

Apêndice II

1. ACORDO DE NÍVEIS DE SERVIÇO (ANS)

A fiscalização terá por base o contido nas métricas dispostas nas tabelas de 1 a 7, abaixo:

Indicador: Disponibilidade do enlace		
Descrição do Indicador	Percentual de tempo, durante o período do mês de operação, em que um enlace (incluindo o CPE) venha a permanecer em condições normais de funcionamento.	
Fórmula de Cálculo	$PM = \frac{(T_0 - \sum T_v)}{T_0} \cdot 100$ Onde: • PM = Percentual Medido; • T₀ = período de operação (um mês) em minutos; e • $\sum T_v$ = somatório dos períodos de tempo em que a métrica for considerada violada, excluindo os casos previstos no TR. No caso de intermitência do serviço, deve-se considerar como tempo de todo o período compreendido entre a primeira violação da métrica e o evento de operacionalização completa do serviço, confirmada após um período de 3 (três) horas sem violações. No caso de inoperância recorrente num período inferior a 3 (três) horas, contado a partir do restabelecimento do enlace da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o enlace estiver totalmente operacional. A indisponibilidade de dados de gerência (coleta não realizada, dados não acessíveis, etc.) será considerada como indisponibilidade do serviço, caso isto implique perda de dados de gerenciamento. Os tempos de inoperância serão os tempos em que os enlaces apresentarem problemas caracterizados pela abertura de chamados técnicos (<i>Trouble Ticket</i>) indicando inoperância, em função de qualquer violação dos limiares de qualidade dos seguintes indicadores: retardo e/ou de taxa de erro de bit e/ou de perda de pacotes. Somente serão desconsiderados os tempos de inoperância, causados por manutenções programadas com a CONTRATANTE, ressalvados, contudo, os casos fortuitos e de força maior.	
Periodicidade de Aferição	Mensal.	
Limiar de Qualidade	Classificação dos enlaces	Disponibilidade mensal mínima (em %)
	D1	99.8% (1.4h de indisponibilidade máxima)
	D2	99.5% (3.5h de indisponibilidade máxima)
	D3	99.17% (6.0h de indisponibilidade máxima)

Pontos de Controle	A CONTRATADA deverá disponibilizar mensalmente ao CONTRATANTE um relatório com os índices apurados por backbone Principal naquele mês. Esse relatório será composto pelo resultado dos testes remotos obtidos nos ativos, devendo evidenciar os períodos de violação do teste. Para os PP, sempre que solicitado pela CONTRATANTE, poderá ser realizada a aferição.
Relatórios de Níveis de Serviço (SLR)	A CONTRATADA deverá disponibilizar, quando solicitado pela CONTRATANTE, relatórios com os índices apurados diariamente, totalizados e apresentados mensalmente por enlace.

Tabela 1: Indicador de Disponibilidade do Enlace

Indicador: Taxa de erro de bit	
Descrição do Indicador	A Taxa de Erro de Bit (TxErr) é definida como a relação entre a quantidade de bits corretamente transmitidos para cada bit transmitido com erro em um determinado enlace pertencente a rede de acesso. A taxa de erro de bit deverá ser medida por solicitação da CONTRATANTE.
Fórmula de Cálculo	$TxErr = BErr/Btot$ Onde: TxErr: Taxa de Erro de Bit BErr = Número de bits enviados com erro no período de aferição (5 minutos) BTot = Número total de bits enviados no período de aferição (5 minutos) O cálculo da TxErr será realizado por solicitação da CONTRATANTE para os enlaces com problemas no meio físico de transmissão da rede de acesso, durante o período de maior tráfego (utilização).
Periodicidade de Aferição:	Sempre que solicitado pela CONTRATANTE, poderá ser realizada a aferição da taxa de erro de bit de um determinado enlace, através de equipamento de teste especializado. A CONTRATADA deverá avaliar a medida da taxa de erro de bit por 5 minutos nos horários de maior tráfego. A CONTRATADA deverá atender a essas solicitações em, no máximo, 4 horas para qualquer enlace.
Limiar de Qualidade	Classificação dos enlaces
	Taxa de erro de Bit – BER (bits/s)
	D1  1×10^{-6}
	D2  1×10^{-6}
	D3  1×10^{-6}
	Nota: Para os enlaces via rádio será considerada a taxa de erro de bit máxima de 1×10^{-6} . A taxa de erro de bit para os enlaces que se interligam a VPN do Backbone principal será no máximo de 1×10^{-6} .
Pontos de Controle	Medições a serem realizadas pela CONTRATADA, permitindo auditoria pela CONTRATANTE para aferição dos valores deste indicador.
Relatórios de Níveis de Serviço (SLR)	A CONTRATADA deverá disponibilizar, quando solicitado pela CONTRATANTE, relatórios com os valores medidos da Taxa de erro de bit por enlace.

Tabela 2: Indicador de Taxa de Erro de Bit

Indicador: Perda de Pacotes

Descrição do Indicador	Representa a quantidade de pacotes perdidos fim a fim. É medida em percentual, tomando como referência o volume total de pacotes que alcançaram o destino (medido na interface LAN do CPE do terminal de destino) dentre o volume total de pacotes transmitidos (medido na interface LAN do CPE do terminal de origem).
Fórmula de Cálculo	$TPP = [(NP_{origem} - NP_{destino}) / NP_{origem}] * 100$ Onde: TPP = Taxa de Perda de Pacotes NP_{origem} = N° de pacotes na origem $NP_{destino}$ = N° de pacotes no destino
Periodicidade de Aferição:	Sempre que a CONTRATANTE julgar necessário, poderá ser solicitada a medição do percentual de perda de pacotes fim a fim, através de equipamento de teste especializado. A CONTRATADA deverá avaliar a medida do percentual de perda de pacotes por 5 minutos nos horários de maior tráfego. A CONTRATADA deverá atender a essas solicitações em, no máximo, 4 horas
Limiar de qualidade	Menor ou igual a 2 %
Pontos de Controle	Medições a serem realizadas pelo Provedor, permitindo auditoria pela CONTRATANTE para aferição dos valores deste indicador.
Relatórios de Níveis de Serviço (SLR)	A CONTRATADA deverá disponibilizar, quando solicitado pela CONTRATANTE, relatórios com os valores das medições solicitadas, referentes ao percentual de perda de pacotes.

Tabela 3: Indicador de Perda de Pacotes

Indicador: Retardo da rede	
Descrição do Indicador	Entende-se com retardo da rede o tempo gasto entre a transmissão do primeiro bit de um pacote até a recepção do último bit do mesmo pacote, em apenas um dos sentidos da transmissão de dados.
Fórmula de Cálculo	A apuração do retardo na rede da CONTRATANTE será efetuada com o envio de pacotes ICMP de tamanho fixo de 32 octetos de dados, entre terminais de origem e destino localizados em OM da rede dentro do mesmo <i>backbone</i> (principal ou regional) e retornando à origem onde será realizada a medição do tempo de resposta destes pacotes. Como o tempo de resposta corresponde ao tempo de ida e volta do pacote, o tempo de retardo será considerado como o tempo de resposta dividido por dois. $\text{Retardo} = \text{Tempo}_{\text{Resposta}} / 2$ O tempo de resposta limite a ser aguardado para cada pacote deverá ser de 5 segundos. Valores superiores a este tempo serão considerados "timeout". Portanto, a ocorrência de <i>timeout</i>, deverá ser considerada quando o tempo de resposta atingir o valor de 6 segundos. Cada medida deverá ser realizada através do envio de uma série de 4

	pacotes ICMP por vez. O valor instantâneo do retardo referente a uma medida será igual à média aritmética dos quatro valores dos tempos de resposta referentes à série de pacotes ICMP enviados, dividida por dois, pois será considerado o retardo apenas em um dos sentidos da comunicação. $\text{Valor}_{\text{Medida}} = \frac{\sum_{i=1}^4 \text{Retardo}_i}{4}$ Os intervalos de observação deverão ser de 10 minutos no horário entre 07h e 12h00 e entre 14h00 e 19h00. Todos os resultados obtidos através das medições deverão ser disponibilizados e considerados no indicador diário de Retardo. Os valores das médias diárias das medidas deverão ser inferiores ao valor estabelecido para o Retardo máximo permitido (limiar de qualidade).
Periodicidade de Aferição	Diária
Limiar de Qualidade	Retardo máximo permitido para as seguintes comunicações. Enlaces terrestres: 80 ms Enlaces com satélite: 850 ms
Pontos de Controle	Medições a serem realizadas pela CONTRATADA, permitindo auditoria pela CONTRATANTE para aferição dos valores deste indicador.
Relatórios de Níveis de Serviço (SLR)	A CONTRATADA deverá disponibilizar mensalmente, quando solicitado pela CONTRATANTE, um relatório com os diversos valores apurados. Os relatórios deverão fornecer os valores diários medidos e as médias de retardo para cada enlace. A CONTRATADA deverá apresentar no prazo máximo de 24 (vinte e quatro) horas após a solicitação da CONTRATANTE, relatórios diários com os valores de Retardo para medição realizada, com a finalidade de acompanhamento, averiguação ou auditoria.

Tabela 4: Indicador de Retardo da Rede

Indicador: Prazo de reparo/restabelecimento de um enlace		
Descrição do Indicador	Prazo limite para reparo/restabelecimento de um enlace (com 100% de operabilidade ou pleno), na ocorrência de inoperância ou falha.	
Fórmula de Cálculo	Apuração do tempo de restabelecimento de um enlace, a partir de consulta na base de dados relativa a solução de gerenciamento da CONTRATADA e comparação com o valor descrito no Limiar de Qualidade deste indicador.	
Periodicidade de Aferição	Mensal.	
Limiar de Qualidade	Classificação dos enlaces	Prazo limite para reparo/restabelecimento permitido (em horas)
	D1	6
	D2	6

	D3	* Nota
	* Nota: para estes níveis de serviço, os prazos limites dependem das distâncias das unidades prediais da CONTRATANTE à capital de sua Unidade da Federação – UF, conforme tabela a seguir:	
	Localização do Ponto de Presença	Prazo limite (em horas)
	Nas cidades sede	6
	Até 100 Km da cidade sede	6
	Até 300 Km da cidade sede	8
	Acima de 300 Km da cidade sede	12
Pontos de Controle	Solicitações abertas na Central de Atendimento da CONTRATADA para reparo de um enlace.	
Relatórios de Níveis de Serviço (SLR)	A CONTRATADA deverá, quando solicitado, disponibilizar mensalmente à CONTRATANTE relatório com os valores apurados, por enlace. Os relatórios deverão fornecer, para cada unidade predial, os valores de tempo de atendimento gasto para reparo/restabelecimento do enlace com indicação das violações dos prazos e consolidação mensal por unidades prediais.	

Tabela 5: Indicador de Prazo de Reparo/Restabelecimento de um Enlace

Indicador: Prazo para Alteração da Taxa de Transmissão de um Enlace		
Descrição do Indicador	Prazo máximo para alteração da taxa de transmissão de um enlace, mediante solicitação da CONTRATANTE. A alteração de transmissão deverá incluir a atualização das informações do enlace na solução de gerência.	
Fórmula de Cálculo	Tempos para alteração da taxa de transmissão de um enlace	
Periodicidade de Aferição	A partir de solicitação da CONTRATANTE	
Limiar de Qualidade	Classificação das Unidades Prediais	Prazo máximo em dias corridos
	D1	15
	D2	15
	D3	15
	Os prazos máximos se referem à taxa de transmissão pretendida. Para atendimento das solicitações de alteração da taxa de transmissão de um enlace, o prazo poderá ser acrescido de 15 dias corridos quando houver necessidade de alterações nas composições dos acessos (acréscimo de hardware, obras civis, troca de equipamentos de terminação/instalação de novos hardwares). A CONTRATADA só fará jus ao acréscimo caso posicione formalmente a CONTRATANTE a respeito da necessidade de alteração na composição dos acessos no máximo 5 (cinco) dias corridos após a data da solicitação da CONTRATANTE.	
Pontos de Controle	Solicitação formal da CONTRATANTE à CONTRATADA. No caso de aplicação de multas e penalidades, considerar-se-á sempre o	

	nível de serviço a ser implementado, independentemente do nível original do enlace.
Relatórios de Níveis de Serviço (SLR)	x-x-x-x-x

Tabela 6: Indicador de Alteração da Taxa de Transmissão

Indicador: Prazo de Atendimento a Novos Endereços (Ponto Novo ou Mudança de Endereço)	
Descrição do Indicador	Prazo máximo de atendimento a solicitações de serviços para futuros endereços (nova unidade predial) ou mudança de endereço da CONTRATANTE. O prazo de atendimento a novos endereços deverá incluir a atualização das informações do enlace na solução de gerência.
Fórmula de Cálculo	Tempo para ativação de novo endereço
Periodicidade de Aferição	A partir de solicitação da CONTRATANTE
Limiar de Qualidade	A solicitação de serviço para futuro endereço (nova unidade predial ou mudança de endereço) da CONTRATANTE deverá obedecer ao prazo máximo de 30 dias corridos.
Pontos de Controle:	Solicitação formal da CONTRATANTE à CONTRATADA.
Relatórios de Níveis de Serviço (SLR):	x-x-x-x

Tabela 7: Indicador de Atendimento a Novos Endereços

2. CAPACIDADES DE EQUIPAMENTOS SD-WAN

2.1. Equipamento SD-WAN Tipo 1 – Pequenas OMs – Links até 34Mbps

- 2.1.1. Throughput de, no mínimo, 900 Mbps para Controle de Aplicação;
- 2.1.2. Throughput de, no mínimo, 4.8 Gbps para Firewall em camada 4, considerando pacotes UDP de 1518 bytes;
- 2.1.3. Suporte a, pelo menos, 700.000 (setecentos mil) sessões concorrentes TCP;
- 2.1.4. Suporte a, pelo menos, 30.000 (trinta mil) novas sessões TCP por segundo;
- 2.1.5. Deve suportar o controle de aplicações encapsuladas no protocolo TLS/SSL, garantido no mínimo de 300Mbps de throughput de SSL Inspection.
- 2.1.6. Throughput de, no mínimo, 4 Gbps de IPSEC/VPN;
- 2.1.7. Deve Suportar no mínimo, 200 clientes VPN SSL simultâneos;
- 2.1.8. Deve Suportar no mínimo, 200 VPN Ipsec site-to-site;
- 2.1.9. Possuir ao menos 5 interfaces 1 GE RJ45.
- 2.1.10. Suportar e estar licenciado para criação de no mínimo 3 instâncias virtuais;
- 2.1.11. Deve estar homologado na ANATEL até a data da licitação;
- 2.1.12. O fabricante ou o equipamento deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria), ou pela Netsecopen.org.

2.1.13. Deverá ser entregue no dia da licitação o certificado comprovando que o equipamento está em conformidade com a norma IEC e Rohs.

2.1.13.1. A solução ofertada deverá permitir que a contratante habilite as funcionalidades de segurança através de um aditivo de licença, sem a necessidade de troca de hardware. E o equipamento em questão deverá suportar o Throughput de, no mínimo, 550Mbps de Threat Protection. ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Proteção contra Malwares habilitadas simultaneamente;

2.2. Equipamento SD-WAN Tipo 2 -Medias - Maior que 34Mbps até 50Mbps

- 2.2.1. Throughput de, no mínimo, 1.7 Gbps para Controle de Aplicação;
- 2.2.2. Throughput de, no mínimo, 9.7 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;
- 2.2.3. Suporte a, pelo menos, 1.450.000 (um milhão e quatrocentos e cinquenta mil) sessões concorrentes TCP;
- 2.2.4. Suporte a, pelo menos, 35.000 (trinta e quatro mil) novas sessões TCP por segundo;
- 2.2.5. Deve suportar o controle de aplicações encapsuladas no protocolo TLS/SSL, garantido no mínimo de 650Mbps de throughput de SSL Inspection.
- 2.2.6. Throughput de, no mínimo, 6 Gbps de IPSEC/VPN;
- 2.2.7. Deve Suportar no mínimo, 200 clientes VPN SSL simultâneos;
- 2.2.8. Deve Suportar no mínimo, 200 VPN Isec site-to-site;
- 2.2.9. Possuir ao menos 10 interfaces 1 GE RJ45.
- 2.2.10. Suportar e estar licenciado para criação de no mínimo 4 instâncias virtuais;
- 2.2.11. Deve estar homologado na ANATEL até a data da licitação;
- 2.2.12. O fabricante ou o equipamento deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria), ou pela Netsecopen.org.
- 2.2.13. Deverá ser entregue no dia da licitação o certificado comprovando que o equipamento está em conformidade com a norma IEC e Rohs.
- 2.2.14. A solução ofertada deverá permitir que a contratante habilite as funcionalidades de segurança através de um aditivo de licença, sem a necessidade de troca de hardware. E o equipamento em questão deverá suportar o Throughput de, no mínimo, 750Mbps de Threat Protection. ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Proteção contra Malwares habilitadas simultaneamente;

2.3. Equipamento SD-WAN Tipo 3 - Maior que 50Mbps até 500Mbps

- 2.3.1. Throughput de, no mínimo, 12.5 Gbps para Controle de Aplicação;
- 2.3.2. Throughput de, no mínimo, 25 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;
- 2.3.3. Suporte a, pelo menos, 3.000.000 (três milhões) sessões concorrentes TCP;

- 2.3.4. Suporte a, pelo menos, 275.000 (duzentos e setenta e cinco mil) novas sessões TCP por segundo;
- 2.3.5. Deve suportar o controle de aplicações encapsuladas no protocolo TLS/SSL, garantido no mínimo de 3.8Gbps de throughput de SSL Inspection.
- 2.3.6. Throughput de, no mínimo, 12.8 Gbps de IPSEC/VPN;
- 2.3.7. Deve Suportar no mínimo, 2000 clientes VPN SSL simultâneos;
- 2.3.8. Deve Suportar no mínimo, 500 VPN Ipsec site-to-site;
- 2.3.9. Possuir ao menos 4 interfaces 10 GE SFP+, 8 interfaces 1GE SFP, e 16 interfaces 1 GE RJ45. As interfaces SFP+ e SFP devem vir com os seus respectivos transceivers do tipo Short Range (SR).
- 2.3.10. Suportar e estar licenciado para criação de no mínimo 8 instâncias virtuais;
- 2.3.11. Deve suportar a instalação em rack padrão 19" com o tamanho máximo de 1U;
- 2.3.12. Suporte a fontes redundantes;
- 2.3.13. Deve estar homologado na ANATEL até a data da licitação;
- 2.3.14. O fabricante ou o equipamento deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria), ou pela Netsecopen.org.
- 2.3.15. Deverá ser entregue no dia da licitação o certificado comprovando que o equipamento está em conformidade com a norma IEC e Rohs.
 - 2.3.15.1. A solução ofertada deverá permitir que a contratante habilite as funcionalidades de segurança através de um aditivo de licença, sem a necessidade de troca de hardware. E o equipamento em questão deverá suportar o Throughput de, no mínimo, 2.87 Gbps de Threat Protection. ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Proteção contra Malwares habilitadas simultaneamente;

2.4. Equipamento SD-WAN Concentrador - Links de 4Gbps.

- 2.4.1. Throughput de, no mínimo, 33 GBps para Controle de Aplicação;
- 2.4.2. Throughput de, no mínimo, 192 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;
- 2.4.3. Suporte a, pelo menos, 39 milhões de sessões concorrentes TCP;
- 2.4.4. Suporte a, pelo menos, 1.9 milhões sessões TCP por segundo;
- 2.4.5. Deve suportar o controle de aplicações encapsuladas no protocolo TLS/SSL, garantido no mínimo de 11.8Gbps de throughput de SSL Inspection.
- 2.4.6. Throughput de, no mínimo, 55 Gbps de IPSEC/VPN;
- 2.4.7. Deve Suportar no mínimo, 10000 clientes VPN SSL simultâneos;
- 2.4.8. Deve Suportar no mínimo, 20000 VPN Ipsec site-to-site;
- 2.4.9. Possuir ao menos 4 interfaces de 40 GE QSFP+, 4 interfaces de 25 GE SFP28, 8 interfaces 10 GE SFP+, 4 interfaces 10 GE RJ45, 8 interfaces SFP e 16 interfaces 1 GE RJ45. As interfaces de QSFP+, SFP28, SFP+ e SFP devem vir com os seus respectivos transceivers do tipo Short Range (SR). Serão aceitos transceivers do tipo Cooper Interface para atender as 4 interfaces de 10 GE RJ45.

- 2.4.10. Suportar a criação de no mínimo 10 instâncias virtuais;
- 2.4.11. Deve suportar a instalação em rack padrão 19" com o tamanho máximo de 2U;
- 2.4.12. Suporte a fontes redundantes do tipo hot swap;
- 2.4.13. Deve estar homologado na ANATEL até a data da licitação;
- 2.4.14. O fabricante ou o equipamento deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria), ou pela Netsecopen.org.
- 2.4.15. Deverá ser entregue no dia da licitação o certificado comprovando que o equipamento está em conformidade com a norma IEC e Rohs.
- 2.4.16. A solução ofertada deverá permitir que a contratante habilite as funcionalidades de segurança através de um aditivo de licença, sem a necessidade de troca de hardware. E o equipamento em questão deverá suportar o Throughput de, no mínimo, 14.93 Gbps de Threat Protection. ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Proteção contra Malwares habilitadas simultaneamente;

3. CARACTERÍSTICAS GERAIS DE EQUIPAMENTOS SD-WAN

- 3.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de SD-WAN e Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);
- 3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 3.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada7;
- 3.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 3.5. Para telnet e ssh, deve haver opção de configurar a interface de origem ao executar o acesso remoto;
- 3.6. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 3.7. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 3.8. Deve suportar BGP, OSPF, RIP2 e roteamento estático;
- 3.9. Para BGP (IPv4 e IPv6), deve suportar o anúncio apenas quando determinadas condições forem atendidas;
- 3.10. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 3.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 3.12. Deve suportar DHCP em IPv4 e IPv6;
- 3.13. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 3.14. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;
- 3.15. Deve suportar NAT dinâmico (Many-to-Many);
- 3.16. Deve suportar NAT estático (1-to-1);
- 3.17. Deve suportar NAT estático bidirecional 1-to-1;

- 3.18. Deve suportar Tradução de porta (PAT);
- 3.19. Deve suportar NAT de Origem;
- 3.20. Deve suportar NAT de Destino;
- 3.21. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 3.22. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 3.23. Deve suportar NAT64;
- 3.24. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 3.25. Enviar log para sistemas de monitoração externos;
- 3.26. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 3.27. Proteção anti-spoofing;
- 3.28. Deve haver suporte ao protocolo ICAP, inclusive de forma segura (SSL).
- 3.29. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 3.30. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 3.31. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 3.32. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
- 3.33. Controle, inspeção e decriptografia de SSL para tráfego de Saída (Outbound);
- 3.34. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 3.35. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 3.36. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 3.37. A solução de SD-WAN deve possuir conectores nativos;
- 3.38. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária, Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração ocorrência de eventos de rede e segurança pré-definidos;
- 3.39. Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN;
 - 3.39.1. Para agilizar a gerência remota do equipamento, deve ser possível carregar conteúdo estático dela a partir de objetos em cache em CDNs;

4. POLÍTICAS

- 4.1. Deverá suportar controles por zonas de segurança;
- 4.2. Deverá suportar controles de políticas por porta e protocolo;
- 4.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

- 4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 4.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 4.6. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
- 4.7. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- 4.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- 4.9. Suporte a objetos e regras IPV6;
- 4.10. Suporte a objetos e regras multicast;
- 4.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

5. CONTROLE DE APLICAÇÕES

- 5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 5.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 5.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, acesso remoto, update de software, protocolos rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 5.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 5.5. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas.
- 5.6. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 5.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
- 5.8. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 5.9. Atualizar a base de assinaturas de aplicações automaticamente;
- 5.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede.;
- 5.11. Deve ser possível adicionar controle de aplicações em múltiplas regras do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

- de
de
- 5.12. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
 - 5.13. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento aplicações proprietárias na própria interface gráfica da solução, sem a necessidade ação do fabricante;
 - 5.14. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
 - 5.15. Deve alertar o usuário quando uma aplicação for bloqueada;
 - 5.16. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
 - 5.17. Deve possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;
 - 5.18. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
 - 5.19. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;
 - 5.20. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
 - 5.21. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

6. IDENTIFICAÇÃO DE USUÁRIOS

- 6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory, base de dados local e outro que seja compatível com a solução;
- 6.2. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 6.3. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 6.4. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 6.5. Deve suportar SAML como método para autenticação na navegação de Internet e para VPN;

7. RECURSOS AVANÇADOS DE SD-WAN

- regras
- 7.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
 - 7.2. Deve ser possível criar políticas que definam os seguintes critérios para match:
 - 7.3. Endereços de origem;
 - 7.4. Grupos de usuários;

- 7.5. Endereços de destino;
- 7.6. DSCP;
- 7.7. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;
- 7.8. A solução de SD-WAN deve suportar health check ativo, passivo e misto, com o objetivo de medir latência, jitter e latência de cada caminho, separadamente:
- 7.9. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 7.10. Passivo: uso do tráfego real para as medições;
- 7.11. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para método ativo;
- 7.12. A solução deve permitir a configuração e uso de várias interfaces SD-WAN. Cada uma com seus links;
- 7.13. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;
- 7.14. Deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado;
- 7.15. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
- 7.16. A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;
- 7.17. Deve permitir a segmentação de várias VRFs sobre um único túnel SD-WAN;
- 7.18. Deve permitir a duplicação e deduplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 7.19. A solução deve permitir a definição do roteamento para cada aplicação;
- 7.20. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
- 7.21. Deve possibilitar a definição do link de saída para uma aplicação específica;
- 7.22. Deve implementar balanceamento de link por hash do IP de origem;
- 7.23. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 7.24. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 7.25. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 7.26. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;
- 7.27. Para IPv4, deve suportar roteamento estático e dinâmico no mínimo com BGP, IBGP, OSPF e RIP2;

- 7.28. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 7.29. Deve ser possível habilitar o FEC para tráfegos específicos. Ex: apenas para aplicações sensíveis a perda de pacote;
- 7.30. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
- 7.31. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:
 - 7.32. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;
 - 7.33. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
 - 7.34. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas.
 - 7.35. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
 - 7.36. O QoS deve possibilitar a definição de fila de prioridade;
 - 7.37. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;
 - 7.38. A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
 - 7.39. Deve possibilitar a definição de bandas distintas para download e upload;
- 7.40. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
 - 7.41. A solução de SD-WAN deve suportar health check ativo, passivo e misto:
 - 7.42. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - 7.43. Passivo: uso do tráfego real para as medições;
 - 7.44. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo;
 - 7.45. A solução de SD-WAN deve suportar IPv6;
 - 7.46. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
 - 7.47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
 - 7.48. O SD-WAN deverá possuir serviço de Firewall Stateful;
 - 7.49. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

- 7.50. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;
- 7.51. Deve ser capaz de bloquear acesso às aplicações;
- 7.52. Deve suportar NAT dinâmico bem como NAT de saída;
- 7.53. Deve suportar balanceamento de tráfego por sessão e pacote;
- 7.54. Suportar VPN IPsec Site-to-Site;
- 7.55. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);
- 7.56. A VPN IPSEC deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;
- 7.57. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 31;
- 7.58. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 7.59. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;
- 7.60. Deve possuir suporte e estar licenciamento para uso de VRFs, em IPv4 e IPv6;
- 7.61. A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance;

8. GERENCIAMENTO CENTRALIZADO DE SD-WAN

- 8.1. O fornecedor deve considerar recursos de gestão centralizada para as soluções NGFW e SD-WAN;
- 8.2. Devem ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados;
- 8.3. Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos elementos de rede;
- 8.4. Pode ser ofertado em hardware, desde que em appliance do próprio fabricante;
- 8.5. A solução de gerenciamento centralizado deve estar licenciada e suportar a gerência de no mínimo 150 dispositivos simultâneos, e o processamento de no mínimo 60 GB/log dia.
- 8.6. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 8.7. O sistema deverá suportar contas de usuário/senha estáticas;
- 8.8. Permitir acesso concorrente de administradores;
- 8.9. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 8.10. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius;
- 8.11. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;
- 8.12. Essas comunicações deverão ser protegidas e criptografadas;
- 8.13. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;
- 8.14. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;

- 8.15. A console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;
- 8.16. Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência.
- 8.17. Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN;
- 8.18. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
- 8.19. A console deverá ser hospedada nas dependências da contratada SD-WAN;
- 8.20. A console de Gerência deverá informar o status ACESSÍVEL/INACESSÍVEL/CONFIGURATION SYNC/ TUNNELS UP/TUNNELS DOWN de cada equipamento SD-WAN/NGFW;
- 8.21. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada equipamento SD-WAN a cada 5 (cinco) minutos no mínimo;
- 8.22. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN;
- 8.23. A solução SD-WAN deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros;
- 8.24. O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e também via API aberta;
- 8.25. O sistema deverá suportar contas de usuário/senha estáticas, bem como integração com serviços de diretório e radius, para fins de gerenciamento;
- 8.26. Permitir acesso concorrente de administradores;
- 8.27. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 8.28. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;
- 8.29. Comunicações entre gerência e equipamentos remotos devem ser criptografadas;
- 8.30. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;
- 8.31. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;
- 8.32. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;
- 8.33. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;
- 8.34. Deve oferecer um portal do cliente fácil de usar, permitindo acesso aos recursos de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;
- 8.35. Deve ter a capacidade de criar relatórios no formato PDF e XML;
- 8.36. A gerência de SD-WAN deve suportar envio de syslog para soluções de terceiros;

- 8.37. Deve ter a capacidade de gerar e enviar relatórios automaticamente, de forma agendada;
- 8.38. Deve permitir a customização dos relatórios, sem custo para o órgão;
- 8.39. Deve permitir especificar o destinatário de cada relatório;
- 8.40. Deve permitir filtrar informações nas abas de visualização;
- 8.41. Deve permitir a alteração do formato dos relatórios: fontes, cores, imagens, gráficos, tabelas e o idioma;

LEONARDO MIRANDA DO NASCIMENTO
Capitão de Corveta (T)
Encarregado da Divisão de Conectividade