PRESIDÊNCIA DA REPÚBLICA

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO(ETP) - TI

Processo nº 00094.000498/2020-61

Histórico de Revisões

Data	Versão	Descrição	Autor
27/10/2020	1.0	Finalização da primeira versão do documento	Robson Martins Guimarães da Silva

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1 - IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

As funções finalísticas exercidas pela Presidência da República exigem o provimento contínuo de acesso pleno e irrestrito às informações de relevância nacional e internacional, as quais muitas vezes são divulgadas e acessadas por meio das mais diversas mídias eletrônicas. Em adição, grande parte dos sistemas de informação que são utilizados para a realização de atividades da área meio e da área fim da Presidência da República são realizadas com o uso da Internet.

Considerando a natureza *sui generis* da Presidência da República como órgão da estrutura governamental do Brasil, seus requisitos de comunicação podem exigir níveis de segurança, de controle e de qualidade acima da média e dos padrões que costumam ser contratados por boa parte dos órgãos governamentais. Assim, a Presidência da República decidiu adotar a estratégia de se tornar *Autonomous System*, passando de mera usuária a partícipe no controle e planejamento de suas comunicações de dados e voz no Sistema de Internet Global.

Como parte deste planejamento e controle, diversas melhorias e incrementos de qualidade de serviço vêm sendo implantados pela Diretoria de Tecnologia no âmbito da infraestrutura de redes e de telecomunicações de dados. Tal conjunto engloba a readequação dos meios de provimento de interligação da Presidência da República com a Internet. Considerando que tal interligação precisa ser provida a diversos sites que compõem a área de atendimento dos serviços de Tecnologias da Informação e Telecomunicação, fornecidos pela Diretoria de Tecnologia com padrões de qualidade e segurança elevados, propõe-se novo processo de contratação de Serviço de Comunicação Multimídia (SCM) contemplando o tráfego de dados, voz e vídeo, provido com tecnologia do tipo *VPN IP/MPLS* (Virtual Private Network - Multiprotocol Label Switching) ou semelhante, para atendimento aos escritórios de representações regionais, Link de Provimento de Acesso a Internet com proteção de ataque contra negação de serviço, provimento de equipamentos e serviços necessários à implantação dos acessos aos concentradores e *Link de Provimento de Acesso a Internet* eventual em todo Território Nacional, para o atendimento de deslocamentos presidenciais quando solicitado.

Em virtude da necessidade de que esse provimento seja ininterrupto, torna-se necessário que em parte dos sites (prédios/palácios) da Presidência da República haja atendimento redundante. Parte destes locais é atendido atualmente por meio da interligação com a INFOVIA, provida por meio de contratação com o SERPRO, sem que haja, em futuro próximo, qualquer outra forma de atendimento redundante eficiente e adequado em qualidade e capacidade que não seja por meio de nova contratação.

Diante disso, trata-se da aquisição de 2 (dois) roteadores BGP (*Border Gateway Protocol*), com o objetivo de implementar uma arquitetura de redundância de equipamentos na interconexão da rede interna da Presidência da República com a redes externas, atendida pelos contratos de Conectividade IP, MPLS, MetroEthernet, de diversos provedores, atendimento de VPN´s, conforme figura abaixo.

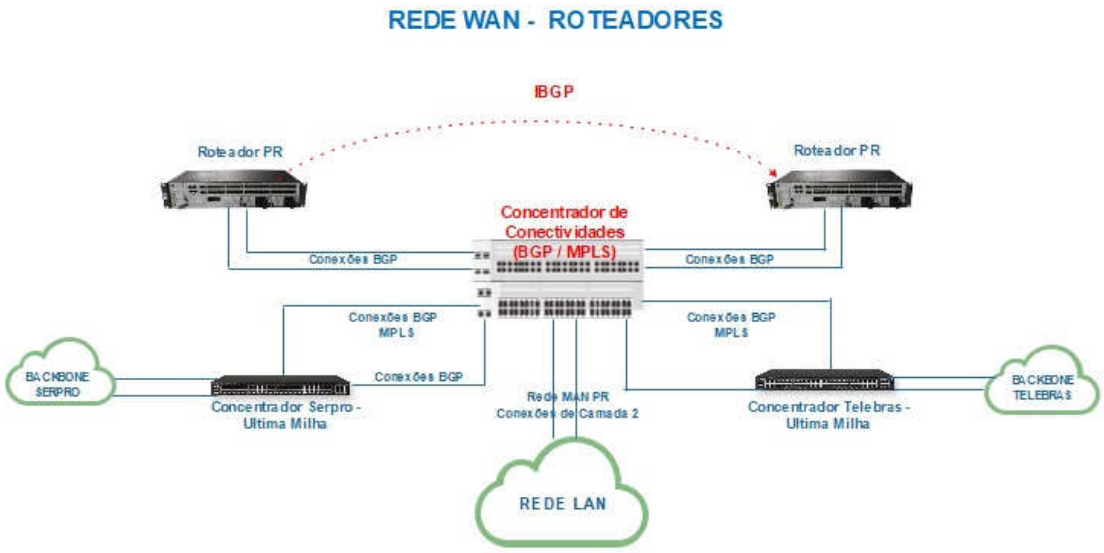

FIGURA 01

1.2 - IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

O objeto de estudo é a aquisição de 2 (dois) roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses, incluindo licenças, suporte técnico, projeto de instalação e configuração dos equipamentos de modo que a Presidência da República do Brasil opere como Sistema Autônomo (AS).

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
01	ROTEADOR DE BORDA COM GARANTIA/SUPORTE TÉCNICO ON-SITE DE 05 (CINCO) ANOS E LICENÇAS	UNIDADE	2
02	PROJETO, INSTALAÇÃO E CONFIGURAÇÃO	SERVIÇO	1

ESPECIFICAÇÃO TÉCNICA MÍNIMA DOS ROTEADORES

INSTALAÇÃO

O equipamento deverá ser montável em rack de 19'', tendo sua altura máxima de 4RUs, devendo este vir acompanhado dos devidos acessórios necessários para instalação.

FONTE DE ALIMENTAÇÃO

O equipamento deve operar nas tensões entre 100 e 240 VCA / 60 Hz, selecionáveis automaticamente;

O equipamento deve possuir, no mínimo, 2 (duas) fontes de alimentação, operando na configuração N+1, ou seja, em caso de falha de uma das fontes o roteador deve permanecer suportando sua capacidade máxima;

A troca de fontes de alimentação deve ser hot-swappable;

Implementar de forma nativa mecanismo de monitoramento e detecção de falhas em suas fontes de alimentação individuais;

A fonte de energia deve vir acompanhada com cabo de energia com 1,80 metros de comprimento mínimo e tomada padrão NBR 14136;

O plugue do cabo de alimentação deverá seguir o padrão brasileiro, conforme estabelece a norma NBR 14136, ou, alternativamente, deverá ser fornecido adaptador para esse padrão.

REFRIGERAÇÃO

O Subsistema de ventilação deve ser redundante, operando na configuração N+1, ou seja, em caso de falha de um dos ventiladores o roteador deve permanecer suportando sua capacidade máxima;

O equipamento deve implementar de forma nativa mecanismo que viabilize detecção de falhas nos principais componentes do subsistema de ventilação;

O equipamento deve implementar de forma nativa mecanismos dos principais componentes do subsistema de ventilação bem como de seus parâmetros de funcionamento;

Deve ser capaz de adaptação automática da velocidade de rotação em função da temperatura do equipamento.

CPU E MEMÓRIA

Deverá possuir configuração de CPU e quantidade necessária de memória DRAM e memória auxiliar que atenda, simultaneamente, a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do fabricante;

Deverá suportar o armazenamento de múltiplas imagens de *software* e configuração (mínimo de 2 imagens e 2 configurações);

Deverá permitir selecionar a imagem de *software* que será utilizada na próxima inicialização;

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;

Deverá permitir selecionar a configuração que será utilizada na próxima inicialização;

Deverá possuir no mínimo 8GB de memória DRAM ou SDRAM, expansível até 16GB, mediante necessidade da Contratante. Caso o equipamento não permita o upgrade especificado, deve ser fornecido já com a capacidade máxima requerida.

Os planos de encaminhamento (forwarding plane) e controle (control plane) devem ser completamente independentes;

CONDIÇÕES DO AMBIENTE

Deve operar em temperatura ambiente entre 10 e 40°C;

Deve ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação), permitindo, por um curto período, funcionamento com umidade relativa de 5% a 85%.

Deve suportar temperatura ambiente de armazenamento entre 0 e 50°C.

FERRAMENTAS DE ATUALIZAÇÃO E TRANSFERÊNCIA DE ARQUIVOS

Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces *ethernet* e serial;

Deve ter a capacidade de atualização de *software* via FTP e via TFTP, em conformidade com a RFC 783 ou RFC 1350;

Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (*Secure Copy*) ou SFTP (*Secure FTP*).

FERRAMENTAS DE CONFIGURAÇÃO

Implementar Telnet e SSH para acesso à interface de linha de comando;

Ser configurável e gerenciável via 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;

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;

Deve permitir a criação de versões de configuração e suporte a "*rollback*" da configuração para versões anteriores.

FERRAMENTAS DE COLETA DE FLUXO

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; e

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 (NetFlow v9 ou SFlow ou JFlow ou HFlow) padronizado;

Deve ser possível definir uma taxa de amostragem para coleta de fluxos, sendo possível uma taxa configurável de 1:1 até 1:10000 fluxos.

CAMADA DE ENLACE

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:

Deve ser permitida a configuração dessa seleção de forma dinâmica;

Implementar, no mínimo, 128 VLANs simultaneamente;

Deverá implementar *link agreggation* padrão IEEE 802.3ad com suporte a LACP padrão IEEE 802.1ax, para interfaces 1Gbps e 10 Gbps;

Deverá implementar a funcionalidade de auto negociação de taxa de transmissão (10/100/1000) e de modo de transmissão (half/full-duplex) e Auto-MDIX (Automatic Media Dependent Interface Crossover) para portas Gigabit Ethernet.

Deverá suportar protocolos de controle de *loop*, tais como:

Padrão IEEE 802.1d (STP – Spanning Tree).

Padrão IEEE 802.1w (RSTP – Rapid Spanning Tree).

Padrão IEEE 802.1s (MSTP – Multiple Spanning Tree).

CAMADA DE REDE

Deve permitir o roteamento nível 3 entre as VLANs;

Deverá suportar jumbo *frames* (até 9012 *bytes*);

Deverá implementar a autonegociação;

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;

Deverá implementar o protocolo de roteamento OSPF com, no mínimo, as seguintes características:

RFC 2328 - OSPF *Version* 2;

RFC 4750 - OSPF Version 2 Management Information Base;

RFC 3101 - OSPF *Not-So-Stubby Area* (NSSA) *Option*;

RFC 3137 - OSPF *Stub Router Advertisement*.

RFC 2740 ou 5340 - OSPF for IPv6;

RFC 3623 - *Graceful* OSPF *Restart*;

RFC 5187 - OSPFv3 *Graceful Restart.*

Deverá implementar Capacidade de pelo menos 3 áreas OSPFv2;

Deverá implementar autenticação MD5 de sessões OSPFv2 e OSPFv3.

Deverá implementar o protocolo de roteamento BGP versão 4 com, no mínimo, as seguintes características:

RFC 3065 - Autonomous System Confederation for BGP;

RFC 1966 - BGP *Route Reflection - An Alternative to Full Mesh* IBGP;

RFC 1997 - BGP *Communities Attribute*;

RFC 2385 - *Protection of BGP Sessions via the* TCP MD5 *Signature Option*;

RFC 2439 - *BGP Route Flap Damping*;

RFC 3392 - Capabilities Advertisement with BGP-4;

RFC 4760 - Multi-Protocol Extensions for BGP-4;

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

RFC 3065 - *Autonomous System Confederations for* BGP;

RFC 4271 - *A Border Gateway Protocol* 4 (BGP-4);

RFC 4456 - *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP).*

RFC 4724 – BGP Gracefull Restart

RFC 4360 - BGP BGP Extended Communities Attribute

Implementar protocolo de roteamento Multiprotocol BGP com suporte a IPv6;

Deverá implementar autenticação MD5 entre os peers BGP;

Permitir limitar a quantidade de rotas recebidas por peer BGP;

Implementar o protocolo BFD para BGP, através de interfaces físicas e lógicas (inclusive túneis GRE);

Implementar roteamento baseado em políticas (Policy Based Routing) com suporte a IPv4 e IPv6, permitindo a definição de políticas de roteamento baseadas em endereços de origem e outras condições especiais;

Com a configuração máxima de memória suportada, deve suportar, no mínimo, 4.000.000 (quatro milhões) de rotas IPv4 e 300.000 (trezentas mil) rotas ou IPv6 simultaneamente na tabela RIB (Routing Information Base);

Deve suportar, no mínimo, 2.000.000 (duas milhões) rotas IPv4 e 200.000 (duzentas mil) rotas IPv6 simultaneamente na tabela FIB (Forwarding Information Base);

Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 3768, ou mecanismo similar de redundância de gateway;

Deve suportar mecanismo de autenticação MD5 entre os peers VRRP;

Deve implementar, no mínimo, 50 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente;

Deverá implementar redistribuição controlada de rotas entre diferentes protocolos.

Deverá ser possível controlar os tipos de rotas que serão redistribuídas;

Permitir a virtualização das tabelas de roteamento VRF (Virtual Routing and Forwarding);

Deve suportar a criação de, no mínimo, 10 tabelas de roteamento virtuais (VRF);

Deve suportar o protocolo MPLS (Label Distribution Protocol, MPLS Virtual Private Network, MPLS QoS, MPLS Traffic Engineering), em

conformidade com, no mínimo, os padrões RFC 2547, 2702, 3031, 3032, 5036, 3107 e 3270;

Implementar mecanismo de controle de *Multicast* através de:

RFC 1112 - *Host Extensions for IP Multicasting*;

RFC 2236 - *Internet Group Management Protocol, Version* 2;

RFC 3376 - *Internet Group Management Protocol, Version* 3;

RFC 2362 - *Protocol Independent Multicast - Sparse Mode* (PIM-SM);

RFC 3569 - *Protocol Independent Multicast - Source-Specific Multicast* (PIM-SSM);

RFC 3973 - *Protocol Independent Multicast - Dense Mode* (PIM-DM);

PIM-SM sobre VRF.

Deve implementar o NAT em conformidade com a RFC 1631 e RFC 3022;

Deve suportar traduções de endereços de rede IPv4 em IPv4 (NAT44) e traduções de endereços de rede IPv4 em IPv6 (NAT64) simultaneamente;

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

PROTOCOLOS DE SERVIÇO

Implementar o protocolo NTPv3 (*Network Time Protocol* versão 3) conforme definições da RFC 1305;

Implementar servidor DHCP de acordo com a RFC 2131 (*Dynamic Host Configuration Protocol*) permitindo a atribuição de endereços IP a estações a partir do roteador;

Suportar "*BOOTP relay agents*" de acordo com a RFC 2131 (*Dynamic Host Configuration Protocol*), permitindo a atribuição de endereços IP a estações localizadas na rede local a partir de um servidor DHCP localizado em uma rede remota;

Deve suportar o padrão IEEE 802.1p para cada porta;

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;

Deverá suportar classificação e marcação de pacotes baseadas em VLAN ID;

Deve suportar a classificação, marcação e remarcação baseadas em CoS (*Class of Service*) para a camada de enlace;

Suportar funcionalidades de QoS de *Traffic Shaping* e *Traffic Policing*;

Deve ser possível a especificação de garantia 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; e descarte do pacote.

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 2474 e RFC 2475;

Deverá implementar RFC 2598 *DiffServ Expedited Forwarding* (EF);

Deverá implementar RFC 2597 *DiffServ Assured Forwarding* (AF);

Deve suportar a classificação, marcação e remarcação baseadas em CoS (*Class of Service*) e DSCP, conforme definições do IETF (*Internet Engineering Task Force*);

Deverá implementar aplicação de políticas de QoS em todas as portas físicas do equipamento.

Implementar RTP (Real-Time Transport Protocol) e a compressão do cabeçalho dos pacotes RTP (IP RTP Header Compression).

REQUISITOS DE GERÊNCIA

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 algoritmo de criptografia AES.

Suportar SNMP sobre IPv6;

Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213;

Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento como: tráfego de interfaces, uso de CPU do processador, uso de memória, QoS, serviços, etc.;

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;

Deverá implementar Syslog Local e comunicação com Syslog Remoto;

Deverá permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao elemento de rede via Telnet ou SSH, possibilitando a definição dos endereços IP de origem das respectivas sessões. O acesso gerencial remoto aos equipamentos deverá ser provido através dos protocolos seguros SSHv2 e HTTPS.

Deve suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs.

Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

SEGURANÇA

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um servidor de Autenticação/Autorização do tipo TACACS e/ou RADIUS:

Deverá implementar RFC 2865 RADIUS *Authentication*;

Deverá implementar RFC 2866 RADIUS *Accounting*;

Deverá implementar definição de grupos de usuários, com diferentes níveis de acesso;

Deverá permitir o controle dos comandos que cada usuário ou grupos de usuários poderão enviar;

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;

Implementar mecanismos de AAA (*Authentication*, *Authorization* e *Accounting*) com garantia de entrega.

Todos os comandos de administração do equipamento, executados por qualquer dos meios de acesso: interface de console, Telnet, SSH, HTTP, HTTPS deverão ser individualmente autorizados e registrados ("Accounting") por este protocolo de controle de acesso administrativo;

Implementar anti-spoofing para IPv4 e IPv6 através de verificação Reverse Path Forwarding (RPF).

LISTAS DE ACESSOS

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;

Deverá implementar contadores para as listas de acesso;

Deverá implementar listas de acesso para o tráfego entrante e sainte;

Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao equipamento via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

FUNCIONALIDADES DE VPN

Suportar serviços de VPN baseados no padrão IPSec (IP *Security Protocol*), compatível com IPv4 e IPv6;

Suportar serviços de VPN baseados no padrão IKE (*Internet Key Exchange*);

Implementar IKE v1 e v2;

Deve suportar criação de VPNs através do conjunto de especificações IPSec.

Devem ser suportadas, no mínimo, as RFC´s:

RFC 4869 - Suite B Cryptographic Suites for IPsec;

RFC 2401 - Security Architecture for the Internet Protocol;

RFC 2402 - IP Authentication Header;

RFC 2406 - IP Encapsulating Security Payload (ESP);

RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP;

RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP) ;

RFC 2409 - The Internet Key Exchange (IKE);

Devem ser suportados, no mínimo, os algoritmos DES (56 bits), 3DES (168 bits), AES-128 e AES-256 para garantia de confidencialidade às conexões IPSEC;

Suportar criação de VPNs de acordo com o conjunto de padrões IPSEC em modo túnel;

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;

Suportar o tráfego protocolo GRE sobre IPSEC;

Suportar o tráfego de IP *Multicast* sobre IPSEC;

Deve permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e túneis IPSEC.

Suporte ao protocolo de Tunelamento GRE (*General Routing Encapsulation* - RFC 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, devendo ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.

REQUISITOS DE INTERFACE

Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS232, com conector RJ45 ou DB9 ou uma porta de console com interface USB;

Possuir no mínimo 06 (seis) interfaces Gigabit-Ethernet, no padrão **SFP** e 04 (quatro) interfaces XGigabit-Ethernet, no padrão **SFP +**;

Deve suportar módulos com interfaces compatíveis com os padrões IEEE 802.3ab (1000BASE-T), IEEE 802.3z (1000BASE-SX, 1000BASE-LX/LH) e IEEE 802.3ae (10GBASE-SR, 10GBASE-LR, e 10GBASE-ER).

Deve suportar módulos 1000BASE-X e 10GBASE-X, para comunicações 1Gbps e 10Gbps em distâncias de, no mínimo, 40km;

Deve ser fornecido os *transceivers* ópticos compatíveis e nas quantidades citadas abaixo:

06 (seis) do tipo 1000BASE-T;

06 (seis) do tipo 1000BASE-SX;

06 (seis) do tipo 10GBASE-LR;

06 (seis) do tipo 10GBASE-SR;

04 (quatro) do tipo 10GBASE-X.

Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo.

DESEMPENHO

Deve suportar, no mínimo, 92 (noventa e dois) Gbps de throughput com todas as funcionalidades de roteamento e segurança ativas simultaneamente para um tráfego IMIX;

Deve suportar uma taxa de comutação de pacotes de no mínimo 60 (sessenta) Mpps considerando-se pacotes de 64 bytes;

CARACTERÍSTICAS GERAIS DE *HARDWARE*

As capacidades de tráfego expressas neste documento se referem a taxas *wire-rate full-duplex* de entrada e saída simultaneamente;

Os equipamentos fornecidos deverão ter homologação da ANATEL e serem fabricados pelo mesmo fabricante;

Deverá ser informado o MTBF de todos os módulos e equipamentos fornecidos;

Deve possuir LEDs de diagnóstico que forneçam informações de alimentação (*on*/*off*) e atividade do equipamento;

Deve possuir LEDs de diagnósticos que forneçam informações e atividades das portas.

Todas as funções *Layer* 2 e *Layer* 3 deverão ser executadas localmente pelo equipamento, não sendo permitido que estas funções sejam executadas em outros módulos externos ao equipamento, devendo inclusive a interface de configuração do equipamento ser única, dispensando assim a necessidade de configuração módulo a módulo;

Deverá implementar geração de logs sobre eventos no hardware, protocolos, módulos e interfaces;

Todos os requisitos, com exceção daqueles de capacidade (prefixos IP e MAC), deverão ser atendidos de forma concomitante, ou seja, a conformidade de um requisito não pode afetar a disponibilidade dos demais.

O equipamento deverá implementar, no momento da entrega, todas as características exigidas nesta especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras;

DOCUMENTAÇÃO TÉCNICA

Deverá vir acompanhado de manual de instalação, configuração e operação do equipamento e dos módulos componentes do mesmo, na língua portuguesa ou inglesa, com apresentação de boa qualidade.

Deverão ser entregues com os equipamentos contratados:

Relação detalhada do(s) componente(s) entregues, em que constem: modelos, características, configurações, versões do(s) software(s) licenciado(s), etc.;

Os arquivos de instalação do(s) software(s) licenciado(s) e suas respectivas licenças;

Toda a documentação técnica, composta por manuais de instalação, configuração e operação, em formato digital.

2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Estima-se a aquisição de 2 (dois) roteadores, conforme requisitos técnicos estabelecidos, para instalação em paralelo na arquitetura de rede planejada da Presidência da República.

Hoje a Presidência da República não detêm em seu patrimônio nenhum roteador BGP, fazendo uso de um roteador alugado, no

âmbito do Contrato nº 27/2020.

3 – ANÁLISE DE SOLUÇÕES

Para o objetivo desejado, verificam-se 3 (três) possíveis solução demanda:

Solução 01 - Aquisição de roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses.

Está opção considera a aquisição de roteadores BGP. Com a aquisição, esta solução viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República nos equipamentos adquiridos, possibilitando a pronta tomada de decisão e ação em eventos de riscos ou falhas.

Está opção viabiliza a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P., com a dupla abordagem de equipamentos de redes, possibilitando a desativação do aluguel de 01 roteador do atual contrato de conexão de Internet (Contrato nº 27/2020 - Telebrás).

Solução 02 - Utilização do Firewall como roteadores BGP (*Border Gateway Protocol*).

Está opção considera o uso do Firewall exercendo as funções de roteadores BGP.

O Firewall da Presidência da República é um Firewall UTM, que possibilita a configuração de algumas funções de roteador. Contudo o hardware não foi projetado para executar todas as funcionalidades específicas requerida por um roteador BGP, mas que eventualmente poderia ser utilizados como um backup em caso de falhas, o que será superado com a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P.

Solução 03 - Aluguel de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas.

Está opção já vem sendo utilizado dentro dos Contratos de conexão de Internet (Contrato nº 54/2017 e nº 27/2020 - Telebrás). Contudo, esta solução tem inviabilizado a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República no equipamento, o que restringe a decisão e tomada de ação em eventos de riscos ou falhas.

Está opção não viabiliza a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P., com a dupla abordagem de equipamentos de redes, pois o atual Contrato apenas prevê o aluguel de 01 roteador.

3.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução
1	**Aquisição** de roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses.
2	**Utilização** do Firewall como roteadores BGP (*Border Gateway Protocol*).
3	**Aluguel** de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas.

3.2 – ANÁLISE COMPARATIVA DAS SOLUÇÕES

Em análise comparativa, a **Solução 1** é a opção viável para Presidência da Republica, pois viabiliza a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P., com a dupla abordagem de equipamentos de redes, bem como viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República nos equipamentos adquiridos, possibilitando a pronta tomada de decisão e ação em eventos de riscos ou falhas.

A Solução 2 não é tecnicamente viável, pois a solução de Firewall não suportaria a necessidade da Presidência da República, pois não foi projetado para executar todas as funcionalidades específicas requerida por um roteador BGP, mas que eventualmente poderia ser utilizados como um backup em caso de falhas, o que será superado com a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P.

A Solução 3 não viabiliza a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P., com a dupla abordagem de equipamentos de redes e não viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República no equipamento, o que restringe a decisão e tomada de ação em eventos de riscos ou falhas.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2		X	

	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

4 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

N/A

5 – ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Solução Única

Descrição:

Aquisição de 02 (dois) roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses, incluindo licenças, suporte técnico, projeto de instalação e configuração dos equipamentos.

Custo Total – Memória de Cálculo

Pesquisa de Preço:

01) **Painel de Preço** - Foi realizada pesquisa de preço no Painel de Preço utilizando o CATMAT 104620, em que foram identificados diversos registros de aquisições, contudo, após análise foram identificado apenas 1 edital de aquisição de roteadores, sendo este a Contratação Similar identificada (Pregão eletrônico nº 975/2020/Serpro). Os demais valores identificados no Painel de Preço não atendem as especificações da aquisição da Presidência da República.

02) **Contratação Similar** - Foi identificado o Pregão eletrônico nº 975/2020/Serpro, no item 13 grupo 4 do Edital nº 975/2020 do Serpro, considerando que o valor adjudicado deve ser divido por 4 para obter o valor unitário para o item. Neste edital não a o serviço especifico para o projeto, instalação e configuração.

03) **Fornecedores** - Foram consultados diversos fornecedores de diferentes fabricantes. As propostas enviadas compõem o Mapa Comparativo de Pesquisa de Preço.

Diante do exposto, **considerando o critério de menor preço para fornecedor,** estima-se o **custo único total** da solução de R$ 276.200,00 (duzentos e setenta e seis mil, duzentos reais).

5.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

DESCRIÇÃO DA SOLUÇÃO	ESTIMATIVA DE TCO AO LONGO DOS ANOS					TOTAL
	ANO 2020	ANO 2021	ANO 2022	ANO 2023	ANO 2024	
SOLUÇÃO ÚNICA	R$ 276.200,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 276.200,00

6 – DESCRIÇÃO DE SOLUÇÃO DE TIC A SER CONTRATADA

Aquisição de 2 (dois) roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses, incluindo licenças, suporte técnico, projeto de instalação e configuração dos equipamentos.

7 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Estimativa de custo único total da solução de R$ 276.200,00 (duzentos e setenta e seis mil, duzentos reais).

8 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

O presente estudo técnico preliminar evidenciou que a contratação garantirá o atendimento às necessidades, sendo viável do ponto de vista técnico e de negócio, aguardando a pesquisa de preço para definição da solução mais vantajosa.

9 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 129, de 12 de maio de 2020, SEI nº 1881485. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnico e Requisitante e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ Robson Martins Guimarães da Silva Matrícula/SIAPE: 1478592 Brasília, 27 de outubro de 2020	_____ Marcelo Abrunhosa Hipólito Matrícula/SIAPE: 1488703 Brasília, 27 de outubro de 2020

AUTORIDADE MÁXIMA DA ÁREA DE TIC
(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)

_____
Maria Clotilde Prado
Matrícula/SIAPE: 1210670
Brasília, 27 de outubro de 2020

Documento assinado eletronicamente por **Marcelo Abrunhosa Hipolito**, **Assistente (GR IV)**, em 29/10/2020, às 12:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Robson Martins Guimarães da Silva**, **Chefe de Divisão**, em 29/10/2020, às 14:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Maria Clotilde Prado**, **Diretor(a) substituto(a)**, em 29/10/2020, às 18:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida informando o código verificador **2166866** e o código CRC **32A7E969** no site: https://sei-pr.presidencia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00094.000498/2020-61 SEI nº 2166866