária e obrigatória à contratação do acesso à internet do Governo do Estado do Rio de Janeiro.

5.2. O objeto desta contratação visa o fornecimento do serviço de acesso à internet para a Rede Governo, com objetivo de centralizar a conexão com a Internet para as unidades descentralizadas abrangidas pela rede IP MPLS.

5.3. O projeto comtempla a fornecimento de links de acesso à Internet Principal e Redundante para o Núcleo da Rede Governo com objetivo garantir a disponibilidade do serviço quando da ocorrência de “falha” no provimento do serviço através do link principal.

5.4. A contratação contempla a instalação e configuração dos equipamentos e enlaces de comunicação, e o gerenciamento pró-ativo do serviço, visando à melhoria do processo de recuperação do serviço em caso de falha.

5.5. O acesso à INTERNET compreende o fornecimento de banda INTERNET dedicada e exclusiva. Neste serviço consta ainda o fornecimento de endereçamento IPs públicos conforme necessidade do PRODERJ.

5.6. As especificações técnicas descritas nesse documento englobam definições do projeto detalhado da rede, premissas de topologia de rede, tecnologias de acesso aplicáveis, capacidades de enlaces de comunicação, aspectos de interconexão e de roteamento, requisitos de qualidade de serviço, definições de gerência de rede e aspectos de segurança da informação.

5.7. Com a presente contratação, pretende-se que o PRODERJ seja um ponto central de

Internet para os sítios abrangidos pela rede IP MPLS. Além disso, o PRODERJ pretende a contratação de links redundantes para fornecimento do serviço de Internet, de forma a garantir a disponibilidade do serviço, mesmo quando de problemas de provimento do serviço pelos links principais.

5.8. Os benefícios a serem auferidos com a implantação dos serviços especificados são, dentre outros:

- Melhores índices de disponibilidade dos sistemas.
- Rapidez, agilidade e segurança aos usuários internos e externos no acesso à informação.
- Utilização dos melhores recursos de TIC para a implantação dos programas e projetos sob a responsabilidade do PRODERJ.
- Ampliação da velocidade da internet para a Rede Governo.
- Redundância no fornecimento do link internet da Rede Governo, garantindo a disponibilidade do serviço, para o PRODERJ e os sítios abrangidos pela internet.

5.9. Implantar uma solução flexível e escalável tanto em capacidade como em funcionalidades permitindo que a Rede Governo adapte-se rapidamente a eventuais aumentos ou diminuições de demanda, ou necessidade de provimento de novos serviços.

5.10. A presente contratação prevê que serão atendidas pelo serviço dedicado à internet as seguintes localidades:

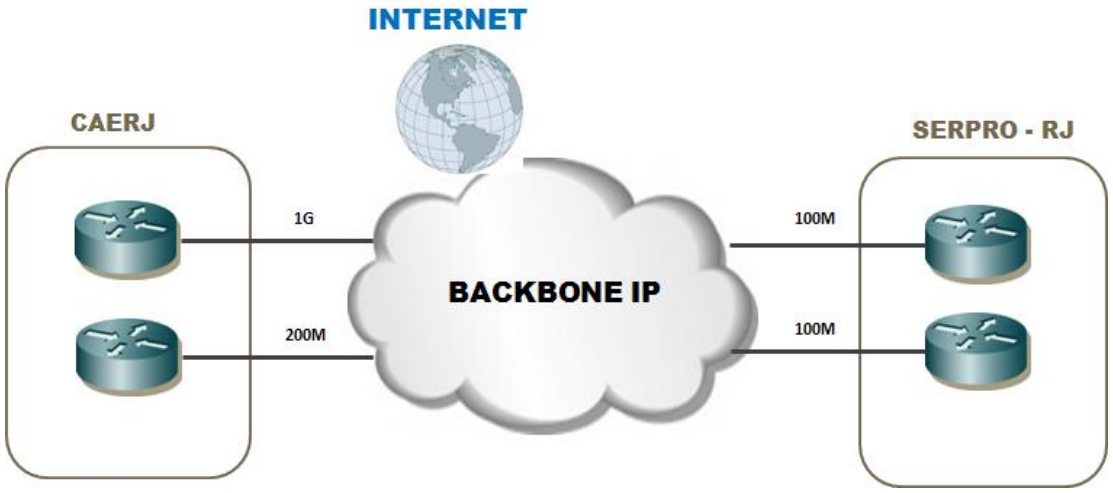
- PRODERJ – Sede no Rio de Janeiro;
- Unidade SERPRO – Jardim Botânico – Rio de Janeiro.

5.11. Portanto, com base nas características atuais das unidades da Rede Governo, e considerando a expectativa de crescimento da utilização dos serviços providos hoje por meio dos sistemas existentes, optou-se por registrar preços utilizando tabelas de patamares para especificar as larguras de banda, de acordo com a necessidade da demanda durante o contrato.

5.12. Os patamares informados poderão ser contratados oportunamente de acordo com o perfil de tráfego apurado.

5.13. A CONTRATADA deverá o acesso de última milha através de fibra ótica e meios próprios, não sendo permitida a subcontratação do meio de acesso.

5.14. Na figura abaixo são mostradas as conexões atuais do Core da Rede Governo, para o acesso à Internet.



5.15. ESPECIFICAÇÕES TÉCNICAS

Cada um dos acessos e respectivos circuitos de comunicação de dados devem apresentar, no mínimo, as seguintes especificações técnicas gerais:

5.15.1. Ter capacidade de expansão até a velocidade máxima de operação da interface utilizada, quando solicitado pelo PRODERJ.

5.15.2. Prover conexão à Rede Corporativa da Rede Governo por meio de pelo menos uma interface do tipo Giga Ethernet Full Duplex.

5.15.3. O acesso de ser dedicado e o serviço deverá possuir a banda garantida de acordo com a velocidade do acesso contratado.

5.15.4. O Serviço fornecido deverá suportar o protocolo IPV6, caso solicitado pelo PRODERJ.

5.15.5. A prestação do serviço compreende a disponibilização, instalação, ativação e configuração do(s) equipamento(s) que compõem o acesso, e outros que possibilitem a utilização do serviço objeto da presente contratação.

5.15.6. A CONTRATADA deverá disponibilizar toda a infraestrutura de telecomunicações (equipamentos e insumos) necessária ao pleno funcionamento dos serviços contratados, sem custo adicional ao PRODERJ.

5.15.7. A CONTRATADA deverá possuir Backbone IP próprio, com conexão própria a outros Provedores de Acesso à Internet Nacionais e Internacionais.

5.15.8. O Backbone da CONTRATADA deverá possuir conexão a mais de dois AS (Autonomous System), independentes e distintos.

5.15.9. A CONTRATADA deverá possuir pelo o menos um POP (ponto de presença) próprio no exterior para a troca de tráfego internacional.

5.15.10. O somatório das bandas de saída nacional e internacional entre os AS de pelo menos 100 Gbps.

5.15.11. O serviço IP dedicado deverá suportar aplicações TCP/IP (Transmission Control Protocol / Internet Protocol), tais como:

- HTTP, HTTPS
- FTP (FileTransfer Protocol)
- TELNET (TERminal NETwork)
- SSH (Secure Shell)
- SMTP (Simple Mail Transfer Protocol)
- SMTPS (Simple Mail Transfer Protocol Secure)
- POP3 (Post Office Protocol version 3)
- LDAP (Lightweight Directory Access Protocol)
- VPN, e tráfego de vídeo e voz sobre IP (VoIP), no sentido para a Internet e vice-versa.

5.15.12. O Provedor deverá dispor de recursos de gerência e supervisão para o circuito.

5.15.13. A CONTRATADA deverá disponibilizar faixa de endereço IP válido, com no mínimo 8 (oito) endereços IP válidos.

5.15.14. A CONTRATADA também deverá disponibilizar quando adequadamente justificado pela CONTRATANTE faixa de endereçamento IP válidos adicionais, com o objetivo de atender as necessidades operacionais da CONTRATANTE.

5.15.15. A CONTRATADA deverá disponibilizar servidores de DNS secundário na função “recursivo”, ou seja, ao receberem uma solicitação de qualquer usuário na qual o mesmo não tenha a informação em cache ou não sendo o seu próprio domínio, ele se encarrega em buscar essa informação em outro servidor de DNS.

5.15.16. Caso os servidores de DNS da CONTARATADA sejam utilizados como secundário, a CONTRATADA deverá gerenciar a transferência dos registros de zona com o seu servidor de DNS primário da CONTRATANTE. A CONTARATADA também deverá fornecer as informações relativas à compatibilidade entre os seus servidores de DNS primários e os servidores secundários.

5.15.17. Servidor NTP (Network Time Protocol) ou acesso a servidores NTP públicos nacionais para sincronismo de horário dos servidores e ativos de rede do PRODERJ.

5.15.18. Os servidores de DNS da CONTRATADA deverão dar suporte à tecnologia DNSSEC (Domain Name System Security Extensions) ou DNS over SSL

(Security Socket Layer).

5.15.19. Os canais de comunicação deverão ser configurados com velocidades simétricas (upstream = downstream).

5.15.20. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 25ms.

5.16. PERSPECTIVA DE CRESCIMENTO DOS NÚMEROS DE SÍTIOS E DA ALTERAÇÃO DA BANDA DE ACESSO

5.16.1. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão de bandas de comunicação, respeitados os limites legais e técnicos, bem como as condições estipuladas nos níveis de serviços.

5.16.2. O PRODERJ poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços ou mesmo a adição de um novo sítio.

5.17. DAS CARACTERÍSTICAS MÍNIMAS DO ROTEADOR

5.17.1. A CONTRATADA deverá prover equipamento roteador e respectivos cabos de comunicação de dados, para cada um dos acessos contratados, a serem instalados nas dependências do PRODERJ com as seguintes características:

5.17.1.1. Ser dimensionado para garantir, em termos de disponibilidade e desempenho, os níveis de serviços exigidos requeridos para o tráfego de Internet da Rede Governo.

5.17.1.2. Ser dedicado ao serviço de acesso à Internet durante o transcorrer do contrato, podendo somente ser desativado ao término deste ou em caso de substituição sujeita à autorização do PRODERJ.

5.17.2. O roteador fornecido pela CONTRATADA deverá atender aos seguintes requisitos mínimos

5.17.2.1. Suportar a configuração de VLAN - Virtual Local Area Networks – (IEEE 802.1Q).

5.17.2.2. Suportar protocolo de gerenciamento SNMP (Simple Network Management Protocol) v1, v2c e v3, de modo a ser acessível pelos sistemas de gerência de redes do GOVERNO DO ESTADO, incluindo configuração de envio de traps.

5.17.2.3. Permitir configuração de contas locais e de contas autenticadas em servidor TACACS (RFC 1492) e RADIUS (RFCs 2138, 2139) para gerenciamento, administração e com suporte de envio de logs para servidor Syslog objetivando os processos de auditoria.

5.17.2.4. Ser gerenciável via SSHv2 (Secure Shell) e console (porta serial RS232C).

5.17.2.5. Suportar controle de acesso administrativo ao equipamento de acordo com a arquitetura AAA (Authentication, Authorization, Accounting), sendo possível especificar os grupos de comando de configuração permitidos a cada grupo de usuários.

5.17.2.6. Suportar os protocolos de alta disponibilidade HSRP - Hot-Standby Routing Protocol (RFC 2281) ou VRRP - Virtual Routing Redundancy Protocol (RCF 5578).

5.17.2.7. Suportar o protocolo de convergência BFD (5881).

5.17.2.8. Suportar configuração de NAT - Network Address Translation (RFC1631).

5.17.2.9. Sistema operacional, na versão mais recente disponível, para as funções de roteamento, serviços IP e gerenciamento.

5.17.3. Possuir conexão on-board para console, de 115,2 Kbps, com interface padrão RJ-45, possibilitando acesso direto via microcomputador.

5.17.4. Suportar os protocolos de roteamento dinâmico OSPF (RFCs 1247, 2583, 2178 e 2328), RIP V1 e V2 (RFCs 2453), BGP, ISIS (RFC 1142) e PIM Sparse Mode (RFC 2362) e rotas estáticas.

5.17.5. Implantar protocolo IPv4 (RFCs 791, 1918), IPV6 (RFC 2460) e os protocolos de WAN Frame- Relay (RFC 1490 e FRF 1.1) e PPP (RFC 1661), com suporte a TCP (RFC 793) e UDP (RFC 768).

5.17.6. Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento, tais como NetFlow, JFlow, NetStream, IPFIX ou similar, contemplando, no mínimo, as seguintes informações: IP de origem e destino; parâmetros “protocol type” do cabeçalho IP e portas TCP/UDP de origem e destino.

5.17.7. Suportar IP Multicast (RFC 1054) e IGMP (RFCs 1112, 2236).

5.17.8. Permitir métodos de priorização de tráfego (QoS - RFC 2212, 2475, 3140, 3248) por tipo de protocolo e por serviços da pilha TCP/IP além de Police e Traffic Shaping (RFC 2698), Weighted Fair Queueing.

5.17.9. Permitir a criação de funções de filtragem (lista de controle de acesso) com pelo menos 20 (vinte) linhas.

5.17.10. Ter o acesso remoto (dial), podendo ser desabilitado por comando.

5.17.11. Possibilita a implantação de segurança para prevenção de intrusos e vírus.

5.17.12. Disponibilizar controle das sessões telnet, com possibilidade de configuração de login para filtrar os endereços IP específicos autorizados a executar sessão telnet.

5.17.13. Implantar o protocolo de gerenciamento SNMP, empregando a MIB II, de acordo com as RFC 1157 e 1213; REPETIDO 5.4.1.7

5.17.14. Disponibilizar endereço de loopback para envio de traps SNMP ao sistema de gerenciamento.

5.17.15. Possuir alimentação elétrica de 110/220V a 60 Hz, regulada automaticamente ou por chaveamento.

5.17.16. Os roteadores da rede (backbone da CONTRATADA) e os instalados nas unidades da Rede Governo deverão ter capacidade para suportar o tráfego com banda completamente ocupada, sem exceder a 70% (setenta) de utilização de CPU e memória, por todo o período do Contrato.

5.17.17. Os roteadores da rede (backbone da CONTRATADA) e os instalados nas unidades da Rede Governo deverão ter capacidade para suportar o tráfego com banda completamente ocupada, sem exceder a 70% (setenta) de utilização de CPU e memória, por todo o período do Contrato.

5.18. DOS TIPOS DE ROTEADORES

Em função da velocidade a ser contratada para o Serviço Centralizado de Acesso à Internet deverão ser utilizados os seguintes tipos de roteadores especificado no item 1.20, conforme recomendação a seguir.

TIPO II: circuitos com velocidade de até 100Mbps.

TIPO III: circuitos com velocidade de até 210Mbps.

TIPO IV: circuitos com velocidade de até 460Mbps.

TIPO V: circuitos com velocidade de até 2Gbps.

5.19. OS REQUISITOS DE INFRAESTRUTURA

5.19.1. Os equipamentos fornecidos pela CONTRATADA deverão ser capazes de operar com a alimentação elétrica de 110V ou 220V e frequência de 60Hz.

5.19.2. A CONTRATADA será responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os

Equipamentos/recursos que forem necessários (roteadores, modems, estações de gerenciamento, meios de transmissão, cabeamento WAN, acessórios necessários, dentre outros) para o provimento dos serviços. Os Equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos.

5.19.3. A infraestrutura interna da rede da CONTRATADA (backbones, POPs, Equipamentos internos, dentre outros) deverá ser atendida por solução de alimentação e proteção elétrica de modo a manter todos os Equipamentos em operação por tempo indeterminado no caso de falta de energia.

5.19.4. A CONTRATADA será responsável pela interligação da rede entre o Distribuidor Geral (DG) de telefonia do prédio em cada um dos sítios e o local físico onde será instalado o roteador CPE para os acessos por rede cabeada.

5.19.5. Para o caso de atendimento do sítio por meio de rede não-cabeada, por exemplo, enlace de rádio frequência terrestre ou satélite, quando a implantação implique a necessidade de execução de obras civis, estas ficarão a cargo da CONTRATANTE, e deverão constar do cronograma que faz parte do Projeto Executivo. Nestes casos, a CONTRATADA apresentará relatório de visita contendo as adequações e providências necessárias para a conclusão da instalação dos circuitos.

5.20. PROJETO EXECUTIVO DO SERVIÇO DE ACESSO À INTERNET

5.20.1. O Projeto Executivo deve conter, no mínimo, as seguintes informações:

- Projeto técnico de implantação dos serviços denominado Plano de Implantação para cada um dos enlaces contratados.
- Procedimentos de instalação do ponto de acesso.
- Descrição de equipamentos e circuitos de comunicação de dados.
- Adaptações necessárias ao ambiente computacional.
- Cronograma de implantação dos serviços.
- Parâmetros de qualidade de serviço.
- Descrição dos níveis de serviço acordados.
- Topologia final de rede.
- Processo de abertura de chamados de suporte técnico e responsáveis pelo atendimento.

5.20.2. Uma vez apresentado, o projeto executivo será submetido à aprovação da equipe técnica do PRODERJ, que detectará os ajustes, se necessários. A CONTRATADA deverá corrigi-lo e reapresentá-lo em no máximo 5 (cinco) dias corridos.

6. SERVIÇO DE GERÊNCIA DE REDE

A CONTRATADA também deverá disponibilizar o Serviço de Gerência de Rede para os Serviços de Rede MPLS e de Acesso à Internet atendendo aos seguintes requisitos:

6.1. A CONTRATADA deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, relatórios, tickets e de nível de serviço.

6.2. A Solução de Gerência da Rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente.

6.3. A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma pró-ativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço, realizando abertura, acompanhamento e fechamento de ocorrências de falhas relacionados com a indisponibilidade, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.

6.4. A abertura da ocorrência deverá ser realizada pela equipe do Serviço de Gerência de Rede da CONTRATADA, imediatamente após a constatação de defeito ou falha em qualquer circuito ou serviço que esteja em funcionamento.

6.5. Após a abertura da ocorrência, em um prazo máximo de até 40 (quarenta) minutos, o atendente responsável pela abertura da mesma, deverá entrar em contato com técnico da CONTRATANTE, após uma triagem inicial com objetivo de comunicar o evento em curso, como também obter uma confirmação do Cliente de que o problema não está sendo causado por uma falha de responsabilidade do mesmo, como falta de energia ou equipamento desligado.

6.6. A solução fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento.

6.7. 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.

6.8. Deverá ser escalável, permitindo futuras ampliações no número de elementos da rede a serem gerenciados.

6.9. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc.

6.10. Deverá permitir acesso de até 5 (cinco) usuários “logados” simultaneamente.

6.11. A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários.

6.12. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação

de clientes específicos, portanto não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plugins nos desktops dos colaboradores da CONTRATANTE.

6.13. O acesso deverá ser via web padrão HTTP e suportar a HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português.

6.14. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets, portanto não serão aceitas soluções que não possuam essa compatibilidade.

6.15. A Solução de Gerência da Rede deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única.

6.16. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari.

6.17. Deverá permitir a exportação das informações para relatórios em formatos comerciais.

6.18. A Solução de Gerência da Rede deverá fornecer, através do portal, visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

- Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações.
- Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados.
- Consumo de banda dos enlaces (entrada e saída) separados por dia e mês;
- Consumo de banda por classe de serviço, separados por dia e mês.
- Ocupação de memória e CPU dos roteadores CPE.
- Retardo dos enlaces separados por dia e mês.
- Perda de pacotes (descarte) no sentido IN e OUT em %.
- Taxa de pacotes com erros em erros por segundo.
- Latência em milissegundos.
- A Solução de Gerência da Rede deverá permitir a apresentação de indicadores que reflitam o nível de SLA (Service Level Agreement) e SLM (Service Level Management) dos serviços contratados.

- Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:
    - Enlace: designação, tecnologia e nível de serviço.
    - Roteador CPE: fabricante e modelo e configuração física (interfaces, memória, slots, dentre outros).
    - Endereçamento lógico: endereços IPs e máscaras.
- A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados.

6.19. A Solução de Gerência da Rede deverá permitir a criação de Relatórios:

- Permitir ser exportados conforme os principais métodos como: pdf, csv, pacote office.
- Relatórios de desempenho sumarizados por período específicos.
- Relatórios de desempenho classificados em uma visão TOP N.
    - Top Roteadores % de utilização de CPU
    - Top N Interfaces % de utilização
    - Top N Interfaces com descartes
    - Top N Interfaces com eventos de Latência
- Relatórios de disponibilidade com períodos específicos.
- Dashboards relacionando falhas, desempenho e disponibilidade.
- Dashboards executivos com visão sumarizada de indicadores operacionais (Pro atividade, Taxa de Reincidência, Reparos no Prazo e Taxa de Falha).

6.20. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados.

6.21. A Solução de Gerência da Rede deverá armazenar os dados por um período de 6 (seis) meses.

7. SERVIÇO DE BACKBONE ANTI-DDOS

7.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (DoS – Denial of Service) e DDOS Distributed Denial of Service).

7.2. A análise deverá ser passiva sem utilização de elementos probes para coleta dos dados a serem analisados.

7.3. A Solução deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não.

7.4. O ataque deve ser mitigado na estrutura da CONTRATADA, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelos Órgãos do Governo do estado do Rio continuem disponíveis aos seus usuários.

7.5. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis.

7.6. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo trafego restante não deverá sofrer nenhuma forma de limpeza ou desvio.

7.7. A solução deverá possuir interface de gerência e operação via WEB em cima de SSL, a interação entre os elementos de limpeza e detecção será feita através desta interface, assim como as configurações de limpeza, análise e os alertas de ataques.

7.8. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.

7.9. Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela CONTRATADA.

7.10. A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico.

7.11. Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE.

7.12. Para a mitigação dos ataques não deverá ser encaminhado o tráfego para limpeza fora do território brasileiro.

7.13. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

7.14. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.

7.15. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATANTE.

7.16. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP.

7.17. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

7.17.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP.

7.17.2. Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.

7.17.3. Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

7.17.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing).

7.18. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da CONTRATADA.

7.19. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole.

7.20. Realizar a comunicação da ocorrência do ataque ao órgão do Governo CONTRATANTE imediatamente após a detecção.

7.21. Disponibilizar relatórios mensais de mitigação de ataques.

7.22. Disponibilizar um Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

7.23. A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra ataques DDOS (Distributed Denial of Service).

7.24. A proteção deverá operar sem exigir o desligamento de qualquer outro circuito de acesso do Órgão, independente de quantos ou quais sejam os demais fornecedores.

7.25. A CONTRATADA deverá disponibilizar acesso a sistema de monitoramento que permita a visualização do tráfego, emissão de relatórios, visualização de alertas e informações da conta associada aos serviços de proteção.

7.26. O serviço deve ter a capacidade de mitigar ataques no perímetro Internacional, em pelo menos dois pontos distintos e na borda Nacional.

7.27. Uma vez que o ataque é detectado pela solução, o equipamento instalado no backbone da operadora, responsável pela mitigação do trafego de ataque, deverá ser alertado e então todo o trafego do cliente deverá ser direcionado imediatamente, sem impactos e/ou interrupção do serviço.

7.28. Conforme os prazos definidos no acordo de nível de serviços a CONTRATADA deverá entrar em contato com o PRODERJ e solicitar autorização para dar início à mitigação do tráfego.

7.29. Caso a CONTRATADA por qualquer razão não consiga contato com o responsável pela área de TIC do PRODERJ, esta poderá tomar as ações de mitigação do ataque que julgar necessárias, comunicando assim que possível a CONTRATANTE.

8. CIRCUITOS TEMPORÁRIOS DE ACESSO À INTERNET

O serviço refere-se ao fornecimento pela CONTRATADA de serviços temporários de acesso à Internet com velocidades variando de 5Mbps, 10Mbps e 100Mbps, tanto para eventos como para outras necessidades transitórias, que possam surgir no decorrer do contrato através de solicitação por demanda exclusiva do PRODERJ para atendimento ao Governo do Estado.

A CONSTRATADA deverá atender as solicitações do PRODERJ sobre demanda para estes itens.

8.1. A CONTRATADA poderá prover os referidos links através de meio físicos e tecnologias que disponham para atender a conexão internet.

8.2. Dentre as tecnologias a serem utilizadas para o provimento do circuito temporário poderá ser considerada eventualmente a utilização de serviço de banda larga, como ADSL na inviabilidade do atendimento temporário através de conexões à internet com banda garantida e IP fixo.

8.3. O cálculo para faturamento atenderá à seguinte regra: 5% do valor do serviço em Contrato, multiplicado pelo número de dias, nunca inferior a 5 (cinco) ou superior a 30 (trinta), não podendo ultrapassar o valor nominal do serviço. Nesses valores estarão inclusos a assinatura e a instalação.

8.4. São estimadas em cerca de 50 (cinquenta) as demandas anuais de circuitos temporários.

9. SERVIÇO WIFI INDOOR

Este serviço tem como objetivo permitir a disponibilização de Acesso Wifi Indoor à Internet pelas Instituições do Governo do Rio à população em seus ambientes de atendimento à população, podendo também ser utilizado pelo Órgão no exercício de suas atividades para prestação de serviços à população do estado.

A solução a ser disponibilizada pela CONTRATADA deverá ser completa, compreendendo a

disponibilização dos Acess Point (AP) como Hotspot, Gerenciamento do serviço e Acesso à Internet, como também a instalação, configuração e manutenção dos equipamentos.

9.1. Características do Serviço

O serviço disponibilizado pela CONTRATADA deverá atender as seguintes características:

9.1.1. A Solução Wifi deverá ser fornecida através de uma plataforma em nuvem, como serviço WaaS (Wifi as a Service).

9.1.2. A solução disponibilizada pela CONTRATADA deverá provê os seguintes itens:

- Portal de Autenticação dos usuários.
- Gerenciamento dos acessos dos usuários.
- Monitoramento da Rede

9.1.3. Disponibilização de plataforma WEB (portal Administrativo) para customização do portal de autenticação dos usuários e gestão da solução pelo Órgão do governo do estado.

9.1.4. A solução disponibilizada pela CONTRATADA deverá atender ao Marco Regulatório da Internet.

9.1.5. A CONTRATADA deverá provê a instalação e configuração dos APs na modalidade de aluguel nas unidades do Governo do estado. Será de responsabilidade da CONTRATANTE o ponto de rede para conexão dos equipamentos como também de energia elétrica.

9.1.6. Solução escalável permitindo a ampliação do número de APs, conforme a necessidade do Governo do Estado.

9.1.7. A Solução deverá permitir por AP a conexão de até 40 usuários simultâneos e cobertura de até 100m2 de área livre.

9.1.8. O AP a ser fornecido pela CONTRATADA deverá atender aos seguintes requisitos mínimos:

9.1.8.1. Fornecimento de Ponto de Acesso WiFi Interno, novo e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta.

9.1.8.2. Deve ser homologado pela ANATEL;

9.1.8.3. Deve ser capaz de operar simultaneamente nos padrões 802.11a/n/ac e 802.11b/g/n, através de rádios independentes (Dual Radio AP);

9.1.8.4. Deve ser um equipamento ponto de acesso WiFi para rede local sem fio de uso interno, sem antenas aparentes, que atenda os padrões IEEE 802.11b/g/n na faixa de 2.4GHz e 802.11a/n/ac na faixa de 5GHz simultaneamente com configuração via software. O equipamento deve ter

capacidade de análise espectral.

9.1.8.5. Possuir funcionamento em modo autônomo sem a necessidade de controlador. Neste modo, permitir configuração e funcionamento do ponto de acesso sem a necessidade do controlador.

9.1.8.6. Possuir funcionamento em modo gerenciado por Controlador WiFi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF.

9.1.8.7. Deverá estar logicamente conectado a um Controlador WiFi, inclusive via roteamento da camada de rede OSI, através de rede pública ou privada.

9.1.8.8. Deve implementar cliente DHCP, para configuração automática de rede;

9.1.8.9. Possuir mecanismo de funcionamento para trabalhar com Controladores WiFi em redundância (principal e redundante).

9.1.8.10. Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) WiFi - operação em modo de “chaveamento de tráfego local”.

9.1.8.11. Operando no modo de “chaveamento de tráfego local”, o controlador WiFi e os pontos de acesso devem:

9.1.8.11.1. O modo de operação de chaveamaneto de trafego local deve prever que se a comunicação entre o ponto de acesso WiFi e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WAN, LAN ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi deve continuar operando e permitindo que os usuários já autenticados na rede e associados aos pontos de acesso continuem a possuir acesso à rede. Deve permitir que os usuarios efetuem roaming entre os pontos de acesso do mesmo site nesta situação.

9.1.8.11.2. Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi em modo de chavemaento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que novos usuários se autentiquem de acordo com 802.1x e se associem à rede sem qualquer prejuízo de acesso aos mesmos.

9.1.8.11.3. Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es)

WiFi, o ponto de acesso WiFi em modo de chavemaento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que os usuarios efetuem fastroaming sem qualquer prejuízo de acesso aos mesmos.

9.1.8.11.4. A solução proposta deve prever o atendimento dos itens anteriores, e alternativamente a CONTRATADA poderá fornecer uma solução de redundância e autenticação para pontos de acesso operando com “chaveamento de tráfego local”, para cada site. Referenciar-se aos itens “Controlador WiFi” e deve ser fornecida com no mínimo 25 pontos de acesso e também com base de usuários de no mínimo 100 usuários. Os custos adicionais deverão ser inseridos no item controlador de redes.

9.1.8.12. Deve permitir a operação de usuários configurados nos padrões IEEE 802.11b/g/n e 802.11a/n/ac simultaneamente.

9.1.8.13. Atender os seguintes requisitos em 802.11n (faixas de 2.4GHz e 5GHz) e 802.11ac (faixas de 5GHz): 3x3 multiple-input multiple-output (MIMO).

9.1.8.14. Operar em Canais de 20MHz para 2,4GHz e possibilitar channel bounding, canal de 40 MHz para 5GHz e canais de 80MHz para 5GHz.

9.1.8.15. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps.

9.1.8.16. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11n: MSC0 – MCS15 (6.5Mbps - 300Mbps).

9.1.8.17. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11ac: MSC0 – MCS9 para 1 e 2 Spatial Streams (6.5Mbps – 886,7 Mbps).

9.1.8.18. Possuir capacidade de selecionar automaticamente o canal de transmissão em 2.4GHz e em 5GHz criando um plano de distribuição de canais entre os pontos de acesso para melhor uso do espectro de rádio frequência.

9.1.8.19. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

9.1.8.20. Implementar o protocolo de enlace CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão.

9.1.8.21. Operar nas modulações DSSS e OFDM.

9.1.8.22. Possuir suporte a pelo menos 16 SSIDs.

9.1.8.23. Possuir suporte a pelo menos 16 Vlans.

9.1.8.24. Permitir habilitar e desabilitar a divulgação do SSID.

9.1.8.25. Possuir padrão WMM (Wi-Fi Multimedia) para priorização de tráfego.

9.1.8.26. Não deve haver licença restringindo o número de usuários por ponto de acesso. O Ponto de Acesso deve permitir, no mínimo, 128 usuários por rádio.

9.1.8.27. O Ponto de acesso deve permitir configuração de base de usuários local para utilização com protocólo 802.1X, com no mínimo 100 usuários.

9.1.8.28. Possuir potência máxima de transmissão de, no mínimo, 20 dBm para IEEE 802.11a/b/g/n/ac.

9.1.8.29. Possuir antenas compatíveis com as freqüências de radio dos padrões 2.4GHz e 5GHz com ganho de, pelo menos 4 dBi, com padrão de irradiação omnidirecional.

9.1.8.30. Possuir, no mínimo, um valor maximo de transmissão maior ou igual a 22 dBm com todas as antenas habilitadas.

9.1.8.31. Deve possuir sensibilidade de recepção de valor menor ou igual:

9.1.8.31.1. -92dBm em 802.11a a 6Mbps;

9.1.8.31.2. -92dBm em 802.11b a 5.5Mbps;

9.1.8.31.3. -92dBm em 802.11g a 6Mbps;

9.1.8.31.4. -92dBm em 802.11n (HT20) a MC0 em 2.4GHz;

9.1.8.31.5. -92dBm em 802.11n (HT20) a MC0 em 5GHz.

9.1.8.31.6. -86dBm em 802.11ac a 6Mbps.

9.1.8.32. Possuir, no mínimo, uma interface IEEE 802.3 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX, com conectores RJ-45, para conexão à rede local fixa.

9.1.8.33. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).

9.1.8.34. Possuir no mínimo 01 LED indicativo do estado de operação;

9.1.8.35. Deve possuir uma trava de segurança compatível à utilizada em desktops e notebooks (Kensington security lock) e que permita a instalação de um cabo de segurança com a finalidade de evitar o furto do equipamento.

9.1.8.36. Deve implementar um mecanismo de controle de associação de banda,

de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN.

9.1.8.37. Implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso.

9.1.8.38. Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN. Deve perimitir esta formação de banda para cliente 802.11a/b/g/n/ac.

9.1.8.39. Deve possuir mecanismo de otimização de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast. Este mecanismo deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes mesmo que esta velocidade não seja o “rate” mandatório.

9.1.8.40. Possibilitar a alimentação via padrão PoE (IEEE 802.3af) utilizando apenas uma porta do switch onde estiver conectado.

9.1.8.41. Possuir estrutura metálica que permita fixação do equipamento em teto e também em parede, devem ser fornecidos os acessórios para que possa ser feita a fixação.

9.1.8.42. Deve ser entregue com todos os acessórios necessários para operacionalização do equipamento, tais como: kits de instalação, softwares, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.

9.1.8.43. Possuir varredura de RF nas bandas 802.11 b/g/n e 802.11 a/n/ac para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado no ponto de acesso sem impacto no seu desempenho.

9.1.8.44. Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:

9.1.8.44.1. EAP-Transport Layer Security (EAP-TLS);

9.1.8.44.2. EAP-TTLS/MSCHAPv2;

9.1.8.44.3. PEAPv0/EAP-MSCHAPv2;

9.1.8.44.4. PEAPv1/EAP-GTC;

9.1.8.44.5. EAP Subscriber Identity Module (EAP-SIM).

9.1.8.45. Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;

9.1.8.46. Possuir criptografia do tráfego local.

9.1.8.46.1. Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;

9.1.8.46.2. Implementar WEP (Wired Equivalent Privacy), chaves de 40 bits e 128 bits;

9.1.8.46.3. Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check-MIC).

9.1.8.46.4. Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES, 128 bits);

9.1.8.47. Deve possuir 802.1X Suplicant de maneira que posso ser capaz de fornecer credenciais ao se conectar a rede cabeada.

9.1.8.48. Deve ser capaz de atender os usuários e realizar a função de “mesh indoor” ou modo “repetidor” de forma simultânea.

9.1.8.49. Deve possuir hardware dedicado para a análise de espectro (ASIC) dedicado para esta função localizado dentro do ponto de acesso.

9.1.8.50. O equipamento deverá suportar a realização de monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências WiFi e Interferências Não-WiFi.

9.1.8.51. Quando em operação de monitoração de espectro, as funções de monitoração real-time em Rádio Frequência (análise espectral) devem ser realizadas via hardware, com chipset (ASIC) dedicado para esta função localizado dentro do ponto de acesso.

9.1.8.52. Quando em operação de monitoração de espectro,, dever detectar e gerar alarmes de interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar, classificar, identificar e localizar em mapa com certa precisão além de gerar alarmes de interferências não-WiFi, tais como Bluetooth, telefones sem fio, câmeras de video sem fio, Microondas e outros

9.1.8.53. Quando em operação de monitoração de espectro, deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente.

9.1.8.54. Suportar operar nos seguintes modos: “Modo Local”, “Modo Monitor” e “Modo Analisador de Espectro”.

9.1.8.55. Operando em “Modo Local” o ponto de acesso deve fornecer informações ao Controlador WiFi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi. Deverá fazer tanto a transmissão de dados WiFi quanto a análise de espectro simultaneamente.

9.1.8.56. Operando em “Modo Monitor” deverá fornecer informações ao Controlador WiFi referente à qualidade do espectro de RF para todos os canais monitorados identificando equipamentos interferentes na rede WiFi e rogue APs.

9.1.8.57. Operando em “Modo Analisador de Espectro” deverá operar de forma exclusiva apenas para monitorar o espectro de RF de forma a fornecer informações para um software analisador de espectro ou para o software de gerenciamento WiFi em todos os canais de 2.4GHz e 5GHz UNII1, UNII2, UNII2 Ext e UNII3 simultâneamente. Se o equipamento não analisar todo o espectro simultâneamente com um único ponto de acesso em modo monitor, será aceita a quantidade necessária de pontos de acesso para análise espectral dos canais de todas as frequências acima descritas de forma simultânea. Este quantitativo será necessário para cada ponto de acesso monitor inserido na rede e os custos totais devem ser adicionados no ítem.

9.1.8.58. Ser fornecido com fonte de alimentação com ajuste automático de tensão 110 e 220 volts e freqüência de 60 Hz.

9.1.8.59. Deve possuir consumo de energia igual ou inferior a 15 Watts.

9.1.8.60. O equipamento ponto de acesso deve ser homologado pela ANATEL.

9.1.8.61. Deve permitir a conexão de usuários em IPv4, IPv6 e Dual-stack.

9.1.8.62. O equipamento deve ser capaz de implementar 802.11 dynamic frequency selection (DFS).

9.1.8.63. Deve possuir suporte à 802.11 Cyclic Shift Diversity (CSD).

9.1.8.64. Deve implementar Maximal Ratio Combining (MRC).

9.2. Funcionalidades do Serviço

A Plataforma de prestação do serviço por parte da CONTRATADA deverá possuir as seguintes funcionalidades.

9.2.1. Captive Portal com opção de cadastramento do usuário ou login social (Facebook).

9.2.2. Plataforma WEB onde o CONTRATANTE poderá customizar seu Captive Portal.

9.2.3. Armazenamento dos logs de acesso e cadastro dos usuários em Datacenter, conforme exigência do Marco Civil da Internet.

9.2.4. Conformidade com as leis de interceptação legal e rastreabilidade de usuários.

9.2.5. Interface simples e intuitiva para gerenciamento das principais funcionalidades do serviço pela e extração de relatórios de utilização e cadastro dos usuários.

9.2.6. Possibilidade de configuração através o portal Adminstrativo CONTRATANTE da limitação do tempo de acesso do usuário e tempo de bloqueio (tempo no qual o usuário deverá aguardar para voltar novamente à utilizar o serviço).

9.2.7. Possibilitar a utilização de mais de um até 4 SSIDs.

9.3. Composição do Serviço

A CONTRATADA deverá também disponibilizar o serviço conforme a composição do serviço descriminada na tabela abaixo:

Itens	Qtde APs	Cobertura	Composição
OPÇÃO I	1	Até 40 usuários simultâneos e 100m^2 de área livre por site	Um (1) AP conforme especificação do item 11.1.8
OPÇÃO II	2	Até 80 usuários simultâneos e 200m^2 de área livre por site	Dois (2) APs conforme especificação do item 11.1.8 e switch POE para interligação dos APs

9.4. Conexão à Internet

A CONTRATADA deverá também disponibilizar conexão à Internet conjuntamente a solução Wifi atendendo aos seguintes requisitos.

1.1.1. Possuir pelo menos 4 (quatro) IPV4 fixos.

1.1.2. As conexões de acesso a Internet para este serviço poderão ser fornecidas por circuitos IP de características simétricas ou assimétricas conforme explicitado na tabela de formação de preços deste edital.

1.1.3. O valor do serviço Wifi deverá ser composto pelo tipo de AP mais o da conexão à Internet.

9.5. Responsabilidades da CONTRATANTE.

1.1.4. O Órgão CONTRATANTE deverá permitir o acesso às áreas técnicas do local da instalação e durante a execução das atividades, com acompanhamento técnico de um profissional que conheça a infraestrutura do local.

1.1.5. O CONTRATANTE deverá ser disponibilizar toda a infraestrutura de dados (cabeamento UTP para interligar os equipamentos) e elétrica para alimentação dos equipamentos no Rack.

1.1.6. Considerando que os pontos de acesso serão fixados em parede, forro ou teto w 'necessário, por qualquer obra civil e acabamentos, como abertura e fechamento do gesso, pintura e recomposição de pisos e paredes.

1.1.7. Infraestrutura de ar condicionado, espaço físico, dentre outros aspectos ligados à infraestrutura necessária para a realização dos serviços são de responsabilidade do CONTRATANTE.

1.1.8. Será de responsabilidade da CONTRANTE a remoção de qualquer solução wireless existente no local, caso prejudique o serviço à disponibilização do serviço.

1.2. Suporte Técnico

A CONTRATADA deverá disponibilizar atendimento de suporte conforme descrito a seguir:

1.2.1. Disponibilização de Central 0800 para prestação de atendimento na modalidade 24x7 (24horas x 7 dias na semana) ao usuário designado pela CONTRANTE como responsável pelo AP (Hotspot).

1.2.2. O atendimento deverá e esclarecer, solucionar e registrar dúvidas e problemas em relação ao serviço disponibilizado pela CONTRATADA.

1.2.3. Suporte de tratamento de falhas em regime 24x7 envolvendo os procedimentos remotos de troubleshooting para possível correção de falhas e o acionamento de equipe de campo para correção do problema localmente.

1.2.4. Disponibilização de número 0800 para reclamações referentes ao acesso à Internet em regime 24x7.

2. SERVIÇO DE VIDEOCONFERÊNCIA

Este serviço consiste na disponibilização por parte da CONTRATADA de Salas Virtuais de Videoconferência Multiponto e colaboração em nuvem com acesso à multidispositivos.

Sala virtual de videoconferência Multiponto: sessão que reúne remotamente diversos usuários em uma mesma conferência, onde há o compartilhamento de vídeo, áudio, documentos e demais formas de dados.

2.1. O serviço deverá permitir, criar e gerenciar a qualquer hora pela web Sala Virtual de Vídeoconferência sem a necessidade de reserva de recursos.

2.2. A CONTRATADA deverá prover, na modalidade de Software como Serviço (SaaS – Software as a Service), licenças de acesso ao Sistema de Videoconferência, como também suportar e garantir os serviços de implantação, operação, manutenção, suporte técnico e treinamento aos usuários do sistema.

2.3. A CONTRATADA deverá também disponibilizar em regime de locação os Terminais de Vídeo conferência para montagem de salas físicas presencias de videoconferência pelos Órgãos do Governo CONTRATANTE.

2.4. Serviço ofertado deverá ser escalável, atendendo as necessidades de Videoconferência, conforme a demanda dos Órgãos do Governo.

2.5. O Serviço ofertado pela CONTRATADA deverá possibilitar os usuários ingressarem em Vídeo Conferência através da Rede Privada do Órgão, como também através da Rede Pública Internet.

2.6. O Serviço ofertado pela CONTRATADA deverá possibilitar os usuários ingressarem em Videoconferência através de dispositivos fixos e móveis: terminais de vídeo conferência (endpoints), smartphones e tablets (Android e IOS), desktops e notebooks (Windows).

2.7. O Sistema deverá permitir a categorização de perfil de usuários conforme definição abaixo:

2.7.1. Perfil de usuário com permissão de criação e gerenciamento da sessão de Videoconferência Virtual e pelo convite ou bloqueio de participantes remotos. Um usuário com este perfil deve ser associado a cada Licença de Sala Virtual de Videoconferência.

2.7.2. Perfil de usuário convidado a ingressar na sala virtual de videoconferência multiponto, interno ou externo à organização (cliente final).

2.8. O serviço deverá possuir as seguintes características:

- Permitir qualidade a Videoconferência em HD e SD ajustável de vídeo e dados.
- Permitir que o usuário conecte-se de forma transparente, a partir de qualquer dispositivo e de qualquer ponto da rede pública de internet.
- Permite controlar o layout de tela.
- Permite moderar a sessão e controlar os participantes.
- Interoperabilidade entre terminais multimídia (endpoints) para intercâmbio de dados;
- Ajuste de vídeo e de banda de internet automático.
- Permite o compartilhamento de tela e de conteúdo.
- Suportar conferências programadas e ad-hoc.
- Possibilitar habilitar e desabilitar a função “mudo” de áudio e habilitar e desabilitar a função exibição de vídeo na sessão de Videoconferência.
- Detecção de nível de fala para seleção da imagem a ser exibida na tela.

2.9. A Solução deverá prover acesso do usuário ao sistema de Videoconferência, através da utilização de navegador Web ou aplicativo móvel, mediante login e senha.

2.10. Deverá ser disponibilizada aplicação pela CONTRATADA que permita a inclusão de participantes nas sessões de Videoconferência, possibilitando aos usuários participarem da sessão de Videoconferência de qualquer localidade.

2.11. A solução disponibilizada deverá possuir as seguintes facilidades:

2.11.1. Compartilha tela, apresentação de arquivos e anotações.

2.11.2. Chat colaborativo.

2.11.3. Gravação da reunião no portal.

2.11.4. Plug-in para agenda do MS Outlook e Google Calendário.

2.11.5. Acesso restrito por login e senha.

2.11.6. Sala de espera antes do início da reunião.

2.11.7. Conexão de até 25 terminais de videoconferência ou telepresença por Sala Virtual de Videoconferência.

2.11.8. Conexão de até 200 participantes em webconferência e audiovisual por Sala virtual de Videoconferência

2.11.9. Segurança de criptografia.

2.12. A solução deverá permitir a utilização com de endpoints existentes do Governo do Rio, desde que seja possível a interoperação através do protocolo SIP ou H.323 com a solução ofertada pela CONTRATADA.

2.13. A CONTRATADA deverá fornecer em regime de locação ao longo do contrato 2 (dois) tipos de modelos de terminais de Videoconferência:

2.13.1. Terminal Executivo: sistema desenhado para uso pessoal e podendo se situar num ambiente de escritório (desktop). Os itens como monitor, câmera, codec e microfone poderão compor um elemento único do terminal ou podem vir separados.

2.13.2. Terminal Sala Física: terminal de Videoconferência composto de no mínimo câmera, codec, microfone e controle remoto. A câmera deverá possuir movimentações horizontal e vertical, zoom ótico, além de microfone integrado e permitindo também o uso de microfone externo.

2.13.3. A TV que será utilizada como Monitor da Videoconferência será disponibilizado pelo Órgão CONTRATANTE do Governo do Rio.

2.14. Especificação dos Tipos de Terminais (Endpoints):

2.14.1. Tipo Executivo:

- Este tipo deve ser desenhado para uso pessoal e poder situar-se sobre um ambiente de escritório (desktop).
- Os itens como monitor, câmera, codec e microfone poderão compor um elemento único do terminal ou podem vir separados. Deverá ser de fácil transporte e instalação.
- O terminal deve suportar resoluções até Full-HD 1080p a 30fps, tanto para a captura e transmissão como para a recepção de vídeo. Adicionalmente, dispor de uma ampla gama de resoluções intermediárias, tais como 360p, 448p, e 720p.
- O terminal pode dispor de um monitor de no mínimo 20 polegadas com tecnologia LCD. Isto garante o tamanho otimizado de tela para uso pessoal, aliada à menor consumo de energia e uma maior durabilidade do mesmo.
- O terminal deve ser equipado com um módulo de áudio especificamente desenhado para videoconferência estéreo. O desenho deve estar perfeitamente integrado à solução compacta.
- O microfone deve estar integrado dentro do equipamento.
- O sistema deve suportar os sinais de banda larga Hi-Fi totalmente compatível às normas, preferencialmente até 20khz, se bem não menor a 14khz em protocolo ITU normatizado:
  - G.711
  - G.728
  - G.722
  - G.722.1
  - AAC-LD
- O sistema deve suportar a transmissão simultânea de dois fluxos de vídeo que sejam de qualquer origem (Vídeo ou HDMI) em comunicações ponto-a-ponto e em sessões de multiponto através do protocolo BFCP.
- O sistema deve suportar a transmissão do conteúdo compartilhado na resolução Full HD (1920 x 1080 pixels).
- O sistema deve permitir a conexão de uma segunda fonte externa de vídeo mediante conexão HDMI para a apresentação e compartilhamento da mesma na segunda fonte de vídeo.
- A compatibilidade da transcodificação e velocidade devem receber suporte em uma sessão de múltiplas redes.

- O sistema deve suportar a criptografia integrada AES ou outro algoritmo de criptografia padrão de 128 bits através da rede IP. A criptografia deve receber suporte em qualquer tipo de sessão, incluídas as sessões de transmissão dual e sessões em multiponto.

- O sistema deve suportar o protocolo de vídeo H.263 e H.264 durante qualquer tipo de sessão, seja de transmissão dual (BFCP) ou de sessões multiponto.

- O sistema deve suportar transmissões duais apresentadas simultaneamente em um único monitor.

- O sistema pode ser operado pelo usuário através de painel de vidro sensível ao toque, do mesmo fabricante do terminal de videoconferência, com display mínimo de 10 polegadas.

- O sistema deve suportar tanto o IPv4 e IPV6, e a conexão física com a rede deve ocorrer sobre interface 10/100/1000 Mbps.

- O sistema deve suportar um algoritmo que previna a perda de um grupo de bits em IP. O algoritmo deve estar conforme a norma e funcionar em todos os terminais de fabricantes distintos.

- Para assegurar a mais alta fidelidade, o sistema deve basear-se em uma plataforma de hardware e software desenhada para videoconferência, não sendo aceitas soluções baseadas em PC.

- A conexão entre o PC e o equipamento será de forma direta, sem nenhum elemento intermediário que a faça possível.

- O sistema deve utilizar SIP como protocolo para registro e controle de funcionalidades. Deverá suportar nativamente a discagem através de SIP URI, com caracteres alfanuméricos e domínios externos.

- O software do sistema deve suportar até cerca de 20% de perda de pacotes sem que se degrade a imagem ou se perceba algum tipo de pixelamento ou redução da resolução. Esta funcionalidade é importante para conexões de equipamentos situados fora da LAN.

- O sistema deve ter conectividade para fone convencional com microfone, a fim de possibilitar a privacidade na comunicação.

- A interface do usuário deverá estar disponível em Português do Brasil.

- O sistema deve suportar mecanismos nativos conexões seguras através de firewalls, permitindo ao usuário manter a criptografia e privacidade mesmo que externamente à rede dos demais equipamentos.

2.14.2. Tipo Sala Física:

Terminal de videoconferência que suporte e possua no mínimo, as seguintes funcionalidades e características técnicas:

- Ser composto de, no mínimo, câmera, codec, microfone e controle remoto.
- Todos os componentes acima devem ser preferencialmente do mesmo fabricante. Caso não sejam, devem ter totalmente compatíveis entre sim e permitir a utilização de todas as funcionalidades solicitadas.
- Possuir câmera com as seguintes características:
  - Movimentação horizontal: -30 a +30 graus.
  - Movimentação vertical: -25 a +5 graus.
  - Campo de visão horizontal: 83 graus.
  - Campo de visão vertical: 51.5 graus.
  - Zoom ótico e digital de no mínimo 5X.
  - Resolução de 1080p30 – 1920x1080 com 30 quadros por segundo.
  - Possuir ajuste de foco automático.
  - Possuir controle de branco manual e automático.
- Possuir microfone integrado e suportar microfone externo omini direcional, com captação de 360 graus.
- Possuir cancelamento de eco.
- Possuir Controle Automático de Ganho (AGC).
- O codec deverá ser entregue em formato de appliance físico, dedicado a processamento de vídeo, não sendo aceitas soluções baseadas em PC ou servidores de aplicação geral.
- Disponibilizar, no mínimo, uma (01) porta ethernet 10/100, com conector RJ-45, e aderente aos padrões IEEE 802.3 e 802.3u, para conexão a rede LAN.
- Suportar alimentação através de Power over Ethernet (PoE)
- Possuir fonte de alimentação operando automaticamente em 100 a 240V e 50 e 60 Hz.
- Ser compatível com o protocolo SIP.
- Permitir velocidade de comunicação ponto a ponto a partir de 384 Kbps

até no mínimo 3 Mbps.

- Permitir a utilização de dual-stack IPv4 e IPv6.
- Suportar DHCP (para aquisição automática de endereço IP).
- Suportar DNS (resolução de endereços IP em nomes/URLs).
- Suportar SSH (acesso remoto seguro via terminal).
- Suportar HTTP/HTTPS (acesso remoto seguro via browser).
- Transmissão de duas fontes independentes de vídeo (dual stream), utilizando o padrão BFCP (SIP), com resolução de até WXGA. A visualização de ambos os vídeos deverá ser possível através de um único monitor.
- Permitir a utilização de solução de travessia de firewall.
- Padrões de vídeo: H.264, H.263+ e H.263.
- Resoluções de vídeo: 1080p (1920x1080), 720p (1280x720), 4CIF (704x576), CIF (352x288) e QCIF (176x144).
- Padrões de áudio: G.711, G.722, G.722.1 e AAC-LD, ou outro protocolo similar que opere na faixa de frequência de 20KHz ou superior.
- Operação por controle remoto sem fios.
- Criptografia de mídia.
- Padrão Advanced Encryption Standard (AES).
- Geração e Troca automática de chaves de criptografia.
- Criptografia em dual stream.
- Gerenciamento remoto seguro através de HTTPS e SSH.
- Mecanismo de ajuste de banda inteligente.
- Permitir visualização de estatísticas de desempenho da chamada em curso.
- Possuir funções de diagnóstico.
- Definição de data e Hora utilizando NTP.
- Discagem por URL.
- Permitir a implementação de qualidade de serviço (QoS) utilizando Differentiated Services.
- Possuir, no mínimo, duas (02) entradas de vídeo, com as seguintes

características, caso a câmera não seja integrada ao terminal de videoconferência.

- Uma (01) entrada HDMI ou DVI ou Vídeo Componente, operando com resolução 1080p, para conexão com a câmera principal.
- Uma (01) entrada HDMI ou VGA para compartilhamento de conteúdo.

- Possuir, no mínimo, uma (01) entrada de vídeo, com as seguintes características, caso a câmera seja integrada ao terminal de videoconferência.
  - Uma (01) entrada HDMI ou VGA para compartilhamento de conteúdo.
- Possuir uma (01) saída de vídeo, com a seguinte característica: Uma (01) saída HDMI ou equivalente, operando com resolução 1080p, para conexão com o monitor principal.
- Possuir três (03) entradas de áudio, com as seguintes características:
  - Uma (01) entrada para o microfone integrado.
  - Uma (01) entrada para microfone de mesa opcional.
  - Uma (01) entrada HDMI audio-in.
- Possuir duas (02) saídas de áudio, com as seguintes características:
  - Uma (01) saída HDMI ou equivalente para o áudio principal.
  - Uma (01) saída analógica RCA mini plug 3.5mm.

3. SERVIÇO DE OPERAÇÃO ASSISTIDA DE SERVIÇOS ESPECILALIZADOS

3.1. Operação Assistida

Este documento descreve o módulo de Gestão de Operação Assistida de Serviços Especializados referente a arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

O objeto desta contratação visa adquirir mão de obra especializada para os serviços da CONTRATANTE mediante a abertura de Ordem de Serviço pelo fiscal do contrato.

3.2. Contextualização do serviço de operação assistida

A Operação Assistida é composta por um conjunto de atividades que permitam o treinamento e capacitação da equipe (equipes de sustentação) da CONTRATANTE responsável pelas atividades de Telecomunicações, Tecnologia da Informação e Comunicação, Segurança da Informação e Segurança Cibernética, transferindo todo o Qualificação Técnica e experiência necessária para a operação dos produtos

(equipamentos, sistemas ou plataformas de serviços).

Durante um período previamente acordado, é prestado todo o suporte necessário para a operacionalidade das atividades citadas acima, auxiliando os tomadores de decisões a fazer escolhas conscientes, priorizando ações e distinguindo entre formas alternativas de ações, até que a CONTRATANTE possa assumir as atividades com sua própria equipe.

A CONTRATADA deverá prover mão de obra especializada para os serviços especializados em Tecnologia da Informação e Comunicação, Segurança da Informação, Segurança Cibernética e Telecomunicações que possam surgir durante a execução do projeto, por se tratar de serviços complexo, a aquisição se faz necessária.

3.3. SERVIÇOS ESPECIALIZADOS E PROFISSIONAIS DA CONTRATADA

A CONTRATADA deverá encaminhar os currículos da sua equipe técnica ao CONTRATANTE, para avaliação quanto ao atendimento das exigências referentes à especialização dos perfis profissionais, com as seguintes informações:

Identificação:

Nome:
Data de nascimento:
RG:
CPF:
Endereço p/ contato:
Telefone p/ contato:
e-mail:

Perfil de atuação:

Área de atuação:
Experiência (tempo expresso em anos):

Formação escolar:

Descrever a formação escolar e incluir cópia do certificado de conclusão do grau escolar estabelecido para o perfil do profissional.

Cursos de Especialização:

Descrever todos os cursos vinculados à área de atuação, devidamente comprovados conforme exigido neste Termo de Referência e no Edital.

Experiência Profissional (Atividades desenvolvidas):

Descrever as experiências adquiridas com as informações de empresa (local), ano e atividades desenvolvidas e comprovadas conforme exigências definidas neste Termo de Referência e no Edital.

Os profissionais alocados pela CONTRATADA para a execução dos serviços de Administrador de Redes de Telecomunicações devem apresentar o perfil mínimo relacionado abaixo:

- Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas.
- Conhecimento e experiência comprovada de no mínimo 05 (cinco) anos na área de administração de redes de telecomunicações;
- Conhecimento e experiência nas Normas brasileiras ABNT NBR 16415:2015 - Caminhos e espaços para cabeamento estruturado e ABNT NBR 14565:2013 - Cabeamento estruturado para edifícios comerciais e data centers de cabeamento estruturado
- Conhecimento e experiência em implementação de Controles de segurança da informação de Redes de Telecomunicações
- Conhecimento e experiência em administração de roteadores Cisco IOS (originalmente Internetwork Operating System)
- Conhecimento e experiência em arquitetura de rede segura
- Conhecimento de protocolos típicos de inter-redes (Frame Relay, X25, ATM, etc.).
-

Os profissionais alocados pela CONTRATADA para a execução dos serviços de Sistemas Operacionais Microsoft/Linux/Unix devem apresentar o perfil mínimo relacionado abaixo:

- Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas.
- Conhecimento e experiência comprovada de no mínimo 05 (cinco) anos na área de Sistemas Operacionais Microsoft/Linux/Unix.
- Conhecimento e experiência em Hardening em Servidores Linux.
- Conhecimento e experiência em Hardening em Servidores Microsoft.
- Conhecimento e experiência em Hardening em Servidores Unix.
- Conhecimento e experiência em implementação de controles em Sistemas Operacionais.
- Conhecimento e experiência em Administração de Virtualizador Microsoft e linux e configurações de máquinas virtuais.

Os profissionais alocados pela CONTRATADA para a execução dos serviços de Administrador de Banco de Dados devem apresentar o perfil mínimo relacionado abaixo:

- Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas.
- Conhecimento e experiência comprovada de no mínimo 05 (cinco) anos na área de administração de Banco de Dados
- Conhecimento e experiência em criar, administrar, monitorar e garantir a recuperabilidade dos Banco de Dados.
- Conhecimento e experiência pela segurança, disponibilidade dos dados, manutenção, instalação, configuração, atualização, testes e monitoramento de um banco de dados ou sistemas de bancos de Dados.
- Conhecimento e experiência em Manutenção e refinamento de bancos de dados, alterações na estrutura do banco para expansão e adaptações de sistemas, monitoramento e identificação de falhas para aperfeiçoamento de bancos de dados, e coordenação de programadores.
- Conhecimento e experiência em Recursos de desempenho e portabilidade (INDEX,TRIGGERS, PACKAGES, PROCEDURES), migração de plataformas, análise de desempenho de sistemas e tratamento de informação para tomada de decisão (Data Warehouse e outros).
-

Os profissionais alocados pela CONTRATADA para a execução dos serviços de Segurança da Informação devem apresentar o perfil mínimo relacionado abaixo:

- Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas.
- Conhecimento e experiência comprovada de no mínimo 05 (cinco) anos na área de administração de Segurança da Informação.
- Conhecimento e experiência comprovada em Gestão de Segurança da Informação em conformidade com as Normas brasileiras ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos e a ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e na ABNT NBR ISO/IEC 27011:2009 - Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.
- Conhecimento e experiência comprovada em Gestão de Riscos em conformidade com a Norma ABNT NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes.
- Conhecimento e experiência comprovada em Gestão de Continuidade de Negócios em conformidade com a ABNT NBR ISO 22301:2013 - Segurança da

sociedade — Sistema de gestão de continuidade de negócios — Requisitos.

- Conhecimento e experiência comprovada em Governança de Tecnologia da Informação e Comunicação em conformidade com as diretrizes da ABNT NBR ISO/IEC 38500:2009 - Governança corporativa de tecnologia da informação e com o Control Objectives for Information and Related Technology (Cobit) versão 5.
- Conhecimento e experiência comprovada em Auditoria/Gestão de Conformidade
- Conhecimento e experiência comprovada em administração de solução automatizada de Governança, Riscos e Conformidade
- Conhecimento e experiência comprovada em Information Technology Infrastructure Library (ITIL v3)
-

Os profissionais alocados pela CONTRATADA para a execução dos serviços de Segurança Cibernética devem apresentar o perfil mínimo relacionado abaixo:

- Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas.
- Conhecimento e experiência comprovada de no mínimo 05 (cinco) anos na área de Segurança Cibernética.
- Conhecimento e experiência em Monitoramento de Rede de Telecomunicações
- Conhecimento e experiência em gestão de incidentes cibernéticos
- Conhecimento e experiência em administração de ferramentas de segurança cibernética
- Conhecimento e experiência em gestão de incidentes cibernéticos
- Conhecimento e experiência em software de inteligência cibernética
- Conhecimento e experiência em administração de logs de eventos de segurança cibernética
- Conhecimento e experiência em administração de ferramentas de gestão de vulnerabilidades técnicas
- Conhecimento e experiência em administração de ferramentas de segurança perímetro de redes de telecomunicações

3.4. MEDIÇÃO DO SERVIÇO

3.4.1. UST - Unidade de Serviço Técnico, é uma unidade de mensuração de esforço para a execução de um serviço que envolva prioritariamente esforço humano não mensurável previamente com precisão ou de difícil mensuração por outras técnicas (qualquer técnica com precisão de mensuração inferior a 90% é candidata a ser substituída pela UST). É bastante utilizada em contratos de

prestação de serviços que envolvam diversos tipos de serviços com variada complexidade.

3.4.2. A medição de uma Unidade de Serviço Técnico servirá como métrica para uma unidade de execução de serviço de Homem x Hora.

3.4.3. Uma Unidade de Serviço Técnico deve ter o valor de R$ 300,00

4. SERVIÇO WIFI EXTERNO

Este serviço contempla por parte da CONTRATADA o fornecimento de acesso à Internet através de Rede sem Fio (WIFI) com objetivo de atender a população do Estado em áreas públicas, como também a serviços específicos dos Órgãos.

Este Serviço será fornecido através de pontos de acessos "Acess Point" Wifi (AP-Wifi), instalados em pontos públicos ao ar livre, provendo acesso gratuito à internet para a população.

Os requisitos técnicos deste serviço estão descritos nas subseções correspondentes a seguir contidas neste documento.

O provimento dos AP-Wifi deve permitir que através do Rio Digital que os serviços de acessos abertos a Internet (gratuitos) sejam prestados visando atender a programas educacionais, sociais, culturais e/ou de desenvolvimento econômico de interesse da gestão do governo.

Para este serviço devem ser fornecidos os recursos de softwares, infraestrutura e todas as informações necessárias para que a CONTRATANTE possa efetivamente realizar a gestão e o monitoramento dos serviços contratados.

Prestar os serviços de operação, suporte e manutenção de todos os recursos. Esse serviço inclui todos os recursos como os roteadores, rádios e equipamentos com capacidade adequada para garantir o desempenho da solução.

Os serviços de suporte, operação e manutenção deverão abranger os seguintes itens:

- Acionar e registrar os serviços de suporte e manutenção através de um serviço de service-desk que ofereça recursos de pronto atendimento para o CONTRATANTE, garantindo um canal único de controle e registros da prestação dos serviços.
- Informar a CONTRATANTE quaisquer eventos ocorridos fora da normalidade quando da execução dos serviços de suporte e manutenção a que venham gerar impactos ou paralisações dos serviços em funcionamento.
- Fornecer relatórios mensais de execução dos serviços e de ocorrências técnicas.
- No caso de substituição de qualquer equipamento ou dispositivo, os substitutos deverão ser novos, sem uso, e estarem atualizados nos modelos e versões de fabricação mais atual.

- Assegurar a correta integração e funcionalidade dos serviços, visando cumprir as especificações técnicas deste serviço.

- Prestar os serviços de suporte e manutenção sempre que possível, em horários e forma de funcionamento (remoto ou presencial) que assegure a continuidade dos serviços com menor impacto possível e em menor espaço de tempo. No caso de necessidade de interrupção de outros serviços ou equipamentos, em decorrência da manutenção a ser efetuada, esta deverá estar devidamente planejada e ser acordada com antecedência junto à CONTRATANTE.

- Executar os serviços de acordo com as boas práticas da prestação dos serviços de TI baseados no ITIL V3.

- Prover identificação para todos os funcionários da CONTRATADA que devem utilizadas quando estiverem realizando os respectivos serviços.

- Executar troubleshooting para encontrar o local exato da falha.

- A CONTRATADA deverá realizar todas configurações e testes para garantir o correto funcionamento do serviço contratado, mantendo os níveis de disponibilidade. Isto envolve rede e roteamento que fazem parte da solução adotada para o serviço de Wifi externo.

- Assegurar uma infraestrutura de alto grau de confiabilidade de forma a garantir disponibilidade, qualidade e segurança para todos os serviços ativos e operacionalizados.

- A solução disponibilizada pela CONTRATADA deverá atender ao Marco Regulatório da Internet.

- A solução de conectividade para o acesso a Internet dos sites comtemplados com o serviço Wifi Externo deverá se dar através de cum circuito de acesso na velocidade de 10Mbps, com banda garantida, simétrico e com disponibilização de pelo menos 4 IPs fixos.

- Considerar a estimativa de no máximo até 04 (quatro) APs-WIFI por localidade, oferecendo um alcance de cobertura e de acesso à Internet no máximo de até 500m, podendo ter uma variação de acordo com as dificuldades do local, devidamente demonstrado após o serviço de site-survey.

- De acordo com o resultado do site-survey poderá ocorrer casos de inviabilidade técnica e/ou econômica para provimento do serviço Wif-Externo. Estes casos deverão ser justificados através de relatórios técnicos junto a CONTRATANTE.

- Para efeito de dimensionamento da capacidade de cada AP-WIFI a ser provido, estima-se que os recursos a serem instalados tenham capacidade de atender as limitações acima requeridas, evitando muitos APs por pontos de acesso de usuários.

- A Solução deverá permitir por AP a conexão de até 40 usuários simultâneos e cobertura de até 100m2 de área livre.

- Possuir uma estrutura de pessoal capacitado, equipamentos, softwares, processos e serviços especializados para prover os serviços desta rede de forma contínua em regime de 24x7x365 (24 horas por dia, sete dias por semanas, todos os dias do ano) garantindo o pleno funcionamento das conexões e serviços providos.

- Prover uma infraestrutura e realizar a operação desta Rede WiFi a partir de um ponto concentrador sendo a controladora Wifi parte integrante do serviço Wifi Externo, devendo possuir capacidade o controle de toda a Wifi contratada.

- Realizar o Gerenciamento completo dos APs-Wifi através de sistemas em ambiente da CONTRATADA, que serão responsáveis por controlar a configuração dos pontos de acesso, gerenciá-los e otimizar o desempenho e a cobertura de radiofrequência da rede Wifi.

- Permitir a conexão de clientes nos padrões WLAN 802.11a/b/g/n e a tecnologia IEEE 802.11ac (draft ou superior) com os APs devendo ser distribuídos de forma a proporcionar as melhores condições de conexão nas áreas definidas pela CONTRATANTE.

- Fornecer equipamento de ponto de acesso para rede local sem fio atendendo aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea.

- Permitir, simultaneamente, a conexão de múltiplos dispositivos legados, nos padrões IEEE 802.11a/b/g /n.

- Permitir movimentação livre dos equipamentos clientes e dos usuários da rede sem fio dentro da área de cobertura, sem desconexões ou novas autenticações (Roaming/Hand-over).

- Oferecer um portal na forma de uma solução de software para registrar os “visitantes” e “usuários” da Rede Wifi de forma poder cadastrar, gerenciar e monitorar esses clientes da rede.

- Prover a funcionalidade dos APs poderem fazer a análise automática do espectro de rádio frequência buscando possíveis interferências e poder fazer o ajuste dos mesmos entre as frequências e canais disponíveis, sem necessidade de intervenção da gerência.

- Disponibilizar através de console web todas as facilidades de gerência da rede wifi que poderá ser acessada a partir de múltiplos navegadores.

- Realizar o Suporte Presencial/Manutenção no local onde os equipamentos da solução estão instalados. Apoiar à equipe de suporte técnico da CONTRATANTE de forma presencial no tratamento das falhas.

- Substituir e configurar os componentes defeituosos por componentes funcionais, quando for o caso.

- Prover serviço de Site-Survey para cada local (site) conforme solicitado por Ordens de Serviços específicas.

- O remanejamento dos APs ou de quaisquer itens integrantes do serviço instalado estará sujeita a uma nova análise de viabilidade e o pagamento de uma nova instalação.

- Toda a instalação do serviço Wifi Externo deverá permanecer no local pelo menos 6 (meses).

- Realizar manutenção corretiva e de reparo na infraestrutura disponibilizada e fornecida (elétrica, lógica, aterramento e demais itens fornecidos).

4.1. Serviço de Site Survey

O serviço de Site Survey deverá contemplar os seguintes itens:

i. Executar a atividade de Site Survey antes de realizar e instalar os serviços de AP-Wifi para fornecer a CONTRATANTE dados e informações relevantes referentes a real necessidade de fornecimento da solução, o dimensionamento correto da infraestrutura e das necessidades de equipamentos e serviços, de forma alocar quantitativos de produtos e serviços com base em uma referência técnica, otimizando instalações e oferecendo qualidade de atendimento.

ii. Ser realizado por profissional devidamente habilitado da CONTRATADA, que será acompanhando por um responsável técnico designado pela CONTRATANTE durante a realização do Site Survey.

iii. Fornecer relatório da conclusão da atividade de Site-Survey, contendo, no mínimo, as seguintes informações:

- Detalhamento da situação do local de instalação e abrangência do serviço.
- Planta lógica e elétrica necessárias à solução contendo os percursos dos cabeamentos lógico e elétrico que interliga todos os equipamentos.
- Memorial descritivo da solução que deverá ser implementada.
- Relação de itens de serviços necessários.
- Área de Cobertura de cada equipamento de rádio frequência.
- Local onde abrigará o restante dos equipamentos necessários.

- Planta Atualizada para receber os serviços de AP-Wifi.
- A planta da área onde o AP-Wifi deverá ser instalado e onde será realizado o Site-Survey deverá ser fornecida pela CONTRATANTE para que a CONTRATADA faça as avaliações e atualizações necessárias.

4.2. Gerência da Rede Wifi

i. A Gerencia da solução de Rede Wifi externo deve ser capaz de permitir uma completa gestão do serviço.

ii. A solução deve permitir consultar o histórico dos alarmes

iii. A solução deve permitir ao usuário/operador filtrar e/ou ordenar os alarmes por meio de campos do alarme

iv. A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados.

v. O portal da solução deve apresentar informações atualizadas e históricas de alarmes

vi. O portal da solução deve ter visões pré configuradas.

vii. O portal da solução deve ser acessado via web browsers de mercado tais como Microsoft Internet Explorer, Google Chrome e Mozila Firefox

viii. Ser capaz de gerenciar centralizadamente outros Pontos de Acesso do mesmo fabricante.

ix. Suporte ao serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.

x. Suporte a monitoração e supressão de Ponto de Acesso indevido.

xi. Prover autenticação para a rede wireless através de bases externas.

xii. Deverá permitir a visualização dos clientes conectados.

xiii. Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.

xiv. Possuir Captive Portal.

xv. Permitir configurar parâmetros de rádio como: banda e canal.

xvi. Possuir lista contendo Pontos de Acesso Aceitos.

xvii. Possibilitar definir número de clientes por SSID.

xviii. Permitir e/ou bloquear o tráfego entre SSIDs.

xix. A comunicação entre o Access Point e a controladora wireless deve poder ser efetuada de forma criptografada.

xx. Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois access points gerenciados.

xxi. Toda a configuração do Ponto de Acesso deve ser executada através da Controladora Wireless.

xxii. Deverá utilizar protocolo de gerenciamento SNMP, para os dispositivos de rede.

xxiii. O Sistema deve poder processar logs de sistemas e/ou traps SNMP para gerenciar as falhas dos equipamentos.

4.3. Recursos e serviços dos pontos de acesso Wifi

Instalar os pontos de acessos WIFI incluindo todos os recursos e serviços necessários para o pleno funcionamento, tais como:

i. Antenas direcionais, setoriais, omnidirecionais.

ii. Conectores e amplificadores.

iii. Fios, cabos elétricos, de RF, UTP, STP, e cabos ópticos.

iv. Racks e demais equipamentos de bastidores de ambientes de Tecnologia da Informação (TI) e de Telecomunicações.

v. Torres, postes e suportes para instalação e fixação dos equipamentos, acompanhados de sistemas próprios de proteção contra descargas atmosféricas, caso necessário.

vi. Switches e no-breaks, caso necessário.

vii. Instalação adicional de energia elétrica estabilizada e dotada de no-break ou UPS, incluindo sistema de proteção de descargas atmosféricas, fios e condutores elétricos, surge protectors, isolantes elétricos, canaletas, eletrocalhas, eletrodutos, braçadeiras, suportes, parafusos e dispositivos de fixação.

viii. Prover os recursos e funcionalidades para instalação dos APs-Wifi.

4.4. Gestão dos Serviços

i. A prestação de serviços prevê o gerenciamento centralizado local e remoto de toda a solução utilizada, por intermédio do centro de gerência do serviço Wifi Externo.

ii. O gerenciamento prevê a utilização de ferramentas que possibilitem a gestão de alarmes, falhas, configuração, inventário e performance.

iii. Deverão ser disponibilizados relatórios periódicos de performance de atendimento do serviço.

iv. Gestão de Incidentes e Demandas

a. A Gestão de Incidentes é responsável por restabelecer a operação normal de um serviço/atividade rapidamente e minimizar o impacto causado por qualquer indisponibilidade.

b. A Gestão de Incidentes será responsável por:
- Receber e registrar os incidentes.
- Classificar os incidentes e fornecer o suporte inicial.
- Investigar e diagnosticar.
- Resolver e restabelecer a operação.
- Fechar o incidente.
- Acompanhar todo o ciclo de vida do incidente e manter o usuário informado.

v. A Gestão de Incidentes deve ser feita por meio de uma ferramenta adequada e automatizada para o registro dos incidentes, que tenha uma base de conhecimento e seja integrada à base de dados da Gestão de Configuração.

vi. A Gestão de Demandas é responsável por atender as demandas de novos serviços e atualização do parque tecnológico.

4.5. Requisitos mínimos Acess Point

i. Deve possuir interface de rede 10/100/1000 no padrão RJ45

ii. Deve suportar ao menos 16 SSIDs simultâneos por rádio.

iii. Possuir potência de transmissão de ao menos 27dBm

iv. Possuir ganho mínimo de 5 dBi por antena em 2.4GHz e 7dBi por antena em 5GHz

v. Deve suportar operar na temperatura de -20 a 60 graus

vi. Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em poste ou parede

vii. Possuir no mínimo 4 antenas externas. Não podem ser do tipo AP interno instalado em caixas hermeticamente fechadas

viii. Possuir a tecnologia MIMO – Multiple-in/Multiple-out - 2x2

ix. Suportar taxas de transferência de 300Mbps por rádio.

x. Possuir PoE – Power over Ethernet padrão 802.3at - possibilitando seu uso sem a necessidade de fontes de energia externas em qualquer porta ethernet

xi. Possuir ao menos 4 filas de tráfego.

xii. Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede.

xiii. Suportar 802.11a/b/g/n.

xiv. Possuir 2 rádios para atuar nas frequências 2.4 GHz b/g/n e 5 GHz a/n simultaneamente

xv. Suporte a extensão multimídia WME.

xvi. Ser capaz de encontrar automaticamente a Controladora Wireless.

xvii. Suporte a 802.11n High-Throughput (HT) Support: HT 20/40.

xviii. Possuir os seguintes certificados e diretivas: FCC 15 B parts 15.107 e 15.109, FCC 15 C parts 15.247 e 15.207 e 15.203, EN55024, CE Standard, RoHS.

xix. Deve suportar a criação de redes mesh.

xx. Deve suportar a criação de enlaces de bridge entre dois Access Point.

xxi. Deve permitir configurar individualmente para cada SSID se o tráfego será tunelado até a controladora ao qual ele está registrado e/ou se será comutado localmente.

xxii. Deve suportar associação dinâmica de usuários à VLANs de acordo com parâmetros de autenticação

xxiii. O equipamento deverá possuir homologação da Agência Nacional de Telecomunicações (ANATEL).