ANEXO VII - REQUISITOS DOS SERVIÇOS INTEGRADOS DE COMUNICAÇÃO DEFINIDA POR SOFTWARE (SD-WAN)

1 INTRODUÇÃO

O presente anexo descreve os requisitos técnicos relacionados à prestação de serviços de comunicação rede WAN Definida por Software (SD-WAN) abrangendo as funcionalidades, implantação, configuração, ambiente de Controle, gestão e monitoramento, assistência e suporte técnico dos componentes, através conectividade via circuitos MPLS, Internet Simétrica e Assimétrica, entre os Data Centers do BNB para as Unidades Distribuídas do Banco.

Os requisitos apresentados são aplicáveis, independentemente e simultaneamente, a todos os grupos de unidades descritas.

Todos os requisitos apresentados têm caráter obrigatório, devendo ser integralmente atendidos pelos licitantes de todos os ITENS, de acordo com a aplicabilidade. O não atendimento a qualquer dos requisitos apresentados, no todo ou em parte, sujeitará o licitante à desclassificação do processo licitatório, às sanções previstas em Contrato e às medidas legais cabíveis.

2 CARACTERÍSTICAS GERAIS DO SERVIÇO

2.1 Finalidade

2.1.1 Além do serviço de SD-WAN das Unidades Distribuídas, será contemplado no mesmo item o serviço de SSE (Security Service Edge) que deverá ser integrado com o serviço de SD-WAN, formando, assim, uma solução completa de SASE (Secure Access Service Edge). Apesar de fazerem parte do mesmo item poderão ser atendidos por fabricantes diferentes, desde que integrados e atendendo todos os itens do exigidos no edital.

2.1.2 Os serviços prestados deverão permitir a critério do Banco a criação de Tenants, sendo possível isolar a comunicação entre grupos de unidades do Banco e obrigatoriamente direcionar o tráfego entre esses grupos para dispositivos de firewall do Banco utilizando inclusive redes/VLAN diferente para rotear esse tráfego permitindo que o tráfego passe por firewall em roteamento e seja devolvido para os dispositivos de SD-WAN.

2.1.3 A critério do Banco e para cada grupo definido pelo Banco, poderá ser definido o tipo de comunicação full-mesh, parcial-mesh ou hub-to-spoke.

2.1.4 Serviços de Monitoramento e Gerenciamento das Soluções Ofertadas, inclusive NOC/SOC com recursos residentes e remotos.

2.2 Fornecimento de infraestrutura

Os serviços a serem prestados deverão contemplar o fornecimento, instalação, configuração, assistência e suporte técnico de toda a infraestrutura necessária à adequada prestação dos serviços ora especificados, incluindo, os seguintes componentes:

2.2.1 Os equipamentos **appliances** para solução de SD-WAN (*Software Defined Wide Area Network*) e seus respectivos appliances ou servidores de gerência no Site Primário, Site Secundário e Unidades Distribuídas fazem parte do escopo, bem como a solução de SSE (*Security Service Edge*);

2.2.2 Cabos, módulos, placas, interfaces, comutadores, memórias e demais acessórios relacionados aos componentes descritos acima;

2.2.3 Ao Banco, caberá providenciar a adequação das instalações físicas de suas unidades distribuídas, no Site Primário e Site Secundário para proporcionar a adequada acomodação dos equipamentos fornecidos no escopo dos serviços, incluindo:

2.2.3.1 Disponibilização de espaço físico para acomodação dos equipamentos, atendendo às recomendações de refrigeração e alimentação elétrica do fabricante dos equipamentos;

2.2.3.1.1 Para a CONTRATADA, caso os componentes ofertados a serem instalados nos datacenters ocupem espaço superior a 20 RU's (rack units), a CONTRATADA deverá entregar um rack 19 polegadas, padrão 44U, para os Sites Primário e Secundário, assim como a adequação de tubulação e encaminhamentos internos para passagem de de cabos e fibras até os racks dos núcleos/distribuição do Banco.

2.2.3.2 Adequação de tubulação e encaminhamentos internos para passagem de cabos;

2.2.3.3 Adequação do cabeamento da rede local das unidades distribuídas e do CAPGV.

2.2.4 Todos os equipamentos fornecidos para a prestação dos serviços serão devidamente patrimoniados e cadastrados em sistema de inventário eletrônico atualmente utilizado pelo Banco para efeitos de controle patrimonial de bens de terceiros;

3 REQUISITOS ESPECÍFICOS PARA OS CIRCUITOS DE ACESSO REMOTOS

3.1 Chaveamento entre os circuitos de acesso pela solução SD-WAN

Ao longo do Contrato, deverá ser possível ao Banco a qualquer momento, de acordo com endereço IP e porta de suas aplicações, definir critérios de chaveamento entre os circuitos de acesso da Unidade. Este chaveamento deverá ser automático ou manual, a critério do Banco.

No chaveamento automático, deverá ser possível definir para cada aplicação do Banco (IP/porta) qual circuito de acesso utilizar, baseado em critérios de disponibilidade e performance/qualidade dos circuitos de acesso disponíveis no momento, conforme requisitos desta especificação.

3.2 Chaveamento para o Site Secundário

Em caso de queda do Site Primário (CAPGV), todo o tráfego oriundo das unidades distribuídas deverá ser chaveado (roteado) para o Site Secundário. A critério do Banco, tal chaveamento poderá ser manual, isto é, com intervenção humana e agendado com o Banco, ou automático, isto é, sem intervenção humana. O método inicial será informado no momento da implantação aos CONTRATADAS.

Também a critério do Banco, o tráfego de determinada operadora poderá ser direcionado para o Site Primário (CAPGV) e/ou Site Secundário.

3.3 Plano de Upgrade para a Solução em Ambiente em Produção

Com base na expectativa de aumento na quantidade de Unidades Distribuídas e/ou Postos, assim como possível incremento de banda dos circuitos atualmente identificados no **ANEXO VIII – Endereços e velocidades**, o Banco reservará um percentual de **até 10%** (dez por cento) do valor do contrato atual para atender a estas demandas, durante a vigência do contrato.

Prevalecem os requisitos de crescimento e aumento de banda de todos os equipamentos, conforme já descrito no Edital, os quantitativos informados na Tabela de Serviços sob Demanda representam apenas uma reserva para serviços que não precisarão de aditivação no contrato atual.

Identificada a necessidade, por parte do Banco, será enviado e-mail à CONTRATADA, com solicitação de upgrade de um link atual (para um perfil de banda disponibilizado neste contrato) ou solicitação de adição de nova unidade, para que a CONTRATADA possa atender à solicitação, sem a necessidade de aditivo contratual, considerando os prazos previstos no **ANEXO XI - ACORDO DE NÍVEIS DE SERVIÇO**.

Os Serviços sob demanda representam uma contingência para o caso de ampliação de banda de Unidades Distribuídas atuais ou criação de novas Unidades Distribuídas/Postos. Os quantitativos não representam obrigação de Contratação por parte do Banco, apenas para utilização caso haja crescimento de demanda/necessidade e sua solicitação ficará a critério do Banco sem necessidade de aditivo no contrato para solicitação dos serviços. Para ambos os casos a OPERADORA será consultada sobre a viabilidade.

Após o atendimento da solicitação, será gerado um **Termo de Ampliação do Remoto (TAR)** e, no mês subsequente, deverá ser enviada planilha com as quantidades de sites e Banda para batimento dos valores a serem pagos, conforme modelo de Proposta, (**Anexo II – Modelo de Proposta**, respeitando os valores já firmados para unidades com a mesma velocidade no mesmo estado da federação.

4 APLICAÇÃO DE POLÍTICAS DE CONTROLE DE TRÁFEGO

4.1 Os serviços deverão ser prestados de modo a possibilitar o controle do tráfego de dados, voz e imagens, de acordo com as classes de serviços definidas neste Anexo. O controle do tráfego deverá ser baseado, dentre outros, nos seguintes parâmetros:

4.1.1 Endereços de origem e destino do Internet Protocol (IP);

4.1.2 Portas de origem e de destino relacionadas aos diversos protocolos que operam em conjunto com o Internet Protocol (IP).

4.1.3 No tráfego previamente marcado pela solução de SD-WAN e/ou marcado pelos equipamentos do Banco.

4.1.4 Os valores de largura de banda que são definidos no Anexo VIII - Endereços e Velocidades para cada classe de serviço (imagem, voz e dados de alta, média e baixa prioridade) representam os limites mínimos garantidos da utilização de cada classe. Caso uma determinada classe não esteja utilizando a capacidade total da largura de banda alocada para a mesma, essa capacidade excedente poderá ser utilizada por outras classes de serviço, respeitando a priorização de tráfego definida pelo Banco no item 4 deste anexo. Exceto as classes de voz e imagem, que não poderão extrapolar o limite estabelecido.

4.1.5 A solução SD-WAN do Banco realizará tuneis entre os sites, inclusive para links MPLS. Por esse motivo, o mesmo IP de origem da interface do dispositivo SD-WAN será usado para diferentes origens e priorizações internas.

Fornecimento de informações

Quando da implantação dos serviços, caberá ao Banco o fornecimento de todas as informações sobre sua infraestrutura de tecnologia, desde que pertinentes aos serviços ora especificados, de modo a permitir a adequada configuração dos componentes envolvidos nos serviços, incluindo:

- Plano de endereçamento utilizado pelo Internet Protocol (IP) na rede interna do Banco e unidades remotas;
- Protocolos de roteamento utilizados;
- Detalhamento de regras e políticas de controle e qualificação de tráfego;
- Detalhamento da caracterização do tráfego de dados, voz e imagens, incluindo suas possíveis subclassificações;
- Padrão de configuração de sistema operacional de roteadores e comutadores.

5 REQUISITOS GERAIS PARA OS EQUIPAMENTOS APPLIANCES SD-WAN

Todos os equipamentos *appliances* a serem fornecidos para atender os serviços de SD-WAN nas Unidades Distribuídas do Banco, no Site Primário e Site Secundário deverão atender ao seguinte conjunto de requisitos:

5.1 Os equipamentos *appliances* SD-WAN destinam-se para uso nas Unidades Distribuídas e Datacenters. Não está previsto o seu uso na Rede Parceiros e Postos neste primeiro momento. Havendo necessidade, a critério do Banco, aditivos contratuais de expansão serão providenciados;

5.2 A solução será composta pelos serviços do SASE NOC (Network Operations Center).

5.3 Deverão ser novos, isto é, sem utilização anterior (exceto se tiverem sido utilizados com o único propósito de homologação citada neste edital);

5.4 Todos os produtos que compõem a solução devem ser fornecidos com o devido licenciamento, incluindo garantia de atualização de software, de manutenção e de troca do hardware pelo período de vigência do Contrato estabelecido pelo Edital;

5.5 Todas as funcionalidades devem estar disponíveis na versão atual da solução ofertada, não serão aceitos equipamentos cujas funcionalidades ainda estão em desenvolvimento (Roadmap);

5.6 Deverão possuir LED’s indicativos do estado de funcionamento do equipamento;

5.7 Os equipamentos fornecidos para SD-WAN nas Unidades Distribuídas deverão implementar “zero-touch” em sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento SD-WAN, mesmo antes do equipamento ser conectado à rede, transformando a atividade remota em uma simples troca física de equipamento, em caso de falha do mesmo, sem a necessidade de configurações individuais nos equipamentos. O Banco entende por zero-touch a possibilidade de conexão do equipamento na unidade remota e somente com um link de internet ativo o equipamento deverá consultar a nuvem do fabricante e entender que deve ser gerenciado pela solução instalada no Banco (on-permise) ou em nuvem e receber toda a configuração de forma automática sem a

necessidade de nenhum tipo de configuração posterior no equipamento remoto, mesmo antes da instalação física;

5.8 A solução SD-WAN deverá ocupar no máximo 2Us (Rack units) em cada Unidade Distribuída e receberá as conexões dos equipamentos do Banco, sendo essas conexões de responsabilidade da CONTRATADA e entre a solução ofertada e o(s) switch(es) do Banco. Trata-se de uma conexão puramente camada 2. Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas ou fornecer prateleira de rack para qualquer equipamento fora desse padrão;

5.9 Nas Unidades Distribuídas, a solução de SD-WAN deverá ter capacidade para receber os acessos primários, secundários e terciários em portas WAN de 1Gbps, padrão Ethernet RJ-45, dedicadas para este fim (não podendo ser interface do tipo celular);

5.10 Deverão atender aos padrões: IEEE 802.2; IEEE 802.3 e IEEE 802.3u, IEEE 802.3z;

5.11 Todas as portas utilizadas na solução deverão ser compatíveis com conexão com switches e roteadores sem necessidade de cabos *crossover*;

5.12 Nas Unidades Distribuídas, a solução SD-WAN deve possuir pelo menos **03 (três)** interfaces 10/100/1000Mbps, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, exclusivas para conexão com a **LAN** do Banco;

5.13 A solução entregue no datacenter deve ser compatível com conexão via SFP+ utilizando fibra padrão OM4 que deverá ser entregue pela CONTRATADA, com padrão de velocidade 10Gbps e conector tipo LC no tamanho de 4 metros ou superior, de forma redundante e sem oversubscription. Toda a conectividade e redundância entre os equipamentos da solução contratada no datacenter é de responsabilidade da CONTRATADA. Devem ser fornecidas no mínimo **04 (quatro)** exclusivas para conexão com a **LAN** do Banco além de **03 (três)** interfaces para recepção dos túneis **WAN** via comunicação MPLS e Internet; O(s) transceiver(s) SFP+ necessário(s) para conexão da interface do equipamento de SD-WAN deverão ser fornecidos em conjunto com a solução. Não será necessário o fornecimento do transceiver para conexão com a rede do Banco;

5.14 Os quantitativos de interfaces aqui especificados são mínimos. O quantitativo real necessário deverá ser considerado de acordo com o dimensionamento efetuado pela CONTRATADA, de acordo com a arquitetura ofertada;

5.15 Para cada equipamento entregue, deve ser entregue 03 (três) cabos UTP de 2,5 metros crimpados com RJ45 de fábrica e com a devida certificação. Os mesmo deverão ser de categoria 6 ou superior. Durante ativação do roteador, o cabo deverá ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação;

5.16 Nos Datacenters, em caso de fornecimento de solução SD-WAN com mais interfaces de conexão, compatíveis com as velocidades 1/10/40Gbps, todas devem ser licenciadas para uso a critério do Banco e devem ser entregues com transceivers de fibra instalados e licenciados. Para os casos com mais de 2 interfaces 10/40Gbps, pelo menos 02 (duas)

deverão vir com transceivers de 40G, as demais poderão vir com transceivers de 1Gpbs/10Gbps. Para todas as interfaces/transceivers de fibra, deverão ser entregues fibras LC compatíveis e com tamanho de 20m mínimo;

5.17 Deverão suportar conexões no ambiente do Banco com tensão elétrica de 110V~220V AC, 50~60Hz, e deverão suportar modo automático;

5.18 Os appliances SD-WAN ofertados destinados aos Datacenters devem possuir fontes redundantes internas e hot-swap;

5.18.1 O conjunto de fontes deve possuir, pelo menos, 2 (duas) conexões independentes, permitindo a sua ligação a circuitos elétricos externos distintos;

5.18.2 Realizar a comutação entre as fontes de forma automática e sem qualquer interrupção no funcionamento do equipamento.

5.18.3 Possuir capacidade para manter a operação do equipamento em condição de consumo máximo mesmo na falha de uma fonte;

5.19 A solução SD-WAN deve obedecer ao princípio básico da arquitetura SDN (Software Defined Networks), separando os planos de encaminhamento de tráfego, controle e gerenciamento em equipamentos distintos. Em caso de falha dos planos de controle ou gerenciamento, não deve haver impacto nos serviços do plano de encaminhamento. O appliance SD-WAN deve atuar de forma eficiente no encaminhamento de tráfego, de acordo com as sinalizações vindas do plano de controle.

5.20 Os planos de encaminhamento (forwarding plane), controle (control plane), plano de gerência e orquestração devem ser logicamente independentes e implementados em equipamentos distintos.

5.21 A solução deve possuir a capacidade de realizar agregação de banda através de uma interface lógica única ou fluxo lógico único, e de forma automática distribuir os dados entre links de distintas velocidades, levando em consideração a utilização de banda completa de cada link sem ocasionar congestionamento nos links de baixa velocidade.

5.22 Deverá permitir uma camada de roteamento virtual sobre a estrutura de rede tradicional, possibilitando o encaminhamento do tráfego por diferentes tipos de circuitos WAN, inclusive circuitos WAN com NAT e endereçamento dinâmico;

5.23 A solução SD-WAN deverá oferecer suporte à orquestração de túneis criptografados desde a Unidade Distribuída até o Data Center, denominados comunicação overlay, o que permitirá independência do tipo de link utilizado (comunicação underlay);

5.24 A solução deverá utilizar estes Overlays para o transporte das aplicações conforme as regras de negócio definidas, estes devem utilizar os protocolos de túnel IPSEC e GRE.

5.25 A solução SD-WAN Central deverá permitir a criação de túneis entre localidades de forma manual, automática e/ou de acordo com a intenção do tráfego.

5.26 A solução SD-WAN Central deverá possuir capacidade suficiente para suportar todas as VPN's (ou equivalentes) de todos os *appliances* das unidades remotas, assim como a quantidade prevista de ampliação, conforme **Anexo II – Modelo de Proposta**;

5.27 Caso haja necessidade de utilizar mais de 02 (dois) equipamentos para composição de throughput da solução SD-WAN central, todos os equipamentos deverão ser da mesma família e modelo, ambos licenciados para operar em modo ATIVO-ATIVO;

5.27.1 Caso haja necessidade de utilizar mais de 02 (dois) equipamentos SD-WAN na solução de SD-WAN central, a CONTRTATADA deverá fornecer comutadores gerenciados e redundantes para interconexão destes equipamentos a menos que utilizem portas especificas/proprietárias para interconexão da solução ou formação de cluster;

5.27.2 Caso sejam fornecidos equipamentos comutadores, não deve haver prejuízo para a solução ofertada no que se refere aos padrões de conectividade, redundância e nível de serviço previstos nesta especificação.

5.27.3 A solução deverá funcionar de forma transparente, sobretudo em relação a balanceamento das conexões e cuidados com assimetria de tráfego.

5.28 A solução SD-WAN Central deverá entregar uma gerência/orquestração integrada e resiliente para toda as unidades, não devendo criar segregação ou grupos estáticos das Unidades Distribuídas na comunicação destas com os DataCenters;

5.29 A solução deve implementar automação na formação de túneis, por meio de associação de perfis de configuração utilizando uma única interface gráfica.

5.30 A solução deverá possibilitar que uma mesma interface WAN possa enviar tráfego simultaneamente através de túneis IPSec SD-WAN e nativamente por fora dos túneis via comunicação underlay.

5.31 A solução de SD-WAN deverá permitir criar VPNs "Full-Mesh", de forma a permitir a comunicação ponto-a-ponto dentro das redes MPLS do acesso primário, das redes MPLS do acesso secundário e dos acessos Internet Simétrica, sem passar necessariamente pelos concentradores (a critério do Banco);

5.32 A solução WAN proposta deve suportar simultaneamente hub e spoke, malha, malha parcial e topologia de malha regional na construção dos Overlays.

5.33 A solução deverá permitir ao administrador definir políticas de encaminhamento de tráfego que levem em consideração a disponibilidade dos links e as métricas de jitter, latência e perda de pacotes para selecionar, de forma totalmente automática ou manual, a critério do Banco, qual caminho uma aplicação irá utilizar de forma dinâmica.

5.34 A comutação de tráfego por pacote deve permitir que um fluxo possa mudar de um link para outro, várias vezes, sem desconectar a sessão tcp ou udp da aplicação. Em caso de falha do link essa comutação deve ocorrer em menos de 1 segundo.

5.35 A solução deve ser composta com uma Console Central de Orquestração, podendo esta ser instalada no Datacenter (on-premises) ou em nuvem do Fabricante, com conexão via Internet. A solução será responsável por fazer toda a configuração dos appliances SD-

WAN, incluindo priorização de tráfego, configurações de QoS, que deverão ocorrer de forma centralizada. A console de gerenciamento SD-WAN deverá ser do mesmo fabricante dos appliances SD-WAN;

5.36 No caso da instalação da solução de gerenciamento e orquestração instalada fora no Datacenter, apenas metadados e dados de gerenciamento poderão ser transmitidos para nuvem e a solução deverá implementar duplo fator de autenticação (MFA) integrado à console em nuvem do fabricante para acesso ao portal de gerenciamento. A indisponibilidade da interface gerência e orquestração não deverá comprometer o funcionamento do serviço/configurações de SD-WAN;

5.37 Deve implementar configuração Zero Touch, onde um equipamento é ligado na localidade e via internet ele busca a configuração na Plataforma de Gerenciamento. A plataforma em Cloud deve ser Multi-Tenancy e suportar múltiplos clientes sendo gerenciados, onda cada cliente deverá possuir o seu login e ter acesso somente aos seus equipamentos.

5.38 Via gerenciamento fornecido, deverá ser possível informar quais são os links disponíveis em cada localidade, bem como a largura de banda consumida por unidade e por link;

5.39 A solução de gerenciamento e configuração dos dispositivos deve ser do mesmo fabricante de SD-WAN;

5.40 A solução de Gerenciamento deverá ser centralizada para o serviço de SD-WAN, concentrando todas as configurações via central de gerenciamento SD-WAN para todos os equipamentos envolvidos nessa solução;

5.41 Deverão permitir upgrade de sistema operacional de forma centralizada, via ferramenta de gerência, e para toda a solução, desde a cópia das novas imagens de sistema se for o caso, como a atualização em questão;

5.42 A solução deverá permitir atualização e sincronização automática de "clock", de forma que os relatórios e todas as informações sejam sincronizados com o horário oficial via NTP (Network Time Protocol);

5.43 Além da configuração centralizada, o equipamento deverá possuir forma de configuração ou acesso local via console out-of-band ou via protocolo HTTPS, sendo conexão serial ou UTP ou USB ou equivalente;

5.44 Deverão estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network Management Protocol), com suporte a RFC 1213 (MIB-II), suporte a SNMPv2c, Suporte ao SNMP v3 e suporte à geração de traps;

5.45 Permitir o gerenciamento dos tuneis VPN através de SNMP;

5.46 Deverão Implementar Network Address Translation (NAT);

5.47 Efetuar o registro em log de todos os acessos efetuados, incluindo data, hora, site, endereço IP e usuário que efetuou o acesso.

5.48 Permitir integração com servidores de log externo (syslog);

5.49 A Solução deverá permitir ao administrador criar cada localidade informando o endereço físico dessa localidade, para que a solução de gerência possa exibi-la no mapa do Dashboard em aplicativo de monitoramento entregue;

5.50 Cada solução de gerenciamento que for instalada nos datacenters (Site Principal e Site Secundário) deverá possuir redundância entre os datacenters. Isto é, caso sejam providos N-equipamentos para atender a solução de gerenciamento no Site Principal, deverão ser providos N-equipamentos para atender a solução de gerenciamento no Site Secundário, com chaveamento automático em até 3 (três) minutos sem perda de informações de gerência durante este período. Enquanto a solução estiver funcionando em contingência (com indisponibilidades no Site Principal ou Site Secundário), haverá apuração de SLA de disponibilidade;

5.51 Em nenhuma hipótese, os equipamentos da solução deverão perder a gerência por motivo de tráfego externo ou interno na unidade remota e no CAPGV. Para isso, a solução poderá implementar, caso precise, gerência out-of-band e/ou interfaces com inteligência para tratar esse tráfego, de forma que a gerência e a rede da unidade remota não fiquem indisponíveis por falha de qualquer das soluções contratadas no Edital;

5.52 Deverá implementar na própria solução todos os protocolos necessários para desempenhar o papel de SD-WAN e Gerenciamento, no mínimo: WCCP ou similar, PBR e BGP. No Site Principal e no Site secundário, a vizinhança entre o Banco e a solução SD-WAN será via roteamento estático e/ou BGP, a ser definido pelo Banco na implementação. Ainda nas redes de datacenter, a conexão lógica com os roteadores concentradores das operadoras MPLS será de responsabilidade da solução contratada, sendo puramente via BGP, se assim definido pelo Banco na implementação;

5.53 O sistema de gerenciamento deverá informar a largura de banda de Inbound e Outbound de cada circuito de comunicação, seja via cadastro manual ou de forma automática. A informação de utilização dos links deverá ser correlacionada com o tamanho real do circuito de comunicação;

5.54 A solução deverá ser capaz de fornecer via portal https visibilidade de dados trafegados por cada link em tempo real (para troubleshoot) e também via portal de relatórios (gerenciamento) após no máximo 5 minutos do tráfego em questão. A necessidade é para todos os links envolvidos e conectados nos equipamentos SD-WAN, inclusive para a comunicação entre Unidades Distribuídas, ou seja, onde o tráfego não passe pelo Datacenter;

5.55 Deverá possuir mecanismos de authentication, authorization and accounting (AAA) através de Servidor RADIUS e/ou TACACS+ e/ou Azure Active Directory e/ou outros Identity Providers;

5.56 A empresa contratada deverá fornecer dois níveis de acesso ao Banco, sendo um deles somente leitura e outro com perfil administrativo para realização de configurações, quando solicitado. Ambos os acessos devem ser fornecidos para todos os equipamentos e softwares envolvidos na solução. Os acessos de leitura deverão permitir a visualização das estatísticas do equipamento passíveis de consulta, como QoS, estatísticas de tráfego, além da configuração dos equipamentos, e qualquer política criada na solução contratada. O acesso mínimo (de leitura) deverá ser fornecido acesso via HTTPS. O acesso deverá permanecer ativo durante todo o Contrato. A solução deverá implementar auditoria sobre as alterações de configuração realizadas por cada usuário. Qualquer alteração feita pelo Banco será de responsabilidade do Banco, cabendo ao CONTRATADO, monitorar e questionar sobre a configuração realizada em até 72h corridas, tornando-se o CONTRATADO responsável pela alteração na sequência para termos de SLA de disponibilidade e demais obrigações contratuais;

5.57 No caso de um equipamento ser compatível com acesso via SSH, será obrigatório o fornecimento do acesso ao Banco, conforme detalhado acima. Utilização de acesso de telnet (sem criptografia) para gerenciamento não será permitido no Banco;

5.58 Deverá ser fornecido usuário de leitura para o Banco para todos os equipamentos e softwares que compõem os equipamentos de SD-WAN e SSE (SASE);

5.59 O não fornecimento de quaisquer desses acessos implicará em sanções administrativas de acordo com o **Anexo XI - Acordo de Níveis de Serviços**, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

5.60 Necessariamente, a solução de SD-WAN contratada nas remotas será o default gateway dos equipamentos naquela unidade remota (estações de trabalho, aparelhos IP, servidores e impressoras.);

5.61 A solução deverá fornecer IP via DHCP server, sendo fornecimento próprio via DHCP server para todas as Unidades Distribuídas. A funcionalidade deverá ser gerenciada/configurada de forma centralizada no mesmo portal SD-WAN . Dentre os parâmetros necessários do DHCP server, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com a solicitação do Banco. Atualmente, o Banco utiliza opções 246 e 248 com string de até 70 caracteres, por exemplo. A solicitação de configuração por parte do Banco não deverá representar custos adicionais ao projeto e deverá atender o SLA definido;

5.62 A solução deverá ser compatível com a implementação de Network Address Translation (NAT);

5.63 Garantir o funcionamento do tráfego de FTP entre as unidades distribuídas e o CAPGV, mesmo quando passar por NAT nos equipamentos fornecidos;

5.64 A solução deverá implementar funcionalidades de Access Control List (ACL) simples e estendidas ou similar com o objetivo de permitir e/ou bloquear tráfego informados pelo Banco;

5.65 A solução SD-WAN Central deverá implementar Agregação de links (802.3ad/LACP) para comunicação com os comutadores do BNB. A agregação poderá ser realizada diretamente pelos appliances ou por comutadores fornecidos com a solução nos cenários onde a distribuição dinâmica de carga entre interfaces ocorra via orquestração centralizada;

5.66 Em caso de falha ou degradação das métricas dos circuitos de comunicação, o tráfego deverá ser desviado automaticamente para outro link ativo e após resolução dos problemas, o retorno do tráfego deverá ser automático, ou seja, sem configuração manual;

5.67 A solução SD-WAN deve permitir a monitoração da latência, do *jitter* e do descarte de pacotes em cada um dos links individualmente e em cada direção (*uplink/downlink*) de forma independente;

5.68 A solução deverá implementar mecanismo de proteção contra variação de latência (*jitter*) ainda que a degradação seja em todos os links, para proteger o tráfego do tipo tempo real (voz e vídeo).

5.69 A solução deve ser capaz de monitorar e qualificar os links (em pelo menos dois níveis de qualificação);

5.70 A solução deve implementar MOS (*Mean Opinion Score*) ou recurso de avaliação de qualidade similar;

5.71 A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

5.71.1 Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente;

5.71.2 Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, *jitter*, perda de pacotes ou largura de banda;

5.72 A solução SD-WAN deve ser capaz de utilizar todos os circuitos disponíveis na unidade distribuída e realizar balanceamento entre os links simultaneamente;

5.73 A solução deve permitir a verificação constante da situação dos links com o objetivo de identificar oscilações ou perdas destes, aplicando penalidades de forma automática, para não impactar os serviços e a experiência dos usuários;

5.74 Deve implementar solução de FEC (*Forward Error Correction*) nas conexões entre os appliances remotos e o datacenter, que possibilitem a redução da perda de pacotes na rede:

5.74.1 Tal funcionalidade deverá ocorrer em ambos os sentidos do tráfego;

5.74.2 Essa função pode ser substituída por duplicação de pacotes por caminhos distintos;

8.74.2.1 No caso de duplicação de pacotes, a solução deverá garantir que os hosts não recebam pacotes duplicados;

5.74.3 Deverá ser possível determinar em qual serviço o FEC ou duplicação de pacotes será habilitado.

5.75 A solução de VPN deverá implementar a funcionalidade de rekey na fase 1 (Envolve a renegociação da SA IKE. Isso garante que o canal seguro usado para negociar as SA IPsec continue protegido) ou 2 (Envolve a renegociação da SA IKE. Isso garante que o canal seguro usado para negociar as SA IPsec continue protegido). Essa funcionalidade deve permitir a renovação das chaves criptográficas utilizadas na comunicação.

5.76 A solução deverá ser capaz de criar Interfaces VLANs L3 e realizar o roteamento dessas redes e realizar a publicação via BGP dessas redes, se assim solicitado pelo Banco;

5.77 Implementar a criação de VLANs, permitindo:

5.77.1 Criar múltiplas VLANs, no mínimo 10;
5.77.2 Configurar a porta LAN da solução para suportar uma única VLAN (Porta de Acesso) ou múltiplas VLANs (Porta em Trunk);
5.77.3 Especificar uma subnet IP e associá-la à VLAN;
5.77.4 Configurar o appliance como o Gateway da VLAN;
5.77.5 Todas as VLANs deverão funcionar em contingência de gateway com o roteador MPLS conforme descrito em item anterior.
5.77.6 Permitir criar regras que impeçam a comunicação entre VLAN's na LAN das unidades distribuídas das quais o SD-WAN é o gateway;

5.78 A solução deverá ser capaz de definir políticas de engenharia de tráfego de forma centralizada com classificação do tráfego nos links disponíveis, utilizando pelo menos os seguintes critérios:

5.78.1 Com base em um único ou vários IPs;
5.78.2 Com base em uma única ou várias Subnet;
5.78.3 Com base em uma ou várias portas TCP/UDP;
5.78.4 Com base no valor do DSCP;
5.78.5 Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN.

5.79 A solução deve implementar controles de políticas de acesso por IP (origem e destino) porta (destino) e protocolo, inclusive nas redes locais onde o *appliance* SD-WAN estiver conectado.

5.80 Deve suportar a consulta a fontes externas de endereços IP, podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego (esta funcionalidade poderá ser atendida no SD-WAN ou no serviço SSE especificado no item 9).

5.81 A solução deverá ser compatível com as classes de QoS informadas na especificação dos circuitos de comunicação e roteadores do Edital;

5.82 A solução deverá alocar/especificar largura de banda do circuito de comunicação conforme a Classe e Nível de prioridade do tráfego;

5.83 A solução de SD-WAN deverá ser capaz de classificar e marcar os pacotes com DSCP (Differentiad Services Code Point), conforme as políticas definidas pelo Banco, para que os roteadores das operadoras contratadas possam dar a devida prioridade e banda necessária para cada tráfego, tanto do lado do datacenter (site principal e site

secundário) como do lado das Unidades Distribuídas. Essa configuração deverá ser realizada de forma centralizada na solução de SD-WAN;

5.84 Para a comunicação via acessos MPLS, a solução de SD-WAN deverá também manter (ou alterar a critério do Banco) a marcação QoS nos casos informados pelo Banco. Será necessário, no mínimo, para manter o tráfego marcado com DSCP EF (VOIP) e AF41 (vídeo) na origem, de acordo com solicitação do Banco. Essa marcação será usada no processo de priorização dos circuitos MPLS na nuvem da operadora. No caso do tráfego destinado via link de internet, por indisponibilidade do link MPLS ou pela qualidade de link internet estar melhor, a marcação recebida pela rede interna deverá ser usada para priorização nas filas de transmissão de QoS da solução SD-WAN.

5.85 A solução deverá possuir a capacidade de classificar e visualizar o tráfego de rede para colocá-lo em uma das classes de serviço de acordo, com pelo menos os seguintes critérios:

- 5.85.1 Com base em um único ou vários IPs;
- 5.85.2 Com base em uma única ou várias Subnet;
- 5.85.3 Com base em uma ou várias portas TCP/UDP;
- 5.85.4 Com base no valor do DSCP;
- 5.85.5 Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN, no mínimo 1.100 aplicações (sendo no mínimo as aplicações Microsoft Office 365, Teams, Windows Update, Youtube, Facebook/Meta, Whatsup, google drive, instagram, Skype, Symantec, Outlook, p2p e acesso remoto.);

5.86 Deverá ser possível verificar, via sistema de gerenciamento, por qual caminho (qual circuito de comunicação) cada aplicação está trafegando. A solução deve ser capaz de fornecer visibilidade em todo o caminho (desde o Data Center até a Unidade Distribuída);

5.87 O tráfego deverá ser capturado, no mínimo, através de flows exportados diretamente dos equipamentos envolvidos nessa contratação, mas obrigatoriamente deve ser independente dos modelos de roteadores ou qualquer outro equipamento externo a solução contratada;

5.88 Deverá ser capaz de apresentar estatísticas de utilização das interfaces em ambos os sentidos, entrada e saída;

5.89 A solução SD-WAN deve permitir monitorar, no mínimo, os seguintes recursos:

- 5.89.1 Principais aplicativos/aplicações que estão usando mais largura de banda na WAN;
- 5.89.2 análise de partes da WAN com a latência mais alta em tempo real.
- 5.89.3 análise de perda média e máxima de pacotes em tempo real, em conjunto e em conexões WAN individuais.
- 5.89.4 identificação/quantificar pacotes que são entregues na WAN, em média e durante os períodos de pico;
- 5.89.5 informações de fluxo do usuário(ou endereço IP) em tempo real para solução de problemas;
- 5.89.6 visualização do túnel Overlay em tempo real para mostrar como vários transportes estão sendo usados pelas políticas de aplicativo
- 5.89.7 gráficos em tempo real que mostram o uso da largura de banda de diferentes classes de tráfego, como voz, vídeo e aplicativos de transferência de arquivos.

5.89.8 visualização da latência no caminho WAN.

5.90 A solução deverá fornecer dados de Internet Protocol Flow Information eXport (IPFIX) ou Netflow ou equivalente tanto para o serviço de gerenciamento do NOC dessa contratação como para as ferramentas do Banco, se solicitado pelo Banco, sem custos adicionais. Atualmente, as ferramentas do Banco são do fabricante CA e o flow deve ser compatível com os produtos desse fabricante (Spectrum Version 10.2.1.0.98 e Network Flow Analysis 9.2.1);

5.91 As informações de relatórios de tráfego devem estar disponíveis por no mínimo 06 (seis) meses;

5.92 Implementar tecnologia para reconhecimento de aplicações e subaplicações (DPI - Deep Packet Inspection);

5.93 Para os Datacenters, a solução SD-WAN deverá suportar a capacidade de roteamento de tráfego (throughput), no mínimo de **30Gbps**;

5.93.1 Para os Datacenters, deverá possuir uma Solução de Firewall incorporado aos equipamentos de SD-WAN do mesmo fabricante, tanto para a solução instalada no Site Principal como no Site Secundário. A solução de firewall deverá possuir *throughput* compatível com o tráfego dimensionado para a solução de SD-WAN central, considerando uso dos recursos de visibilidade camada 7 do tráfego e criptografia dos túneis VPN;

5.94 Para dimensionamento da solução das Unidades Distribuídas, a título de roteamento de tráfego (throughput), suportar a soma dos links daquela Unidade, conforme Anexo VIII - Endereços e Velocidades do Edital, permitindo escalar o crescimento de 100% (cem por cento), sem a necessidade de troca do equipamento. Isto é, caso o somatório de larguras de banda de determinada localidade seja 320Mbps, o equipamento deverá suportar o tráfego WAN de pelo menos 640Mbps;

5.95 Caso o licenciamento de firewall/SD-WAN seja separado do licenciamento do throughput de roteamento, será permitido o licenciamento de firewall/SD-WAN de acordo com a soma dos links daquela Unidade naquele momento. Desde que este licenciamento acompanhe o crescimento de até o limite de 100% (cem por cento), sem custos adicionais ao Banco, e implementado de maneira transparente e sem impacto para o roteamento da unidade.

5.96 Nas Unidades Distribuídas, deverá possuir uma Solução de Firewall incorporado aos equipamentos de SD-WAN, do mesmo fabricante. A solução de firewall deverá possuir *throughput* compatível com o tráfego dimensionado para a solução de SD-WAN daquela unidade, considerando inclusive o crescimento mencionado acima, com o uso dos recursos de visibilidade camada 7 do tráfego e criptografia dos túneis VPN.

5.97 O recurso de firewall dos appliances SD-WAN de cada unidade deverá implementar regras de liberações de acesso para Internet (breakout) a critério do BANCO. A replicação e ativação da regra/política deverá ser feita de forma automática após publicação centralizada. Deverá ser possível criar liberações de acesso para destinos, informando o endereçamento IP ou redes sumarizadas válidas na internet, domínio de internet (URL) por aplicação reconhecida pelo fornecedor de SD-WAN sendo no mínimo

as aplicações Microsoft Office 365, Teams, Windows Update, Youtube, Facebook/Meta, WhatsApp, google drive, instagram, Skype, Cortex XDR, Outlook, p2p e acesso remoto.;

5.98 Para as Unidades Distribuídas, a funcionalidade de firewall deverá realizar bloqueio de qualquer tráfego originado na Internet, sem que nenhuma publicação da rede do Banco seja possível para acesso externo. Somente deverá ser permitido nas Unidades Distribuídas tráfego via VPN (via Internet e via MPLS), ou seja, tunel VPN fechado entre os dispositivos SD-WAN parte desta solução, sendo a exceção, somente os tráfegos explicitamente liberados conforme regras acima descritas (breakout). O tráfego sem criptografia é aceito somente na falha do appliance de SD-WAN remoto, onde obrigatoriamente somente a rede MPLS será usada para trafegar informações;

5.99 A solução deverá suportar a quantidade de 200 sessões simultâneas por usuário, no mínimo. A quantidade mínima de usuários por unidade está disponível **no Anexo VIII - Endereços e Velocidades**;

5.100 Deverá permitir regras globais para controles de segurança de camada L4 - L7 para as Unidades Distribuídas;

5.101 Deverá permitir regras de controle de segurança baseado em Protocolos (TCP e UDP) para as Unidades Distribuídas;

5.102 Deverá permitir engenharia de tráfego inteligente para identificar e classificar aplicativos até o nível de protocolo de aplicação (L7), implementando políticas de roteamento dinâmicas baseadas em condições de rede em tempo real e priorizando tráfego para aplicativos críticos de negócios.

5.103 Deverá permitir SLAs de aplicação, garantindo níveis de serviço específicos para todos os aplicativos, assegurando desempenho e disponibilidade, monitoramento contínuo do desempenho dos aplicativos e ajuste automático das políticas de tráfego para manter os SLAs e apresentar relatórios detalhados sobre o cumprimento dos SLAs e desempenho dos aplicativos.

5.104 Deverá permitir regras de controle de segurança baseado em IP e Porta de Origem e em IP e Porta de Destino, com a capacidade de implementação de máscaras de subnet de comprimento variável para as Unidades Distribuídas;

5.105 As regras deverão permitir bloquear ou liberar o tráfego com base em aplicações customizadas pelo administrador, sendo que deverá ser possível fazer a definição com base nos critérios mínimos, abaixo relacionados:

5.105.1 Com base em um único ou vários IPs;
5.105.2 Com base em uma única ou várias Subnet;
5.105.3 Com base em uma ou várias portas TCP/UDP;
5.105.4 Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN;

5.106 A solução SD-WAN deverá implementar a infraestrutura de chave pública (PKI), de forma integrada, usando a autoridade de certificação (CA) ou através de uso do pre-shared key para troca de chave entre o appliances;

5.107 A solução deverá ser capaz de suportar para fechamento dos túneis criptografados:

5.107.1 Autenticação via Pre-Shared Key ou Certificado Digital X.509;

5.107.2 Suportar os protocolos IKE versões 1 e 2 para troca de chaves;

5.107.3 Deve suportar os algoritmos de criptografia AES-128 e AES-256;

5.107.4 Deve suportar, no mínimo, dois tipos de Algoritmos de Hash (MD5, SHA1, SHA256);

5.107.5 Deve suportar os Grupos de Diffie–Hellman Group14 (2048 Bits) e Group 19 (256 Bits eliptic curve);

5.108 A solução deverá possuir recursos de proteção, no mínimo contra os seguintes tipos de ataques:

5.108.1 Denial-of-Service (DoS)

5.108.2 TCP-based attacks : Invalid TCP Flags, TCP Land, e TCP SYN Fragment

5.108.3 ICMP-based attacks: ICMP Ping of Death e ICMP Fragment

5.108.4 IP Unknown Protocol

5.109 A contingência da solução SD-WAN deve ocorrer em âmbito local e global. Todas as necessidades de hardware (incluindo comutadores) e software (incluindo protocolos) necessários para a redundância e alta disponibilidade da solução exigidas nessas especificações devem ser fornecidas pela solução contratada;

5.110 Cada solução SD-WAN instalada nos datacenters (Site Principal e Site Secundário) deverá possuir redundância N+1 e alta disponibilidade para todos os componentes em cada datacenter, de forma que quaisquer indisponibilidades em N-equipamentos SD-WAN sejam chaveadas automaticamente em até 3 (três) minutos sem perda de performance, dentro do mesmo datacenter inicialmente, após esse período. Enquanto a solução estiver funcionando em contingência, haverá apuração de SLA de disponibilidade;

5.111 Em âmbito global, cada unidade distribuída deve possuir concentração para 2 (dois) sites concentradores/datacenters funcionando em modo ativo-ativo;

5.112 A solução SD-WAN das Unidades Distribuídas deverá implementar alta disponibilidade para, pelo menos, o circuito primário MPLS. Em caso da falha de um equipamento SD-WAN, o circuito primário MPLS deverá continuar ativo e em funcionamento, de maneira totalmente automática e transparente para o usuário, isto é, sem intervenção manual, podendo a solução utilizar protocolos de alta disponibilidade, como VRRP (Virtual Router Redundancy Protocol) disponibilizados pelos roteadores, ou bypass em hardware, especificamente para o circuito primário MPLS ou ainda prover appliances SD-WAN (N+1) com alta disponibilidade que sejam compatíveis com as especificações dos roteadores e topologia do Banco descritas no Edital. Para a alta disponibilidade, todas as necessidades físicas (como cabos, interfaces ou mesmo outros switches ou roteadores com portas "gigabit") e de software (no mínimo, protocolos e licenças) capazes de manter a alta disponibilidade deverá ser fornecidas em conjunto com a solução contratada;

5.113 Nas Unidades Distribuídas, em caso de indisponibilidade dos equipamentos do serviço SD-WAN, a solução deverá ainda bloquear todo e qualquer tráfego originado e/ou destinado diretamente à Internet. A falha do serviço de SD-WAN deverá indisponibilizar a comunicação direta com a Internet na unidade remota, inclusive em nível de camada

2 do modelo de referência OSI, sem prejuízo do chaveamento do tráfego para o circuito MPLS, conforme já descrito;

5.114 Durante a implantação da Solução SD-WAN e durante a falha de equipamentos, na vigência do Contrato, a solução implantada deverá permitir que sites que já possuem a nova solução SD-WAN continuem se comunicando com os sites que ainda não a possuem (ou que estejam em contingência, via comunicação MPLS);

5.115 Nas Unidades Distribuídas, caberá ao Banco o fornecimento de conectividade camada 2 (sem roteamento) entre a rede corporativa do Banco e os appliances da nova solução. A solução contratada deverá ser compatível com 802.1Q (passagem de VLANs) no caso de VLANs criadas nos roteadores da operadora MPLS;

5.116 É de responsabilidade da solução contratada implementar recursos para identificar e proteger os equipamentos SD-WAN de todo e qualquer tráfego interno a partir da unidade remota do Banco, seja por tempestades de broadcast, unicast, multicast ou por qualquer outro motivo. Todo problema interno na unidade não deverá ser replicado para outras redes do Banco. As unidades do Banco não possuem outros equipamentos L3 configurados além dos aqui contratados, diversas redes do Banco são "/16" e com endereçamentos válidos, porém não publicados para internet;

5.117 Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (Site Primário <-> Site Secundário), via roteamento dinâmico e sem intervenção manual;

5.118 Roteamento dinâmico implementado na LAN do CAPGV entre concentradores e roteador gateway. O protocolo de roteamento na LAN do CAPGV será definido pelo Banco durante implementação, atualmente é via BGP.

5.119 Deverá ser oferecido Treinamento de Operação de toda a solução SD-WAN ofertada com carga mínima de 40h, sendo esse ministrado nas dependências do CAPGV 4h por dia e contemplando no mínimo 1 turma de até 15 pessoas presenciais e outras 10 pessoas transmitindo remotamente via Teams onde será gravado pelo Banco do Nordeste como forma de treinamento e documentação para os profissionais internos. O treinamento deverá ser ministrado durante ou imediatamente após a implantação, a critério do Banco, pelo CONTRATADO ou por empresa contratada por este;

5.120 A instalação e configuração da solução ofertada é de responsabilidade da CONTRATADA, bem como toda a conexão de cabos e demais necessidades envolvidas na solução entregue, incluindo a conexão entre os roteadores dos circuitos de dados (primários, secundário e terciários) com a solução SD-WAN e a rede do Banco, de forma a causar o menor impacto possível nas migrações e manter os requisitos de segurança e disponibilidade exigidos no Edital, onde é fundamental que a conexão com qualquer circuito de internet seja realizada fisicamente passando pelo appliance de SD-WAN, por no mínimo:

5.120.1 Caso a solução de SD-WAN seja instalada na Unidade Distribuída antes da instalação dos novos circuitos de comunicação, a mesma deverá ser instalada utilizando os atuais circuitos de comunicação para encaminhamento do tráfego. Caberá ao vencedor desse item acompanhar com o NOC de

gerenciamento, mesmo que de forma remota, toda a conexão dos novos circuitos de dados com a rede do Banco, mantendo os requisitos de segurança solicitados no Edital, inclusive durante período de migração/implantação;

5.120.2 Caso a solução de SD-WAN seja instalada depois dos novos circuitos de dados, caberá ao contratado a conexão entre a solução de SD-WAN com os novos circuitos, bem como com a rede do Banco. No momento da migração, já será de responsabilidade do NOC contratado o acionamento da operadora para resolução de problemas de circuito de comunicação, seja relacionado com configuração ou com a ativação do mesmo;

5.120.3 O Banco se responsabilizará pela disponibilização de racks ou bancadas para instalação (caso não disponha de espaço no rack) e da infraestrutura elétrica necessária, tais como réguas e pontos de energia;

5.120.4 Caberá ao Banco o agendamento da instalação inicial com as suas Unidades e com as CONTRATADAS, de acordo com o cronograma definido pelas CONTRATADAS.

5.121 A solução SD-WAN deverá ser capaz de permitir integração segura entre unidades distribuída e plataformas SaaS (Software as Service) de outros fabricantes, de forma a diminuir a latência na comunicação e aumentar o desempenho das aplicações.

5.122 A solução deve oferecer suporte à integração com a solução SSE ofertada para segurança avançada na Internet.

6 REQUISITOS GERAIS DA SOLUÇÃO DE SECURITY SERVICE EDGE (SSE)

9.1 A solução de segurança na borda deverá suportar, no mínimo, as seguintes funcionalidades:

6.1.1 Filtro de URL;

6.1.2 Controle de Aplicação;

6.1.3 Proteção Contra Malwares Modernos;

6.1.4 Prevenção de Ameaças;

6.1.5 ZTNA (Zero Trust Network Access).

6.2 A solução deverá ser disponibilizada numa arquitetura em nuvem;

6.3 A solução disponibilizada deverá ter capacidade de receber via redirecionamento ou interceptar de maneira ativa e realizar inspeção e tratamento de todo o tráfego web de forma a controlar os acessos a serviços SaaS (Gerenciados e não gerenciados), IaaS, Web e Aplicações Internas (Nuvem pública ou *on-premises*);

6.4 A solução deverá ser fornecida como SaaS (Software as a Service) em ambiente externo ao Banco. Isto é, não serão permitidas soluções de segurança do tipo *on-premises*.

6.5 A solução deve possuir console de gestão web para toda a plataforma de segurança, incluindo:

6.5.1 Painel de Política;

6.5.2 Painel de Relatório;

6.5.3 Painel de Incidentes;

6.5.4 Painel de Configuração;

6.5.5 Painel Analítico.

6.6 O fabricante da solução deverá possuir ao menos 2 (dois) gateways no Brasil, não sendo permitidas soluções genéricas agregadas através de appliances físicos e/ou virtuais;

6.7 Todo o processamento do tráfego deverá ser realizado em Datacenters localizados no Brasil;

6.8 A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet, saindo apenas com IPs designados para o fabricante da solução SSE e alocados no Brasil.

6.9 A solução deverá garantir SLA de latência para, no mínimo, as aplicações do Microsoft Office 365 ou possuir *peering* estabelecendo conexão direta entres os POPs do fabricante SSE e o Datacenter da Microsoft no Brasil;

6.10 A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-2 e ISO 27001;

6.11 Deverá ser possível realizar a interceptação do tráfego de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, para no mínimo as seguintes formas:

6.11.1 Túnel Seguro (IPSEC ou SSL);

6.11.2 Integração com a Plataforma de SDWAN ofertada;

6.11.3 Integração com NGFW/UTM (IPSEC);

6.11.4 Agente (Windows e MacOS);

6.12 Os serviços de segurança devem ser fornecidos de maneira transparente às redes remotas;

6.13 A solução deve fornecer a capacidade de associar e atribuir toda a atividade do usuário, usando uma representação de identidade conforme integrações com:

6.13.1 *Azure Active Directory*;

6.13.2 Federação (SSO) utilizando SAML v2.0.

6.14 Suportar recurso de autenticação única para todo o ambiente de rede da CONTRATANTE, utilizando a plataforma de autenticação *Active Directory* ou outra plataforma com suporte à SAML;

6.15 A solução deverá executar suas funcionalidades em defender a rede contra ameaças avançadas, vírus e ameaças escondidas em tráfego HTTPS e aplicações com SSL criptografado;

6.16 A solução deverá ser capaz de descriptografar e inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.2 ou superior;

6.17 O tráfego SSL/TLS deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao tráfego não criptografado;

6.18 A solução deverá suportar e estar devidamente licenciada para:

6.18.1 No mínimo a quantidade de **12.000 (doze mil)** usuários autenticados com serviços ativos e identificados pela solução;

6.18.2 Até a quantidade de **8 (Oito) Gbps** de troughput para todos as funcionalidades ativas simultaneamente, conforme **Anexo II – Modelo de Proposta**;

6.18.3 A solução de ***ZTNA (Zero Trust Network Access)*** deverá suportar pelo menos **12.000 (doze mil)** usuários, sendo até **3.500 (três mil e quinhentos) simultâneos**, conforme **Anexo II – Modelo de Proposta**;

6.18.4 No mínimo a quantidade de dispositivos informada no **Anexo II – Modelo de Proposta**, identificados pela solução.

6.18.5 Em caso de prorrogação, a solução deverá estar preparada para atender 4.000 usuários simultâneos para atender o 5° ano.

6.19 A solução deverá possibilitar a execução de descriptografia SSL para todo o tráfego WEB, e deverá ser escalável para suportar ao longo do contrato a quantidade total de usuários licenciados;

6.20 Deverá permitir a configuração de portas diferentes da porta padrão utilizada pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites;

6.21 A solução deverá verificar os certificados digitais de sites acessados por meio do protocolo HTTPS. Em caso de certificados digitais inválidos, a solução deverá ser configurável para, de acordo com preferência da CONTRATANTE, bloquear ou permitir o acesso aos sites;

6.22 Deverá permitir configurar regras de exceção a sites HTTPS que não devem ter seu tráfego inspecionado;

6.23 A solução deverá ser capaz de se integrar com a solução de SD-WAN ofertada;

6.24 O licenciamento e a garantia pelo fabricante para toda a solução deverão estar ativos durante toda a vigência do contrato;

Filtro de URLs

6.25 A solução deverá suportar a criação de políticas baseadas no controle por URL e categorias de URLs;

6.26 O perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

6.27 A solução deverá possuir:

6.27.1 Pelo menos 70 categorias distintas de URLs;

6.27.2 A capacidade de classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

6.27.3 Categoria específica para classificar domínios recém registrados;

6.27.4 Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática, possuindo, ainda, interface complementar disponibilizada pelo fabricante para inclusão e sugestão de alteração de classificação de URL;

6.28 A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas na plataforma:

6.28.1 Categoria de URL;

6.28.2 Usuários e Grupos do Active Directory;

6.28.3 Profile de prevenção de malwares, podendo ser definido de forma global ou por política de acesso;

6.28.4 Atividade realizada na URL/Aplicação;

6.28.5 IP de Origem;

6.28.6 Ação: allow e block;

6.28.7 Tipo/extensão de arquivo.

6.29 A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

6.30 A solução deverá suportar:

6.30.1 A criação de categorias de URLs customizadas;

6.30.2 A exclusão de URLs do bloqueio, por categoria;

6.30.3 A customização de página de bloqueio;

6.30.4 Rastreamento de sites e análise em, no mínimo, 40 idiomas;

6.30.5 Identificação e categorização de sites acessados através de tradutores (ex. Google Translate);

6.30.6 A capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

6.31 A solução deverá permitir:

6.31.1 Um mecanismo para sobrescrever as categorias de URL;

6.31.2 A criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);

6.31.3 Especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (por exemplo: dia da semana e hora).

6.32 A solução deverá possuir mecanismo de Controle de URL que apresenta contagem de utilização de regra de acordo com a utilização (*hit count*);

6.33 A solução deverá possibilitar:

6.33.1 Categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

6.33.2 A inspeção de tráfego HTTPS *Outbound* deverá efetuar o "*man-in-the-middle*", ou seja, a solução deverá prover mecanismo de descriptografia para inspeção completa do tráfego de saída para a internet;

6.33.3 Implementação de filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das estações dos clientes da COTRATANTE.

6.33.4 O cadastro manual de usuários e grupos diretamente na interface de gerência remota ou, para os grupos, sincronismo através de integração com o Active Directory/AzureAD;

6.33.5 O bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

6.33.6 Salvar nos logs, no mínimo, as informações do campo *UserAgent* do cabeçalho HTTP nos acessos a URLs;.

6.34 A solução deverá utilizar modelos de inteligência preditiva no reconhecimento de URLs maliciosas em tempo real não cadastradas na base de categorização do fabricante da solução.

6.35 A solução deverá possuir a capacidade de detectar técnicas de *phishing* ou falsificação de imagens;

Controle de Aplicação

6.36 A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

6.37 A solução deverá contar com módulos de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

6.38 Pela solução deverá ser possível:

6.38.1 A liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

6.38.2 Adicionar políticas de controle de aplicações e perfis de segurança para todo o tráfego web direcionado para a nuvem SSE, não se limitando somente a possibilidade de habilitar controle de aplicações em parte do tráfego;

6.38.3 A criação de políticas por geolocalização, permitindo que o tráfego de uma aplicação para um determinado país seja bloqueado ou redirecionado;

6.38.4 A criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

6.38.4.1 Nível de risco da aplicação;

6.38.4.2 Categoria de aplicações.

6.39 A solução deverá reconhecer pelo menos 3.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e webmail;

6.40 A solução deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos assinaturas, decoders de protocolos e heurísticas;

6.41 A solução deverá diferenciar:

6.41.1 Tráfegos *peer-to-peer* (*bittorrent*, *emule e neonet*.), permitindo o bloqueio desse tipo de tráfego;

6.41.2 Aplicações proxies (ultrasurf, ghostsurf e freegate.) permitindo o bloqueio desse tipo de tráfego;

6.41.3 Tráfegos de mensageiros instantâneos (facebook Chat, WhatsApp e telegram.) possuindo granularidade de controle para os mesmos;

6.42 A solução deverá diferenciar e controlar partes das aplicações, incluindo, mas não limitado: Permitir o WhatsApp WEB e bloquear a transferência de arquivos, permitir o facebook e bloquear chat;

6.43 Pela solução deverá ser possível:

6.43.1 Inspecionar o *payload* do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

6.43.2 Aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a *encrypted bittorrent* e aplicações VOIP que utilizam criptografia proprietária.

6.44 Caso a solução não tenha assinaturas pré-definidas de uma aplicação, a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP e HTTPS;

6.45 Pela solução deverá ser possível atualizar a base de assinaturas de aplicações automaticamente;

6.46 O fabricante da solução deverá disponibilizar um serviço para solicitação de inclusão de aplicações na base de assinaturas do mesmo;

Proteção Contra Malwares Modernos

6.47 A solução deverá possuir nuvem de inteligência onde seja responsável em atualizar toda a base de segurança através de assinaturas;

6.48 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real;

6.49 A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise, devendo permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado (*sandbox*). Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

6.50 A solução deverá prevenir o uso de *exploits* avançados;

6.51 Na solução, a análise deverá prover:

6.51.1 Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

6.51.2 Informações sobre as ações do Malware na máquina infectada;

6.51.3 Informações sobre as URLs não confiáveis utilizadas pelo novo Malware;

6.51.4 Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;

6.51.5 Detecção de aplicações não confiáveis, utilizadas pelo Malware;

6.51.6 Atualização das assinaturas de Antivírus e Antispyware de maneira automática na plataforma SSE.

6.52 A solução deverá possuir:

6.52.1 Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP e HTTPS;

6.52.2 Mecanismo de detecção *antibot*, que inclui pelo menos, reputação de endereço IP;

6.52.3 Funcionalidade de detecção e bloqueio de *call-backs*.

6.53 A solução deverá prevenir contra ameaças de dia zero:

6.53.1 Via tráfego de internet;

6.53.2 Que possam burlar o sistema operacional emulado;

6.53.3 Através de tecnologias em nível de emulação e código de registro.

6.54 A solução deverá ser capaz de implementar:

6.54.1 Detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve permitir inspecionar arquivo PDF com até 2MB (dois MegaBytes);

6.54.2 Visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (*sandbox*) suportados;

6.54.3 Análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

6.55 A solução deverá permitir ainda:

6.55.1 Identificação e bloqueio de malware nas comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

6.55.2 Análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) no ambiente controlado;

6.55.3 Submissão manual de arquivos para análise através do serviço de *Sandbox*.

6.56 Em caso de falso positivo, a solução deve permitir a criação ou a solicitação de inclusão de *Whitelist* baseado no *hash* do arquivo;

Prevenção de Ameaças

6.57 A solução deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto à movimentação entre nuvens (SaaS Gerenciado e SaaS não gerenciado);

6.58 Na solução deverá ser possível criar políticas de segurança baseadas no nível de risco da aplicação. Ex: selecionar na política de segurança o bloqueio de todas as aplicações de *cloud storage* com nível de risco alto na base do fabricante da solução;

6.59 Deve conter, no mínimo, as seguintes informações sobre as aplicações comparadas na interface gráfica da solução:

6.59.1 Informações sobre vulnerabilidades e *exploits* já sofridos;

6.60 A solução deverá possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou referentes a incidentes de vírus e Bots;

6.61 A solução deverá suportar referência cruzada com CVE;

6.62 A solução deverá ser capaz de categorizar os seguintes tipos de domínio:

6.62.1 Domínios de DNS dinâmicos;

6.62.2 Domínios identificados previamente como sendo distribuidores de *Malwares*;

6.62.3 Domínios identificados anteriormente em campanhas de *Phishing*;

6.62.4 Domínios identificados previamente como *Graywares* os quais podem usar de técnicas de instalação de aplicações não desejadas;

6.62.5 Domínios Estacionários os quais são sites com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares;

6.62.6 Domínio de anonimização de Proxy utilizados com uma forma de driblar a análise de conteúdo.

6.63 Os requisitos abaixo descritos neste item poderão ser atendidos pela solução SSE ou pela solução SDWAN ofertada:

6.63.1 A solução deverá possuir sistema de análise automática para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

6.63.2 A solução deve proteger contra ataques do tipo envenenamento de cache DNS (*DNS Cache Poisoning*), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

6.63.3 A solução deverá permitir *updates* em tempo real para ameaças e novos ataques feitos através de DNS.

ZTNA (*Zero Trust Network Access*)

6.64 A solução deve possuir a capacidade de controlar o acesso de usuários remotos a aplicações internas da CONTRATANTE através da nuvem do fabricante, onde o usuário remoto tenha acesso apenas a aplicação especificada na política de segurança e não a um segmento de rede interna;

6.65 A solução deve ser implementada com agente único na estação de trabalho do usuário remoto;

6.66 A solução deve garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

6.67 Ser possível configurar através da console gráfica da solução quais aplicações internas serão acessadas através do *Tenant* da solução;

6.68 Ser autossuficiente e se ajustar automaticamente do ponto de vista de performance caso algum ponto de presença venha a falhar sem a necessidade do administrador ou cliente configurar nenhuma regra;

6.69 Trabalhar em modo híbrido onde seja possível publicar os atalhos de acesso a aplicações presentes nos datacenters da CONTRATANTE e nas nuvens públicas indicadas pela mesma;

6.70 A solução deve permitir definir a conformidade de estações com sistemas operacionais Windows e MacOS, com as políticas organizacionais baseadas no mínimo nos seguintes critérios:

6.70.1 Presença de processo(s) em execução;

6.70.2 Presença de arquivos em disco;

6.70.3 Participação em domínio do AD;

6.70.4 Existência de Certificado Digital no dispositivo;

6.70.5 Que somente as máquinas que estejam com solução antimalware ativada possam acessar os serviços internos.

6.71 A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

6.71.1 Máquinas em conformidade: A partir de uma máquina remota, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação;

6.71.2 Máquinas não conformes: A partir de uma máquina remota, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso a aplicação.

6.71.3 Geolocalização: A partir de uma máquina remota tentando se conectar de um país não permitido, deverá ter sua conexão bloqueada.

6.72 Pela solução deve ser possível criar políticas de segurança onde pode ser especificado:

6.72.1 Usuário do AD;

6.72.2 Grupo do AD;

6.72.3 Aplicação Privada;

6.72.4 Perfil de segurança (no mínimo: Filtro de URLs e Controle de Aplicação);

6.72.5 Ação: Permitir e/ou Bloquear.

6.73 A solução deve realizar verificação contínua de confiança, onde uma vez que o acesso a um aplicativo é concedido:

6.73.1 A Confiança deverá ser continuamente avaliada com base em mudanças nas condições de segurança na estação;

6.73.2 Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real;

6.74 A solução deve gerar logs dos acessos realizados por usuários remotos as aplicações internas, no mínimo, com as seguintes informações:

6.74.1 Regra de segurança que foi aplicada no tráfego;

6.74.2 Ação tomada pela solução;

6.74.3 Usuário;

6.74.4 Endereço IP;

6.74.5 País de origem;

6.74.6 Sistema operacional;

6.74.7 Aplicação de destino;

6.74.8 Porta de destino;

6.74.9 Protocolo;

6.74.10 Bytes trafegados na sessão;

6.74.11 Hora de início ou término da sessão.

Relatórios

6.75 Ser capaz de visualizar, de forma direta na solução, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados, URLs acessadas e ameaças identificadas;

6.76 Ser capaz de visualizar, de forma direta na solução, o *throughput* de dados utilizado pela rede de computadores conectados ao serviço em nuvem. Esse requisito poderá ser atendido pela solução SSE ou pela solução SDWAN ofertada;

6.77 Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar tráfego de arquivos maliciosos, dentre outras ameaças. Deve permitir o download do relatório em formato PDF;

6.78 Ser capaz de visualizar, de forma direta na solução, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

6.79 Possibilitar a geração de, pelo menos, os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);

6.80 A contratada deverá disponibilizar, no mínimo, 365 dias de retenção de dados para disponibilizar relatórios. Os relatórios devem ser disponibilizados atendendo aos seguintes critérios:

6.80.1 No mínimo 30 dias na própria console da solução de SASE/SSE;

6.80.2 No mínimo 12 (doze) meses, podendo ser na própria console da solução de SSE ou em uma solução externa ao ambiente SSE, contanto que forneça, no mínimo, os seguintes formatos de relatórios:

6.80.2.1 Relatório de acesso a internet por usuário, contendo as informações de data, hora, URL destino, categoria da URL, regra de acesso e aplicação;

6.80.2.2 Relatório de acesso a internet por URL destino, contendo as informações de usuários e categoria da URL;

6.80.2.3 Relatório de acesso a internet por Aplicação, contendo as informações de usuários;

Gerenciamento

6.81 Deve ter administração por console de gerenciamento web para toda a plataforma SSE, incluindo os recursos abaixo listados:

6.81.1 Filtro de URL;

6.81.2 Controle de Aplicação;

6.81.3 Proteção Contra Malwares Modernos;

6.81.4 Prevenção de Ameaças;

6.81.5 ZTNA (Zero Trust Network Access).;

6.82 O gerenciamento da solução deverá ser baseado em plataforma WEB, com acesso via browser padrão de mercado, utilizando comunicação criptografada (TLS, versão 1.2 ou superior);

6.83 A solução deverá ter a capacidade para criação das contas de usuário na própria console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação.

6.84 A solução deverá ter a capacidade de utilizar contas de usuários do AD interno do Banco para autenticação na console de gerenciamento, através de integração com o *Azure Active Directory*;

6.85 A solução deve estar licenciada e permitir o uso de duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução. Caso a solução necessite de mais de uma console de gerenciamento, todas devem estar licenciadas e permitir o uso do MFA;

7 INTEGRAÇÃO DO TRÁFEGO DE DADOS, VOZ E IMAGENS

7.1 Definição de classes de tráfego

7.1.1 Deverão ser criadas diferentes classes de tráfego em quantidade e com características que permitam a perfeita integração, numa mesma infraestrutura, do tráfego de dados, voz e imagens entre as unidades distribuídas e o CAPGV, de modo a atender os requisitos apresentados.

7.2 Classificação do tráfego

7.2.1 O tráfego de dados, voz e imagens gerado pelos diferentes sistemas do Banco instalados nas unidades distribuídas, no Site Primário e Site Secundário deverá ser adequadamente classificado, priorizado, encaminhado e entregue pelos equipamentos fornecidos no escopo dos serviços de SD-WAN, de modo a garantir o perfeito funcionamento dos

respectivos sistemas. Isso deve ser feito respeitando os critérios de priorização de cada classe de tráfego, conforme indicado nos itens abaixo.

7.3 Tráfego de imagens

7.3.1 A rede de serviços integrados deverá interligar os sistemas de videoconferência instalados nas unidades distribuídas, Site Secundário e no Site Primário, permitindo o estabelecimento de chamadas de videoconferência, incluindo som e imagem, para cada unidade distribuída, tendo como destino uma outra unidade distribuída, Site Secundário ou o Site Primário. Os sistemas de videoconferência instalados nas unidades distribuídas, Site Secundário e no Site Primário já estão equipados com interfaces para transformação dos sinais de som e imagens e seus respectivos protocolos em pacotes tipo Internet Protocol (IP). Tais interfaces deverão ser interligadas aos comutadores de rede locais nas unidades distribuídas, Site Secundário e no Site Primário. A interligação dos sistemas de videoconferência aos equipamentos comutadores das redes locais das unidades distribuídas, Site Secundário e do Site Primário, bem como as necessárias configurações nesses mesmos sistemas de videoconferência, são de responsabilidade do Banco, estando fora do escopo dos serviços ora especificados.

7.4 Unidades envolvidas

7.4.1 Todas as unidades distribuídas poderão dispor de recursos para realização de videoconferência, e deverão, portanto, ter seus serviços devidamente preparados para tal. Quaisquer alterações ou inclusões de novas unidades serão solicitados ao CONTRATADA a qualquer momento, sem ônus para o Banco.

7.5 Tráfego de dados

7.5.1 O tráfego de dados (exceto voz e vídeo) entre as unidades distribuídas e o CAPGV deverá ser diferenciado em 3 níveis de prioridade além do Best Effort (BE), a saber: alta (mission critical), média (transactional) e baixa (bulk data). Em cada nível de prioridade deverá ser permitido até 3 grupos de classificação com diferentes probabilidades de descarte, no mínimo, no nível AF2, será permitida a marcação AF21, AF22 e AF23. Os dados classificados como de alta prioridade deverá ser encaminhados, até o limite pré-estabelecido, com prioridade sobre os dados classificados como de média prioridade, que por sua vez deverão ser encaminhados, até o limite pré-estabelecido, com prioridade sobre os dados classificados como de baixa prioridade. O tráfego relacionado aos serviços de voz e imagens deverá ter prioridade sobre todas as classes de dados, de modo a garantir o perfeito funcionamento e integração de todos os serviços. Conforme mencionado abaixo nesse anexo, deverá ser permitido o transbordo de dados entre as classes, conforme será informado pelo Banco durante implantação.

7.6 Alocação de Largura de Banda

7.6.1 A caracterização das três classes de dados (alta, média e baixa), da classe de voz e da classe imagem deverá seguir a associação definida nas tabelas abaixo:

Alocação de Largura de Banda					
Mapeamento das Classes de Serviços			Tabelas		
			A	B	C
Tráfego de Voz		Classe EF	15%	15%	15%
Tráfego de Imagem		Classe AF4	15%	10%	10%
Tráfego de Dados	Alta	Classe AF3	30%	36%	36%
	Média	Classe AF2	14%	15%	15%
	Baixa	Classe AF1	10%	15%	15%
Best Effort			12%	5%	5%
TOTAL			96%	96%	96%

7.6.2 A referida associação trata-se de um exemplo e poderá sofrer alteração na fase de implementação em caráter inicial e não definitivo, cabendo a realização de alterações (sem ônus para o Banco) após a implantação e respectiva avaliação pelo Banco de que tal associação atende ao perfil de tráfego presente na rede.

7.6.3 Respeitando o valor máximo de reserva de 96%, a divisão entre as classes deverá ser composta por números inteiros sem a obrigatoriedade de serem múltiplos de 2 ou 5.

7.6.4 No caso de a quantidade de tráfego exceder o reservado para cada classe, deverá ser possível o transbordo de tráfego entre classes, da maior para a de menor prioridade, onde o tráfego excedente da classe AF31, no mínimo, poderá ser remarcado como AF13, a ser definido pelo Banco durante implantação.

7.6.5 As informações referentes aos serviços (IP/porta/protocolo), que deverão ser associados a cada mapeamento das Classes de Serviços, serão repassadas ao início da implantação e ao longo da vigência contratual ao CONTRATADO, que deverá realizar as marcações apropriadas afim que de as operadoras respeitem em seus respectivos backbones os percentuais; podendo ser alteradas em virtude de novas aplicações/serviços, definições de negócios, melhorias na segurança da informação ou outro critério apontado pelo Banco.

7.6.6 As Operadoras que proveem a comunicação de Internet e MPLS receberá o tráfego devidamente marcado nas interfaces dos seus CPEs, seja pelas soluções já existentes no Banco de vídeo e voz, seja pela solução SD-WAN.

7.6.7 Os percentuais de banda reservados para cada aplicação, dentro das classes de serviço, poderão ser objeto de ajustes durante o prazo contratual, de acordo com as tabelas acima definidas, sem ônus para o Banco. A solicitação de alteração poderá ser feita por unidade remota e deverá respeitar o SLA de configuração.

7.7 Tráfego de gerência para a solução SD-WAN

7.7.1 O tráfego gerado entre a solução de gerenciamento no Site Primário e Site Secundário (definido no **Anexo X - Requisitos de Gerenciamento dos Serviços**) e os equipamentos que serão monitorados deverá ser classificado como pertencente ao tráfego de dados de média prioridade.

7.7.2 A critério do Banco, a prioridade deste tráfego pode ser alterada, após implementação e respectiva avaliação, sem ônus para o Banco.

7.8 Topologia da solução

7.8.1 Deverá ser fornecido desenho esquemático ilustrando todos os aspectos dos requisitos de conectividade, tanto para as unidades distribuídas, postos de crédito quanto para Parceiros como para o Site Primário e Site Secundário. Através deste desenho deverá ser possível identificar a topologia projetada para as redes WAN e LAN, visualizando detalhes sobre as respectivas concentrações, para todos os circuitos.

7.8.2 A arquitetura da rede de comunicações ofertada deverá ser modular, possibilitando escalonar a contratação de aumentos de velocidade para cada um dos circuitos contratados, conforme necessidades futuras do Banco, permitindo ampla flexibilidade de reconfiguração.

7.8.3 As portas e circuitos de acesso deverão permitir aumento de largura de banda de acordo com a demanda futura do Banco, de modo que, quando solicitado pelo Banco, a CONTRATADA procederá a reconfiguração e ativação da nova largura de banda, incluindo os respectivos custos envolvidos nas faturas mensais.

8 REQUISITOS DE SEGURANÇA

Caberá ao Banco estabelecer as políticas de segurança a serem aplicadas aos serviços de telecomunicações CONTRATADAs, equipamentos roteadores que compõe a solução e estarão localizados nas dependências do Banco. O Banco terá o direito de verificar a correta aplicação dessas políticas, através da realização de auditorias realizadas a seu critério, de forma remota, dos equipamentos que compõe a solução. Para garantir os níveis de segurança esperados na infraestrutura por onde trafegarão as informações do Banco, os provedores deverão atender, no mínimo, aos seguintes requisitos:

8.1 Aplicar em suas redes, para os equipamentos instalados no CAPGV e unidades distribuídas, a política de segurança definida pelo Banco para os serviços de telecomunicações, como por exemplo a política atual do Banco que proíbe todo e qualquer acesso de gerenciamento aos equipamentos roteadores via telnet, sendo no mínimo exigido acesso via SSH;

8.2 Restringir as informações de segurança a uma equipe restrita de técnicos de segurança, assumindo toda responsabilidade por perdas e danos comprovados que o Banco venha a sofrer em decorrência de dolo, negligência, imperícia ou imprudência dos componentes dessa equipe;

8.3 O licitante deverá manter o software dos equipamentos roteadores e/ou appliances atualizados e aplicar tempestivamente correções de vulnerabilidades de segurança publicadas pelo fornecedor, que sejam julgadas importantes pelo Banco;

9 GLOSSÁRIO

Unidades Distribuídas: Agências, Centrais Operacionais (CENOPs), Unidades de Recuperação de Crédito, Superintendências e demais unidades administrativas do Banco residindo fora do CAPGV;

Parceiros: Entidades parceiras do Banco do Nordeste, responsáveis pela troca de informações bancárias de conteúdo restrito para realização de negócios;

Postos de Crédito: unidades responsáveis pela operacionalização dos produtos de microcrédito (Postos Crediamigo) e crédito rural (Postos Agroamigo) do Banco.

CAPGV: Centro Administrativo Presidente Getúlio Vargas. Sede principal do Banco, onde reside sua administração superior;

Site Primário: Sede primária do Banco, onde residem os principais recursos e serviços centralizados de infraestrutura;

Site Secundário: Sede secundária do Banco, onde reside a redundância dos principais recursos e serviços centralizados de infraestrutura;

Circuito de acesso terciário: conjunto de trechos contínuos de meios de comunicação, completamente independentes daqueles utilizados pelos circuitos de acesso primários e secundários, isto é, sem que haja compartilhamento de qualquer tipo de recurso, exceto em casos onde for fisicamente impossível, o qual interliga uma unidade distribuída, Site Secundário ou o CAPGV a um ponto de presença do fornecedor dos serviços. Usado para balanceamento, contingenciamento do tráfego de dados em caso de falha dos circuitos de acesso primário e secundário, ou para determinados tráfegos escolhidos pelo Banco e roteados na solução SD-WAN;

Circuito de acesso Posto: conjunto de trechos contínuos de meios de comunicação que interliga o posto de crédito a um ponto de presença do fornecedor dos serviços. Usado para tráfego integrado de dados, voz e imagens;

Controle do tráfego: aplicação de mecanismos de identificação, classificação, restrição, filtragem, priorização, ou qualquer outro mecanismo relacionado, sobre fluxos de dados, voz ou imagens;

Ponto de presença: instalações físicas administradas e mantidas pelo fornecedor dos serviços, às quais estão interligados seus diversos clientes. Local onde estão instalados e em operação os equipamentos que compõem o *backbone* do fornecedor dos serviços;

Backbone: conjunto de meios de comunicação e equipamentos, geralmente de alta capacidade de tráfego, usados para interligar os diversos pontos de presença do fornecedor dos serviços;

Ponto de concentração: armário de fiação (*rack*) ou quadro instalado em parede no qual se concentra a terminação do cabeamento horizontal de cada pavimento ocupado por qualquer parte de uma unidade distribuída;

SD-WAN (*Software Defined* – WAN): rede de longa distância definida por software. Cuja solução ora contratada terá a capacidade de determinar os melhores caminhos e rotas para o trafego integrado de dados, voz e imagens entre os Sites Primário e Secundário e as Unidades Distribuídas;

SSE (*Security Service EDGE*): Solução de Gateway de Web Segura de Próxima Geração (NG-SWG) que será responsável pelos serviços de proxy remoto para todas as unidades.

SASE (*Secure Access Service EDGE*): Conceito empregado para a solução completa que engloba SD-WAN e SSE.

NGFW: Solução de Sistemas de firewall de próxima geração.

UTM: Sistemas gerenciamento unificado de ameaças.

NOC/SOC SASE: Centro(s) de Operação(es) de Rede do BANCO e/ou equipe(s) responsável(is) pelo gerenciamento, implementação, correção e controle de toda a solução SD-WAN atual, solução SASE futura, monitoramento dos componentes ofertados pelos provedores de internet e MPLS.

NOC/SOC da Contratada: Centro de Operação de Rede e Segurança responsável pelo gerenciamento, configuração, implementação, suporte, assistência técnica, correção, gerenciamento de SLA e controle de toda a solução, incluindo ajustes de configuração, roteamento, engenharia de tráfego, aplicações de QoS, de funcionalidades de Segurança e demais ajustes necessários da solução ofertada.

Appliance: dispositivo de hardware separado e dedicado com *software* integrado (*firmware*), especificamente projetado para fornecer um serviço específico.

CPE: *Customer Premises Equipment* – Qualquer equipamento instalado nas dependências da Unidade, com a finalidade de conectar e compatibilizar a WAN com a rede local.