GOVERNO DO ESTADO DO RIO DE JANEIRO

SECRETARIA DE ESTADO DA CASA CIVIL E GOVERNANÇA

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO

DIRETORIA DE INFRAESTRUTURA TECNOLÓGICA

ENCARTE TÉCNICO II

REDE IP INTERNET SIMÉTRICA

Sumário

1. INTRODUÇÃO

Este documento apresenta os projetos:

- **Acesso dedicado à Internet para a Rede IP Governo e órgãos provedores de serviços de tecnologia.**

1.1. Este encarte complementa o Termo de Referência, constituindo a documentação necessária e obrigatória à contratação da atualização tecnológica da Rede de Longa Distância e acesso à internet do Governo do Estado do Rio de Janeiro.

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

1.3. A CONTRATADA deverá fornecer links para órgãos e secretarias que já possuem acesso dedicado simétrico à Internet, cujos endereços constem no Anexo II - Local de Prestação dos Serviços de Internet;

1.4. A CONTRATADA deverá garantir o nível de disponibilidade especificado neste Encarte Técnico;

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

2. CONTEXTUALIZAÇÃO

2.1. Atualmente, o provimento de acesso à Internet para as unidades do Governo do Estado é bastante heterogêneo. A conexão com a Internet é feita de forma independente, existindo vários contratos e diferentes formas de prestação dos serviços;

2.2. Atualmente o provimento de internet da Rede IP Governo se dá através do PRODERJ, Contrato nº 003/2019;

2.3. 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. A banda contratada prevê a criação de uma interface L3 exclusiva para o acesso Internet;

2.4. 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;

2.5. Com a presente contratação, pretende-se que o PRODERJ seja um ponto central de Internet para os sítios abrangidos pela Rede IP Governo, com garantia de disponibilidade compatível com a criticidade do serviço.

2.6. 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 IP Governo.
- Garantia da disponibilidade do serviço para o PRODERJ e os sítios abrangidos pela internet.

2.7. Implantar uma infraestrutura correta e adequada para a operação da rede e verificação do atendimento dos níveis de serviços das conexões.

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

2.9. A presente contratação prevê que serão atendidas pelo serviço dedicado à internet uma das seguintes localidades:

- PRODERJ – Sede no Rio de Janeiro (SERPRO);
- Unidade CICC – Cidade Nova – Rio de Janeiro.

2.10. Portanto, com base nas características atuais das unidades da Rede IP 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.

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

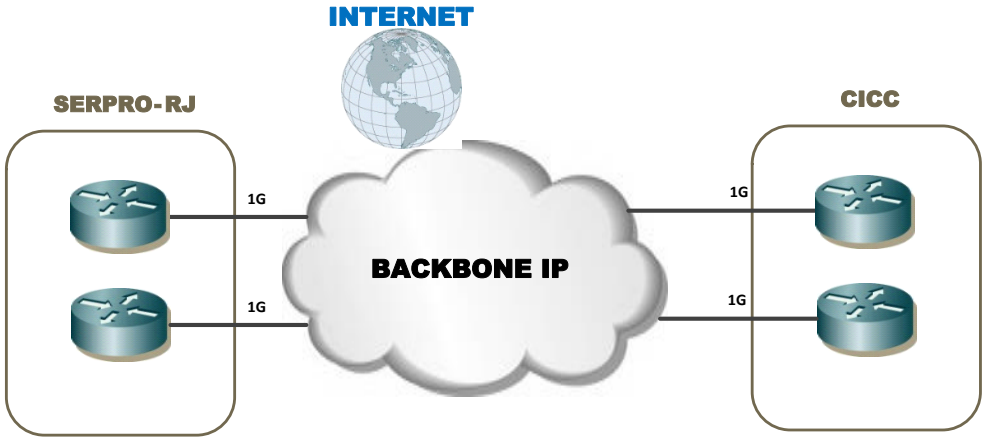
2.12. A topologia a ser implantada deverá ser efetuada mediante ativação de circuito de comunicação de dados, instalação de equipamentos e prestação de serviços de instalação, configuração, suporte técnico e gerenciamento proativo de falhas, conforme especificações técnicas constantes nesse documento;

2.13. A CONTRATADA deverá se encarregar de prover o meio físico de interligação entre a sua rede e a Rede IP Governo, atendendo aos parâmetros definidos nesta especificação, ficando este serviço sob sua inteira responsabilidade;

2.14. A solução adotada pela CONTRATADA deverá atender a todas as normas técnicas exigidas pelos órgãos públicos competentes e responsáveis pela regulamentação;

2.15. A CONTRATADA poderá subcontratar os meios de acesso à última milha, no termos no Termo de Referência, sem que isso implique e transferência de responsabilidade, que será exclusiva da CONTRATADA vencedora do certame;

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



3. ESPECIFICAÇÕES TÉCNICAS

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

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

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

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

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

3.5. 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;

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

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

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

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

3.10. Realizar, manter e prover meios de acessos, com no mínimo 10 Gbps, entre o enlace principal instalado no Datacenter do PRODERJ e o Ponto de Troca de Tráfego (PTT-RJ). A realização desta ligação deve estar no projeto de implementação do enlace principal do PRODERJ que atenderá à Rede IP Governo, para garantir a continuidade dos serviços providos e sem tarifação de tráfego;

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

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

- HTTP, HTTPS
- FTP (File Transfer 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.

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

3.14. A CONTRATADA deverá disponibilizar faixa de endereço IP válido, com no mínimo 512 (quinhentos e doze) endereços IP válidos;

3.15. 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.

3.16. 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;

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

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

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

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

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

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

4.1. 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;

4.2. O CONTRATANTE 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, sem que isso enseje custos de qualquer natureza ao solicitante.

5. DAS CARACTERÍSTICAS MÍNIMAS DO ROTEADOR

5.1. 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 CONTRATANTE com as seguintes características:

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

5.1.2. 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.

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

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

5.2.2. 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.

5.2.3. 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.

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

5.2.5. 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.

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

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

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

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

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

5.2.11. 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.

5.2.12. Implantar protocolo IPv4 (RFCs 791, 1918), IPV6 (RFC 2460) e o protocolo de WAN PPP (RFC 1661), com suporte a TCP (RFC 793) e UDP (RFC 768).

5.2.13. 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.

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

5.2.15. 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.

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

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

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

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

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

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

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

5.3. Os roteadores da rede (backbone da CONTRATADA) e os instalados nas unidades da Rede IP 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.

6. SOLUÇÃO DE FIREWALL/IPS

Com o objetivo de permitir o controle das conexões dos distintos Órgãos e Unidades à Internet, bem como o acesso da grande rede aos sistemas hospedados, a CONTRATADA deverá prover solução de Firewall/IPS exclusivamente ao PRODERJ que deverá ter, no mínimo, as especificações a seguir.

6.1. 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;

6.2. 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);

6.3. 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;

6.4. 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" ou quantidade de tráfego de cada regra de filtragem individualmente.) 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;

6.5. 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;

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

6.7. 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;

6.8. 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;

6.9. Deve implementar políticas de controle de acesso baseadas em informações de horário ("time-based access control");

6.10. 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;

6.11. 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;

6.12. 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;

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

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

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

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

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

6.18. 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);

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

6.20. Deve possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para um endereço de destino especificado;

6.21. 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".

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

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

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

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

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

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

6.28. Deve suportar versões do cliente IPSEC VPN fornecido com appliance para, no mínimo, os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Windows 10, Linux (Intel) e MacOS;

6.29. Deve estar licenciado, ou suportar sem o uso de licença, 20.000 (vinte mil) túneis IPSEC VPN do tipo client-to-site simultâneos;

6.30. Deve estar licenciado, ou suportar sem o uso de licença, 20.000 (vinte mil) clientes de VPN SSL (WebVPN);

6.31. Deve suportar a terminação túneis IPSEC do tipo "site-to-site" (LAN-to-LAN);

6.32. Deve suportar a terminação simultânea de conexões IPSEC VPN;

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

6.34. 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;

6.35. 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;

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

6.37. 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;

6.38. 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;

6.39. 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;

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

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

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

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

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

6.45. Deve ser possível a associação de diferentes pools de endereços IP aos diferentes grupos de

usuários que solicitarem conexão ao concentrador VPN;

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

6.47. Deve suportar NAT (Network Address Translation);

6.48. 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);

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

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

6.51. 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;

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

6.53. 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;

6.54. 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);

6.55. Deve suportar protocolo Syslog para geração de logs de sistema;

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

6.57. 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;

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

6.59. Deve ser gerenciável via SNMP, v2c e v3;

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

6.61. 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;

6.62. 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;

6.63. Deve permitir o armazenamento de pacotes capturados em formato tcpdump;

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

6.65. 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+;

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

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

6.68. 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;

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

6.70. Deve suportar a operação como IGMP Proxy Agent;

6.71. Deve suportar inspeção stateful de tráfego IPv6;

6.72. Deve suportar simultaneamente a criação de regras IPv4 e IPv6;

6.73. Deve suportar roteamento estático;

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

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

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

6.77. Deve suportar stateful failover de conexões IPv6;

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

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

6.80. 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;

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

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

6.83. 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 independente do usuário.

6.84. 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”);

6.85. 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);

6.86. Deve permitir a customização de regras de detecção de novas aplicações;

6.87. 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.

6.88. 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.

6.89. 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.

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

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

6.92. Deve permitir armazenamento dos arquivos de configuração diretamente no appliance;

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

6.94. 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;

6.95. Deve permitir a inspeção em túneis GRE;

6.96. 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;

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

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

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

6.100. Deve possuir capacidade a resistência às ferramentas de evasão;

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

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

6.103. 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;

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

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

6.106. 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;

6.107. 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;

6.108. 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.

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

6.110. 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);

6.111. Deve possibilitar que os pacotes sejam capturados para análise;

6.112. 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;

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

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

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

6.116. 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;

6.117. 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.

6.118. 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.

6.119. 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.

6.120. 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;

6.121. 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.

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

6.123. 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;

6.124. 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.

6.125. 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);

6.126. Deve ser fornecido com pelo menos 8 (oito) interfaces 1 Gigabit Ethernet;

6.127. Deve ser fornecido com pelo menos 4 (quatro) interfaces 10 Gigabit;

6.128. Deve suportar pelo menos 50.000.000 (cinquenta milhões) conexões simultâneas em sua tabela de estados de Stateful Firewall;

6.129. Deve suportar a criação de pelo menos 350.000 (trezentos e cinquenta mil) novas conexões TCP por segundo para a funcionalidade de Stateful Firewall;

6.130. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 40 Gbps (Quarenta Gbps) para pacotes UDP;

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

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

6.133. Deve suportar a terminação de pelo menos 20.000 túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

6.134. Deve possuir desempenho de, no mínimo, 10Gbps (Cinco Gbps) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;

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

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

6.137. Deve reconhecer mais de 4000 (quatro mil) aplicações com atualizações automáticas;

6.138. Deve suportar pelo menos 80 categorias de URL;

6.139. Deve possuir mais de 280 Milhões de URL categorizadas;

6.140. 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 automática e periódica 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.

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

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

6.143. 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 automaticamente 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;

6.144. 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 presença de malware na rede monitorada;

6.145. 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;

6.146. 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;

6.147. 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;

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

6.149. 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;

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

6.151. 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,C PIO_ODC,JAR,LHA,MSCAB,MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_EN C,ACCDB,HLP,MAIL,MDB,MDI,MNY,MSCHM,MSOLE2,MSWORD_MAC5,MWL,NE W_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS.

6.152. 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.

6.153. A solução ofertada deve ser totalmente do mesmo fabricante;

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

6.155. A solução deverá se integrar com o SNOC, através de envio de logs via syslog, e ferramentas de segurança fornecido pela CONTRATADA vencedora do Lote I e/ou do PRODERJ, sem que isto retire as suas responsabilidades conforme Termo de Referência e este Encarte Técnico.

7. SERVIÇO DE GERÊNCIA DE REDE

A CONTRATADA também deverá disponibilizar o Serviço de Gerência da Rede IP Simétrica em conformidade com os seguintes requisitos:

7.1. 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;

7.2. 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;

7.3. A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano, para os enlaces classificados como críticos, e 8 horas por dia, 5 dias por semana (horário comercial) para os enlaces classificados como básicos;

7.4. A abertura do chamado 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 e seja da responsabilidade da Operadora correspondente. Após a abertura do chamado, em um prazo máximo de 45 (quarenta e cinco) minutos, o atendente responsável pela abertura de chamado deverá entrar em contato com técnico do CONTRATANTE, informando as providências já tomadas e a estimativa para solução do problema;

7.5. 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;

7.6. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto não serão aceitos soluções que possuem acessos segmentados aos módulos;

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

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

7.9. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente;

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

7.11. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clients 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;

7.12. 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.

7.13. 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;

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

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

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

7.17. 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 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.

7.18. 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).

7.19. 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.

7.20. A Solução de Gerência da Rede deverá armazenar os dados por um período de 12 (doze) meses.

8. SERVIÇO DE ANTI-DDOS

8.1. 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);

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

8.3. 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;

8.4. 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;

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

8.6. 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;

8.7. 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;

8.8. 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;

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

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

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

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

8.13. 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;

8.14. 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.;

8.15. 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.;

8.16. 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:

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

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

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

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

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

8.18. 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.;

8.19. Realizar a comunicação da ocorrência do ataque ao órgão do Governo CONTRATANTE

imediatamente após a detecção;

8.20. Disponibilizar relatórios mensais de mitigação de ataques;

8.21. 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;

8.22. 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);

8.23. 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;

8.24. A solução ofertada não poderá afetar a visibilidade do endereço de origem das requisições, mantendo o tráfego legítimo livre de qualquer modificação;

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

8.26. 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;

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

8.28. 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;

8.29. O Serviço de Backbone (Anti-DDOS), deverá possuir o seguinte SLA (Service Level Agremment):

8.29.1. Prazo para entrega de relatórios mensais: até 5 (cinco) dias úteis.

8.29.2. Prazo para entrega de relatórios de incidente (após mitigação do ataque): até 5 (cinco) dias úteis.

8.29.3. Atendimento às solicitações em regime 24x7xtodos os dias do ano:

8.29.3.1. Prioridade 1: Requisição de adição/retirada de rede monitorada, modificação na lista de contatos autorizados do cliente, relatórios de dados do tráfego do cliente monitorado em um período especifico. Prazo máximo de 2 horas

8.29.3.2. Prioridade 2: Requisição da lista de redes monitoradas, alertas e mitigações, informações sobre ataques recebidos, lista de contatos autorizados pelo cliente. Prazo máximo de 8 horas.

8.29.4. SLA de Mitigação de Ocorrência de Incidentes:

Item	Ocorrências	Prazo
Tempo de Detecção	Início do Ataque Detecção do Ataque Contato com PRODERJ	Até 15 minutos

8.29.5. A CONTRATADA deverá entrar em contato com o PRODERJ e solicitar autorização para dar início à mitigação do tráfego;

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

9. OS REQUISITOS DE INFRAESTRUTURA

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

9.2. 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;

9.3. 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;

9.4. 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;

9.5. 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.

10. REQUISITOS DE IMPLANTAÇÃO DOS SERVIÇOS

10.1. Para cada um dos acessos contratados deverão ser prestados serviços de ativação dos circuitos de comunicação de dados, bem como instalação e configuração dos equipamentos;

10.2. Os serviços de ativação e instalação dos circuitos e equipamentos deverão ser prestados no ambiente computacional da Rede IP Governo;

10.3. A CONTRATADA deverá em, no máximo, de 30 (trinta) dias corridos, contados a partir da assinatura do Contrato, apresentar Projeto Executivo contendo o Plano de Implantação dos Serviços para cada uma das localidades contratadas;

10.4. Os planos de implantação contidos no projeto executivo deverão ser aprovados pelo CONTRATANTE em até 15 (quinze) dias corridos após sua apresentação. Os planos de implantação deverão prever a disponibilidade do serviço de internet da Rede IP Governo, garantindo a migração sem a interrupção dos serviços existentes;

10.5. Após a validação dos Planos de Implantação contidos no Projeto Executivo, a CONTRATADA deverá entregar a solução totalmente operacional, com os níveis de serviços exigidos, incluindo equipamentos e circuitos de comunicação, quando se iniciará os trabalhos de atestação e conformidade;

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

10.7. Caso o Projeto Executivo não seja aprovado pelo CONTRATANTE, a CONTRATADA deverá corrigi-lo e reapresentá-lo em no máximo 5 (cinco) dias corridos após a comunicação da sua rejeição;

10.8. O início da implantação dar-se-á somente após a aprovação pelo CONTRATANTE do Projeto Executivo e dos testes realizados no ambiente de testes;

10.9. O atraso na entrega do Projeto Executivo poderá causar sanções à CONTRATADA conforme condições elencadas na Cláusula Das Sanções do Termo de Referência;

10.10. A CONTRATADA deverá apresentar durante a implantação, semanalmente, relatórios de acompanhamento das atividades, nos quais deverão constar as atividades realizadas e a duração de cada atividade;

10.11. A CONTRATADA deverá documentar, em forma de relatório, o estado da infraestrutura física antes e depois das instalações realizadas, inclusive com fotografias do ambiente que sofreu alterações, antes e depois das instalações realizadas;

10.12. Todo o processo de instalação e implantação da solução será acompanhado e supervisionado pela Gerência de Redes e Telecomunicações da Diretoria de Infraestrutura Tecnológica do PRODERJ, à qual a licitante vencedora deverá se reportar antes de qualquer ação e decisão referente à implantação da solução em tela;

10.13. A não aceitação pelo CONTRATANTE das soluções adotadas, devido a não conformidade com as solicitações deste Estudo Técnico, poderá resultar em rescisão total ou parcial do contrato de prestação de serviços;

10.14. Os equipamentos instalados deverão vir com a última versão de firmware disponibilizada pelo fabricante, de modo a minimizar a probabilidade de atualização de versões assim que a solução estiver totalmente operacional;

10.15. Os trabalhos de migração e instalação de equipamentos poderão ocorrer fora do período de expediente do CONTRATANTE, a saber: de 19h às 23h, nos finais de semana e feriados de modo que o impacto seja o mínimo possível ao ambiente computacional;

10.16. A CONTRATADA ficará obrigada a manter sigilo sobre todas as informações referentes à solução implantada, bem como acerca das instalações do CONTRATANTE, sendo vedada qualquer divulgação destas informações sem prévia autorização, por escrito, do órgão, cabendo penalizações

administrativas e sanções legais cabíveis, em caso de descumprimento;

10.17. Os custos externos ao ambiente da CONTRATANTE com realização de canalização, entradas, tubulações, entre outros, serão realizados pela licitante sem ônus adicional ao CONTRATANTE;

10.18. A passagem doa cabos para prestação dos Serviços serão de responsabilidade da CONTRATADA, sendo recomendada vistoria para verificação das condições de infraestrutura predial do Backbone da Rede IP Governo;

10.19. O CONTRATANTE deverá prover as condições de infraestrutura física em seu ambiente, como tubulações, energia elétrica e climatização adequada para que o serviço possa ser prestado pela CONTRATADA;

10.20. A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da instalação e configuração da solução, na área de prestação dos serviços, mesmo que fora do exercício;

10.21. Os roteadores destinados ao funcionamento do serviço, alocados em ambiente da CONTRATADA, deverão ser acessíveis a partir de plataformas de gerenciamento SNMP, localizadas na rede interna do PRODERJ;

10.22. Uma vez instalados, os equipamentos deverão ser cadastrados em software de gerenciamento SNMP disponível no PRODERJ, que contará com o apoio da CONTRATADA, se necessário;

10.23. Os agentes SNMP instalados nos equipamentos deverão suportar mensagens nas versões v1, v2c e v3, para realização de consultas de objetos da MIB II (RFC 1213) e da host-resources-MIB (RFC 1514);

10.24. Após a assinatura do contrato, o PRODERJ informará à CONTRATADA os endereços IP dos seus sistemas de gerenciamento da rede (NMS) que deverão estar autorizados a realizar consultas SNMP (get) nos equipamentos da rede, receber traps SNMP e o nome da comunidade (community string) que deverá ser configurado;

10.25. Todos os roteadores destinados ao funcionamento da rede, alocados em ambiente da CONTRATANTE, deverão ser capazes de encaminhar mensagens syslog para plataformas de armazenamento de logs, localizadas na rede interna do PRODERJ;

10.26. Após a assinatura do contrato, o PRODERJ informará à CONTRATADA os endereços IP dos seus sistemas de armazenamento que deverão receber as mensagens syslog;

10.27. Deverá ser disponibilizada a geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, dos níveis de serviço contratados;

10.28. O serviço de gerenciamento deve atuar de forma proativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço estabelecida no Termo de Referência e este Encarte Técnico, realizando abertura, acompanhamento e fechamento de chamados técnicos relacionados com indisponibilidade e desempenho no serviço de rede WAN, operando em regime 24 horas por dia, 7 dias por semana, anualmente durante toda a vigência do contrato;

10.29. A indisponibilidade dos dados de gerência (coleta não realizada, dados não acessíveis) será contabilizada como indisponibilidade do(s) serviço(s) associado(s), passível de desconto, no período

em que os dados não forem coletados ou ficarem inacessíveis, caso isto implique em perda de dados de gerenciamento.

11. PROJETO EXECUTIVO

11.1. 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.

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

12. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA OS ACESSOS À INTERNET

12.1. Uma série de indicadores deverá ser a calculada pela CONTRATADA periodicamente como condição para pagamento dos serviços. A CONTRATADA deverá disponibilizar mensalmente ao CONTRATANTE, relatórios digitais com o cálculo dos indicadores, totalizados e apresentados mensalmente por enlace.

12.2. Essas métricas servirão como limiar de qualidade do serviço, compondo o que será denominado de Níveis Mínimos de Serviço (NMS).

12.3. No Termo de Referência encontram-se a definição básica destes indicadores e sua fórmula de cálculo.

12.4. Classificam-se cada sítio como básico ou crítico, sendo o primeiro com atendimento 8x5 e dias comerciais, e o segundo 24x7x365;

12.5. Cada endereço constante no Anexo II receberá uma única classificação, e a CONTRATADA deverá ter condições de atender a possível mudança quando solicitado pelo CONTRATANTE durante a vigência contratual;

12.6. Índice Disponibilidade Mensal do Enlace (IDM)

12.6.1. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede WAN estará operacional em um determinado período de tempo, para cada sítio da rede corporativa

do Governo do Estado do Rio de Janeiro. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês.

12.6.2. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

Nível	IDM	Serviços
N1	≥ 99,80% ou 1h 27m 7s / mês	Serviços de Acesso à Internet do Datacenter PRODERJ
N2	≥ 99,30% ou 5hs 4m 55s / mês	Serviços de Acesso à Internet demais órgãos e secretarias – região metropolitana
N3	≥ 99,03% ou 7hs 2m 31s / mês	Serviços de Acesso à Internet demais órgãos e secretarias – região não metropolitana

Tabela 1 – Índice de Disponibilidade Mensal (IDM)

12.7. Taxa de Erro de Bit (TxErr)

Para o Serviço de Acesso à Internet a TxErr será medida da Taxa de Erro da conexão do acesso ao Backbone IP da CONTRATADA.

Nível	TxErr	Acessos
N1	$\leq 10^{-7}$	Conexões dos Acessos à Internet

Tabela 2 – Taxa de Erro de Bit

12.8. Taxa de Perda de Pacotes (TPP)

Para o Serviço de Acesso à Internet a Taxa de Perda de Pacotes deverá se ser menor ou igual a 2%.

A perda de pacote do Backbone IP do Núcleo do Backbone IP da CONTRATADA deverá ser menor que 1%.

12.9. Tempo de Retardo (RTT)

Para os Serviços de Acessos à Internet o Tempo de Retardo deverá atender aos limiares abaixo, considerando a medição ao primeiro elemento de roteamento do Backbone IP da CONTRATADA.

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

Tabela 3 – Tempo de Retardo

12.10. Prazo de Reparo (PR)

Para os Serviços de Acesso à Internet o Prazo de Reparo deverá atender o limiar abaixo.

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

Tabela 4 – Prazo de Reparo (PR)

12.11. Prazo de Alteração de Transmissão de um Enlace (PAT)

Para os Serviços de Acesso à Internet o Prazo de Alteração de Transmissão de um Enlace deverá atender ao limiar abaixo

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

Tabela 5 – Prazo de Alteração de Transmissão (PAT)

12.12. Prazo de Atendimento a Novos Endereços (PAN)

Para os Serviços de Acesso à Internet, o Atendimento à Novos Endereços deverá ser de **45 dias**.

12.13. As métricas apresentadas nesse subitem e nos Níveis Mínimos de Serviço (NMS) deverão ser avaliadas como fins de verificação da qualidade dos serviços prestados pela CONTRATADA.

13. REQUISITOS DO SERVIÇO DE SUPORTE TÉCNICO

13.1. A CONTRATADA deverá disponibilizar um número único nacional não tarifado (0800) para abertura de chamados de suporte técnico, como também o Serviço de Gerência fornecido pela CONTRATADA deverá ser capaz de gerenciar os níveis de serviços acordados;

13.2. A assistência técnica on-site deverá ser prestada nas instalações do CONTRATANTE, sítios e unidades especiais conforme os prazos estipulados nos Níveis Mínimos de Serviço (NMS);

13.3. No momento de abertura do chamado deverá ser fornecido ao CONTRATANTE um número único de identificação do chamado;

13.4. Os chamados somente poderão ser abertos e fechados após autorização do CONTRATANTE;

13.5. Os serviços de suporte técnico deverão incluir serviços de atualização dos Equipamentos componentes da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de software de Equipamentos;

13.6. A CONTRATADA deverá disponibilizar, ainda, um número de telefone ao CONTRATANTE para contato com a área de 2º nível para solução de problemas urgentes que necessitem a atuação imediata, tais como: reinício de interfaces de roteadores, conferência de aplicação de políticas nos roteadores, lista de acesso, ativação de modo debug de forma temporário para diagnóstico, verificação de logs, configuração de velocidade e modo de operação de interfaces, elaboração de listas de acesso temporárias e reinício de equipamentos;

13.7. O CONTRATANTE reserva-se o direito de promover, a qualquer tempo, alterações nas políticas de utilização do serviço de acesso à Internet, ficando a CONTRATADA, neste caso, será obrigada a prestar o suporte técnico necessário à implementação dessas diretrizes nos equipamentos por ela empregados na prestação os serviços, inclusive nos roteadores locados, sem prejuízo das condições de funcionamento previstas no edital;

13.8. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo CONTRATANTE;

13.9. Em caso de reiterado inadimplemento do SLA, o CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato;

13.10. Durante a vigência do contrato, a CONTRATADA deverá manter preposto aceito pela Administração do CONTRATANTE para representá-la administrativamente sempre que houver necessidade.

14. ACEITAÇÃO DOS SERVIÇOS

14.1. A implantação do serviço de Rede IP Internet Simétrica, dar-se-á por implantação de enlaces em cada sítio. Os sítios e enlaces a serem contratados serão definidos durante a assinatura do contrato.

14.2. Os serviços de implantação de cada enlace serão verificados individualmente, e estarão sujeitos a dois tipos de aceitação: denominados: Termo de Aceitação Provisória e Termo de Aceitação Definitiva.

14.3. Critérios para Aceitação Provisória dos serviços de implantação

14.3.1. A Aceitação Provisória dar-se-á em até 15 (dez) dias úteis após a entrega do serviço do sítio, com a observação do GOVERNO DO ESTADO, de normalidade no provimento dos serviços para este enlace.

14.3.2. Para os sítios que fizerem parte do ambiente de teste, o prazo para a aceitação provisória contará a partir da data do início dos testes.

14.3.3. Caso haja rejeição na aceitação do serviço do sítio, o CONTRATANTE poderá solicitar a suspensão da implantação até que possíveis problemas sejam sanados, sem que isso gere direito à CONTRATADA de protelar a implantação dos demais sítios dentro dos prazos definidos.

14.3.4. Os testes de aceitação provisória dos serviços de rede serão compostos, no mínimo, por testes de conectividade/funcionais e testes de contingência.

14.3.5. A aceitação ocorrerá caso os resultados dos testes estejam conforme os requisitos do projeto.

14.3.6. Um enlace da rede será considerado aceito nos testes de conectividade/funcionais, se:

14.3.6.1. O tempo de retardo da conexão e o desempenho do roteador CPE estiverem dentro dos limites estabelecidos nos Níveis Mínimos de Serviços (NMS) por um período de 2 (dois) dias úteis.

14.3.6.2. A taxa de erro de bit estiver dentro dos limites estabelecidos nos Níveis Mínimos de Serviços (NMS), quando solicitado pelo GOVERNO DO ESTADO.

14.3.6.3. A transação padrão de um sistema corporativo definido pelo PRODERJ puder ser completada com sucesso, dentro das características da aplicação.

14.3.7. A configuração lógica do roteador CPE for fornecida ao PRODERJ.

14.3.8. Os equipamentos CPEs puderem ser visualizados, consultados e terem seus dados de monitoramento coletados por ferramentas apropriadas do PRODERJ.

14.3.9. Após a execução dos testes, e verificado que o enlace implantado atende os requisitos conforme descrito nos itens anteriores, a Gerência de Redes e Telecomunicações do PRODERJ emitirá o Termo de Recebimento Provisório (TRP) do enlace contratado.

14.4. A aceitação final se dará após o término do Período de Funcionamento Experimental (PFE), que se inicia com a emissão do TRP e se encerra após o decurso de um período completo de 10 (dez) dias corridos sem nenhuma ocorrência de erros no enlace contratado. A este período sem ocorrência de falhas, denominaremos “Período No-failures”.

14.4.1. Período No-failures: quando todas as pendências forem retiradas, será marcado o início de um período que se estenderá por 10 (dez) dias, no qual a solução não deverá apresentar falhas de projeto/especificação. Este período será reiniciado sucessivamente todas as vezes que for detectada alguma falha, adiando assim a conclusão do PFE.

14.5. Ao final do PFE, concluído com sucesso, será emitido o Termo de Recebimento Definitivo (TRD), pela Comissão de Recebimento do PRODERJ.

14.6. A emissão do TRD não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas.

15. MODELO DE PRESTAÇÃO DOS SERVIÇOS

15.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

15.2. O modelo de prestação de serviços conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo CONTRATANTE, tais como

abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas pró-ativamente pela CONTRATADA, por meio do serviço de gerência da rede. A prestação dos serviços englobará prazos e condições da entrega da solução, incluindo requisitos de implantação e migração da solução.

15.3. Os níveis mínimos de serviço contratados, apresentados nos Níveis Mínimos de Serviços (NMS) serão registrados e monitorados pela CONTRATADA e o CONTRATANTE, e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade. Essa condição será fundamento para efetuar os pagamentos previstos, durante toda a vigência do contrato.

15.4. Os pagamentos serão efetuados, mensalmente, em moeda corrente nacional e em até 15 (quinze) dias úteis após apresentação das notas fiscais. Os critérios detalhados para o pagamento mensal estão definidos no Termo de Referência.