

**TERMO DE REFERÊNCIA****ESPECIFICAÇÕES TÉCNICAS****1 OBJETO**

- 1.1 Aquisição de solução de Tecnologia da Informação de NPB (Network Packet Broker) com o objetivo de capturar, decriptar, redirecionar, filtrar e monitorar os fluxos de tráfego de rede, com painel de gerenciamento centralizado e garantia de 60 (sessenta meses), incluindo os serviços de entrega, instalação, suporte técnico e transferência de conhecimento, conforme quantidades e especificações técnicas constante deste documento:

<b>Equipamento</b>	<b>Quantidade</b>
Concentrador para Tráfego SSL	16
Concentrador para Visibilidade de Tráfego	06
Agregador para Visibilidade de Tráfego	04
Links Multimodo Espelhados com TAP físico	120
Links Monomodo Espelhados com TAP físico	24
Hosts espelhados com TAP virtual	300
Gerência Centralizada	02

**2 ESPECIFICAÇÕES TÉCNICAS GERAIS**

- 2.1 A solução deve ser composta por único fabricante, incluindo concentrador de tráfego, agregadores de tráfego, transceivers e TAPs com vista a não desperdício de recursos técnicos e facilidade de integração.
- 2.2 Todos os modelos de equipamentos que compõem a solução deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).
- 2.2.1 Fica flexibilizado a exigência de certificado de homologação para os transceivers e TAPs.
- 2.3 A solução para visibilidade de tráfego SSL deve possuir funcionalidades que assegurem a alta disponibilidade da solução adotando mecanismos de clusterização ou similares, mesmo para sites distintos.
- 2.4 A solução para visibilidade de tráfego espelhado deve possuir funcionalidades que assegurem a alta disponibilidade da solução adotando mecanismos de clusterização ou similares, mesmo para sites distintos.
- 2.5 Não será aceito administração em forma de aplicativo cliente e/ou solução de administração executado em JVM (Java Virtual Machine);
- 2.6 A solução deve ser operada, em sua essência, através da gerência centralizada, sendo permitido que algumas configurações específicas sejam realizadas individualmente em cada equipamento.

- 2.7 A solução deve ser operada, em sua essência, através da gerência centralizada, sendo permitido que algumas configurações específicas sejam realizadas individualmente em cada equipamento.
- 2.8 Deve suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.
- 2.9 Todas as interfaces físicas da solução devem estar habilitadas e licenciadas para uso sem necessidade de nenhum recurso extra.
- 2.10 Todos os equipamentos devem permitir ser fixados em rack(s) de 19" (dezenove polegadas) ou fornecidos na forma de módulos de outros equipamentos com fixação em rack(s) de 19". Devem ser fornecidos kits de suporte específico para este fim. Eventuais ajustes na estrutura do rack (fixação de colunas, etc.) necessários para a instalação da solução devem ser executados pela CONTRATADA.
- 2.11 Os equipamentos devem ser fornecidos com todos os componentes, cabos, conectores, porcas, trilhos, parafusos, e demais itens, necessários à instalação em rack padrão 19 polegadas.
- 2.12 Devem ser fornecidos cabos de alimentação com conector padrão IEC C13/C14 e NBR 14136 compatíveis com a potência da fonte de alimentação. O padrão do cabo de alimentação a ser fornecido ficará a critério do CONTRATANTE.
- 2.13 Suportar e operar nas faixas de tensão de entrada de 100-240 VAC em 60 Hz, automaticamente.
- 2.14 Todos os ativos gerenciáveis da solução devem possuir ao menos uma interface 1GbE RJ45 dedicada para gerenciamento.
- 2.15 Os componentes de hardware devem ser fornecidos com fontes redundantes (mínimo de 2 (duas) fontes e 2 (duas) conexões elétricas).
- 2.16 Todos os equipamentos devem possuir suas fontes de alimentação integradas ao equipamento.
- 2.17 Todos os equipamentos devem possuir o fluxo do ar da frente para trás (front-to-back).
- 2.18 Todos os equipamentos devem implementar de forma nativa mecanismo de monitoramento e detecção de falhas internas.
- 2.19 Os equipamentos fornecidos devem ser novos, sem uso anterior, e devem estar em linha de produção atual pelo fabricante no momento da entrega da proposta.
- 2.20 Devem ser fornecidas todas as licenças de software necessárias para atendimento completo desta especificação, durante toda a vigência contratual, inclusive suas atualizações, conforme detalhado nesta especificação.

- 2.21 O software licenciado para os equipamentos deverá ser do tipo perpétuo ou do tipo subscrição.
- 2.21.1 O licenciamento do tipo perpétuo deve funcionar sem limite de tempo e perda de recursos ou funcionalidades.
- 2.21.2 O licenciamento do tipo subscrição deve funcionar por todo período contratual, com adicional de 5 (cinco) anos, sem perda de recursos ou funcionalidades.
- 2.22 Os equipamentos ofertados devem possuir quantidade de memória e poder de processamento suficientes para garantir o atendimento de todos os requisitos desta especificação, mesmo em sua utilização máxima.
- 2.23 O acesso aos dispositivos componentes desta solução deve ser via SSL, por meio de uma interface GUI criptografada (HTTPS), acessível a múltiplos usuários simultaneamente, por meio dos navegadores WEB mais populares ou aplicação proprietária que acompanha a solução.
- 2.24 A solução ofertada deve atender todas as necessidades e funcionalidades descritas nesta especificação de forma adequada e completamente compatível ao ambiente do CONTRATANTE mesmo que, para isso, seja necessária a entrega de itens com configurações acima das especificadas.
- 2.25 Todos os gráficos, relatórios, ferramentas de busca, gerenciamento e análise de dados da solução de NPB devem estar disponíveis ao usuário em formato de páginas web, por meio dos navegadores mais populares, suportando, pelo menos, a plataforma Microsoft Windows.
- 2.26 A solução deve permitir a auditoria de mudanças de configuração do sistema por meio de LOGs, onde estas alterações devem ser gravadas.
- 2.27 Deve permitir configuração customizada baseadas nos perfis de acesso (RBAC – Role Base Access Control).
- 2.28 Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- 2.29 Deve possuir suporte a MIB II.
- 2.30 Deve implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
- 2.31 Deve suportar SNMP trap sobre IPv4 ou IPv6.
- 2.32 Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento.
- 2.33 Deve permitir a gravação de log externo (syslog).
- 2.34 Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

- 2.35 Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos.
- 2.36 Deve suportar configuração total da solução através de console local RS-232, RJ-45 ou cabo proprietário fornecido pela CONTRATADA.
- 2.37 Deve possuir gerenciamento através de interface Web (HTTPS) e CLI.
- 2.38 Deve implementar o protocolo NTP (Network Time Protocol).
- 2.39 Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS ou LDAP.
- 2.40 Deve suportar IPv4 ou IPv6 para TACACS+.
- 2.41 Deve implementar o protocolo SSHv2 para acesso à interface de linha de comando.
- 2.42 Deve proteger a interface de comando do equipamento através de senha.
- 2.43 A solução deve implementar as seguintes configurações para agregação e encaminhamento de pacotes das portas de Rede para as portas de Ferramentas, tanto para os fluxos Out-of-Band (Cópia de Tráfego) quanto para Inline, respectivamente:
  - a) Uma para Uma;
  - b) Uma para Várias - Com suporte a balanceamento;
  - c) Várias para Uma;
  - d) Várias para Várias - Com suporte a balanceamento.
- 2.44 Deve permitir criar filtros (regras) baseados em, no mínimo, os seguintes campos:
  - a) Endereços MAC de origem e destino;
  - b) Endereço IPv4 de origem/destino;
  - c) Portas TCP e UDP de origem e destino;
  - d) VLAN ID;
  - e) Ethertype;
  - f) IPFrag;
  - g) TTL;
  - h) TOS;
  - i) Protocol;

- j) TCP Control Mask/Bits;
  - k) DSCP;
  - l) Versão do Protocolo IPv4 e IPv6;
  - m) Endereço IPv6 de origem/destino.
- 2.45 A solução deve suportar, no mínimo, 16000 (dezesesseis mil) filtros (regras).
- 2.46 Deve permitir a inserção e remoção de novos filtros (regras) sem a necessidade de reiniciar o(s) equipamento(s), ou seja, a aplicação destes filtros (regras) deve acontecer em tempo real.
- 2.47 Deve suportar overlapping de filtros (regras), ou seja, onde mais de um filtro pode ser aplicado a mesma porta de entrada (ingress) para definir qual será a porta de saída (egress).
- 2.48 A solução deve implementar funcionalidade Mesh/Cluster.
- 2.49 O Mesh/Cluster deve permitir a configuração e gerenciamento de 2 (dois) ou mais Agregadores de Tráfego como um único equipamento lógico. Não serão aceitas soluções em cascata para o atendimento desta funcionalidade.
- 2.50 O Mesh/Cluster deve permitir a configuração de todos os Agregadores de Tráfego a partir de uma única interface WEB (HTTPS) e CLI.
- 2.51 A funcionalidade de Mesh/Cluster deve suportar a criação de 1 (um) ou mais filtros (regras) que se utilizem de portas de Rede em um equipamento físico e direcionem este tráfego para portas de Ferramenta localizadas em outro equipamento físico, independentemente da quantidade de equipamentos entre estes equipamentos. Não serão aceitas soluções em cascata para o atendimento deste item.
- 2.52 A funcionalidade de Mesh/Cluster deve permitir redundância a solução em caso de falha de um dos equipamentos, sendo capaz de redirecionar o tráfego automaticamente via outro caminho disponível entre a captura e a ferramenta que irá utilizá-lo.
- 2.53 Deve suportar o conceito de FABRIC que permite a criação de filtros que se estendem por múltiplos agregadores ou Mesh/Cluster de agregadores.
- 2.54 Deve permitir a configuração de circuitos entre Mesh/Cluster de agregadores, permitindo que o tráfego recebido em um cluster seja entregue para uma ferramenta em outro cluster.

### **3 ESPECIFICAÇÕES TÉCNICAS PARA VISIBILIDADE DE TRÁFEGO SSL**

- 3.1 A solução de abertura de tráfego SSL deve ser composta por equipamentos dedicados (concentrador de tráfego), devendo operar em alta disponibilidade.
- 3.2 A funcionalidade de alta disponibilidade da solução deve adotar mecanismos de clusterização ou similares.
- 3.3 Realizar o bypass lógico, não intervindo de nenhuma maneira no tráfego da

rede.

- 3.4 Inspecionar e descriptografar o tráfego SSL e o tráfego TLS e encaminhá-lo aos equipamentos de segurança (firewalls, antivírus, WAF, IPS).
- 3.5 Encaminhar apenas o tráfego de interesse para cada equipamento de segurança (firewalls, antivírus, WAF, IPS).
- 3.6 Encaminhar cópia do tráfego descriptografado para o concentrador out-of-band.
- 3.7 Criptografar o tráfego após o mesmo ser analisado pelos equipamentos de segurança que atuam de forma inline, tais como IPS, WAF e similares.
- 3.8 Possibilitar a escolha de qualquer porta TCP para descriptografia.
- 3.9 Realizar descriptografia de SSL/TLS independente da porta padrão (RFC do protocolo) utilizada, evitando abuso de protocolo.
- 3.10 Possuir políticas de tráfego configuráveis por origem e destino, permitindo ignorar a inspeção para categorias ou URLs específicas, ou seja, inspecionar somente o que for definido pela CAIXA de acordo com a origem e destino do tráfego.
- 3.11 O appliance deverá trabalhar em modo in-line transparente no segmento de rede a ser analisado.
- 3.12 Tolerar, no mínimo, os seguintes protocolos de criptografia:
  - a) TLS 1.0
  - b) TLS 1.1
  - c) TLS 1.2
  - d) TLS 1.3
- 3.13 Tolerar chaves de 1024 bits, 2048 bits e 4096 bits
- 3.14 Tolerar os algoritmos de chave pública RSA, DHE e ECDHE com PFS (Perfect Forward Secrecy).
- 3.15 Tolerar o algoritmo de criptografia simétrica AES para decriptação inline e os algoritmos AES, 3DES e RC4 para decriptação out-of-band.
- 3.16 Tolerar os algoritmos de hash SHA, SHA256, SHA384, POLY1305 para decriptação inline e os algoritmos MD5, SHA-1, SHA-2 para decriptação out-of-band.
- 3.17 Utilizar cifras com algoritmos públicos de criptografia reconhecidos por entidades nacionais e internacionais reguladoras do assunto.
- 3.18 Ser capaz de utilizar certificado digital da estrutura interna de PKI da CAIXA baseada no padrão X.509.

- 3.19 Tolerar OCSP (Online Certificate Status Protocol) ou OCSP stapling para confirmar a validade do certificado bem como a integridade da CA (Certificate Authority).
- 3.20 Efetuar busca à Lista de Certificados Revogados (LCR) por meio dos protocolos HTTP, LDAP, CRLDP, OCSP ou OCSP stapling.
- 3.21 Validar a autenticidade do certificado digital utilizado pelo site, no mínimo, quanto à (ao):
- a) Confiabilidade da cadeia de certificação.
  - b) Integridade do certificado digital.
  - c) Prazo de validade do certificado digital.
  - d) Prazo de validade do certificado digital.
  - e) Revogação do certificado digital.
- 3.22 Permitir a deciptação ou o descarte da sessão TLS para os casos de uso de certificados inválidos, expirados, auto assinados ou certificados emitidos por autoridades certificadoras desconhecidas e não confiáveis.
- 3.23 Cada concentrador de tráfego SSL deve possuir as seguintes características:
- a) no mínimo 08 interfaces de 100Gbps
  - b) no mínimo 24 interfaces de 40Gbps
  - c) tamanho máximo de 3RU
  - d) throughput nominal de, no mínimo, 50Gbps de tráfego descriptografado
- 3.23.1 Deverão ser fornecidos 24 (vinte e quatro) transceivers QSFP28 40G BiDi multimodo e 8 (oito) transceivers QSFP28 100G BiDi multimodo, com sobressalente de 2 (dois) transceivers QSFP28 40G LR4 monomodo e 2 (dois) transceivers QSFP28 100G LR4 monomodo.
- 3.24 Deverão ser fornecidos os seguintes cabos fanout de fibra ótica multimodo 50/125µm, padrão OM4, com conectores MPO macho/LC duplex, comprimento do segmento LC de 3 metros, polaridade tipo A (direto), revestimento LSZH e cor aqua:
- a) 25 fanout de 5 metros
  - b) 25 fanout de 10 metros
- 3.24.1 Tais cabos podem ser fornecidos por fabricantes diferentes dos demais itens deste edital.
- 3.24.2 Os conectores utilizados nos cabos devem possuir certificação ANATEL.
- 3.24.3 O cabo utilizado deve possuir certificação ANATEL com o número da certificação impresso na capa externa.

**4 ESPECIFICAÇÕES TÉCNICAS PARA VISIBILIDADE DE TRÁFEGO**

- 4.1 A solução deve ser do tipo Network Packet Broker (NPB).
- 4.2 A solução deve ser compatível e funcionar com as soluções de Monitoração e Diagnóstico do Desempenho de Rede disponíveis no mercado.
- 4.3 Os equipamentos ofertados devem possuir funcionalidades e hardware específicos para concentração, agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceitas soluções genéricas tais como switches, firewalls, balanceadores de carga ou similares.
- 4.4 A solução deve suportar interfaces de 10Gbps, 25Gbps, 40Gbps e 100Gbps através da adição ou substituição módulos, sem causar impacto no desempenho dos equipamentos ofertados.
- 4.5 Deve ser capaz de processar todo o tráfego de rede oriundo de todos os pontos de captura.
- 4.6 Deve implementar Test Access Point ou Terminal Access Point (TAPs) para interceptação física de tráfego de rede, ou permitir a utilização de TAP externo para essa função.
- 4.7 Deve ser capaz de capturar tráfego de rede a partir de Switch Port Analyzer (SPAN).
- 4.8 Deve suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.
- 4.9 Todas as interfaces físicas da solução devem estar habilitadas e licenciadas para uso sem necessidade de nenhum recurso extra.
- 4.10 Deve ser capaz de gerar flows do tráfego capturado e encaminhar para ferramenta de monitoração.
- 4.11 Deve implementar funcionalidade Tunnel, que permite encapsulamento e desencapsulamento de tráfego entre 2 (dois) equipamentos através de redes L3 (roteadas).
- 4.12 A funcionalidade de Tunnel deve suportar o encapsulamento e o desencapsulamento utilizando protocolo L2GRE ou VXLAN, permitindo transportar o tráfego encapsulado através de diferentes redes L3.
- 4.13 A solução deve suportar balanceamento entre diferentes túneis, permitindo utilizar duas ou mais ferramentas da mesma solução como destino para todo o tráfego encapsulado.
- 4.14 Deve implementar a funcionalidade Packet Trimming (Corte do Pacote), otimizando o tráfego que será encaminhado para as ferramentas reduzindo o tamanho do pacote.
- 4.15 A funcionalidade de Packet Trimming deve ser configurável para cortar o pacote das seguintes formas:



- a) Dinâmico, ou seja, a partir de um campo específico do cabeçalho ethernet definido pelo usuário;
  - b) Estático, ou seja, a partir de um valor específico definido pelo usuário.
- 4.16 Deve implementar terminação Encapsulated Remote Switch Port Analyzer (ERSPAN) para as versões I, II ou III permitindo terminar um tráfego espelhado de equipamentos que suportam ERSPAN.
- 4.17 Deve implementar a funcionalidade Masking (Alteração de dados), que é capaz de modificar determinadas informações contidas no tráfego de rede antes de redirecioná-lo para as ferramentas, para atendimento de normas de proteção de dados, quando necessário.
- 4.18 A funcionalidade Masking deve ser capaz de trocar uma determinada informação como o CPF do usuário por outros caracteres (XXX.XXX.XXX-XX, por exemplo), de modo que essa informação específica seja protegida antes de ser enviada para as soluções.
- 4.19 Deve implementar a funcionalidade Protocol Stripping (Remoção de Cabeçalho), permitindo identificar e remover TAGs de VLANs e cabeçalhos específicos dos pacotes de rede.
- 4.20 A funcionalidade de Protocol Stripping deve suportar a remoção de pelo menos os seguintes cabeçalhos:
- a) VLAN;
  - b) MPLS;
  - c) VNTag;
  - d) VxLAN;
  - e) Fabric Path;
  - f) GRE;
  - g) QinQ;
  - h) GTP.
- 4.21 A funcionalidade de Protocol Stripping também deve suportar a remoção de cabeçalhos que não estejam pré-definidos, permitindo assim a customização de um valor de deslocamento e quantidade de bytes deverão ser removidos, permitindo assim a remoção de cabeçalhos não padronizados.
- 4.22 Deve implementar a funcionalidade Packet De-Duplication (remoção de pacotes duplicados), enviando somente uma única cópia do pacote para as ferramentas.
- 4.23 A funcionalidade de Packet De-Duplication deve implementar remoção de pacotes duplicados IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet.

- 4.24 A funcionalidade Packet De-Duplication deve detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s), inclusive se utilizado em modo Mesh/Cluster.
- 4.25 A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:
- a) IPv4 ToS;
  - b) IPv6 TC;
  - c) Número da Sequência TCP;
  - d) VLAN ID;
- 4.26 Deve implementar a funcionalidade de geração de metadados como NetFlow, IPFIX e CEF.
- 4.27 Deve suportar geração de NetFlow nas versões v5 e v9 e IPFIX.
- 4.28 Permitir que a solução de Network Packet Broker possa integrar com ferramentas como SIEM, observabilidade, NAC, entre outras:
- a) Deve implementar a funcionalidade de geração de flow de rede enriquecido com metadados da camada de aplicação.
  - b) Deve implementar a exportação de, no mínimo, cinco mil (5000) diferentes atributos da camada de aplicação para soluções analíticas como SIEM e plataformas de observabilidade.
  - c) Os metadados extraídos da camada de aplicação devem permitir a identificação de ações específicas de usuários tais como login e acessos em arquivos.
  - d) Deve implementar a geração de metadados para o tráfego de aplicações como YouTube, MongoDB, Postgres, MySQL e Whatsapp.
  - e) Deve implementar o envio de metadados usando os protocolos IPFIX, Syslog em formato ou JSON sobre protocolos HTTP e HTTPS.
  - f) Deve implementar templates pré-definidos com conjuntos de atributos para exportação dos metadados.
  - g) Deve implementar a integração com o Kafka.
- 4.29 Cada concentrador de tráfego espelhado deve possuir as seguintes características:
- a) no mínimo 24 interfaces de 100Gbps
  - b) no mínimo 08 interfaces de 40Gbps
  - c) tamanho máximo de 3RU

- d) throughput nominal de, no mínimo, 1Tbps para processar as funcionalidades de filtragem, corte do pacote, mascaramento de informação, encapsulamento e desencapsulamento de forma simultânea
  - e) throughput nominal de, no mínimo, 500 Gbps para processar as funcionalidades de deduplicação e geração de Netflow/IPFIX de forma simultânea
- 4.30 Deverão ser fornecidos 8 (oito) transceivers QSFP28 40G BiDi multimodo e 24 (vinte e quatro) transceivers QSFP28 100G BiDi multimodo, com sobressalente de 2 (dois) transceivers QSFP28 40G LR4 monomodo e 2 (dois) transceivers QSFP28 100G LR4 monomodo.
- 4.31 Cada agregador de tráfego espelhado deve possuir as seguintes características:
- a) no mínimo 64 interfaces, variando entre as velocidades de 10Gbps, 25Gbps, 40Gbps e 100Gbps através da adição ou substituição transceivers
  - b) tamanho máximo de 2RU
  - c) throughput nominal de, no mínimo, 2Tbps de tráfego
- 4.31.1 Será permitido o uso de breakout patch panel utilizando portas de 40Gbps e 100Gbps para transformá-las em portas de 10Gbps e 25Gbps.
- 4.32 Deverão ser fornecidos os seguintes transceivers para as portas de cada agregador:
- a) 16 transceivers QSFP28 100G BiDi multimodo
  - b) 48 transceivers QSFP28 40G BiDi multimodo
- 4.33 Deverão ser fornecidos os seguintes cabos de fibra ótica multimodo 50/125µm, padrão OM4, com conectores LC/LC duplex, revestimento LSZH e cor aqua:
- a) 50 fibras de 20 metros
  - b) 50 fibras de 35 metros
- 4.33.1 Tais cabos podem ser fornecidos por fabricantes diferentes dos demais itens deste edital.
- 4.33.2 O cabo utilizado deve possuir diâmetro nominal de até 5,0 mm
- 4.34 Deverão ser fornecidos os seguintes cabos de fibra ótica monomodo 9/125µm, padrão OM4, com conectores LC/LC duplex, revestimento LSZH e cor aqua:
- a) 50 fibras de 35 metros
- 4.34.1 Os conectores utilizados devem possuir perda por inserção (IL) máxima de 0,35 dB e perda por retorno (RL) maior que 30 dB.

- 4.34.2 O cabo utilizado deve possuir diâmetro nominal de até 2,0 mm
- 4.35 Todos os cabos de fibra ótica devem possuir certificação ANATEL com o número da certificação estampado na capa externa.
- 4.36 Os cabos devem ser embalados e certificados em fábrica com o registro da certificação etiquetado nas embalagens individuais de plástico.

## **5 ESPECIFICAÇÕES TÉCNICAS PARA TAP FÍSICO**

- 5.1 Deve vir acompanhado dos acessórios para montagem em rack 19", incluindo o chassi de instalação em rack, se necessário, devendo está distribuído em, no mínimo, 8 (oito) racks;
- 5.2 Possuir altura máxima de 2 RU (3,5");
- 5.3 Ser totalmente passivo, ou seja, não é necessário nenhum tipo de alimentação elétrica, software e configuração para o seu funcionamento;
- 5.4 Replicar todo tráfego da rede, inclusive erros de CRC em todas as camadas;
- 5.5 Suportar as seguintes características de velocidade, fibra, conector e Split Ratio: 40/100G BiDi, Multimodo 850nm, 50 microns, conector LC e Split Ratio de 50/50;
- 5.6 Suportar as seguintes características de velocidade, fibra, conector e Split Ratio: 40/100G LR, Monomodo 1310nm, 9 microns, conector LC e Split Ratio de 50/50;

## **6 ESPECIFICAÇÕES TÉCNICAS PARA TAP VIRTUAL**

- 6.1 Deve ser um dispositivo virtual com funcionalidades de TAP.
- 6.2 Deve ter capacidade e licença para coletar um volume de, no mínimo, 250 TB (duzentos e cinquenta terabytes) por dia para todo o ambiente virtualizado do CONTRATANTE. Em caso de licenciamento por host deve ser fornecido licenciamento para, no mínimo, 300 (trezentos) hosts.
- 6.3 Permitir sua implementação em ambientes VMware ESXi 6.0 ou superior e no mínimo outro hypervisor como: Microsoft Hyper-V, KVM ou OpenStack KVM.
- 6.4 A solução deve ser compatível com ambiente de nuvem privada baseado em Kubernetes e compatível com as nuvens públicas Azure, Google e AWS.
- 6.5 Permitir monitoração de forma segura, com alta disponibilidade e performance através de ambientes virtualizados.
- 6.6 Possuir gerenciador em único ponto central para toda a solução de NPB fornecida.
- 6.7 Permitir o isolamento do tráfego de interesse a ser monitorado com filtros do L2 ao L4 (modelo OSI).
- 6.8 Permitir o encapsulamento de tuneis VXLAN ou ERSPAN ou L2GRE.

- 6.9 Deve seguir capturando o tráfego da VM quando esta for migrada para outro HOST.
- 6.10 Permitir a mobilidade das máquinas virtuais, de forma que quando ocorrer migração de uma VM, todas as configurações de filtros (regras) sejam reaplicadas para esta VM após sua migração.
- 6.11 Possuir recurso de monitoração de vMotion e DRS (VMware Distributed Resource Scheduler).
- 6.12 A coleta do tráfego entre VMs deve ser feita através de integração via API com o VMware, não sendo aceitas soluções que utilizem do modo promíscuo ou que faça qualquer alteração no kernel do Hypervisor.
- 6.13 Deve permitir a implementação de configurações para manter conformidade com requerimentos: SOX, PCI, HIPAA.
- 6.14 Deve implementar a funcionalidade Packet De-Duplication (Desduplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas de monitoramento, nativamente no ambiente virtual.
- 6.15 Deve implementar a geração de NetFlow v5, v9 e IPFIX.
- 6.16 Deve implementar a geração de Netflow sem amostragem, trazendo visibilidade de 100% do tráfego.
- 6.17 Deve implementar a filtragem do tráfego de rede baseado em aplicações (camada 7).
- 6.18 Deve implementar a decriptação passiva (out-of-band) do tráfego TLS.

## **7 ESPECIFICAÇÕES TÉCNICAS PARA GERÊNCIA CENTRALIZADA**

- 7.1 Deve ser fornecido um software capaz de controlar, administrar, gerenciar e monitorar a solução de Visibilidade de Rede.
- 7.2 O software deve estar licenciado para todos os ativos da solução de NPB fornecida.
- 7.3 A console de gerenciamento deve ser única e deve abranger todos os itens ativos e gerenciáveis da solução.
- 7.4 A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros.
- 7.5 O software de gerenciamento poderá ser fornecido em forma de Appliance Virtual compatível com hypervisors VMware.
- 7.6 A solução deve ser capaz de visualizar e gerenciar os dados e métricas coletadas. Em múltiplos segmentos monitorados em uma única console (centralizada), permitindo desta forma integração, maior segurança, escalabilidade, robustez e disponibilidade da solução.
- 7.7 Possuir interface gráfica para a criação dos filtros (regras), onde é possível

selecionar as portas de Rede e as portas de Ferramentas, independentemente do equipamento físico. Os filtros (regras) criados para estes tráfegos deverão ser aplicados através desta mesma interface Web (HTTPS), facilitando a operação e entendimento dos fluxos.

- 7.8 A solução deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização.
- 7.9 Deve permitir a visualização da topologia da solução de visibilidade para todos os equipamentos ativos e gerenciáveis.
- 7.10 Deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas.
- 7.11 A solução deve permitir o inventário detalhado de atributos dos ativos da solução, atendendo, no mínimo, números seriais, módulos instalados, status do equipamento e versão de software instalado.
- 7.12 A solução deve permitir o armazenamento das configurações dos dispositivos.
- 7.13 A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia.
- 7.14 Deve permitir o upgrade do sistema operacional dos dispositivos, individualmente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente.
- 7.15 A ferramenta deve permitir a execução do reset dos dispositivos.
- 7.16 A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição.
- 7.17 A solução deve possuir dashboards com, no mínimo, as seguintes informações:
  - a) Total de portas que estão perdendo pacotes;
  - b) Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta;
  - c) TOP portas com maior utilização;
  - d) Visualização simplificada de todos os filtros (regras) aplicados, indicando as portas de Redes e Ferramentas.

## **8 INFORMAÇÕES COMPLEMENTARES**

- 8.1 A Proponente deverá informar que possui autorização do fabricante para comercializar o produto no Brasil.

- 8.2 A comprovação deve ser feita por meio de declaração, fornecida juntamente com a proposta e destinada a Caixa e com referência explícita ao corrente processo de aquisição.
- 8.3 A Proponente, deverá apresentar declaração destinada à Caixa e com referência explícita a este processo de aquisição, que comprove os requisitos abaixo:
- a) Possuir contrato de suporte com o fabricante, no Brasil, para o produto e pelo tempo especificado;
  - b) Possuir contrato de garantia firmado com o fabricante, no Brasil, para o produto e pelo tempo especificado;
  - c) Permitir que a Caixa verifique diretamente junto aos fabricantes a correspondência entre o suporte e garantias contratadas e as exigidas neste edital.
- 8.4 A Proponente deverá apresentar, em sua proposta, descritivo do “Roadmap” dos equipamentos que compõe a solução, com informações relativas ao ciclo de vida (“End-of-Life”, “End-of-Sale” e “End-of-Support”) de cada um deles e dos seus componentes.
- 8.5 A Proponente não poderá ofertar equipamentos ou software com ciclo de vida anunciado pelo fabricante (“End-of-Life”, “End-of-Sale” e “End-of-Support”).