ANEXO II - REQUISITOS DOS SERVIÇOS INTEGRADOS DE COMUNICAÇÃO DE DADOS, VOZ E IMAGENS PARA UNIDADES DISTRIBUÍDAS E POSTOS DE CRÉDITO DO BANCO

1. INTRODUÇÃO

1.1.1. O presente anexo descreve os requisitos técnicos relacionados à prestação dos serviços integrados de comunicação de dados, voz e imagens para interligação das unidades distribuídas do Banco do Nordeste do Brasil S/A às suas sedes.

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

1.1.3. 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. Os serviços especificados neste anexo têm por finalidade a interligação entre as unidades distribuídas e postos de crédito do Banco e as suas sedes localizadas em Fortaleza - CE, integrando numa mesma infraestrutura o suporte ao tráfego de dados, voz e imagens, através das tecnologias: Multiprotocol Label Switching (MPLS) e Internet.

2.1.2. Além do serviço de SDWAN das unidades remotas, será contemplado no mesmo item o serviço de SSE (*Security Service Edge*) que deverá ser integrado com o serviço de SDWAN, 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.

2.1.3. Também fará parte deste anexo as especificações para interligação do Banco do Nordeste com a sua Rede Parceiros (ATP, Banco do Brasil, Caixa Econômica, Cielo e outros) através da tecnologia MPLS (somente).

2.1.4. 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 SDWAN.

2.1.5. 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.

2.1.6. Todas as Unidades de um mesmo grupo que dispõem de tecnologia MPLS como acesso primário devem, a critério do Banco, manter comunicação ponto-a-ponto (sem passar necessariamente pelos concentradores) entre si, full-mesh, sobre o acesso primário, enquanto o acesso primário de ambas estiver ativo, independente da necessidade de subcontratação de outras provedoras pelo CONTRATADO do ITEM 1.

2.1.7. As Unidades de um mesmo grupo que dispõem de tecnologia MPLS como acesso secundário devem, a critério do Banco, manter comunicação ponto-a-ponto, full-mesh, sobre o acesso secundário, enquanto o acesso secundário de ambas estiver ativo, independente da necessidade de subcontratação de outras provedoras pelo CONTRATADO do ITEM 1. Sendo que as Unidades que dispõem de tecnologia Internet Simétrica devem, a critério do Banco, manter comunicação ponto-a-ponto, VPN full-mesh, enquanto os seus acessos Internet estiverem disponíveis, independente da

necessidade de subcontratação de outras provedoras pelo CONTRATADO do ITEM 1.

2.1.8. Os serviços serão providos por meio do fornecimento, para cada unidade do Banco, de um circuito de acesso primário terrestre MPLS, do acesso secundário por Internet Determinística, e outro(s) acesso(s) terciário baseado(s) em Internet Determinística ou assimétrica (incluindo o uso de tecnologia GPON) ou simétrica (incluindo EPON), de acordo com as coberturas disponíveis e todos independentes entre si, exceto as Unidades denominadas Postos de Crédito, que terão apenas um acesso baseado em Internet Determinística, além de solução de serviços de gerenciamento e automação de circuitos WAN, com provimento de ferramentas e equipe especializada em gestão.

2.1.9. A rede de parceiros será provida totalmente por link MPLS, tanto os acessos primários quanto secundários.

2.2. **Fornecimento de infraestrutura**

2.2.1. Os serviços de circuitos de acesso a serem prestados no ITEM 1 deverão contemplar o fornecimento, instalação, configuração, assistência e suporte técnico de toda a infraestrutura necessária à adequada prestação dos serviços ora especificados, incluindo, além dos recursos que compõem o backbone do fornecedor dos serviços, os seguintes componentes:

2.2.1.1. Circuitos de acesso primários via MPLS terrestres para as unidades distribuídas, Parceiros, para concentração no CAPGV e no Site Secundário, englobando todos os equipamentos necessários e demais componentes relacionados. Os circuitos e acessos para as unidades remotas do Banco deverão possuir estrutura totalmente separada dos circuitos de parceiros, incluindo o acesso físico e roteadores concentradores;

2.2.1.2. Circuitos de acesso secundários via Internet Determinística Dedicada terrestre ou MPLS terrestre, dependendo da localidade. Para as unidades distribuídas Internet, para os Parceiros do Banco MPLS. Englobando todos os equipamentos e demais componentes relacionados. Os circuitos secundários e acessos para as unidades remotas do Banco, e circuito de parceiros, deverão possuir estrutura (acesso e pontos de presença – POP) totalmente separada dos circuitos primários, incluindo os acessos físicos e roteadores concentradores;

2.2.1.3. Circuitos de acesso terciários via Internet Determinística ou Assimétrica, dependendo da localidade e da cobertura, para as unidades distribuídas, englobando todos os equipamentos e demais componentes relacionados. Esses circuitos deverão possuir acessos e pontos de presença – POP totalmente separados dos circuitos primários e secundários;

2.2.1.4. Circuitos de acesso primários via Internet Determinística Dedicada terrestre para os Postos de Crédito;

2.2.1.5. Caso numa determinada localidade o licitante disponha, por exemplo, de 02 (dois) Pontos de Presença (POP) com infraestruturas e acessos totalmente independentes entre si, estes poderão ser utilizados para atender até 02 (dois) links remotos, desde que realmente não compartilhem recursos, e que uma indisponibilidade ou perda de performance em um deles não afete o funcionamento e performance de ambos os links;

2.2.1.6. Equipamentos roteadores para o CAPGV, Site Secundário, Parceiros, unidades distribuídas (circuitos primários) e postos de crédito;

2.2.1.7. Cabos, módulos, placas, interfaces, memórias e demais acessórios relacionados aos componentes descritos acima (para ambos os ITENS);

2.2.1.8. Os equipamentos roteadores a serem fornecidos no CAPGV e Site Secundário poderão ser substituídos por comutadores de rede local que implementem funcionalidades de roteamento, desde que atendidos todos os demais requisitos para os serviços ora especificados;

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

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

2.2.1.9.2. Adequação de tubulação e encaminhamentos internos para passagem de cabos;

2.2.1.9.3. Adequação do cabeamento da rede local das unidades distribuídas, postos de crédito, do CAPGV e Site Secundário, exceto nas unidades distribuídas que dispuserem de equipamentos do tipo Access Point, em que o CONTRATADO deverá se responsabilizar pelo encaminhamento do cabeamento e fixação dos equipamentos nos locais indicados pelo Banco.

2.2.2. Ao CONTRATADO, caberá providenciar a adequação das instalações físicas externas eventuais em cada Parceiro do Banco, como, por exemplo, Golden Jump;

2.2.3. Os equipamentos *appliances* para solução de SDWAN (*Software Defined Wide Area Network*) e seus respectivos appliances ou servidores de gerência no CAPGV, Site Secundário e unidades distribuídas fazem parte do escopo de atendimento do ITEM 2, bem como a solução de SSE (*Security Service Edge*);

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;

2.2.5. O Banco do Nordeste se reserva o direito de, durante a vigência do CONTRATO, realizar diligências técnicas a fim de certificar que a infraestrutura entregue pela CONTRATADA do ITEM 1 é realmente independente nos termos deste edital. Tais diligências podem acontecer através do pedido de envio por parte do BANCO à CONTRATADA do ITEM 1 de plantas topográficas em formato .PDF com a identificação fim-a-fim da infraestrutura utilizada para atender a determinada(s) unidade(s), ou através de visitas aos pontos de presença que atendem determinada(s) unidade(s), a critério do Banco. As visitas deverão ser sempre acompanhadas de técnico indicado pela CONTRATADA do ITEM 1, que será responsável pela correta identificação dos locais e equipamentos utilizados, a fim de demonstrar a independência dos recursos de acesso ao meio e pontos de presença das Unidades atendidas neste edital.

3. REQUISITOS PARA OS EQUIPAMENTOS ROTEADORES (ITEM 1)

3.1. **Requisitos GERAIS**

3.1.1. Todos os equipamentos roteadores a serem fornecidos para atender os circuitos de acesso primário, secundário e terciário nas unidades distribuídas do Banco, postos de crédito, no CAPGV, Site Secundário e Parceiros deverão atender ao seguinte conjunto de requisitos gerais:

3.1.1.1. Deverão ser novos, isto é, sem utilização anterior;

3.1.1.2. Todos os equipamentos roteadores para circuitos MPLS deverão ser do mesmo fabricante para cada localidade e incluindo os roteadores concentradores no caso de MPLS;

3.1.1.3. Todos os equipamentos roteadores para circuitos Internet deverão ser do mesmo fabricante para cada localidade, podendo estes serem diferentes do modelo proposto para os circuitos MPLS;

3.1.1.4. Deverá possuir LED's indicativos do estado de funcionamento do equipamento;

3.1.1.5. Deverá possibilitar a obtenção de estatísticas de tráfego e falhas das portas *inband* utilizadas na solução;

3.1.1.6. Deverão estar equipados com recursos que permitam a reconfiguração dinâmica das diversas portas e módulos utilizados na solução, inclusive permitindo a ativação e desativação de portas e módulos sem causar reinício, instabilidade ou qualquer impacto que venha a comprometer o funcionamento do equipamento;

3.1.1.7. Os equipamentos devem implementar ajuste de clock, utilizando NTP (*Network Time Protocol*);

3.1.1.8. Deverão permitir as atualizações de versões de código utilizando os protocolos *File Transfer Protocol* (FTP), SFTP (SSH *File Transfer Proocol*) ou *Trivial File Transfer Protocol* (TFTP);

3.1.1.9. Deverão permitir enviar logs para servidores remotos (Syslog) (não será objeto deste certame o fornecimento de servidor para Syslog), onde pelo menos 1 (um) será informado pelo Banco;

3.1.1.10. Deverão implementar *traceroute* para o descobrimento do caminho seguido por um pacote dentro da rede;

3.1.1.11. Todas as portas são configuráveis MDI/MDIX, dispensando o uso de cabos cross over ou quaisquer configurações para conexões a outros switches;

3.1.1.12. Deverão implementar *Internet Protocol Flow Information eXport* (IPFIX) ou Netflow v.9 ou equivalente;

3.1.1.13. Todos os roteadores MPLS devem ter interfaces loopback dedicadas para o gerenciamento do Banco em faixa de rede especificada pelo Banco. Os acessos de gerenciamento serão realizados através dessa interface;

3.1.1.14. 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 ao SNMP v3. Deverá ser fornecida uma comunidade (*community*) SNMP de leitura em todos os roteadores fornecidos na solução. Essa comunidade

(*community*) será acessada a partir do CAPGV e Site Secundário;

3.1.1.15. Deverá ser fornecido usuário com acesso via SSH em todos os roteadores com permissão “somente leitura” para o BANCO, incluindo possibilidade de visualização de TODA e qualquer configuração e estatísticas de tráfego dos equipamentos para apoio no momento dos incidentes, devendo permanecer ativa durante todo o Contrato. O acesso deverá fornecer também permissão em nível de leitura para todas as estatísticas do equipamento passíveis de consulta, como QoS, estatísticas de tráfego, status de protocolos de roteamento, etc;

3.1.1.16. Deverão estar equipados com 1 (uma) porta de comunicação out-of-band para gerenciamento de configuração ou isolar uma porta de comunicação do roteador através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso;

3.1.1.17. Na implantação de cada roteador, os CONTRATADOS deverão fornecer todas as gerências solicitadas conforme previsto no Edital. O não fornecimento desses acessos implicará em sanções administrativas de acordo com o Anexo VI - Acordo de Níveis de Serviços, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

3.1.1.18. Deverão possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas, ocupando uma unidade (1U) para as remotas e até 03 (três) unidades (3U) para os concentradores;

3.1.1.19. Deverão implementar IPV4 e IPV6;

3.1.1.20. Deverão Implementar *Network Address Translation* (NAT) para os principais protocolos da pilha TCP/IP;

3.1.1.21. Deverão implementar *Access Control List* (ACL) simples e estendidas;

3.1.1.22. Deverão possuir mecanismos de *authentication*, *authorization and accounting* (AAA) através de Servidor RADIUS e TACACS+;

3.1.1.23. As fontes de alimentação principal deverão funcionar com tensão elétrica de 110V~220V AC, 50~60Hz, de modo automático.

3.1.2. Para cada equipamento roteador, deverão ser entregues 1 (um) cabo UTP de 2,5 metros crimpado com RJ45 de fábrica e com a devida certificação. Os mesmos deverão ser de categoria 6 ou superior. Durante ativação do roteador, os cabos deverão ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação.

3.1.3. Objetivando manter a uniformidade nas funcionalidades em uso entre os novos equipamentos comutadores (switches) e os já instalados nas Unidades Distribuídas, onde a maioria são dos fabricantes Huawei e Cisco, os novos equipamentos deverão assegurar completa compatibilidade com os equipamentos já instalados.

3.2. **Requisitos dos EQUIPAMENTOS ROTEADORES <u>CONCENTRADORES</u> MPLS (Unidades Distribuídas) (ITEM 1)**

3.2.1. Os equipamentos roteadores concentradores MPLS que ficarão no Site Primário e Secundário serão responsáveis por receber os links concentradores MPLS das unidades remotas e dos links de Parceiros, deverão atender:

3.2.1.1. Deverão ser providos 04 (quatro) concentradores MPLS para assumir o tráfego de MPLS das unidades distribuídas e

parceiros. Sendo 02 (dois) no site primário e 02 (dois) no secundário.

3.2.1.2. Suportar a RFC 3545 ou 2508 (CRTP) com no mínimo 1900 (mil e novecentos) sessões simultâneas;

3.2.1.3. Suportar capacidade de roteamento de tráfego (throughput) mínima de 5Gbps full duplex.

3.2.1.4. Implementar RMON (Remote Network Monitoring MIB), com suporte a RFC 2819. Deve ser permitido o acesso de leitura a pelo menos aos grupos “Statistics, History, Alarm e Events”, a partir de solução de gerencia do Banco ou de empresa por ele indicado;

3.2.1.5. O fabricante dos equipamentos roteadores deverá possuir certificado de qualidade emitido pela International Standard Organization (ISO) relacionado aos processos de projeto e fabricação desses equipamentos;

3.2.1.6. Deverão ser fornecidos equipamentos que permitam a adição e remoção de módulos e interfaces de rede sem a necessidade de desligamento do mesmo (mecanismo conhecido como “Hot Swap”), de forma a permitir a troca de componentes removíveis do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso;

3.2.1.7. Implementar os protocolos de roteamento Open Shortest Path First (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771);

3.2.1.8. Implementar VRF (virtual routing and forwarding) ou similar garantindo o isolamento de tabelas de roteamento garantindo total independência do tráfego entre tabelas diferentes.

3.2.1.9. Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP) e deverão ser fornecidos privilégios de acesso de leitura para usuários designados pelo Banco para uso deste monitoramento, via SSH e software de gerenciamento do Banco;

3.2.1.10. Possuir compatibilidade com todos os recursos técnicos solicitados para a contratação dos links MPLS.

3.2.1.11. Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q em todas as interfaces abaixo descritas;

3.2.1.12. Possuir pelo menos 04 (quatro) interfaces 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 Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, sendo duas dessas interfaces dedicadas ao fornecimento LAN para o Banco;

3.2.1.13. Possuir pelo menos 02 (duas interfaces 10Gbps, utilizando SFP+ e conector LC para fibra do tipo multimodo padrão 10GBASE-SRentregues com line cord de 2 (dois) metros ou superior conectados, sendo as duas interfaces dedicadas ao fornecimento LAN para o Banco.

3.2.1.14. Trabalhar em alta disponibilidade (ativo/ativo ou ativo/passivo, a critério do Banco) entre os circuitos de acesso primário e secundário;

3.2.1.14.1. No caso de interrupção dos serviços que trafegam através do circuito de acesso primário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso secundário, mantendo-se os requisitos mínimos especificados nos itens anteriores. O contrário também deverá ocorrer, isto é, em caso de interrupção dos serviços que trafegam no circuito secundário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso primário, respeitando os requisitos mínimos;

3.2.1.14.2. O chaveamento dos serviços entre os circuitos de acesso primário e secundário de Parceiros, em caso de falha do circuito primário ou secundário, deverá garantir o retorno à operação normal quando do fim da falha acontecer, em sua plenitude, de forma automática, em até 3 (três) minutos a partir do início ou fim da falha. Isso deve acontecer sem qualquer intervenção humana, quer seja para realizar configuração em equipamento ou sistema de gerência, quer seja para realizar mudanças físicas na infraestrutura fornecida;

3.2.1.14.3. Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (CAPGV Site Primário ←→Site Secundário), via roteamento dinâmico e sem intervenção manual;

3.2.1.15. Roteamento dinâmico IMPLEMENTADO entre os roteadores remotos e os concentradores da Rede de Parceiros. As redes publicadas no roteamento serão informadas pelo Banco durante implementação, podendo haver a necessidade de NAT em algumas comunicações. O protocolo de roteamento será definido pelo Banco durante implementação, podendo ser OSPF ou BGP;

3.2.2. O(s) transceiver(s) SFP/SFP+ necessário(s) para conexão da interface dos concentradores deverão ser fornecidos em conjunto com a solução. Não será necessário o fornecimento de transceiver para o lado da conexão com a rede/equipamento do Banco;

3.3. **Requisitos dos EQUIPAMENTOS ROTEADORES <u>REMOTOS</u> MPLS (Unidades Distribuídas) (ITEM 1)**

3.3.1. Os equipamentos roteadores que serão fornecidos para as Unidades Distribuídas contempladas com acesso MPLS deverão, além dos requisitos gerais, atender:

3.3.1.1. Possuir pelo menos 02 (duas) 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;

3.3.1.2. Possuir pelo menos 01 (uma) interface RJ-45, compatível com a velocidade do circuito, 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 ou

IEEE802.3z 1000BASE-X, exclusiva para conexão WAN da CONTRATADA do ITEM 1;

3.3.1.3. As interfaces dedicadas para a LAN na rede do Banco devem ser compatíveis com conexão em modo Bridge, ou seja, com uma interface L3 (roteamento da unidade remota), que utiliza duas conexões físicas (duas interfaces), permitindo assim a conexão em diferentes appliances na rede LAN do Banco e fazendo parte do mesmo domínio de broadcast, com 1 (um) único IP (L3) para cada interface, bem como para subinterfaces (compatíveis com 802.1q);

3.3.1.4. Implementar os protocolos de roteamento Open Shortest Path First (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771); Ambos os protocolos de roteamento (OSPF e BGP) devem ser também compatíveis com IPV6;

3.3.1.5. Implementar roteamento estático para o Internet Protocol (IP);

3.3.1.6. O roteador deverá ser capaz de fornecer IP via DHCP server para todas as unidades remotas. Dentre os parâmetros necessários, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com 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 seguir o padrão SLA;

3.3.1.7. O roteador deve ser capaz de criar Interfaces VLANs L3 e realizar o roteamento dessas redes internamente na unidade remota, bem como realizar o roteamento para toda a rede do Banco;

3.3.1.8. O roteador deverá ser compatível com 802.1Q, no caso de subinterfaces criadas. Atualmente o Banco possui segmentação lógica para redes de videoconferência, por exemplo. A criação de novas redes não deverá representar custos adicionais ao projeto e deverá seguir o padrão SLA;

3.3.1.9. Deverá suportar o encaminhamento e armazenamento de pelo menos 30.000 rotas IPv4 e 10.000 rotas IPv6;

3.3.1.10. Implementar o protocolo Virtual Redundant Router Protocol (VRRP) com monitoração de circuito e ativação automática do roteador secundário em caso de falha;

3.3.1.11. Implementar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR);

3.3.1.12. Implementar a RFC 791 Type of Service – TOS;

3.3.1.13. Implementar a RFC 2474 Diffserv – DS;

3.3.1.14. Implementar Traffic Shaping;

3.3.1.15. Implementar Weighted Random Early Detection (WRED) ou Weighted Tail Drop (WTD) como mecanismo de prevenção de congestionamento;

3.3.1.16. Implementar IP Precedence;

3.3.1.17. Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q nas interfaces 1000BaseT ethernet utilizadas para interligação com a rede local das Unidades Distribuídas, CAPGV e Site Secundário;

3.3.1.18. Implementar Network Address Translation (NAT) para os principais protocolos da pilha TCP/IP;

3.3.1.19. Implementar Access Control List (ACL) simples e estendidas;

3.3.1.20. Implementar mecanismos de marcação de precedência (802.1p);

3.3.1.21. Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP), e deverão ser fornecidos privilégios para usuários designados pelo Banco para uso deste monitoramento, via acesso de gerencia e via software de gerenciamento do Banco.

3.4. **Requisitos dos EQUIPAMENTOS ROTEADORES CONCENTRADORES DE INTERNET (Utilização pelo Banco) (ITEM 1)**

3.4.1. Os equipamentos roteadores concentradores que serão fornecidos para concentração Internet, além dos requisitos gerais e dos requisitos do item 2.4 (EQUIPAMENTOS ROTEADORES CONCENTRADORES MPLS), atender:

3.4.1.1. Deverão ser providos 04 (quatro) concentradores INTERNET para assumir o tráfego de INTERNET das unidades distribuídas e postos de crédito. Sendo 02 (dois) no site primário e 02 (dois) no secundário;

3.4.1.2. Capacidade de concentrar as VPNs dos links remotos dos circuitos dos postos de crédito, bem como ser responsáveis pelo roteamento e publicação de rotas dinâmicas. Caberá ao Banco definir se a comunicação será ou não via VPN (comunicação criptografada);

3.4.1.3. Possuir pelo menos 04 (quatro) interfaces 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;

3.4.1.4. Possuir pelo menos 08 (oito) interfaces, com conector LC, para fibras óticas multimodo (LM), 10 Gbps, full-duplex. Todas estas interfaces deverão ser non-blocking e deverão ser entregues com os respectivos tranceivers multimodo padrão 10GBASE-SR;

3.4.1.5. Trabalhar em alta disponibilidade (ativo/ativo ou ativo/passivo, a critério do Banco) entre os circuitos de acesso primário e secundário;

3.4.1.5.1. No caso de interrupção dos serviços que trafegam através do circuito de acesso primário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso secundário, mantendo-se os requisitos mínimos especificados nos itens anteriores. O contrário também deverá ocorrer, isto é, em caso de interrupção dos serviços que trafegam no circuito secundário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso primário, respeitando os requisitos mínimos;

3.4.1.5.2. O chaveamento dos serviços entre os circuitos de acesso primário e secundário de Parceiros, em caso de falha do circuito primário ou secundário,

deverá garantir o retorno à operação normal quando do fim da falha acontecer, em sua plenitude, de forma automática, em até 3 (três) minutos a partir do início ou fim da falha. Isso deve acontecer sem qualquer intervenção humana, quer seja para realizar configuração em equipamento ou sistema de gerência, quer seja para realizar mudanças físicas na infraestrutura fornecida;

3.4.1.5.3. Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (CAPGV ←→ Site Secundário), via roteamento dinâmico e sem intervenção manual;

3.4.1.6. Roteamento dinâmico IMPLEMENTADO entre os roteadores remotos e os concentradores da Rede de Parceiros. As redes publicadas no roteamento serão informadas pelo Banco durante implementação, podendo haver a necessidade de NAT em algumas comunicações. O protocolo de roteamento será definido pelo Banco durante implementação, podendo ser OSPF ou BGP;

3.4.1.7. Deverá suportar o encaminhamento e armazenamento de pelo menos 2.000.000 rotas IPv4 e 2.000.000 rotas IPv6;

3.4.1.8. O equipamento deve possuir pelo menos 16 GB de memória RAM.

3.4.1.9. Os equipamentos roteadores utilizados nos concentradores (CAPGV e Site Secundário) para a Internet deverão possibilitar o aumento de no mínimo 4 interfaces físicas em cada concentrador, mediante solicitação do Banco, para a conexão de mais circuitos de comunicação, além de capacidade para processamento IMPLEMENTADA de tráfego mínimo de 20Gbps cada roteador;

3.4.1.10. No concentrador, deverão ser fornecidos equipamentos que permitam a adição e remoção de módulos e interfaces de rede sem a necessidade de desligamento do mesmo (mecanismo conhecido como “Hot Swap”), de forma a permitir a troca de componentes removíveis do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso;

3.4.1.11. Deverão implementar VRF (virtual routing and forwarding) ou funcionalidade semelhante de segregação de tabela de roteamento.

3.4.1.12. Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA (sendo a função de IP-SLA source obrigatória nos roteadores concentradores) ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP), e deverão ser fornecidos privilégios para usuários designados pelo BANCO para uso deste monitoramento

3.4.1.13. A estes roteadores deverá ser concedido o acesso de escrita com privilégios de administrador ao BANCO. Não será permitido à CONTRATADA do ITEM 1 a administração desses equipamentos. A CONTRATADA do ITEM 1, assim, será desobrigada a prestar gerenciamento, e suporte técnico em caso de problemas de configuração ocasionados pelo BANCO. Contudo, não haverá prejuízo das obrigações da CONTRATADA

do ITEM 1 no tocante aos requisitos de assistência técnica em casos de problemas de hardware. Bem como sem prejudicar o suporte técnico no que tange ao direito de atualização de firmwares, por exemplo;

3.4.1.14. NÃO faz parte do escopo deste edital o provimento dos circuitos de acesso concentradores de INTERNET. Estes serão de responsabilidade do BANCO, e eventuais problemas causados por estes acessos serão abonados de quaisquer SLAs às contratadas deste certame.

3.5. **Requisitos dos EQUIPAMENTOS ROTEADORES REMOTOS DE INTERNET (Unidades Distribuídas) (ITEM 1)**

3.5.1. O fornecimento dos equipamentos roteadores remotos de Internet para Unidades Distribuídas será facultado ao CONTRATADO, podendo atender este edital sem prover equipamentos deste tipo. Sendo suficiente a entrega do acesso compatível com a velocidade determinada para a localidade e via fornecimento de cabo UTP ethernet (categoria 6 ou superior) dentro da sala indicada pelo BANCO em cada unidade. Nesse caso, o CONTRATADO deverá ainda informar:

3.5.1.1. Endereço IP fixo;

3.5.1.2. Máscara compatível;

3.5.1.3. Default gateway.

3.5.2. Caso o CONTRATADO deseje fornecer os equipamentos roteadores remotos que serão fornecidos para as Unidades Distribuídas que terão acessos de Internet (Simétrica e Assimétrica), estes deverão atender:

3.5.2.1. Deverão ser fornecidos e gerenciados pela operadora. O Banco deverá ter acesso às informações do equipamento relacionado ao status das interfaces, serviços disponíveis e versão de sistema operacional. O acesso deverá ser garantido via CLI, interface gráfica ou via portal de gerenciamento do provedor de serviço, desde que seja possível buscar as informações acima.

3.5.2.2. Não deverão sobre nenhuma hipótese fornecer internet via Wi-Fi, sendo obrigatório a desativação (shutdown) caso disponível no equipamento, e deverá ter somente uma interface ativa para conexão direta no equipamento de sdwan, e outra interface para conexão externa com a própria operadora. Todas as outras interfaces, se for o caso, deverão estar em shutdown. O Banco poderá a qualquer momento solicitar relatório sobre o status das portas.

3.5.2.3. Para cada equipamento deverá ser fornecido 1 (um) cabo UTP categoria 6 ou superior. Caberá a operadora a conexão do equipamento com o equipamento sdwan em interface a ser especificada pelo Banco em momento de implantação, caso o equipamento SDWAN esteja instalado antes da ativação do link de internet.

3.5.2.4. Deverão ser compatíveis com o tipo de acesso a que estão provendo: Simétrico ou Assimétrico (ADSL ou modelo de atendimento realizado via discagem PPOE);

3.6. **Requisitos dos EQUIPAMENTOS ROTEADORES REMOTOS (Postos de Crédito) (ITEM 1)**

3.6.1. Os equipamentos roteadores que serão fornecidos para os Postos de Crédito contemplados com acesso Internet Determinística Dedicada terrestre, terão, além dos requisitos gerais, que atender:

3.6.1.1. Possuir pelo menos 16 (dezesseis) 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;

3.6.1.1.1. Será aceito o fornecimento de equipamento com menos interfaces, desde que seja fornecido em conjunto, sem custo adicional, equipamento switch gerenciável para complementar a quantidade de interfaces 10/100/1000Mbps RJ-45.

3.6.1.2. Possuir pelo menos 01 (uma) interface RJ-45, compatível com a velocidade do circuito, 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 ou IEEE802.3z 1000BASE-X, exclusiva para conexão WAN da CONTRATADA do ITEM 1; e mais 01 (uma) interface RJ-45, compatível com a velocidade do circuito, 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 ou IEEE802.3z 1000BASE-X para conexão com outros circuitos a critério do BANCO;

3.6.1.3. As interfaces dedicadas para a LAN na rede do Banco devem ser compatíveis com conexão em modo Bridge, ou seja, com uma interface L3 (roteamento da unidade remota), que utiliza duas conexões físicas (duas interfaces), permitindo assim a conexão em diferentes appliances na rede LAN do Banco e fazendo parte do mesmo domínio de broadcast, com 1 (um) único IP (L3) para cada interface, bem como para subinterfaces (compatíveis com 802.1q);

3.6.1.4. Implementar os protocolos de roteamento *Open Shortest Path First* (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771); Ambos os protocolos de roteamento (OSPF e BGP) devem ser também compatíveis com IPV6;

3.6.1.5. Implementar roteamento estático para o *Internet Protocol* (IP);

3.6.1.6. O roteador deverá ser capaz de fornecer IP via DHCP server para todas as unidades remotas. Dentre os parâmetros necessários, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com 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 seguir o padrão SLA;

3.6.1.7. O roteador deve ser capaz de criar Interfaces VLANs L3 e realizar o roteamento dessas redes internamente na unidade remota, bem como realizar o roteamento para toda a rede do Banco;

3.6.1.8. O roteador deverá ser compatível com 802.1Q, no caso de subinterfaces criadas. Atualmente o Banco possui segmentação lógica para redes de videoconferência, por exemplo. A criação de novas redes não deverá representar custos adicionais ao projeto e deverá seguir o padrão SLA;

3.6.1.9. Implementar o protocolo *Virtual Redundant Router Protocol* (VRRP) com monitoração de circuito e ativação automática do roteador secundário em caso de falha;

3.6.1.10. Implementar *Weighted Round Robin* (WRR) ou *Shaped Round Robin* (SRR);

3.6.1.11. Implementar a RFC 791 Type of Service – TOS;

3.6.1.12. Implementar a RFC 2474 Diffserv – DS;

3.6.1.13. Implementar *Traffic Shaping*;

3.6.1.14. Implementar *Weighted Random Early Detection* (WRED) ou *Weighted Tail Drop* (WTD) como mecanismo de prevenção de congestionamento;

3.6.1.15. Implementar IP *Precedence*;

3.6.1.16. Implementar o protocolo de marcação de quadros (*tagging*) de redes locais padrão IEEE 802.1q nas interfaces 1000BaseT ethernet utilizadas para interligação com a rede local das Unidades Distribuídas, CAPGV e Site Secundário;

3.6.1.17. Implementar *Network Address Translation* (NAT) para os principais protocolos da pilha TCP/IP;

3.6.1.18. Implementar *Access Control List* (ACL) simples e estendidas;

3.6.1.19. Implementar mecanismos de marcação de precedência (802.1p);

3.6.1.20. Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP), e deverão ser fornecidos privilégios para usuários designados pelo Banco para uso deste monitoramento, via acesso de gerência e via software de gerenciamento do Banco.

3.6.1.21. Não serão permitidas soluções que possuem disco rígidos em sua arquitetura;

3.6.1.22. Fornecer suporte a VPN IPSec, incluindo:

3.6.1.22.1. Criptografia 3DES-168 bits, AES-128 e AES-256;

3.6.1.22.2. Capacidade de implementar topologias site-to-site e *client-to-site*;

3.6.1.22.3. Suportar *Diffie-Hellman* Group 1, Group 2, Group 5, Group 14, Group 19 e Group 20;

3.6.1.22.4. Autenticação MD5 e SHA-1;

3.6.1.22.5. Internet Key Exchange (IKEv1 e v2);

3.6.1.22.6. Autenticação via certificado IKE PKI.

3.6.1.23. Implementar recurso de NAT (*Network AddressTranslation*) tipo *one-to-one*, *one-to-many*, *many-to-many*, *many-to-one*, e tradução simultânea de endereço IP, porta TCP de conexão (NAPT), e NAT transversal em VPN IPSec;

3.6.1.24. Possuir servidor de DHCP (*dynamic host configuration protocol*) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do equipamento;

3.6.1.25. Possibilitar a aplicação de regras de firewall que garantam que os usuários conectados acessem somente as VPNs estabelecidas pelo roteador, e deste com o recurso de ZTNA

informado neste edital, impossibilitando que demais acessos ocorram por meios diferentes desses informados;

3.6.1.26. Suportar endereçamento na interface de WAN por PPPOE (*Point-to-point Protocol Over Ethernet*), IP estático e dinâmico, por DHCP;

3.6.1.27. Permitir alta disponibilidade das interfaces WAN pelo menos na modalidades ativo-passivo (redundância);

3.6.1.28. A CONTRATADA deste item deverá permitir a conexão de outros circuitos, a critério do BANCO, a este equipamento, desde que o BANCO se responsabilize pela contratação e gestão dos mesmos. Caberá à contratada a configuração deste equipamento para receber o novo circuito;

3.6.1.29. Possuir gerenciamento de banda de entrada e saída, com classes de serviço por DSCP (*differentiated services code points*);

3.6.1.30. Possuir mecanismo que possibilite o funcionamento transparente dos protocolos FTP, SIP e H.323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

3.6.1.31. Possuir fonte de alimentação operando nas tensões 110/220V, com seleção automática de voltagem, e frequência de 50/60Hz.

3.6.1.32. Deve possuir no mínimo 128 MB de memória RAM;

3.6.1.33. Deve possuir memória Flash para armazenamento do sistema operacional. Sistema Operacional do Tipo “Hardenizado” não serão aceitos. Apenas os que forem armazenados em memória flash;

3.6.1.34. Deve suportar, no mínimo, 30 (trinta) usuários com acessos simultâneos, à taxa de 100Mbps, no mínimo, através de interfaces wireless (ver detalhes das especificações wireless logo abaixo) ou 50 (cinquenta) usuários simultâneos em casos de superintendências (ver anexo Modelo de Proposta);

3.6.1.35. Deve suportar pelo menos 5 (cinco) túneis VPN do tipo site-to-site já licenciados;

3.6.1.36. Suportar 5 (cinco) túneis VPN IPSEC do tipo client-to-site, baseado na aquisição de licenciamento;

3.6.1.37. Suportar, no mínimo, 5 (cinco) conexões do tipo SSL, sendo fornecida com pelo menos uma licença habilitada por equipamento;

3.6.1.38. 5 (cinco) interfaces de VLAN;

3.6.1.39. Prover autenticação de usuários para os serviços TELNET, SSH, FTP, HTTP e HTTPS de forma simultânea;

3.6.1.40. Permitir a autenticação dos usuários utilizando servidores LDAP, AD e RADIUS;

3.6.1.41. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

3.6.1.42. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;

3.6.1.43. Suportar padrão IPSec, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

3.6.1.44. Suportar a criação de túneis seguros sobre IP (IPSec tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

Requisitos de VPN:

3.6.1.45. Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

3.6.1.46. Suporte a certificados PKI X.509 para construção de VPNs;

3.6.1.47. Possuir suporte a VPNs IPSec site-to-site, VPNs IPSec client-to-site;

3.6.1.48. Deve permitir a arquitetura de vpn hub and spoke.

Acesso Wireless:

3.6.1.49. Deverá atender os requisitos de Acces Point descritos no item 3.7 interna ou externamente ao equipamento roteador;

3.6.1.50. Será facultado o fornecimento de *access point* para atender os itens de wireless especificados neste item, caso o equipamento roteador cotado não tenha essa função. Nesse caso, a conexão desse ao roteador não deverá consumir as postas de LAN acima especificadas.

Requisitos de Gerenciamento:

3.6.1.51. Suportar SNMP (Simple Network Management Protocol), com suporte a RFC 1213 (MIB-II). Deve ser fornecida uma comunidade (community) SNMP de leitura em todos os equipamentos na solução. Essa comunidade (community) será acessada a partir do CAPGV e Site Secundário;

3.6.1.52. Deve ser permitido o acesso de leitura a partir de solução de gerência do BANCO ou de empresa por ele indicado;

3.6.1.53. Deverá permitir a visualização dos usuários conectados (cabeados ou não);

3.6.1.54. Suportar Internet Protocol Flow Information eXport (IPFIX), Netflow v.9 ou o equivalente a:

3.6.1.54.1. Prover os seguintes relatórios que permitam a análise do tráfego que passa pelos equipamentos dos pontos, sob forma on-line, ou com atraso não superior a 15 minutos, e histórico, com possibilidade de apresentação das informações em formato tabular e gráfico:

a) Verificação do consumo de banda de um ou mais pontos de atendimento, permitindo filtro por endereço IP;
b) Detalhamento das conversações (socket) e protocolos de rede utilizados por um determinado endereço IP;
c) Verificação do consumo de banda total, sob forma percentual, utilizada por um ou mais aplicativos, com possibilidade de filtro por endereço IP ou faixa de endereços IPs.

3.6.1.55. Implementar o envio de mensagens de Syslog para um servidor indicado pelo BANCO;

3.6.1.56. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e administração do equipamento;

3.6.1.57. Permitir a conexão simultânea de vários administradores

3.6.1.58. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o equipamento;

3.6.1.59. Possuir mecanismo para realizar remotamente, pela interface gráfica, cópias de segurança (backup) e restauração, sem a necessidade de se reinicializar o sistema (no caso de realização de backups);

3.6.1.60. Permitir a visualização e o gerenciamento em tempo real ou com atraso não superior a 15 minutos de todas as conexões TCP e sessões UDP que se encontrem ativas através do equipamento, por serviços e endereços IP de origem e destino;

3.6.1.61. Permitir a visualização, em forma gráfica, do percentual do uso de CPU;

3.6.1.62. Permitir a visualização em tempo real ou com atraso não superior a 15 minutos, dos serviços com maior tráfego e os endereços IPs mais acessados;

3.6.1.63. Possibilitar o controle do tráfego, pelos endereços de origem e destino da comunicação;

3.6.1.64. Possuir suporte a LOG via Syslog;

3.6.1.65. Possibilitar o registro da comunicação realizada através do equipamento, sob demanda do administrador, das conexões abertas e das conexões recusadas pelo mesmo;

3.6.1.66. Prover mecanismo(s) de consulta às informações registradas e integradas à interface de administração;

3.6.1.67. Possibilitar a análise dos seus registros (LOGs) por pelo menos um programa analisador de LOG disponível no mercado;

3.6.1.68. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, possibilitando exportar os dados visualizados para arquivo formato PCAP também via interface gráfica ou CLI;

3.6.1.69. Deverá ser fornecido acesso via SSH em todos equipamentos com permissão “somente leitura” para o BANCO, incluindo possibilidade de visualização da configuração para auditorias quando necessário.

3.7. **Requisitos dos EQUIPAMENTOS ACCESS POINTS (AP’s) (ITEM 1)**

3.7.1. Os equipamentos *Access Point*s (AP’s) que serão fornecidos para os postos e unidades distribuídas serão contemplados em conjunto com acesso Internet Determinística Dedicada terrestre ou 5G (desde que garanta banda mínima dedicada), nos moldes dos Postos de Crédito, e terão, além dos requisitos gerais, que atender:

3.7.1.1. No caso das Superintendências, as funções de rádio devem ser providas por equipamentos dedicados, isto é, não podem ser providas pelos equipamentos roteadores fornecidos. Contudo, será permitido que o roteador atenda funções de controladora, segurança e controle de acesso;

3.7.1.2. Possuir funcionamento em modo gerenciado por Controlador Wi-Fi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF;

3.7.1.3. As funções de controladora poderão ser fornecidas internamente aos *Access Points* aqui especificados ou através do CPE fornecido a unidade/posto;

3.7.1.4. Possuir uma interface de rede RJ-45 Ethernet *Auto-sensing* que suporte as velocidades de 100/1000/2.5Gbps, atendendo as

especificações do padrão 802.3bz **ou** uma interface Ethernet Auto-sensing com MDI e MDX que suporte as velocidades de 10/100/1000Gbps;

3.7.1.5. Possuir interface de radio *Bluetooth Low Energy* (BLE) integrada;

3.7.1.6. Deve implementar cliente DHCP, para configuração automática de rede;

3.7.1.7. Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) Wi-Fi (se houver controladora) - operação em modo de “chaveamento de tráfego local”;

3.7.1.8. Operando no modo de “chaveamento de tráfego local”, que poderá ocorrer quando a comunicação entre o ponto de acesso Wi-Fi e o(s) Controlador(es) Wi-Fi (se houver controladora) for interrompida por qualquer motivo, como, por exemplo: falha no link WAN, LAN ou no(s) próprio(s) Controlador(es) Wi-Fi, o controlador Wi-Fi e os pontos de acesso deverão:

3.7.1.8.1. Continuar operando e permitindo que os usuários já autenticados na rede e associados aos pontos de acesso continuem a possuir acesso à rede;

3.7.1.8.2. Possuir meios de continuar operando e ter funcionalidade que permitam que novos usuários se autentiquem de acordo com 802.1x ou via PSK e se associem à rede sem qualquer prejuízo de acesso aos mesmos;

3.7.1.8.3. Mesmo sem acesso à controladora (se houver controladora), os *Access-points* deverão possuir capacidade para armazenar *logs* de autenticação, erros, alertas, etc

3.7.1.9. A solução proposta deve prever o atendimento dos itens anteriores, e alternativamente, a CONTRATADA poderá fornecer uma solução de redundância e autenticação local para os pontos de acesso operando com “chaveamento de tráfego local”.

3.7.1.10. Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g,ac, 802.11n draft 2.0, 802.11ax e 802.11ac ou superior e implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

3.7.1.11. Deve implementar o padrão de segurança WPA3, comprovando esta funcionalidade através de certificação da Wi-Fi Alliance;

3.7.1.12. Deve implementar os padrões 802.11a/b/g/n/ac/ax Wave 2;

3.7.1.13. Deve possuir antenas integradas ao equipamento, compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac com ganho de, pelo menos, 5 dBi na faixa de 5.0 GHz e IEEE 802.11/b/g/n com ganho de, pelo menos, 3 dBi na faixa de 2.4

3.7.1.14. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11ac: MSC0 – MCS9 para 1 e 2 Spatial Streams (6.5Mbps - 1,3Gbps) para ambientes com até 30 usuários ou 1, 2 e 3 Spatial Streams para acima disso (ver Anexo com quantitativos de usuários por ambiente);

3.7.1.15. Possuir potência máxima de transmissão de, no mínimo, 21 dBm em 2.4GHz e 24dBm em 5GHz

3.7.1.16. Deverá implementar operação em 2x2:2 MIMO com diversidade espacial em 2,4 GHz;

3.7.1.17. Deverá implementar operação em 4x4:4 MIMO com diversidade espacial em 5 GHz;

3.7.1.18. Deve implementar padrão Wi-Fi 6 (802.11ax) nas frequências 2.4G e 5G simultaneamente;

3.7.1.19. Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN. Deve permitir esta formação de banda para cliente 802.11 a/g/n/AC;

3.7.1.20. Possuir estrutura metálica que permita fixação do equipamento em teto e também em parede;

3.7.1.21. Possuir varredura de RF nas bandas 802.11 b/g/n e 802.11 a/n/ac para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado no ponto de acesso;

3.7.1.22. Deve possuir uma trava de segurança compatível à utilizada em desktops e notebooks (Kensington security lock ou similar) e que permita a instalação de um cabo de segurança com a finalidade de evitar o furto do equipamento. O equipamento deve vir acompanhado com o cabo de segurança.

3.7.1.23. Deve prover 3 Gbps por AP, considerando ambas frequências;

3.7.1.24. Possuir capacidade de selecionar automaticamente o canal de transmissão;

3.7.1.25. Implementar o protocolo de enlace CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão;

3.7.1.26. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;

3.7.1.27. Possuir suporte a pelo menos 16 SSIDs e 16 VLANs;

3.7.1.28. Permitir habilitar e desabilitar a divulgação do SSID;

3.7.1.29. Possuir padrão WMM (Wi-Fi Multimedia) da Wi-Fi Alliance para priorização de tráfego;

3.7.1.30. Não deve haver licença restringindo o número de usuários por ponto de acesso. O Ponto de Acesso deve permitir, no mínimo, 300 usuários por rádio;

3.7.1.31. Deve possuir no mínimo 02 rádios (dual radio) operando simultaneamente em frequências distintas;

3.7.1.32. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono);

3.7.1.33. Possuir, no mínimo, 01 LED indicativo do estado de operação;

3.7.1.34. Deve implementar um mecanismo de controle de associação de banda, de forma que usuários com capacidade de comunicação em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN;

3.7.1.35. Implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso;

3.7.1.36. Deve permitir a conexão de usuários em IPv4, IPv6 e Dual-stack;

3.7.1.37. O equipamento deve ser capaz de implementar 802.11e com WMM;

3.7.1.38. Os equipamentos devem realizar a monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências Wi-Fi e Interferências Não-Wi-Fi e simultaneamente atender os usuários da rede Wi-Fi;

3.7.1.39. Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para identificação de interferências não 802.11, analise de espectro, e evita-las automaticamente;

3.7.1.40. Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação;

3.7.1.41. Deve operar nos seguintes modos: “Modo Local”, “Modo Monitor” e “Modo Analisador de Espectro”;

3.7.1.42. Operando em “Modo Local” o ponto de acesso deve fornecer informações ao Controlador Wi-Fi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede Wi-Fi. Deve fazer tanto a transmissão de dados Wi-Fi quanto a análise de espectro simultaneamente, sem prejuízo ao fornecimento de Wi-Fi aos usuários;

3.7.1.43. Operando em “Modo Monitor” deve fornecer informações ao Controlador Wi-Fi referente à qualidade do espectro de RF para todos os canais monitorados em 2.4GHz e em 5GHz, simultaneamente, identificando equipamentos interferentes na rede Wi-Fi e rogue APs;

Segurança da Informação

3.7.1.44. Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:

3.7.1.44.1. EAP-Transport Layer Security (EAP-TLS);

3.7.1.44.2. PEAPv0/EAP-MSCHAPv2;

3.7.1.44.3. PEAPv1/EAP-GTC;

3.7.1.44.4. EAP Subscriber Identity Module (EAP-SIM).

3.7.1.45. Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.

3.7.1.46. Deve implementar suplicante 802.1x par identificar o pontos de acesso, ao ser conectado na estrutura de rede cabeada.

3.7.1.47. Possuir modulo de criptografia em hardware.

3.7.1.48. Implementar WPA-2 (*Wi-Fi Protected Access* com algoritmo de criptografia AES, 128 bits).

Alimentação

3.7.1.49. Possibilitar a alimentação via padrão PoE (802.3af ou PoE+ (IEEE 802.3at), utilizando apenas uma porta do switch onde estiver conectado;

3.7.1.50. Todos os *access points* deverão sem alimentados por portas PoE do próprio roteador ou através de *power injectors* fornecidos pelo CONTRATADO.

Modo Auto Gerenciado

3.7.1.51. A solução deve operar em modo auto gerenciado, ou seja, onde não há necessidade da utilização de um controlador WLAN para as configurações dos parâmetros da rede wireless, políticas de segurança, QoS e gerenciamento de RF, onde os Pontos de acesso fazem parte de um Cluster para compartilhamento destas informações e controle da rede:

3.7.1.52. Além de operar em modo auto gerenciado, deverá permitir que os pontos de acesso sejam convertidos para um ambiente com controladora WLAN, ou seja, somente através de atualizações de software, sem necessidade de troca de hardware, permitindo que os Pontos de acesso sejam registrados e controlados por uma controladora WLAN, caso necessário.

Controle de Acesso

3.7.1.53. A solução (access point, controladora ou mesmo o roteador) deverá implementar controle de acesso de forma que diferencie os tipos de usuários conectados de forma a definir o perfil do usuário;

3.7.1.54. A solução (access point, controladora ou mesmo o roteador) deverá permitir a atribuição de cotas mensais para cada perfil de usuário;

3.7.1.55. A solução (access point, controladora ou mesmo o roteador) deverá permitir atribuição de perfil de acesso para cada tipo de usuário (redes sociais, streaming, downloads, etc);

3.7.1.56. A solução (access point, controladora ou mesmo o roteador) deverá permitir que os funcionários e colaboradores acessem a rede sem fio através do seu login e senha da rede (Active Directory) e a partir do seu cargo ou função, seja determinado seu perfil de acesso (Cotas, velocidade, perfil de acesso, etc);

3.7.1.57. A identidade dos visitantes deverá ser validada através de SMS que será enviada ao número celular do mesmo no momento do cadastro;

3.7.1.58. O pacote de SMS deverá estar incluso na solução;

3.7.1.59. A solução deverá permitir o bloqueio de usuários cadastrados;

3.7.1.60. Deve implementar mecanismo de autenticação através de portal Web (Captive Portal) que pode ser atendido por solução em Cloud para os usuários visitantes, temporários ou clientes corporativos;

3.7.1.61. Estes usuários autenticados através do portal Web devem se autenticar e ser desviados para segmentos específicos da rede LAN(VLANs);

3.7.1.62. O controlador Wi-Fi deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes, temporários ou clientes corporativos.

Gerenciamento

3.7.1.63. A solução deve apresentar uma gerência centralizada para está arquitetura através de padrão Web, que deverá permitir a realização de todas as configurações necessárias para a rede Wireless;

3.7.1.64. Serão aceitas soluções de gerência com gestão em nuvem. A solução de gerência deverá ser entregue de maneira virtualizada (Instalada em ambiente virtual do contratante) e com licenças perpétuas para todos os Pontos de Acesso adquiridos, seguindo as especificações contidas no item 3.6

3.7.1.65. Ainda em caso de perda da comunicação com a plataforma de gerencia, a solução deve disponibilizar de forma automática, uma interface web local, para gerenciamento dos Pontos de acesso, durante o evento de falha.

3.7.1.66. 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;

3.7.1.67. A plataforma de gestão deve permitir a criação de grupos de equipamentos, de forma que permita a visualização e aplicação de configurações por grupos;

3.7.1.68. Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento;

3.7.1.69. Acesso ao sistema através de cliente com browser padrão (HTTPS);

3.7.1.70. Deve permitir a realização de atualizações de software através da plataforma de gerencia, e permitir também o agendamento para que a atualização seja feita em uma janela de manutenção;

3.7.1.71. Implementar varredura de RF contínua ou sob demanda, com identificação de APs irregulares;

3.7.1.72. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;

3.7.1.73. Implementar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance;

3.7.1.74. Ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;

3.7.1.75. Permitir o uso de voz e dados sobre um mesmo SSID;

3.7.1.76. Otimizar o desempenho e a cobertura da radiofrequência;

3.7.1.77. Possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest)

3.7.1.78. Permitir autenticação de usuário utilizando RADIUS e LDAP;

3.7.1.79. Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim

3.7.1.80. Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos EAP: PEAP, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de servidor RADIUS externo

3.7.1.81. Possuir suporte a autenticação IEEE 802.1X, com o método PEAP/EAP-GTC, e com utilização de base de usuários LDAP externa

3.7.1.82. Permitir a seleção / uso de servidor Radius ou LDAP com base no SSID

3.7.1.83. Deve suportar utilização de Portal Captivo externo a solução

3.7.1.84. Permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN (wireless)

3.7.1.85. Realizar o controle de autorização baseado em perfis de acesso;

3.7.1.86. Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;

3.7.1.87. Permitir o bloqueio de comunicação entre clientes wireless – L2 bridging;

3.7.1.88. Implementar filtros baseados em protocolos;

3.7.1.89. Implementar listas de controle de acesso (ACLs);

3.7.1.90. Permitir a aplicação de políticas de camada 4, de acordo com as características do usuário. Por exemplo, um usuário que pertença ao grupo de gerentes (cadastrado no Radius ou Active Directory) terá permissão de acesso ao protocolo FTP no servidor de ERP;

3.7.1.91. Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede;

3.7.1.92. Permitir o controle de banda disponível (bandwidth contracts) por usuário, por aplicação ou SSID;

3.7.1.93. Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;

3.7.1.94. Implementar roaming de camada 2 e de camada 3;

3.7.1.95. Implementar segurança IEEE 802.11i;

3.7.1.96. Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP e TKIP ;

3.7.1.97. Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.1n e 802.11ac para identificação de ataques e APs intrusos não autorizados (rogues);

3.7.1.98. Realizar a varredura no canal de operação do AP sem impacto na performance da rede WLAN;

3.7.1.99. Permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN;

3.7.1.100. Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para identificação de interferências não 802.11, analise de espectro, e evita-las automaticamente;

3.7.1.101. Utilizar os APs como ”sensores” de RF para fazer a monitoração do ambiente Wireless;

3.7.1.102. Implementar mecanismos para detecção de APs não autorizados (rogues);

3.7.1.103. Realizar a contenção automática dos APs Rogue através da rede WLAN;

3.7.1.104. Realizar a identificação e contenção de redes “AD-HOC;

3.7.1.105. Deve implementar funcionalidades de WIPS (Wireless Intrusion Prevention System) com detecção de ataques à rede sem fio e tomada automática de ações de defesa no próprio conjunto de AP;

3.7.1.106. Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID (Service Set Identifier) que podem ser percebidos pelos Ponto de Acesso;

3.7.1.107. Deve implementar o protocolo NTP ou SNTP;

3.7.1.108. Implementar o envio de traps SNMP;

3.7.1.109. Implementar tagging de VLANs através do protocolo 802.1Q;

3.7.1.110. Realizar a descoberta automática dos APs na infraestrutura wireless, permitido que novos APs se configurem automaticamente ao serem ligar a rede existente;

3.7.1.111. Possuir a funcionalidade da utilização do protocolo Bonjour na infraestrutura, permitindo que os serviços divulgados via mDNS sejam controlados, filtrados e disponibilizados entre diferentes subnets, tornando assim possível a utilização em redes com múltiplas subnets e um número grande de dispositivos.

4. MEIOS FÍSICOS DOS CIRCUITOS PRIMÁRIOS, SECUNDÁRIOS E TERCIÁRIOS (ITEM 1)

4.1. Os circuitos de acesso primários, secundários e terciários das unidades distribuídas, postos Parceiros, Site Secundário (independente da localidade/tecnologia) e do Site Primário (CAPGV) deverão constituir-se de meios físicos terrestres ou 5G e dedicados, independentes, podendo cada trecho que compõe cada circuito de acesso ser constituído exclusivamente por um ou mais dos seguintes meios:

4.1.1. Fibra óptica;

4.1.2. Cabo metálico; ou

4.1.3. 5G.

4.2. Deverá ser observado ainda que o circuito primário, secundário e terciário não compartilharão os mesmos recursos de acesso ao meio e Pontos de Presença, exceto em casos onde for fisicamente impossível;

4.3. A última milha deverá obrigatoriamente ser fornecida por meio terrestre (fibra óptica ou cabo metálico).

5. REQUISITOS ESPECÍFICOS PARA O CAPGV E SITE SECUNDÁRIO PARA CIRCUITOS MPLS (ITEM 1)

5.1. Quantidade de equipamentos roteadores e comutadores

5.1.1. Deverão ser fornecidos equipamentos roteadores em quantidade suficiente para suportar o tráfego de/para cada um dos grupos especificados, independentemente. Esse requisito aplica-se ao conjunto de todas as unidades distribuídas, e separadamente à conexão com os parceiros do Banco, respeitando os demais requisitos aplicáveis.

5.2. Capacidade dos equipamentos roteadores e comutadores

5.2.1. Os equipamentos roteadores e comutadores fornecidos deverão ser capazes de trafegar, sem a ocorrência de subdimensionamento, toda a largura de banda disponível entre a concentração e as unidades distribuídas, incluindo a largura de Internet.

5.2.2. A título de roteamento de tráfego (throughput) estes equipamentos deverão suportar a soma dos links das Unidades, conforme Anexo III - Endereços e Velocidades do Edital, permitindo crescimento de 100% (cem por cento), sem a necessidade de troca dos equipamentos na concentração e unidades distribuídas.

5.3. **Capacidade de instalação e remoção de módulos e interfaces**

5.3.1. Deverão ser fornecidos equipamentos que permitam a adição e remoção de módulos e interfaces de rede sem a necessidade de desligamento ou reinício do mesmo (mecanismo conhecido como “Hot Swap”), de forma a permitir a troca de componentes do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso.

5.4. **Infraestrutura de Acesso no Concentrador**

5.4.1. Deverá ser provida infraestrutura de acesso totalmente redundante nos concentradores conforme abaixo detalhado:

5.4.1.1. 01 acesso concentrador primário para a rede primária MPLS das Unidades e Parceiros no Site Primário (CAPGV);

5.4.1.2. 01 acesso concentrador secundário para a rede primária MPLS das Unidades e Parceiros no Site Secundário (CAPGV);

5.4.1.3. 01 acesso concentrador primário para a rede secundária das Unidades Distribuídas e Parceiros no Site Primário (CAPGV);

5.4.1.4. 01 acesso concentrador secundário para a rede secundária das Unidades Distribuídas e Parceiros no Site Secundário (CAPGV);

5.4.2. Considerando que a rede Parceiros prevê o provimento remoto com duas operadoras distintas (Operadora 1 e 2, link primário e secundário), os acessos concentradores acima deverão considerar a chegada de ambas as operadoras em ambos os datacenters. Por isso, a quantidade de acessos acima informada é a mínima. Sendo assim, será permitido que o acesso concentrador da Operadora 2 (link secundário) da Rede Parceiros seja compartilhado com os acessos concentradores da Rede primária das Unidades Distribuídas, desde que esses acessos sejam encaminhados por rotas distintas e sejam providos por backbones também distintos dentro da cidade de Fortaleza-CE;

5.4.3. Para cada acesso concentrador MPLS será fornecido pelo CONTRATADO um CPE concentrador seguindo as especificações já descritas;

5.4.4. Devendo os circuitos de comunicação utilizar tecnologia determinística e ter encaminhamentos distintos para interligar-se ao ponto de presença do fornecedor. Os concentradores da Rede Parceiros não poderão ser compartilhados com os outros concentradores. Os concentradores ou enlaces dos circuitos primários das unidades remotas não poderão ser compartilhados com os concentradores ou enlaces dos circuitos secundários das unidades remotas, visto que são estruturas de acesso obrigatoriamente separadas.

5.5. **Redundância e recuperação automática de falhas**

5.5.1. No caso de falha em qualquer um dos recursos de acesso no concentrador, equipamento roteador, interface ou porta de equipamento, ou qualquer outra falha em componente fornecido que afete os serviços, todo o tráfego afetado deverá ser redirecionado para os outros recursos que permaneçam em operação, devendo todas as características e funcionalidades do serviço serem mantidas plenamente, mantendo-se atendido ainda o requisito de capacidade de transmissão para cada circuito de acesso em operação. Essa comutação deverá ser realizada na nuvem da operadora contratada.

5.5.2. O restabelecimento dos serviços em caso de falha e o retorno à operação normal quando do fim da falha deverão acontecer, em sua plenitude, de forma

automática em até 3 (três) minutos a partir do início ou fim da falha. Isto deve acontecer sem qualquer intervenção humana, quer seja para realizar configuração em equipamento ou sistema de gerência, quer seja para realizar mudanças físicas na infraestrutura fornecida.

5.6. **Distribuição de carga nos circuitos de acesso**

5.6.1. A implementação da solução do CONTRATADO do ITEM 1 deverá assegurar a divisão do tráfego através da funcionalidade de distribuição de carga entre os enlaces de acesso primário e secundário, de forma totalmente transparente para o Banco. Esse critério deverá ser aplicado independentemente, tanto para a capacidade de transmissão quanto de recepção.

5.6.2. Deverá ser possível também a implementação da distribuição da carga entre os roteadores concentradores localizados no CAPGV e Site Secundário.

6. REQUISITOS ESPECÍFICOS PARA OS CIRCUITOS DE ACESSO REMOTOS

6.1. **Requisitos específicos para os Circuitos de Acesso Primário (MPLS) (Unidades Distribuídas e Parceiros)**

6.1.1. Cada unidade distribuída e Parceiro deverão ser atendidos por um circuito de acesso primário, que utilizará tecnologia determinística para conexão ao backbone MPLS e dará o suporte ao tráfego de dados, voz e imagens (quando houver) da respectiva unidade distribuída.

6.1.2. As tecnologias secundárias e terciárias deverão possuir meios físicos completamente diferentes e independentes entre si e dos sistemas fornecidos para os circuitos de acesso primários, isto é, sem que haja compartilhamento de recurso entre os circuitos de acessos primário, secundário e terciário, incluindo subsestações e pontos de presença.

6.1.3. Caso não haja meios distintos de acesso de entrada na Unidade Remota (ex: postes e dutos subterrâneos), os acessos primários, secundários e terciários poderão compartilhar o acesso que já estiver previamente instalado.

6.1.4. **Instalação do circuito**

6.1.4.1. Todos os serviços necessários à instalação do circuito, tais como passagem de cabos e tubulações, ficarão a cargo do CONTRATADO.

6.1.5. **Capacidade dos circuitos de acesso**

6.1.5.1. A capacidade de transmissão mínima dos circuitos de acesso das unidades distribuídas está especificada no Anexo III - Endereços e Velocidades. Tal capacidade já considera o tráfego integrado de dados, voz e imagens a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

6.1.5.2. A capacidade de transmissão especificada deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente.

6.2. **Requisitos específicos para os Circuitos de Acesso Secundários (MPLS - Parceiros e Internet Determinística - Unidades Distribuídas)**

6.2.1. Todos os Parceiros serão atendidos por circuito de acesso secundário do tipo MPLS, conforme item anterior.

6.2.2. Entretanto, as unidades distribuídas serão atendidas por um circuito de acesso secundário do tipo Internet Determinística Simétrica, isto é, dedicada e com garantia de 100% (cem por cento) do tráfego de upload e download. Este acesso deverá ser determinístico e utilizará os meios abaixo que darão suporte ao tráfego de dados, voz e imagens (quando houver) da respectiva unidade distribuída.

6.2.3. Essas tecnologias deverão possuir meios físicos completamente diferentes e independentes dos sistemas fornecidos para os circuitos de acesso primários, isto é, sem que haja compartilhamento de qualquer tipo de recurso entre o circuito de acesso primário e o circuito de acesso secundário.

6.2.4. Cada circuito de acesso secundário de Internet Determinística deverá ser fornecido juntamente com o 01 (um) endereço IP público, exclusivo e dedicado àquela unidade distribuídas, assim como a sua respectiva máscara e default gateway.

6.2.5. Todas as tecnologias acima estarão sujeitas aos requisitos de SLA estabelecidos no Anexo VI - Acordo de Níveis de Serviços e poderão, a critério do Banco e respeitando a cobertura do CONTRATADO, serem alteradas durante a vigência contratual.

6.2.6. **Instalação do circuito**

6.2.6.1. Todos os serviços necessários para instalação do circuito, tais como passagem de cabos e tubulações ficarão a cargo do CONTRATADO.

6.2.7. **Capacidade dos circuitos de acesso**

6.2.7.1. A capacidade de transmissão mínima dos circuitos de acesso das unidades distribuídas está especificada no Anexo III - Endereços e Velocidades. Tal capacidade já considera o tráfego integrado de dados, voz e imagens (quando houver) a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

6.2.7.2. A capacidade de transmissão especificada deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente, de forma dedicada, isto é, 100% (cem por cento) para download e 100%(cem por cento) para upload.

6.3. **Requisitos específicos para os Circuitos de Acesso Terciários (Internet Simétrica ou Assimétrica) (Unidades Distribuídas)**

6.3.1. Cada Unidade Distribuída deverá ser atendida por um circuito de acesso terciário do tipo Internet Simétrica ou Assimétrica, de acordo com a disponibilidade do CONTRATADO. Este acesso utilizará os meios físicos já especificados.

6.3.2. Cada circuito de acesso terciário Simétrico deverá ser fornecido juntamente com o 01 (um) endereço IP público, exclusivo e dedicado àquela Unidade, assim como a sua respectiva máscara e default gateway.

6.3.3. Caso durante a vigência contratual o CONTRATADO do ITEM 1 apresente disponibilidade de atendimento em tecnologia superior a porventura instalada (mantendo os aspectos de independência dos demais acessos), por exemplo: MPLS para Internet ou Internet Simétrica em detrimento da Internet Assimétrica, este se obriga a informar a viabilidade ao Banco e a enviar proposta de preço para realização de aditivo, a critério do Banco, para alteração da tecnologia.

6.3.4. Todas as tecnologias acima estarão sujeitas aos requisitos de SLA estabelecidos no Anexo VI - Acordo de Níveis de Serviços e poderão, a critério do Banco, e respeitando a cobertura do CONTRATADO, serem alteradas durante a vigência contratual.

6.3.5. **Instalação do circuito terciário**

6.3.5.1. Todos os serviços necessários para instalação do circuito, tais como passagem de cabos e tubulações ficarão a cargo do CONTRATADO.

6.3.6. **Capacidade dos circuitos de acesso**

6.3.6.1. A capacidade de transmissão mínima dos circuitos de acesso das unidades distribuídas está especificada no Anexo III - Endereços e Velocidades. Tal capacidade já considera o tráfego integrado de dados, voz e imagens (quando houver) a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

6.3.6.2. A capacidade de transmissão especificada para os acessos simétricos determinísticos deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente, de forma dedicada, isto é, 100% (cem por cento) para download e 100%(cem por cento) para upload.

6.3.6.3. Caso seja fornecido acesso assimétrico, durante a vigência contratual, a capacidade de transmissão e recepção deverá atender os limites estabelecidos pela ANATEL pela Resolução Resolução nº 717/2019. Atualmente, a ANATEL estabelece que a largura de banda média percebida ao final do mês não pode ser inferior a 80% (oitenta por cento) para download e upload. Estando sujeito a alterações, conforme regulamentações da ANATEL.

6.4. **Requisitos específicos para os Circuitos de Acesso Posto (Internet Determinística) (Postos de Crédito)**

6.4.1. Todos os Postos de Crédito serão atendidos por circuito de acesso tipo Internet Determinística, isto é, dedicada e com garantia de 100% (cem por cento) do tráfego de upload e download. Este acesso deverá ser determinístico e utilizará os meios físicos abaixo que darão suporte ao tráfego de dados, voz e imagens (quando houver) da respectiva unidade distribuída.

6.4.2. Cada circuito de acesso Internet Determinística deverá ser fornecido juntamente com o 01 (um) endereço IP público, exclusivo e dedicado àquela unidade distribuídas, assim como a sua respectiva máscara e default gateway.

6.4.3. Todas as tecnologias acima estarão sujeitas aos requisitos de SLA estabelecidos no Anexo VI - Acordo de Níveis de Serviços e poderão, a critério do Banco e respeitando a cobertura do CONTRATADO, serem alteradas durante a vigência contratual.

6.4.4. **Instalação do circuito**

6.4.4.1. Todos os serviços necessários para instalação do circuito, tais como passagem de cabos e tubulações ficarão a cargo do CONTRATADO.

6.4.5. **Capacidade dos circuitos de acesso**

6.4.5.1. A capacidade de transmissão mínima dos circuitos de acesso dos postos de Crédito está especificada no Anexo III - Endereços e Velocidades. Tal capacidade já considera o tráfego integrado de dados, voz e imagens (quando houver) a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

6.4.5.2. A capacidade de transmissão especificada deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente, de forma dedicada, isto é, 100% (cem por cento) para download e 100%(cem por cento) para upload.

6.5. **Chaveamento entre os circuitos de acesso pela solução SD-WAN (ITEM 2)**

6.5.1. 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.

6.5.2. 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 do item 1.10.

6.6. **Chaveamento para o Site Secundário (ambos os ITENS)**

6.6.1. Em caso de queda do Site Primário (CAPGV), todo o tráfego oriundo das unidades distribuídas, Parceiros e Postos 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 CONTRATADOS.

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

7. APLICAÇÃO DE POLÍTICAS DE CONTROLE DE TRÁFEGO

7.1. 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:

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

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

7.1.3. No tráfego previamente marcado pela solução do ITEM 2 e/ou marcado pelos equipamentos do Banco.

7.2. No caso da tecnologia MPLS, a rede do Contratado deverá suportar todas as funcionalidades de VPN, MPLS e QoS. Deverão ser seguidos os seguintes padrões das RFCs 2474 e 2475 – DiffServ, complementados pela RFC 2597 – Assured Forwarding Per-hop Behaviors (AF PHB) e pela RFC 2598 – Expedited Forwarding (EF).

7.2.1. Os valores de largura de banda que são definidos no Anexo III - 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.

7.2.2. No caso dos links MPLS, deverá ser possível realizar o transbordo de uma classe para outra classe, realizando a remarcação do pacote. Por exemplo, no caso de uma classe que marque um pacote AF31 chegar a seu limite de ocupação de largura de banda, deverá ser possível encaminhar o tráfego como transbordo, remarcando esse para AF12, por exemplo, onde esse respeitará as regras definidas na nova classe. O critério será informado pelo Banco em fase de implantação, podendo ser alterado durante o Contrato.

7.2.3. Ainda sobre os links MPLS, deverá ser possível manter a marcação DSCP realizada na LAN por outros equipamentos e realizar a devida priorização, ou seja, o algoritmo de classificação deverá permitir a priorização com base no DSCP, mesmo quando pacotes internos da LAN tiverem o mesmo IP de origem e marcações DSCP diferentes. 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. Além de utilizar a marcação DSCP recebida da LAN, os roteadores das operadoras poderão, a critério do Banco, possuir também uma lista (ACL) definida com IP e porta dos principais serviços do Banco.

7.2.4. As configurações referentes à probabilidade de descarte de pacotes, especificadas na RFC 2597, deverão ser suportadas pela Rede MPLS, porém não serão utilizadas num primeiro momento, podendo, no futuro, serem solicitadas para que seja possível a escolha de tráfegos específicos que terão pacotes descartados antes dos outros.

7.2.5. O CONTRATADO do ITEM 1 deverá prover uma rede IP logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da Internet. O mecanismo para implementar o isolamento e a qualidade de serviços é o MPLS/VPN. Essa garantia deverá ser implementada “fim-a-fim”.

Fornecimento de informações

7.2.6. 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:

7.2.6.1. Plano de endereçamento utilizado pelo Internet Protocol (IP) na rede interna do Banco e unidades remotas;

7.2.6.2. Protocolos de roteamento utilizados;

7.2.6.3. Detalhamento de regras e políticas de controle e qualificação de tráfego;

7.2.6.4. Detalhamento da caracterização do tráfego de dados, voz e imagens, incluindo suas possíveis subclassificações;

7.2.6.5. Padrão de configuração de sistema operacional de roteadores e comutadores.

8. REQUISITOS GERAIS PARA OS EQUIPAMENTOS APPLIANCES SD-WAN (ITEM 2)

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

8.1.1. 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 de Crédito neste primeiro momento. Havendo necessidade, a critério do Banco, aditivos contratuais de expansão serão providenciados;

8.1.2. A solução será composta pelos serviços de SASE NOC (*Network Operations Center*).

8.1.3. Deverá ser fornecido usuário de leitura para o Banco para todos os equipamentos e softwares que compõem o ITEM 2;

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

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

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

8.1.7. 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;

8.1.8. 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;

8.1.9. A instalação e configuração da solução ofertada é de responsabilidade do CONTRATADO, 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 manter as necessidades 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 exemplo;

8.1.9.1. Caso a solução de SD-WAN seja instalada na unidade remota antes da instalação dos novos circuitos de comunicação (ITEM 1), 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;

8.1.9.2. Caso a solução de SD-WAN seja instalada depois dos novos circuitos de dados (ITEM 1), caberá ao contratado do ITEM 2 a conexão entre a solução de SD-WAN com os novos circuitos (ITEM 1), 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;

8.1.9.3. 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;

8.1.9.4. Caberá ao Banco o agendamento da instalação inicial com as suas Unidades e com as CONTRATADAS dos ITENS 1 e 2, de acordo com o cronograma definido pelas CONTRATADAS dos ITEMS 1 e 2.

8.1.10. Para cada equipamento entregue, deve ser entregue 1 (um) cabo UTP de 2,5 metros crimpado com RJ45 de fábrica e com a devida certificação. O mesmo deverá ser de categoria 6 ou superior. Durante ativação do roteador, o cabo deverá ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação;

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

8.1.12. A solução SD-WAN deverá ocupar no máximo 2Us (Rack units) em cada unidade remota e receberá as conexões dos equipamentos do Banco, sendo essas conexões de responsabilidade do CONTRATADO 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;

8.1.13. A solução de SD-WAN deverá ter capacidade para receber os acessos primários, secundários e terciários em portas do tipo WAN, padrão Ethernet RJ-45, dedicadas para este fim;

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

8.1.15. 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;

8.1.16. A solução deverá permitir atualização e sincronização automática de "clock", de forma que os relatórios e todas as informações sejam sincronizados com a hora do Banco via NTP (Network Time Protocol);

8.1.17. 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;

8.1.18. O monitoramento sobre a solução do ITEM 1 deverá possibilitar criação de alertas para alteração de status de protocolos usados como BGP por exemplo, e VRRP caso sejam usados, evidenciando e alarmando falhas de intermitência. Atualmente o monitoramento é feito utilizando envio de logs para servidores remotos (Syslog);

8.1.19. Todas as portas utilizadas na solução deverão ser compatíveis com conexão com switches e roteadores sem necessidade de cabos cross over;

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

8.1.21. 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;

8.1.22. Para os Datacenters, suportar capacidade de roteamento de tráfego (*throughput*), no mínimo de 20Gbps;

8.1.23. Para dimensionamento da solução das Unidades Distribuídas, a título de roteamento de tráfego (*throughput*) e visibilidade de aplicações camada 7 (firewall), suportar a soma dos links daquela Unidade, conforme Anexo III - Endereços e Velocidades do Edital, permitindo 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 130Mbps, o equipamento deverá suportar o tráfego WAN de pelo menos 260Mbps;

8.1.24. Os equipamentos fornecidos para SD-WAN nas unidades remotas 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, entender que deve ser gerenciado pela solução instalada no Banco (*on-permise*)_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;

8.1.25. A solução deverá fornecer IP via DHCP server, sendo fornecimento próprio via DHCP server para todas as unidades remotas. 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;

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

8.1.27. Durante a implantação ou durante a falha de equipamentos na vigência do Contrato, a solução deverá permitir que sites que já possuem a nova solução continuem se comunicando com os sites que ainda não a possuem;

8.1.28. 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;

8.1.29. 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);

8.1.30. A solução deverá permitir ao administrador definir políticas de encaminhamento de tráfego que levem em consideração a disponibilidade e o congestionamento dos links e, em caso de falha ou congestionamento dos circuitos de comunicação, o tráfego deverá ser desviado automaticamente para outro link ativo, seguindo uma sequência pré-definida pelo Banco em tempo de implantação. Após resolução em falha de link ou ausência do congestionamento, o retorno do tráfego deverá ser automático, ou seja, sem configuração manual;

8.1.31. Caso o link não esteja indisponível ou congestionado, a solução deverá permitir ao administrador definir políticas de engenharia de tráfego que levem em consideração 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;

8.1.32. 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:

8.1.32.1. Com base em um único ou vários IPs;

8.1.32.2. Com base em uma única ou várias Subnet;

8.1.32.3. Com base em uma ou várias portas TCP/UDP;

8.1.32.4. Com base no valor do DSCP;

8.1.32.5. Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN.

8.1.33. A solução deverá suportar a quantidade de 20 sessões simultâneas por usuário, no mínimo. A quantidade de usuários por unidade está disponível no Anexo III - Endereços e Velocidades;

8.1.34. Cada solução SD-WAN instalada nos datacenters (Site Principal e Site Secundário) deverá possuir redundância N+N 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;

8.1.35. Cada solução de gerenciamento instalado 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;

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

8.1.37. Todas as necessidades de hardware e software (incluindo protocolos) necessários para a redundância e alta disponibilidade exigidas nessas especificações devem ser fornecidas pela solução contratada;

8.1.38. A solução SD-WAN das unidades remotas 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 do ITEM 1 (desde que aderentes às especificações do item 1.5), 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 (por exemplo, protocolos e licenças) capazes de manter a alta disponibilidade deverá ser fornecidas em conjunto com a solução contratada.;

8.1.39. Nas unidades remotas, 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 referencia OSI, sem prejuízo do chaveamento do tráfego para o circuito MPLS, conforme já descrito;

8.1.40. Deverá implementar na própria solução todos os protocolos necessários para desempenhar o papel de SD-WAN e Gerenciamento, como por exemplo. WCCP, PBR, BGP, etc. 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;

8.1.41. Nas unidades remotas, 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. Atualmente, o Banco possui segmentação lógica para redes de videoconferência, por exemplo;

8.1.42. 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;

8.1.43. Implementar a criação de VLANs, permitindo:

8.1.43.1. Criar múltiplas VLANs, no mínimo 10;

8.1.43.2. Configurar a porta LAN da solução para suportar uma única VLAN (Porta de Acesso) ou múltiplas VLANs (Porta em Trunk);

8.1.43.3. Especificar uma subnet IP e associá-la à VLAN;

8.1.43.4. Configurar o appliance como o Gateway da VLAN;

8.1.43.5. Todas as VLANs deverão funcionar em contingência de gateway com o roteador MPLS conforme descrito em item anterior.

8.1.44. 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, bem como não possuem configurações de firewall. Diversas redes do Banco são "/16" e com endereçamentos válidos, porém não publicados para internet;

8.1.45. 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;

8.1.46. 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 remotas. Essa configuração deverá ser realizada de forma centralizada na solução de SDWAN;

8.1.47. 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, por exemplo, 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 SDWAN

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

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

8.1.50. 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;

8.1.51. 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:

8.1.51.1. Com base em um único ou vários IPs;

8.1.51.2. Com base em uma única ou várias Subnet;

8.1.51.3. Com base em uma ou várias portas TCP/UDP;

8.1.51.4. Com base no valor do DSCP;

8.1.51.5. Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN;

8.1.52. 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 remotas, ou seja, onde o tráfego não passe pelo Datacenter;

8.1.53. As informações de relatório de tráfego devem estar disponíveis por no mínimo 6 meses;

8.1.54. O tráfego deverá ser capturado, por exemplo, através de flows exportados diretamente dos equipamentos envolvidos nessa contratação, mas obrigatoriamente deve ser independente de roteadores ou qualquer outro equipamento externo a solução contratada;

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

8.1.56. 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. O(s) transceiver(s) SFP+ necessário(s) para conexão da interface do equipamento do ITEM 2 deverão ser fornecidos em conjunto com a solução. Não será necessário o fornecimento do transceiver para conexão com a rede do Banco;

8.1.57. Deverá ser possível verificar, via portal de relatório, por qual caminho (qual circuito de comunicação) cada aplicação está trafegando;

8.1.58. 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;

8.1.59. 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;

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

8.1.61. A solução deve ser composta com uma Console Central, 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;

8.1.62. No caso da instalação da solução de gerencialmente e orquestração instalada fora no Datacenter, deverá ser implementada duplo fator de autenticação (MFA) integrado a console em núvel do fabricante para acesso ao portal de gerenciamento. A indisponibilidade da interface de gerência não deverá comprometer o funcionamento do serviço/configurações de SD-WAN.

8.1.63. 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.

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

8.1.65. 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;

8.1.66. A solução deverá fornecer dados de 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);

8.1.67. Deverá possuir uma Solução de Firewall incorporado à solução de SD-WAN do mesmo fabricante para as unidades remotas, tanto para a solução instalada no Site Principal e no Site Secundário, como para as unidades remotas. A solução de firewall deverá possuir throughput compatível com o tráfego dimensionado para a solução de SD-WAN para realizar a visibilidade camada 7 do tráfego. A mesma visibilidade camada 7 deve ser provida para os equipamento da solução instalada no Site Principal e no Site Secundário;

8.1.68. O firewall nas unidades remotas 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 fornecidor de sdwan sendo no mínimo as aplicações microsoft office 365 (incluindo teams), windows update;

8.1.69. Para as unidades remotas, 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 remotas 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;

8.1.70. Deverá permitir regras globais para controles de segurança de camada L4 - L7 para as unidades remotas;

8.1.71. Deverá permitir regras de controle de segurança baseado em Protocolos (TCP e UDP) para as unidades remotas;

8.1.72. 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 remotas;

8.1.73. 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 abaixo:

8.1.73.1. Com base em um único ou vários IPs;

8.1.73.2. Com base em uma única ou várias Subnet;

8.1.73.3. Com base em uma ou várias portas TCP/UDP;

8.1.73.4. Com base no valor do DSCP;

8.1.73.5. Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN;

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

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

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

8.1.74.3. Deve suportar os algoritmos de criptografia AES-128, e AES-256;

8.1.74.4. Deve suportar os Algoritmos de Hash MD5, SHA1 e SHA256;

8.1.74.5. Deve suportar os Grupos de Diffie–Hellman Group1 (768 Bits) e Group 2 (1024 Bits);

8.1.75. Deverá possuir mecanismos de authentication, authorization and accounting (AAA) através de Servidor RADIUS e/ou TACACS+.

8.1.76. A solução SD-WAN deverá ser capaz de permitir integração segura entre unidades distribuída e plataforma SaS (Software as Service), como o Microsoft Office365, de forma a diminuir a latência na comunicação e aumentar o desempenho das aplicações.

9. REQUISITOS GERAIS DA SOLUÇÃO DE *SECURITY SERVICE EDGE* (SSE) (ITEM 2)

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

9.1.1. Filtro de URL;

9.1.1.1. Controle de Aplicação;

9.1.1.2. Proteção Contra Malwares Modernos;

9.1.1.3. Prevenção de Ameaças;

9.1.1.4. ZTNA (Zero Trust Network Access).

9.1.2. A solução deverá ser disponibilizada numa arquitetura em nuvem;

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

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

9.1.5. Neste edital, nos referiremos aos ambientes de nuvem e de data center da contratada de forma intercambiável;

9.1.6. A contratada assegurará que não haverá armazenamento de informações de qualquer espécie fora da rede do banco e assegurará também que não haverá processamento de informações em seu *data center* ou nuvem que se refiram:

9.1.6.1. Aos usuários e clientes do Banco;

9.1.6.2. Aos produtos, serviços e processos do Banco;

9.1.6.3. Aos relacionamentos do Banco com seus clientes, fornecedores, colaboradores, parceiros e outras entidades físicas ou jurídicas com as quais o Banco venha a se relacionar.

9.1.7. Os encargos financeiros referentes ao provimento, gerenciamento, configuração, segurança e manutenção dos referidos recursos de comunicação serão de inteira responsabilidade do CONTRATADO, incluindo o fornecimento de equipamentos, tais como: roteadores, modems e/ou switches;

9.1.8. A capacidade desses recursos deverá ser periodicamente revista, sendo redimensionados quando necessário e seus custos assumidos pelo CONTRATADO.

9.1.9. Em caso de utilização do data center do CONTRATADO para provimento de algum serviço, este deverá ser certificado como CPD TIER 3, cabendo comprovação por documentação emitida pelo *Uptime Institute Professional Services* ou equivalente;

9.1.10. O BANCO poderá solicitar os scripts de configuração dos equipamentos utilizados para a solução de conectividade para verificá-los conforme a política de segurança da Instituição, bem como acesso de leitura a estes equipamentos. Não havendo conformidade, o CONTRATADO deverá adequá-lo de acordo com as orientações do BANCO.

9.1.11. A solução deve possuir console única de gestão para toda a plataforma de segurança, incluindo:

9.1.11.1. Painel de Política;

9.1.11.2. Painel de Relatório;

9.1.11.3. Painel de Incidentes;

9.1.11.4. Painel de Configuração;

9.1.11.5. Painel Analítico.

9.1.12. O fabricante da solução deverá possuir ao menos 2 (dois) pops físicos no Brasil;

9.1.13. O processamento do tráfego, quanto as políticas de segurança definidas, deverá ser realizado em Datacenter localizado no Brasil;

9.1.14. A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-1 Type II / SSAE-16 Type II, SOC-2 Type I, Soc-2 TypeII, SOC-3, ISO 50001, ISO 14001, ISO 9001 e ISO 27001;

9.1.15. A plataforma deverá possuir peering direto aos sistemas autônomos de - no mínimo – os seguintes serviços e CDNs:

9.1.15.1. AWS;

9.1.15.2. Microsoft;

9.1.15.3. Google;

9.1.15.4. Akamai.

9.1.16. A solução deverá garantir SLA de latência para pelo menos as aplicações do Microsoft Office 365;

9.1.17. A solução deverá prover visibilidade e controle em tempo real para aplicações gerenciadas e não gerenciadas SaaS, não se restringindo a acessos realizados por meio do browser, mas também em aplicativos móveis e clientes instalados no desktop;

9.1.18. Ser compatível no mínimo com os sistemas operacionais e navegadores:

9.1.18.1. Windows (a partir da versão 10);

9.1.18.2. Linux (a partir da versão Red Hat 7);

9.1.18.3. Mac OS X (a partir da versão 10.6);

9.1.18.4. Mozilla Firefox (a partir da versão 45.4.0 ESR);

9.1.18.5. Google Chrome (a partir da versão 54);

9.1.18.6. Apple Safari (a partir da versão padrão do Mac OS X 10.6);

9.1.18.7. Microsoft Edge (a partir da versão padrão do Windows 10).

9.1.19. A interceptação do tráfego poderá ocorrer de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, dentre as formas:

9.1.19.1. Túnel Seguro (IPSEC e GRE);

9.1.19.2. Proxy Explícito (Browser e Arquivo PAC);

9.1.19.3. Integração com Plataformas SD-WAN;

9.1.19.4. Integração com NGFW/UTM (IPSEC e GRE);

9.1.19.5. Agente (Windows, Mac, iOS e Android);

9.1.19.6. Proxy Reverso;

9.1.19.7. Perfil Móvel;

9.1.19.8. Integração via API com Provedor de Serviço em Nuvem.

9.1.20. Os serviços de Segurança devem ser fornecidos de maneira transparente às redes remotas;

9.1.21. A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet. Esta funcionalidade deverá garantir que a mesma faixa de endereço não seja compartilhada entre vários clientes.

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

9.1.22.1. *Active Directory On-Premises*;

9.1.22.2. *Azure Active Directory*;

9.1.22.3. Federação (SSO) via SAML v2.0.

9.1.23. Suportar recurso de autenticação única para todo o ambiente de rede da CONTRATANTE, utilizando as plataformas de autenticação Active Directory e LDAP;

9.1.24. A solução deverá ser capaz de prover acesso às aplicações internas sem a necessidade de instalação de máquinas virtuais na rede de destino como ponte de acesso;

9.1.25. 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;

9.1.26. A solução deverá inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.1, TLS 1.2, TLS 1.3 e versões TLS posteriores lançadas;

9.1.27. Os tráfegos SSL/TLS devem ser inspecionados pelas mesmas políticas de filtragem aplicadas ao tráfego não criptografado;

9.1.28. A solução deverá suportar e estar devidamente licenciada para:

9.1.28.1. No mínimo a quantidade de usuários informada **Anexo IX – Modelo de Proposta** usuários autenticados com serviços ativos e identificados pela solução;

9.1.28.2. No mínimo a quantidade de Gbps da performance informada no **Anexo IX – Modelo de Proposta** para todos as funcionalidades ativas;

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

9.1.29. 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 de usuários licenciados;

9.1.30. A solução deverá suportar a interceptação ativa para qualquer tipo de aplicação TCP e UDP que seja cliente-servidor e redirecionar para o destino desejado pela CONTRATANTE;

9.1.31. Deverá permitir a configuração de portas diferentes da porta padrão utilizada pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites, possibilitando, no mínimo, a configuração de 50 portas;

9.1.32. 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;

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

9.1.34. Possuir a capacidade de atuar como Proxy explícito e transparente;

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

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

9.1.37. O fabricante da solução deverá disponibilizar, no mínimo, 365 dias de retenção de dados para análise e construção de relatórios;

Filtro de URLs

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

9.1.39. 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;

9.1.40. A solução deverá possuir:

9.1.40.1. Pelo menos 70 categorias distintas de URLs;

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

9.1.40.3. Categoria específica para classificar domínios recém registrados (com menos de 30 dias);

9.1.40.4. Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

9.1.41. A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas de filtro de conteúdo WEB:

9.1.41.1. Categoria de URL;

9.1.41.2. Usuários e Grupos do Active Directory;

9.1.41.3. Profile de prevenção de malwares;

9.1.41.4. Atividade realizada na URL/Aplicação;

9.1.41.5. IP de Origem;

9.1.41.6. IP de Destino;

9.1.41.7. País de origem e destino;

9.1.41.8. Ação: allow, block e alert;

9.1.41.9. Tipo de arquivo.

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

9.1.43. A solução deverá suportar:

9.1.43.1. A criação de categorias de URLs customizadas;

9.1.43.2. A exclusão de URLs do bloqueio, por categoria;

9.1.43.3. A customização de página de bloqueio;

9.1.43.4. Rastreamento de sites e análise em 40 idiomas;

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

9.1.43.6. 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.

9.1.44. A solução deverá permitir:

9.1.44.1. Um mecanismo para sobrescrever as categorias de URL;

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

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

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

9.1.46. A solução deverá possibilitar:

9.1.46.1. Categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

9.1.46.2. A inspeção de tráfego HTTPS (*Inbound/Outbound*), sendo que para a opção de Outbound não será necessário efetuar o "*man-in-the-middle*", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

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

9.1.46.4. O cadastro manual de usuários e grupos diretamente na interface de gerência remota;

9.1.46.5. Bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

9.1.46.6. 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);

9.1.46.7. Salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: *UserAgent, Referer*, e X-*Forwarded* For.

9.1.47. 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.

9.1.48. A solução deverá ser capaz de detectar e prevenir roubo de credenciais, controlando os sites onde o usuário pode enviar credenciais corporativas com base na classificação do endereço, em tempo real.

9.1.49. A solução deverá possuir a capacidade de detectar técnicas de phishing ou falsificação de imagens;

Controle de Aplicação

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

9.1.51. 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;

9.1.52. Pela solução deverá ser possível:

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

9.1.52.2. Adicionar controle de aplicações em todas as regras de segurança da solução, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

9.1.52.3. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do AD;

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

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

9.1.52.5.1. Nível de risco da aplicação;

9.1.52.5.2. Categoria de aplicações.

9.1.53. 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;

9.1.54. A solução deverá suportar:

9.1.54.1. Múltiplos métodos de identificação e classificação das aplicações, por pelo menos assinaturas, Decoders de protocolos e heurísticas;

9.1.54.2. A criação de aplicações customizadas pela interface gráfica, usando expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos HTTP, FTP, DNS, IRC, SMB, SMTP, Telnet, SSL, SSH, SQL e IMAP.

9.1.55. A solução deverá diferenciar:

9.1.55.1. Tráfegos *peer-to-peer (bittorrent, emule, neonet*, etc.), possuindo granularidade de controle para os mesmos;

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

9.1.55.3. Aplicações proxies (*ultrasurf, ghostsurf, freegate*, etc.) possuindo granularidade de controle para os mesmos.

9.1.56. 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;

9.1.57. Pela solução deverá ser possível:

9.1.57.1. Inspecionar o *payload* do pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

9.1.57.2. Realizar filtragens/inspeções dentro de portas TCP conhecidas, por exemplo porta 80 http, buscando por aplicações que potencialmente expõem o ambiente como: *peer-to-peer* ou mensageiros instantâneos;

9.1.57.3. Configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

9.1.57.4. Identificar o uso de táticas evasivas, ou seja, deverá ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como ataques utilizando comunicação TLS;

9.1.57.5. 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.

9.1.58. 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, FTP, E-mail e extensão de arquivos;

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

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

Proteção Contra Malwares Modernos

9.1.61. A solução deverá possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança através de assinaturas;

9.1.62. 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;

9.1.63. 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.

9.1.64. A solução deverá prevenir o uso de exploits avançados;

9.1.65. Na solução, a análise deverá prover:

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

9.1.65.2. Informações sobre as ações do Malware na máquina infectada;

9.1.65.3. Informações sobre as URLs não confiáveis utilizadas pelo novo Malware;

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

9.1.65.5. Detecção de aplicações não confiáveis, utilizadas pelo Malware;

9.1.65.6. Assinaturas de Antivírus e Antispyware de maneira automática.

9.1.66. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

9.1.67. A solução deverá possuir:

9.1.67.1. Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

9.1.67.2. Mecanismo de detecção antibot, que inclui pelo menos, reputação de endereço IP;

9.1.67.3. Funcionalidade de detecção e bloqueio de call-backs.

9.1.68. A solução deverá prevenir contra ameaças de dia zero:

9.1.68.1. Via tráfego de internet;

9.1.68.2. Que possam burlar o sistema operacional emulado;

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

9.1.69. A solução deverá ser capaz de implementar:

9.1.69.1. Modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

9.1.69.2. Detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 20MB;

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

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

9.1.69.5. Permissão ao usuário final o recebimento dos arquivos livres de malware, desde que aprovados e/ou autorizados via console de administração.

9.1.70. A solução deverá suportar ainda:

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

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

9.1.70.3. Submissão manual de arquivos para análise através do serviço de Sandbox.

9.1.71. A solução deve permitir a criação de Whitelist baseado no hash do arquivo;

Prevenção de Ameaças

9.1.72. 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);

9.1.73. 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;

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

9.1.74.1. Informações sobre vulnerabilidades e exploits já sofridos;

9.1.74.2. Certificações e normas que a aplicação está aderente. Ex: PCIDSS, SOC-1, SOC-2 e SOC-3;

9.1.74.3. Informações sobre privacidade de dados. Ex: ao armazenar dados na aplicação, o cliente continua sendo proprietário dos dados.

9.1.75. A solução deverá prover capacidade de controle contra vazamento de dados para data-in-rest e data-in-motion podendo ser classificados em estruturados e não estruturados em nuvens sancionadas (SaaS e IaaS) e nuvens não sancionadas (Exemplo: 4shared, Smallpdf, PDFConverter, OneDrive Personal, dentre outras);

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

9.1.77. A solução deverá suportar:

9.1.77.1. Várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

9.1.77.2. Referência cruzada com CVE.

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

9.1.78.1. Domínios de DNS dinâmicos;

9.1.78.2. Domínios identificados previamente como sendo distribuidores de Malwares;

9.1.78.3. Domínios identificados anteriormente em campanhas de Phishing;

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

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

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

9.1.81. 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;

9.1.82. 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;

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

ZTNA (*Zero Trust Network Access*)

9.1.84. 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;

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

9.1.86. A solução deverá:

9.1.86.1. Garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

9.1.86.2. Tornar disponível a aplicação a partir de configuração na console, sem a necessidade de convergência ou alteração de rotas locais para adequação ao serviço.

9.1.87. Ser possível configurar na console gráfica da solução quais aplicações internas serão acessadas através do Tenant da solução;

9.1.88. 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;

9.1.89. 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;

9.1.90. Ao se conectar remotamente na solução para acesso a uma aplicação interna da CONTRATANTE, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

9.1.91. 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:

9.1.91.1. Presença de criptografia de disco PGP e/ou BitLocker;

9.1.91.2. Presença de processo(s) em execução;

9.1.91.3. Presença de arquivos em disco;

9.1.91.4. Participação em domínio do AD;

9.1.91.5. Existência de Certificado Digital no dispositivo;

9.1.91.6. Que somente as máquinas que estejam com solução antimalware ativa e com base de vacinas atualizada, possam acessar os serviços internos.

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

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

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

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

9.1.93.1. Usuário do AD;

9.1.93.2. Grupo do AD;

9.1.93.3. Aplicação Privada;

9.1.93.4. Ação: Permitir e/ou Bloquear.

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

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

9.1.94.2. Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real.

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

9.1.95.1. Regra de segurança que foi aplicada no tráfego;

9.1.95.2. Ação tomada pela solução;

9.1.95.3. Usuário;

9.1.95.4. Endereço IP;

9.1.95.5. País de origem;

9.1.95.6. Porta de origem;

9.1.95.7. Sistema operacional;

9.1.95.8. Aplicação de destino;

9.1.95.9. Porta de destino;

9.1.95.10. Protocolo;

9.1.95.11. Bytes tráfegados na sessão;

9.1.95.12. Hora de início e término da sessão.

Relatórios

9.1.96. Ser capaz de visualizar, de forma direta na solução e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

9.1.97. Ser capaz de visualizar, de forma direta na solução e em tempo real, o throughput de dados utilizado pela rede de computadores conectados ao serviço em nuvem;

9.1.98. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar tentativas de exploração de vulnerabilidades, tentativas de intrusão e outras ameaças. Deve permitir o download do relatório em formato PDF;

9.1.99. Ser capaz de visualizar, de forma direta na solução e em tempo real, a largura de banda utilizada por política e por protocolo TCP/UDP/IPV4 e IPV6;

9.1.100. Ser capaz de visualizar, de forma direta na solução e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

9.1.101. 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);

Gerenciamento

9.1.102. Deve ter administração centralizada por console único de gerenciamento;

9.1.103. As configurações de todas as funcionalidades da solução deverão ser realizadas através da mesma console;

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

9.1.105. 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.

9.1.106. A solução deverá ter a capacidade de utilizar contas de usuários do AD para autenticação na console de gerenciamento;

9.1.107. A solução deve suportar duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução.

10. INTEGRAÇÃO DO TRÁFEGO DE DADOS, VOZ E IMAGENS (SD-WAN e acessos MPLS) (exceto Parceiros)

10.1. Definição de classes de tráfego

10.1.1. 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, Site Secundário e o CAPGV, de modo a atender os requisitos apresentados.

10.2. Classificação do tráfego

10.2.1. 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 do ITEM 2 (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.

10.2.2. O CONTRATADO do ITEM 1, de acessos MPLS, deverá garantir que os pacotes marcados pela solução SD-WAN, vindos do Banco, serão garantidos dentro dos seus backbones de acordo com os percentuais e classes estabelecidos nos itens 4.7 e 4.8, sem que haja qualquer remarcação, incluindo para o tráfego entre unidades distribuídas diferentes, ou seja, dentro do perfil de tráfego full mesh.

10.3. **Capacidade de transmissão para tráfego de voz**

10.3.1. Os serviços prestados pelo CONTRATADO do ITEM 1 para fornecimento MPLS deverão implementar os recursos necessários, incluindo controle do retardo máximo, controle da variação do retardo, quebra do tamanho de pacotes, compressão de cabeçalho RTP, mecanismos de fragmentação e interleaving (LFI), dentre outras funcionalidades, de modo a garantir o perfeito funcionamento das chamadas de voz entre as centrais telefônicas.

10.4. **Tráfego de imagens**

10.4.1. 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.

10.5. **Capacidade de transmissão para tráfego de videoconferência**

10.5.1. Os serviços prestados pelo CONTRATADO do ITEM 1 deverão implementar os recursos necessários, incluindo controle do retardo máximo, controle da variação do retardo, quebra do tamanho de pacotes, dentre outras funcionalidades, de modo a garantir o perfeito funcionamento das chamadas entre os sistemas de videoconferência atualmente em uso pelo Banco. De acordo com especificações do fabricante dos sistemas de videoconferência, cada chamada de videoconferência poderá requerer pelo menos 512Kbps de capacidade de transmissão para seu efetivo funcionamento, incluso o overhead do protocolo IP.

10.5.2. **Unidades envolvidas**

10.5.2.1. 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 CONTRATADO a qualquer momento, sem ônus para o Banco.

10.6. **Tráfego de dados**

10.6.1. 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, como por exemplo, no nível AF2, será permitida a marcação AF21, AF22 e AF23. Os dados classificados como de alta prioridade deverão 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.

10.7. **Interoperabilidade entre as operadoras**

10.7.1. O CONTRATADO do ITEM 1 deverá garantir a interoperabilidade entre o tráfego de agências distintas de forma transparente ao Banco, utilizando a infraestrutura de roteadores e comutadores instalados por cada operadora no Site Primário e Site Secundário como meio de interconexão física entre suas redes MPLS. Tal interoperabilidade deverá ser assegurada através de configuração nos equipamentos da operadora, que funcionarão como gateways, atendendo a seguinte definição das classes de serviço em seus backbones:

Mapeamento das Classes de Serviços		
Tráfego de Voz		Classe EF
Tráfego de Imagem		Classe AF4
Tráfego de Dados	Alta	Classe AF3
	Média	Classe AF2
	Baixa	Classe AF1

10.7.2. De acordo com as prioridades do tráfego definidas pelo Banco, os critérios acima deverão ser obedecidos pelas operadoras, seguindo os padrões descritos nas RFCs 2474 e 2475 – DiffServ, complementados pela RFC 2597 – Assured Forwarding Per-hop Behaviors (AF PHB) e pela RFC 2598 – Expedited Forwarding (EF).

10.7.3. Os serviços prestados pela operadora deverão permitir a criação de VPN (Virtual Private Network) através de MPLS (Multiprotocol Label Switiching), construída de acordo com a RFC 2547 e a RFC 3031. Também deverá ser garantida a configuração de QoS (Quality of Service) sobre MPLS/VPN, de acordo com a RFC 3270 e a RFC 2983.

10.7.4. O tráfego de voz deverá ser mapeado para a classe EF e o tráfego de imagem deverá ser mapeado para a classe AF4. O tráfego de dados de alta prioridade, média prioridade e baixa prioridade deverão ser mapeados respectivamente para as classes AF3, AF2 e AF1.

10.7.5. A soma da porcentagem de reserva de cada circuito de dados será informada pelo Banco durante implementação e poderá sofrer alteração durante todo o Contrato, de acordo com solicitação do Banco. A soma da porcentagem de todas as classes não passará de 96%, ficando livre para a operada até 4% do acesso para utilização de tráfego de gerência que será especificado, configurado e mantido pela própria operadora.

10.8. **Alocação de Largura de Banda**

10.8.1. 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%

10.8.2. 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.

10.8.3. 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.

10.8.4. No caso da 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, por exemplo, poderá ser remarcado como AF13, a ser definido pelo Banco durante implantação.

10.8.5. As informações referentes aos serviços (IP/porta/procolo), 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 do ITEM 2, 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.

10.8.6. O CONTRATADO do ITEM 1 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.

10.8.7. Além da operadora ter de manter e priorizar a marcação recebida pela conexão de rede LAN, normalmente com origem do equipamento do ITEM 2 de SD-WAN, a operadora de MPLS em cada unidade distribuída terá uma lista básica de marcação com base em IP, protocolo e Porta para classificar/marcar. Essa lista poderá igualmente sofrer alterações durante o Contrato. Uma vez que mesmo na indisponibilidade da solução SD-WAN, o tráfego continuará sendo mantido pelo circuito MPLS remanescente, devendo este, pois, utilizar a marcação de QoS contida na lista.

10.8.8. 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 ou por tipo de link MPLS e deverá respeitar o SLA de configuração.

10.9. **Tráfego de gerência para a solução SD-WAN**

10.9.1. O tráfego gerado entre a solução de gerenciamento no Site Primário e Site Secundário, pertencente ao ITEM 2 (definido no Anexo V - Requisitos de Gerenciamento dos Serviços), e os equipamentos que serão monitorados deverá ser classificado como pertencente ao tráfego de dados de média prioridade.

10.10. **Topologia da solução**

10.10.1. Deverá ser fornecido desenho esquemático ilustrando todos os aspectos dos requisitos de conectividade, tanto para as unidades distribuídas, 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, tanto para os circuitos primários quanto para os secundários.

10.10.2. 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.

10.10.3. 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, o CONTRATADO procederá a reconfiguração e ativação da nova largura de banda, incluindo os respectivos custos envolvidos nas faturas mensais.

11. REQUISITOS DE SEGURANÇA

11.1.1. Caberá ao Banco estabelecer as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados, equipamentos roteadores e appliances de SD-WAN 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:

11.1.1.1. O CONTRATADO para prover qualquer circuito MPLS deverá prover uma rede IP logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da Internet. O mecanismo para implementar o isolamento e a qualidade de serviços é o MPLS/VPN. Essa garantia deverá ser implementada “fim-a-fim”;

11.1.1.2. 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;

11.1.1.3. 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;

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

11.1.1.5. Para os circuitos de comunicação MPLS, e conforme já especificado nesse anexo, deverá ser fornecido usuário local para acesso via SSH com permissão somente de leitura visando a verificação de configurações e acompanhamento de resolução de incidente. Todas as configurações dos equipamentos deverão ser visíveis por esse usuário fornecido durante todo o Contrato. Para os links de Internet Determinística e internet assimétrica o acesso poderá ser SSH ou HTTPS, ou ambos se for implementando pelo roteador.

12. GLOSSÁRIO

Unidades Distribuídas: agências, centrais operacionais (CENOPs), unidades de recuperação de crédito, superintendências, postos bancários 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;

CAPGV: Centro Administrativo Presidente Getúlio Vargas. Sede principal do Banco, onde reside sua administração superior e os principais recursos e serviços centralizados de infraestrutura de tecnologia da informação;

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

Circuito de acesso primário: conjunto de trechos contínuos de meios de comunicação que interliga uma unidade distribuída ou Parceiro ou CAPGV a um ponto de presença do fornecedor dos serviços. Usado para tráfego integrado de dados, voz e imagens;

Circuito de acesso secundário: conjunto de trechos contínuos de meios de comunicação, completamente independentes daqueles utilizados pelos circuitos de acesso primários, isto é, sem que haja compartilhamento de qualquer tipo de recurso, exceto em casos onde for fisicamente impossível, o qual interliga uma unidade distribuída, Parceiro, Site Secundário ou o CAPGV a um ponto de presença do fornecedor dos serviços. Usado para balanceamento do tráfego integrado de dados, voz e imagens com o circuito de acesso primário, ou em caso de falha do circuito de acesso primário;

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 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 SDWAN e SSE.

NOC: Centro de Operação de Rede responsável pelo gerenciamento, implementação, correção e controle de toda a solução SASE e links de parceiros, unidades distribuídas e postos de crédito, incluindo ajustes de engenharia de tráfego, aplicações de QoS e gerenciamento de SLA dos circuitos de acesso aqui contratados.

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