**ANEXO II – REQUISITOS TÉCNICOS DA SOLUÇÃO**
**PROCESSO ADMINISTRATIVO Nº 142/2023**

O seguinte caderno de especificações técnicas define os requisitos técnicos mínimos da Solução que deverão ser observados pela Contratada para atendimento das necessidades do Coren-SP relacionadas à contratação de serviços de **Solução Integrada de Segurança de Rede, Autenticação e Conectividade.**

Os requisitos técnicos se encontram divididos em seções, organizadas em títulos tecnicamente classificados, correspondendo aos itens de serviço do grupo único que formam a Solução como um todo.

## 1. DO GERENCIAMENTO CENTRALIZADO DA SOLUÇÃO E RELATORIA/CENTRALIZAÇÃO DE LOGS

### 1.1. DO GERENCIAMENTO CENTRALIZADO

**1.1.1.** O equipamento destinado ao gerenciamento centralizado deverá ser um virtual appliance hospedado em ambiente da CONTRATADA, disponibilizado na modalidade de nuvem ou em ambiente da contratante em virtualização HYPERVISOR, desde que seja do mesmo fabricante dos equipamentos de SD-WAN e NGFW para fins de interoperabilidade.

**1.1.2.** Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

**1.1.2.1.** Possuir compatibilidade com o Microsoft Hyper-V 2022 e superior;

**1.1.2.2.** Não deverá limitar o número de múltiplas vCPUs;

**1.1.2.3.** Não deverá definir limites para a expansão da memória RAM;

**1.1.2.4.** Deverá gerenciar, no mínimo, 30 (trinta) unidades (NGFW ou Sistemas Virtuais) dos equipamentos SD-WAN/NGFW de forma simultânea;

**1.1.2.5.** Como parte da visibilidade dos dispositivos gerenciados centralmente, a Solução deverá ter visibilidade do status do link, desempenho do aplicativo, utilização da largura de banda e conformidade com o SLA objetivo;

**1.1.2.6.** Possuir a capacidade de automatizar fluxos de trabalho e configurações para dispositivos gerenciados em uma única console;

**1.1.2.7.** Possuir recurso de Multi-tenancy para separar os dados de gerenciamento da infraestrutura lógica ou geograficamente e permitir a implantação do zero touch para o rápido provisionamento em massa;

**1.1.2.8.** Executar backups de configuração automáticos em até 5 (cinco) nós, contendo atualizações de todos os dispositivos gerenciados;

**1.1.2.9.** Possuir a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console e exibir sua localização geográfica em um mapa;

**1.1.2.10.** Permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança.

**1.1.3.** A ferramenta de Gerenciamento da Solução deverá:

**1.1.3.1.** Suportar acesso via SSH, cliente, WEB (HTTPS), SNMP V2 e API aberta;

**1.1.3.2.** Permitir acesso concorrente de administradores;

**1.1.3.3.** Possuir interface baseada em linha de comando para administração da solução de gerência;

**1.1.3.4.** Possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

**1.1.3.5.** Possuir funcionalidade de bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

**1.1.3.6.** Possibilitar a definição de perfis de acesso à console com permissões granulares, tais como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

**1.1.3.7.** Gerar alertas automáticos via E-mail;

**1.1.3.8.** Gerar alertas automáticos via SNMP;

**1.1.3.9.** Gerar alertas automáticos via Syslog;

**1.1.3.10.** Suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora incluindo recorrência no agendamento;

**1.1.3.11.** Permitir ao Administrador transferir os backups para um servidor SCP;

**1.1.3.12.** Permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

**1.1.3.13.** Permitir aos administradores se autenticarem nos servidores de gerência através de bases externas TACACS, LDAP e RADIUS;

**1.1.3.14.** Permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

**1.1.3.15.** Suportar sincronização do relógio interno via protocolo NTP;

**1.1.3.16.** Registrar as ações efetuadas por quaisquer usuários;

**1.1.3.17.** Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

**1.1.3.18.** Permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

**1.1.3.19.** Permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

**1.1.3.20.** Permitir criar administradores que tenham acesso à todas as instancias de virtualização;

**1.1.3.21.** Garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

**1.1.3.22.** Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema de prevenção a intrusão (IPS – Intrusion Prevention System), antivírus, filtro de URL;

**1.1.3.23.** Permitir usar palavras chaves ou cores para facilitar identificação de regras;

**1.1.3.24.** Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

**1.1.3.25.** Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

**1.1.3.26.** Permitir a criação de regras que fiquem ativas em horário definido;

**1.1.3.27.** Permitir a criação de regras com data de expiração;

**1.1.3.28.** Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (ou, alternativamente, garantir que esta exigência seja plenamente atendida por meio diverso);

**1.1.3.29.** Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

**1.1.3.30.** Possuir um sistema de backup/restauração de todas as configurações da solução de gerência, assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

**1.1.3.31.** Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;

**1.1.3.32.** Permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

**1.2.** DA RELATORIA E CENTRALIZAÇÃO DE LOGS

**1.2.1.** O equipamento deve ser um virtual appliance hospedado em ambiente da CONTRATADA, disponibilizado na modalidade de nuvem, ou implantando dentro do ambiente da contratante em virtualização HYPERVISOR, desde que, seja do mesmo fabricante da solução de SD-WAN e NGFW para fins de interoperabilidade.

**1.2.2.** Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

**1.2.2.1.** Possuir compatibilidade com o Microsoft Hyper-v 2022 e superior;

**1.2.2.2.** Gerenciar, no mínimo, 30 (trinta) unidades (NGFW ou Sistemas Virtuais) dos equipamentos da solução de NGFW de forma simultânea;

**1.2.2.3.** Suportar a coleta de até 5GB de logs por dia;

**1.2.2.4.** Suportar armazenamento de até 30 dias de regras habilitadas de segurança (UTM) ou de acordo com o ambiente de storage da Contratante;

**1.2.2.5.** Não deverá limitar o número de múltiplas vCPUs;

**1.2.2.6.** Não deverá haver limites para a expansão da memória RAM;

**1.2.2.7.** O licenciamento do produto com todas as funcionalidades relatadas deve ser válido durante todo o período do fornecimento do serviço;

**1.2.2.8.** Suportar o acesso via SSH, WEB (HTTPS) e SNMP V2 para gerenciamento da Solução;

**1.2.2.9.** Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando na console de gerenciamento;

**1.2.2.10.** Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

**1.2.2.11.** Possuir suporte para SNMP versão 2 e 3 com disponibilidade de MIB;

**1.2.2.12.** Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

**1.2.2.13.** Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

**1.2.2.14.** Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH;

**1.2.2.15.** Suportar a autenticação de usuários de acesso à plataforma via: LDAP, Radius e TACACS+;

**1.2.2.16.** Garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;

**1.2.2.17.** Possuir mecanismo para que logs antigos sejam removidos automaticamente, após estarem consolidados na solução de guarda e análise de logs e relatoria;

**1.2.2.18.** Permitir a extração de relatórios;

**1.2.2.19.** Garantir a exportação dos logs;

**1.2.2.20.** Possuir relatórios pré-definidos;

**1.2.2.21.** Permitir a geração de relatórios de logs de tráfego de dados;

**1.2.2.22.** Possuir a capacidade de personalização de gráficos como barra, linha, tabela e pizza, para inserção aos relatórios;

**1.2.2.23.** Possuir mecanismo para exibir de forma detalhada informações complementares nos relatórios em tempo real;

**1.2.2.24.** Possibilitar o download dos arquivos de logs recebidos;

**1.2.2.25.** Possibilitar o envio de maneira automática de relatórios por e-mail;

**1.2.2.26.** Permitir a customização de quaisquer relatórios fornecidos pela Solução, exclusivamente a critério da Contratante, adaptando-o às suas necessidades;

**1.2.2.27.** Possuir a capacidade de definir filtros nos relatórios;

**1.2.2.28.** Ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;

**1.2.2.29.** Garantir a capacidade de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;

**1.2.2.30.** Dispor de relatórios contemplando informações do ambiente, dos eventos de segurança e incidentes, das ameaças, do uso da navegação web, de IPS, da utilização da rede, entre outros;

**1.2.2.31.** Disponibilizar uma avaliação consolidada das ameaças cibernéticas;

**1.2.2.32.** Dispor de painel gráfico para análise das ameaças detectadas englobando controle de aplicação, IPS, filtro web e antivírus, demonstrando ainda os principais destinos, principais ameaças, principais incidentes de vírus, entre outros.

**2. DA SOLUÇÃO DE FIREWALL (UTM/NGFW)**

**2.1.** DOS REQUISITOS GERAIS

**2.1.1.** A Solução deverá consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD- WAN, não sendo permitido appliances virtuais ou solução open source (produto montado). Ademais, não serão aceitas soluções baseadas em PCs de uso geral e sim soluções baseadas em appliances desenvolvidos especificamente para a função de firewall.

**2.1.1.1.** Por funcionalidades de NGFW se entendam o reconhecimento de aplicações, a prevenção de ameaças, a identificação de usuários e o controle granular de permissões;

**2.1.1.2.** Por funcionalidades de SD-WAN se entendam o roteamento inteligente, o uso do melhor link por aplicação, a abstração do tráfego em relação aos circuitos físicos e o controle do tráfego por aplicação.

**2.1.2.** A Solução de comunicação de dados entre as unidades utilizará equipamentos com a tecnologia SD-WAN, **todos da mesma marca e compatíveis entre si, de forma a garantir a compatibilidade e interoperabilidade da Solução**;

**2.1.3.** A Gestão do Firewall, naquilo que se refere à aplicação de regras, bloqueios, políticas, entre outras funcionalidades, deverão ser de forma híbrida entre a Contratada e Contratante;

**2.1.4.** A Contratada deverá fornecer acesso aos equipamentos (senhas de acesso), para a contratante para fazer a gestão híbrida dos equipamentos;

**2.1.5.** Considerando a criticidade e o período previsto de contratação, os componentes da Solução deverão ser novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios necessários às suas instalações;

**2.1.6.** Todos os roteadores e equipamentos necessários para a conexão entre os pontos deverão ser fornecidos, instalados, configurados, mantidos, gerenciados e operados pela Contratada;

**2.1.7.** Em caso de atualização de sistema que acrescentem novas funcionalidades aos equipamentos elas devem funcionar sem a necessidade de aquisição de nova licença;

**2.1.8.** Caso o fabricante remova o produto de linha, o mesmo deve substituir o produto entregue pela nova geração com capacidade e funcionalidades igual ou superior ao removido da linha de produção;

**2.1.9.** Os equipamentos deverão possuir garantia do fabricante de hardware e software durante a vigência do contrato;

**2.1.10.** Os equipamentos deverão possuir licenciamento perpetuado para as funcionalidades;

**2.1.11.** Deve possuir licenciamento durante a vigência do contrato para as subscrições de filtro de conteúdo, Antivírus, Controle de aplicação, IPS e outras que façam parte do produto e da oferta.

**2.1.12.** As funcionalidades de segurança e SD-WAN que compõem a Solução poderão funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos especificados neste caderno

e acompanhem os mesmos termos de garantia, atualizações e manutenção, suporte e gerenciamento centralizado;

**2.1.13.** A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7;

**2.1.14.** Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 2U cada;

**2.1.15.** Deverão ser disponibilizados cabos de alimentação e, caso necessários, kits do tipo trilho para adaptação;

**2.1.16.** O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

**2.1.17.** Os equipamentos disponibilizados deverão possuir suporte a 256 VLAN Tags 802.1Q;

**2.1.18.** Os equipamentos disponibilizados deverão possuir suporte a agregação de links 802.3ad LACP.

**2.2.** DOS REQUISITOS DOS DISPOSITIVOS DE PROTEÇÃO DE REDE

**2.2.1.** Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

**2.2.1.1.** Possuir suporte a VLANs;

**2.2.1.2.** Possuir suporte a roteamento multicast (PIM-SM);

**2.2.1.3.** Suportar BGPv4/BGP4+, OSPFv2/v3, RIP e roteamento estático;

**2.2.1.4.** Possuir suporte a DHCP Relay;

**2.2.1.5.** Possuir suporte a DHCP Server;

**2.2.1.6.** Suportar sub-interfaces ethernet lógicas;

**2.2.1.7.** Suportar NAT dinâmico (Many-to-Many);

**2.2.1.8.** Suportar NAT estático (1-to-1);

**2.2.1.9.** Suportar NAT estático bidirecional 1-to-1;

**2.2.1.10.** Suportar Tradução de porta (PAT);

**2.2.1.11.** Suportar NAT de Origem;

**2.2.1.12.** Suportar NAT de Destino;

**2.2.1.13.** Suportar NAT de Origem e NAT de Destino simultaneamente;

**2.2.1.14.** Implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

**2.2.1.15.** Suportar NAT46, NAT64;

**2.2.1.16.** Implementar o protocolo ECMP;

**2.2.1.17.** Permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

**2.2.1.18.** Enviar log para sistemas de monitoração externos;

**2.2.1.19.** Possuir a funcionalidade de enviar logs para os sistemas de monitoração externos via protocolo SSL;

**2.2.1.20.** Deverá possuir proteção anti-spoofing;

**2.2.1.21.** Deverá suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

**2.2.1.22.** Deverá suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

**2.2.1.23.** Deverá suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.

**2.2.1.24.** Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

**2.3.** DA CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DOS DISPOSITIVOS

**2.3.1.** A configuração em alta disponibilidade dos dispositivos ofertados na Solução deverá sincronizar:

**2.3.1.1.** Sessões;

**2.3.1.2.** Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;

**2.3.1.3.** Associações de Segurança das VPNs;

**2.3.1.4.** Tabelas FIB;

**2.3.2.** A Configuração em alta disponibilidade da Solução contratada deverá possibilitar, ainda:

**2.3.2.1.** Possibilitar monitoração de falha de link no modo de alta disponibilidade (HA);

**2.3.2.2.** Possuir suporte a criação de sistemas virtuais no mesmo appliance;

**2.3.2.3.** Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

**2.3.2.4.** Controlar, inspecionar e realizar descriptografia de SSL para tráfego de Saída (Outbound);

**2.4.** DAS FUNCIONALIDADES DE IPS:

**2.4.1.** Os seguintes requisitos relacionados às funcionalidades de IPs deverão ser atendidos pela Solução ofertada:

**2.4.1.1.** Permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

**2.4.1.2.** Possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

**2.4.1.3.** Possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

**2.4.1.4.** Possuir capacidade de remontagem de pacotes para identificação de ataques;

**2.4.1.5.** Utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas;

**2.4.1.6.** Realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego.

**2.4.1.7.** Possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego;

**2.4.1.8.** Possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

**2.4.1.9.** Possuir assinaturas para bloqueio de ataques de buffer overflow;

**2.4.1.10.** Implementar, pelo menos, os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo;

**2.4.1.11.** Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento;

**2.4.1.12.** Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos;

**2.4.1.13.** Possibilitar a criação de políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos;

**2.4.1.14.** Possibilitar a criação de políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, entre outros;

**2.4.1.15.** Possibilitar escanear e bloquear conexões a servidores de botnet;

**2.4.1.16.** Dispor de opção para bloquear URLs maliciosas mediante base de dados local;

**2.4.1.17.** Possibilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS;

**2.4.1.18.** Suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS;

**2.4.1.19.** Suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros;

**2.4.1.20.** Possibilitar o filtro de assinaturas com base no identificador CVE;

**2.4.1.21.** Possibilitar a criação de uma assinatura de IPS utilizando o identificador CVE, bem como um “wildcard” do CVE para abranger mais de um identificador. As assinaturas deverão dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;

**2.4.1.22.** Incluir proteção contra ataques de negação de serviços;

**2.4.1.23.** Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

**2.5.** DAS FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

**2.5.1.** Os seguintes requisitos relacionados às funcionalidades de proteção contra ameaças avançadas deverão ser atendidos pela Solução ofertada:

**2.5.1.1.** Possuir funções de antivírus e anti-spyware;

**2.5.1.2.** Possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;

**2.5.1.3.** Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros);

**2.5.1.4.** Dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas;

**2.5.1.5.** Permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;

**2.5.1.6.** Permitir o bloqueio de download de arquivos por tamanho;

**2.5.1.7.** Realizar a mitigação de ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

**2.5.1.8.** Dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros.

**2.5.2.** Dentre as análises efetuadas, a Solução deverá suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back.

**2.5.2.1.** A solução de sandbox deverá ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque;

**2.5.2.2.** A solução de sandbox deverá ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente;

**2.5.3.** A Solução deverá analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deverá, ainda, disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento.

**2.6.** DAS FUNCIONALIDADES DE FILTROS WEB E DE CONTEÚDO

**2.6.1.** Os seguintes requisitos relacionados às funcionalidades de filtro WEB e de conteúdo deverão ser atendidos pela Solução ofertada:

**2.6.1.1.** Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

**2.6.1.2.** Possibilitar a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

**2.6.1.3.** Possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

**2.6.1.4.** Permitir SSO por meio da identificação pela base do Active Directory, de forma que os usuários não precisem 'logar' novamente na rede para navegar pelo firewall;

**2.6.1.5.** Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

**2.6.1.6.** Possuir a função de exclusão de URLs do bloqueio;

**2.6.1.7.** Permitir a customização de página de bloqueio;

**2.6.1.8.** Dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário;

**2.6.1.9.** Possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego;

**2.6.1.10.** Possuir funcionalidade que permita o bloqueio de tráfego HTTP POST (método utilizado para envio de informação a um determinado website);

**2.6.1.11.** Fltrar e remover Java Applets, ActiveX e cookies do tráfego web inspecionado;

**2.6.2.** Possuir, em sua base de dados, uma lista de bloqueio contendo URLs de certificados maliciosos;

**2.6.3.** Filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo;

**2.6.4.** Permitir, além do Web Proxy explícito, suporte ao proxy Web transparente.

**2.7.** DO FIREWALL TIPO 1 - EQUIPAMENTO UTM/NGFW:

**2.7.1.** Deverão ser disponibilizados 2 (dois) equipamentos principais, destinados à unidade Sede do Coren-SP, com instalação definida para cada segmento de rede (front-end e back-end).

**2.7.2.** Desempenho mínimo dos equipamentos (throughput mínimo) conforme Datasheet do fabricante:

**2.7.2.1.** UTM/NGFW (Full com todas as funcionalidades de segurança): 3.5Gbps;

**2.7.2.2.** IPS: 5Gbps;

**2.7.2.3.** VPN SSL: 2 Gbps;

**2.7.3.** Quantidade Mínima de Interfaces (fora as interfaces que eventualmente sejam necessárias para o funcionamento das conexões SD-WAN com as Subseções/NAPEs):

**2.7.3.1.** Oito (8) interfaces de 1gb (RJ45);

**2.7.3.2.** Quatro (4) interfaces de 10gb (fibra SFP(+) ou Oito (8) interfaces de 1gb (fibra SFP(+));

**2.7.3.3.** As interfaces tratadas nos subitens acima devem ser entregues junto com os equipamentos e estarem prontas para uso na entrega do objeto, incluindo eventuais licenciamentos adicionais que sejam necessários para isso.

**2.7.4.** Máximo de usuários simultâneos autenticados no firewall: Sem limite de licença ou de software;

**2.7.5.** Máximos de sessões simultâneas no firewall: mínimo de 3 (três) milhões;

**2.7.6.** Os equipamentos disponibilizados deverão incluir licenças para SSL VPN (ou VPN especifica do fabricante através de cliente próprio) para, pelo menos, 500 (quinhentos) usuários simultâneos no firewall externo (onde as conexões VPN serão feitas);

**2.7.7.** A VPN client-to-site deverá possuir, pelo menos, uma possibilidade de configuração rápida e utilização intuitiva por parte dos usuários como um cliente próprio de VPN ou cliente do fabricante, que agregue outras funções de segurança dessa contratação, como o Zero Trust por exemplo;

**2.7.8.** Os equipamentos ofertados deverão dispor de suporte completo ao SD-WAN ofertado e integração com os demais firewalls ofertados na Solução contratada pelo Coren-SP;

**2.7.9.** Ademais, os seguintes requisitos técnicos relacionados às funcionalidades dos dispositivos de proteção do tipo 1 deverão ser atendidos pela Solução ofertada:

**2.7.9.1.** Possibilitar a definição de quais máquinas, tipos, SOs, poderão acessar a VPN SSL, seja utilizando funcionalidade da VPN ou do Zero Trust;

**2.7.9.2.** Possibilitar a conferência de se a máquina é do Coren-SP ou não. Para isso poderá utilizar diversas técnicas presentes no mercado, como utilização de certificação digital nas máquinas autorizadas, ou outros;

**2.7.9.3.** Possibilitar o bloqueio temporário de IPs nas hipóteses de 'match' em determinada regra de negação, na tentativa de acesso a portas em blacklist e nas ações de portscan, IPscan, DoS ou DDoS;

**2.7.9.4.** Possuir funcionalidades de reconhecimento de aplicações, de prevenção de ameaças e de identificação de usuários;

**2.7.9.5.** Possuir otimização para a análise de conteúdo de aplicações;

**2.7.9.6.** Possuir suporte a Policy based routing ou policy based forwarding;

**2.7.9.7.** Suportar sub-interfaces ethernet logicas;

**2.7.9.8.** Suportar SD-WAN de forma nativa;

**2.7.9.9.** Permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

**2.7.9.10.** Enviar log para sistemas de monitoração externos, simultaneamente;

**2.7.9.11.** Possuir suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

**2.7.9.12.** Dispor de funcionalidade de Inspeção SSL sem limitação de licenciamento caso a solução ofertada possua licenciamento, deve ser fornecido em sua capacidade máxima;

**2.7.9.13.** Permitir a integração com repositório de logs de forma segura e otimizada;

**2.7.9.14.** Suportar, na console de administração, ao menos, o idioma inglês;

**2.7.9.15.** Realizar controles de políticas por porta e protocolo;

**2.7.9.16.** Realizar controles de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

**2.7.9.17.** Realizar controle de políticas por usuários do AD, grupos de usuários do AD, IPs, redes e zonas de segurança;

**2.7.9.18.** Suportar a inspeção UTM/NGFW (Application Control e Webfiltering, no mínimo) diretamente às políticas de segurança;

**2.7.9.19.** Suportar o padrão de indústria 'syslog' protocol para armazenamento;

**2.7.9.20.** Suportar integração com Solução de SIEM multi fabricante;

**2.7.9.21.** Suportar a integração nativa com soluções de sandboxing;

**2.7.9.22.** Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

**2.7.9.23.** Reconhecer e permitir configurações de ações de permissão ou bloqueio de pelo menos 100 aplicações diferentes, em camada 7, 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, VPN, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

**2.7.9.24.** Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como utilização da rede Tor;

**2.7.9.25.** De-criptografar pacotes, para tráfego criptografado SSL, a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

**2.7.9.26.** Atualizar a base de assinaturas de aplicações automaticamente;

**2.7.9.27.** Permitir, o fabricante, a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

**2.7.9.28.** Possibilitar a diferenciação de tráfegos de Instant Messaging (Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

**2.7.9.29.** Possibilitar a diferenciação de aplicações Proxies (Psiphon, Freegate etc.) possuindo granularidade de controle/políticas para os mesmos;

**2.7.9.30.** Possibilitar a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

**2.7.9.31.** Possibilitar a criação de grupos estáticos de aplicações baseados em características das aplicações como categoria da aplicação;

**2.7.9.32.** Possuir, para proteção do ambiente contra ataques módulo de IPS, Antivírus e Anti-Spam integrados no próprio appliance de firewall;

**2.7.9.33.** Possuir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus);

**2.7.9.34.** Possibilitar bloqueios por reputação da origem;

**2.7.9.35.** Garantir a operação das funcionalidades de IPS e Antivírus em caráter permanente, podendo ser utilizadas por tempo indeterminado dentro do período do contrato e respectivas licenças;

**2.7.9.36.** Sincronizar as assinaturas de IPS e Antivírus quando implementado em alta disponibilidade;

**2.7.9.37.** Permitir o bloqueio de exploração de vulnerabilidades;

**2.7.9.38.** Realizar proteção contra ataques de negação de serviços;

**2.7.9.39.** Possuir os seguintes mecanismos de inspeção de IPS:

**a)** Análise para detecção de anomalias de protocolo;

**b)** IP Defragmentation;

**c)** Remontagem de pacotes de TCP;

**d)** Bloqueio de pacotes malformados;

**2.7.9.40.** Ser imune e capaz de impedir ataques básico, tais como, Syn flood, ICMP flood, UDP flood etc.;

**2.7.9.41.** Detectar e bloquear a origem de portscans;

**2.7.9.42.** Bloquear ataques efetuados por worms conhecidos;

**2.7.9.43.** Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

**2.7.9.44.** Possuir assinaturas para bloqueio de ataques de buffer overflow;

**2.7.9.45.** Identificar e bloquear comunicação com botnets;

**2.7.9.46.** Registrar na console de monitoração as seguintes informações sobre ameaças identificadas as seguintes informações: nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

**2.7.9.47.** Permitir identificar, na ocorrência de eventos, o país de onde partiu a ameaça;

**2.7.9.48.** Incluir proteção contra vírus em conteúdo HTML e Javascript e softwares espiões (spyware) e worms;

**2.7.9.49.** Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

**2.7.9.50.** Possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente ou explícito;

**2.7.9.51.** Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

**2.7.9.52.** Possuir, pelo menos, 60 categorias ou subcategorias de URLs;

**2.7.9.53.** Possuir a função de exclusão de URLs ou categorias do bloqueio;

**2.7.9.54.** Possibilitar a implementação de controle de navegação por usuário e grupo do AD sem necessidade de instalação de programas clientes em estações de trabalho dos usuários;

**2.7.9.55.** Possibilitar a implementação de controle de navegação por usuário e grupo do AD para usuários de serviços de terminal remoto em servidores RDS Windows Server;

**2.7.9.56.** Possuir funcionalidade de DLP para os principais tipos de conteúdo e/ou para criação de conteúdos customizáveis;

**2.7.9.57.** Possuir suporte a Link Aggregation;

**2.7.9.58.** Possuir suporte a multiwan load balance;

**2.7.9.59.** Possuir suporte a failover de WAN;

**2.7.9.60.** Possuir suporte total a IPv6;

**2.7.9.61.** Possibilitar o fechamento VPN site-to-site com serviços como Azure e AWS;

**2.7.9.62.** Permitir a escolha do Administrador referente a qual link de saída de internet será usado dependendo da regra em questão;

**2.7.9.63.** Dispor de funcionalidade de filtragem e visualização de logs em tempo real e históricos;

**2.7.9.64.** Permitir controle de consumo de banda pelo menos por regra de firewall, origem ou aplicação;

**2.7.9.65.** Permitir a customização de página de bloqueio de internet/navegação;

**2.7.9.66.** Suportar web proxy transparente com inspeção de SSL, sem necessidade de configurações na máquina dos usuários, apenas através de roteamento de gateway padrão;

**2.7.9.67.** Possibilitar a criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e RADIUS;

**2.7.9.68.** Possuir integração com o Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. A funcionalidade em questão não deverá possuir limites licenciados de usuários ou qualquer tipo de restrição de uso, a exemplo de utilização de sistemas virtuais, segmentos de rede, etc;

**2.7.9.69.** Possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory de forma que, caso seja necessário instalar cliente nas estações, esse deverá ser o mesmo utilizado no ZTNA e outras funcionalidades de segurança;

**2.7.9.70.** Possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

**2.7.9.71.** Permitir que se faça o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, se expanda um portal de autenticação residente no firewall (Captive Portal), nas hipóteses de falha do SSO;

**2.7.9.72.** Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

**2.7.9.73.** Proporcionar, com a finalidade de controlar aplicações de camada 7 e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda (a exemplo de Youtube, Ustream etc.), permitir ou negar esse tipo de aplicação, devendo, ademais, ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de streaming de vídeo;

**2.7.9.74.** Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, destino, usuário e grupo, aplicações e porta;

**2.7.9.75.** Permitir a criação de filtros para arquivos e dados pré-definidos em HTTP e SMTP;

**2.7.9.76.** Realizar identificação de arquivos por extensão e tipo (primeiros bits);

**2.7.9.77.** Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

**2.7.9.78.** Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

**2.7.9.79.** Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

**2.7.9.80.** Permitir a utilização das funcionalidades de VPN Site-to-Site e Client-To-Site;

**2.7.9.81.** Suportar VPN em IPv4 e IPv6;

**2.7.9.82.** Permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

**2.7.9.83.** Permitir que todo o tráfego dos usuários remotos de VPN (SSL ou IPSEc) seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

**2.7.9.84.** Permitir criar políticas de firewall, de controle de aplicações, IPS, Antivírus e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

**2.7.9.85.** Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

**2.7.9.86.** Permitir bloqueios de APT;

**2.7.9.87.** Proporcionar compatibilidade com do agente de VPN SSL ou IPSEC client-to-site com: Windows 10 (32 e 64 bits) ou superior, Windows 11 (32 e 64 bits) ou superior Linux Ubuntu 21.04 LTS ou superior e Mac OS v10.15 (Catalina) ou superior, Android 12 ou superior e iOS 15 ou superior;

**2.7.9.88.** Suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

**2.7.9.89.** Permitir criação de regras de navegação e firewall apenas na gerência centralizada ou na console dos firewalls principais, com replicação automática para os

firewalls remotos instalados nas Subseções e NAPEs, aplicando o controle SD-WAN para uso de internet pelo link local das unidades descentralizadas, utilizando a banda local, sem comprometer o link da unidade Sede, mas ainda assim aplicando as políticas de navegação e segurança definidas;

**2.7.9.90.** Bloquear o acesso a conteúdo indevido ao utilizar a pesquisa de buscadores web, tais como Google, Yahoo etc., independentemente de a opção Safe Search estar habilitada no navegador do usuário.

**2.8.** DO FIREWALL TIPO 2 – EQUIPAMENTO UTM/NGFW

**2.8.1.** Deverá ser disponibilizado um (1) equipamento UTM/NGFW para cada unidade descentralizadas em funcionamento do Coren-SP, para controle de SD-WAN e políticas de segurança das Subseções e NAPEs do Coren-SP relacionadas no Termo de Referência.

**2.8.2.** Os equipamentos disponibilizados deverão receber e aplicar as políticas geradas em console centralizada ou na gerência do próprio firewall da unidade Sede (Firewall Tipo 1).

**2.8.3.** Os seguintes requisitos técnicos relacionados às funcionalidades dos dispositivos de proteção do tipo 2 deverão ser atendidos pela Solução ofertada:

**2.8.3.1.** Throughput de, no mínimo, 4 Gbps com a funcionalidade de firewall habilitada;

**2.8.3.2.** Suporte a, no mínimo, 650.000 de conexões simultâneas (TCP);

**2.8.3.3.** Suporte a, no mínimo, 30.000 novas conexões por segundo (TCP);

**2.8.3.4.** Throughput de no mínimo 2,5 Gbps de VPN IPSec, com pacotes de, no mínimo, 512 bytes;

**2.8.3.5.** Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos;

**2.8.3.6.** Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de clientes VPN IPSEC simultâneos;

**2.8.3.7.** Suportar, no mínimo, 900 Mbps de throughput de IPS;

**2.8.3.8.** Suportar, no mínimo, 700 Mbps de throughput de controle de aplicação;

**2.8.3.9.** Suportar, no mínimo, 300 Mbps de throughput de Inspeção SSL;

**2.8.3.10.** Throughput de, no mínimo, 490 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware;

**2.8.3.11.** Possuir, ao menos, 4 interfaces RJ45;

**2.8.3.12.** Possuir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD- WAN;

**2.8.3.13.** Possuir fonte de alimentação com fonte DC de 100–240V AC, 50–60hz.

As funcionalidades a seguir devem seguir funcionando, mesmo após o vencimento do contrato de suporte e licenciamento: SD-WAN, controle de aplicação e stateful firewall;

**3. DA CONEXÃO E PROTEÇÃO DE USUÁRIOS REMOTOS (MFA E ZERO TRUST)**

**3.1.** A presente seção contempla requisitos relacionados à VPN (já especificada na seção 2 deste documento, que trata dos firewalls), à Autenticação Multifatorial (MFA) e ao Zero Trust (ZTNA).

**3.2.** DA AUTENTICAÇÃO MULTIFATORIAL (MFA)

**3.2.1.** As funcionalidades da solução de autenticação multifatorial ofertada não deverão excluir ou impactar em termos de desempenho àquelas das demais parcelas da Solução a ser contratada pelo Coren-SP, mas sim, complementá-las, em termos de funcionalidades.

**3.2.2.** Considerando a projeção de demanda da Contratante, a Solução ofertada ao Coren-SP deverá possibilitar a utilização da autenticação multifatorial para, pelo menos, 750 (setecentos e cinquenta) usuários simultaneamente[1].

**3.2.3.** A Solução poderá corresponder a um appliance dedicado instalado na infraestrutura da Contratante ou hospedada em Nuvem, desde que atenda aos requisitos definidos neste caderno de especificações técnicas.

**3.2.4.** A MFA, para o ambiente do Coren-SP, se prestará à autenticação de duplo fator para os usuários VPN cliente-to-site, do Firewall UTM/NGFW e para outras aplicações Web via protocolos de integração.

**3.2.5.** Ademais, os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

**3.2.5.1.** Possuir capacidade de integração com aplicações Web desenvolvidas internamente no Coren-SP. Ademais, a Solução deverá possuir funcionalidade que permita a criação de um Hub MFA ou Portal/Gateway para implementar a autenticação MFA à frente de aplicações que não possuam suporte às integrações MFA da Solução ofertada (no presente caso, a Contratada poderá utilizar de outra aplicação do mesmo fabricante da Solução MFA ofertada para atendimento do requisito);

**3.2.5.2.** Possuir capacidade de configuração de MFA em um portal SAML;

**3.2.5.3.** Para o provisionamento das autorizações de acesso dos usuários na interface de administração da Solução, deverá ser utilizada, ao menos, a integração com o serviço de diretório AD, correspondendo à associação de usuários aos grupos de usuários (perfis), sendo obtida do serviço de diretório AD;

**3.2.5.4.** Suportar múltiplos domínios de Microsoft Active Directory;

**3.2.5.5.** Para utilização pelos usuários para autenticação em múltiplos dispositivos, a Solução deverá suportar, no mínimo, os sistemas operacionais: Windows, Android e iOS, utilizando aplicativo próprio ou aplicativo de autenticação de mercado gratuito, como o Authy, o MS Authenticator ou o Google Authenticator;

**3.2.5.6.** Disponibilizar portal de autoatendimento ao usuário para provisionamento e/ou desprovisionamento do seu dispositivo. O portal em questão deverá possuir, no mínimo, autenticação por meio de usuário e senha de diretório (AD/LDAP) e através de integração SAML;

[1] Importa destacar que, a princípio, o Coren-SP estima a contratação inicial de aproximadamente 300 (trezentas) licenças, de forma que as demais licenças serão incorporadas ao objeto de faturamento à medida do incremento das demandas do Coren-SP, durante a vigência do instrumento contratual, com ativações solicitadas por meio do envio de Ordens de Serviço (OS) à Contratada.

**3.2.5.7.** Possibilitar que o usuário não consiga remover a exigência do uso do fator adicional da solução;

**3.2.5.8.** Registrar todas as atividades realizadas, tanto de usuários quanto de administradores, gerando log com, no mínimo, as informações de data e hora, usuário, endereço de origem e informações completas das operações;

**3.2.5.9.** Registras as falhas e exceções em log com informações suficientes para identificação da falha, com no mínimo as informações de data e hora, usuário e endereço de origem;

**3.2.5.10.** Manter o histórico de todas as informações geradas pela solução e que sofreram inclusões, alterações e exclusões por parte dos usuários da solução;

**3.2.5.11.** Permitir a consulta e exportação das trilhas de auditoria, logs e históricos;

**3.2.5.12.** Disponibilizar geração de relatório de utilização do múltiplo fator de autenticação;

**3.2.5.13.** Não limitar a quantidade de aplicações a ser utilizada;

**3.2.5.14.** Dispor de mecanismos de contingência para que, caso ocorra a interrupção da conexão de acesso à internet ou na ocorrência de indisponibilidade do serviço, os usuários possam continuar se autenticando no ambiente;

**3.2.5.15.** Dispor de capacidade de integração com o Security Assertion Markup Language – SAML;

**3.2.5.16.** Dispor de capacidade de integração com o Active Directory Federation Services – ADFS;

**3.2.5.17.** Dispor de capacidade de integração com Remote Authentication Dial-In User Service – RADIUS;

**3.2.5.18.** Disponibilizar, pelo menos, os seguintes fatores de autenticação:

**a)** Push Notification (notificação enviada para uma aplicação instalada no dispositivo do usuário);

**b)** Software Token – OTP (One Time Password);

**c)** OTP enviado por Short Message Service – SMS;

**3.2.5.19.** Permitir a criação de políticas para definir quais usuários terão obrigatoriedade de utilização de múltiplo fator de autenticação;

**3.2.5.20.** Permitir a criação de políticas baseadas no comportamento do usuário (MFA Adaptativo) para permitir o acesso ou não ao ambiente, pelo menos para os seguintes itens (pode ser utilizada outra solução do mesmo fabricante (com licença inclusa) para atendimento desse requisito):

**a)** Redes autorizadas;

**b)** Por geolocalização;

**c)** Dispositivo.

**3.2.5.21.** Possuir compatibilidade com os navegadores Microsoft Edge, Mozilla Firefox e Google Chrome;

**3.2.5.22.** Permitir acesso aos administradores da Solução via interface Web, não exigindo a instalação de complementos, plug-ins ou extensões para seu pleno funcionamento;

**3.2.5.23.** Permitir a criação de diferentes perfis de usuários, com diferentes níveis de autorização, permissões e visões, garantindo que as permissões de acesso sejam gerenciadas a partir da interface da solução;

**3.2.5.24.** Permitir que somente usuários administradores sejam capazes de criar, alterar ou remover usuários e suas permissões associadas conforme perfis.

**3.3.** DO MODELO DE SEGURANÇA DE CONFIANÇA ZERO (ZERO TRUST NETWORK ACCESS - ZTNA)

**3.3.1.** As funcionalidades da solução de segurança de confiança zero ofertada não deverão excluir ou impactar em termos de desempenho àquelas das demais parcelas da Solução a ser contratada pelo Coren-SP, mas sim, complementá-las, em termos de funcionalidades.

**3.3.2.** Considerando a projeção de demanda da Contratante, a Solução ofertada ao Coren-SP deverá possibilitar a utilização do ZTNA para, pelo menos, 750 (setecentos e cinquenta) usuários simultaneamente[2].

**3.3.3.** O ZTNA poderá ser parte integrante da Solução de firewall, ser um appliance dedicado instalado na infraestrutura da Contratante ou uma solução em Nuvem, desde que atenda aos requisitos definidos neste caderno de especificações técnicas.

**3.3.4.** O gateway das conexões do agente cliente deverá ser o próprio firewall ofertado ou recurso de nuvem;

**3.3.5.** O ZTNA, para o ambiente do Coren-SP, se prestará a garantir que apenas máquinas autorizadas e seguras acessem a rede do Coren-SP, seja na infraestrutura local, seja por cliente VPN client-to-site, podendo o ZTNA utilizar o mesmo cliente de VPN, ou outros.

**3.3.6.** Ademais, os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

**3.3.6.1.** Possuir possibilidade de integração com aplicações web desenvolvidas internamente no Coren-SP, executando checagens no cliente para autorizar ou não o acesso a aplicação;

**3.3.6.2.** Possuir funcionalidade de Proxy ZTNA para publicação de um serviço pra internet sem necessidade de passar pela VPN, fazendo todas as checagens de segurança do cliente através de atribuição de tags (rótulos);

**3.3.6.3.** Possuir cliente a ser instalado nos endpoints para atribuição de tags de segurança, minimamente compatível com Windows 10 ou superior, Linux, últimas versões do MacOS, iOS e Android;

**3.3.6.4.** Possibilitar que os clientes endpoint sejam instalados remotamente pela gerência;

[2] Importa destacar que, a princípio, o Coren-SP estima a contratação inicial de aproximadamente 300 (trezentas) licenças, de forma que as demais licenças serão incorporadas ao objeto de faturamento à medida do incremento das demandas do Coren-SP, durante a vigência do instrumento contratual, com ativações solicitadas por meio do envio de Ordens de Serviço (OS) à Contratada.

**3.3.6.5.** Possibilitar a atribuição automática pelo programa cliente de tags de segurança, a partir de regras definidas na gerência. As tags em questão poderão ser manipuladas na gerência centralizada, bem como poderão ser criadas políticas para tratamento dos endpoints com base nas tags recebidas;

**3.3.6.6.** Permitir ou negar acesso a uma determinada rede/recurso/serviço com base na tag atribuída;

**3.3.6.7.** Realizar envio das tags aos clientes em tempo real, sem a necessidade de estarem na rede da empresa ou na VPN, através, apenas, de conexão com a internet;

**3.3.6.8.** Realizar a atribuição de tags com base, minimamente, nos seguintes requisitos:

**a)** Se está logado no domínio AD da empresa;

**b)** Se a máquina está remota ou local na empresa (pelo menos por range IP);

**c)** Se a máquina possui Antivírus ativado e qual versão;

**d)** Se a máquina executa algum programa em blacklist;

**e)** Se a máquina possui vulnerabilidades (sistema e aplicativos não atualizados e vulneráveis);

**f)** Se a versão do sistema operacional é aceitável ou não;

**g)** Se a máquina possui um determinado certificado;

**h)** Se a máquina possui uma chave de registro especifica;

**i)** Se a máquina possui um arquivo específico;

**j)** Se faz parte de um grupo específico do AD.

## 4. DOS SERVIÇOS CONECTIVIDADE (SD-WAN E LINKS)

**4.1.** A presente seção contempla requisitos relacionados aos serviços de conectividade, relacionados à tecnologia SD-WAN e aos serviços de links dedicados de comunicação de dados para acesso à internet destinado à unidade Sede e unidades descentralizadas do Coren-SP.

### 4.2. DA TECNOLOGIA SD-WAN

**4.2.1.** Entende-se como tecnologia SD-WAN a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos.

**4.2.2.** As funcionalidades da tecnologia SD-WAN deverão ser contempladas no UTM/NGFW;

**4.2.3.** Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

**4.2.3.1.** Prover recursos de roteamento inteligente, definindo, mediante regras preestabelecidas, o melhor caminho a ser tomado para uma aplicação;

**4.2.3.2.** Possibilitar o monitoramento e identificação de falhas mediante a associação de health check, permitindo testes de resposta por ping, http e tcp/udp echo;

**4.2.3.3.** Permitir a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

**4.2.3.4.** Permitir a definição do roteamento para cada aplicação;

**4.2.3.5.** Permitir padrões de escolha do link, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

**4.2.3.6.** Possibilitar a definição do link de saída para uma aplicação específica;

**4.2.3.7.** Implementar balanceamento de link por hash do IP de origem e de destino;

**4.2.3.8.** Implementar balanceamento de link por peso. Na opção em questão, deverá ser possível definir o percentual de tráfego que será escoado por cada um dos links. Ademais, deverá suportar o balanceamento de, no mínimo, dois links;

**4.2.3.9.** Implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

**4.2.3.10.** Possuir suporte a Policy based routing ou policy based forwarding;

**4.2.3.11.** Suportar roteamento estático e dinâmico (OSPF, BGP);

**4.2.3.12.** Possibilitar a agregação de túneis IPsec;

**4.2.3.13.** Possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

**4.2.3.14.** Permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

**4.2.3.15.** Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, a Solução deverá, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

**a)** por endereço de origem;

**b)** por endereço de destino;

**c)** por usuário e grupo;

**d)** por aplicações;

**e)** por porta.

**4.2.3.16.** Possibilitar, pelo QoS, a definição de tráfego com banda garantida, a exemplo de banda mínima disponível para aplicações de negócio;

**4.2.3.17.** Possibilitar, pelo QoS, a definição de tráfego com banda máxima, a exemplo de banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc.;

**4.2.3.18.** Possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

**4.2.3.19.** Possibilitar, pelo QoS, a definição de fila de prioridade;

**4.2.3.20.** Possibilitar a definição de banda máxima e garantida por aplicação, devendo, também, suportar essas definições com base em categorias de URL, IPs de origem e destino, logins e portas;

**4.2.3.21.** Possuir a capacidade de agendar intervalos de tempo durante os quais as políticas de shaping/QoS poderão ser alteradas, a exemplo de regra de controle de banda mais permissivas durante o horário de almoço;

**4.2.3.22.** Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que se enquadrarem na regra ou por IP, a exemplo de 10 Mbps de banda garantida por IP ou para todos os IPs que se enquadrem na regra;

**4.2.3.23.** Possibilitar a definição de bandas distintas para download e upload;

**4.2.3.24.** Prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

**4.2.3.25.** Suportar IPv6;

**4.2.3.26.** Possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

**4.2.3.27.** Possibilitar o bloqueio de acesso a aplicações;

**4.2.3.28.** Suportar NAT dinâmico bem como NAT de saída;

**4.2.3.29.** Suportar balanceamento de tráfego por sessão e pacote;

**4.2.3.30.** Implementar balanceamento de link por custo configurado do link;

**4.2.3.31.** Suportar o balanceamento de, no mínimo, 5 links;

**4.2.3.32.** Suportar o balanceamento de links de interfaces físicas, sub- interfaces lógicas de VLAN e túneis IPSec;

**4.2.3.33.** Suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;

**4.2.3.34.** Gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;

**4.2.3.35.** Suportar Zero-Touch Provisioning;

**4.2.3.36.** Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de latência, jitter e perda de pacotes;

**4.2.3.37.** Configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Tais valores serão utilizados pela solução para decidir qual link será utilizado;

**4.2.3.38.** Permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;

**4.2.3.39.** A checagem de estado de saúde deverá suportar teste com Ping, HTTP e DNS;

**4.2.3.40.** As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e protocolo;

**4.2.3.41.** Suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD- WAN;

**4.2.3.42.** Suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;

**4.2.3.43.** Possibilitar a utilização do balanceamento round robin na agregação de duas ou mais IPSEC VPNs determinando o peso para cada VPN;

**4.2.3.44.** Possibilitar especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida;

**4.2.4.** Nas localidades em onde houver disponibilidade de banda larga, a Solução deverá ser capaz de promover redundância entre os links de internet dedicada e internet banda larga de forma que na eventualidade de indisponibilidade do link principal (internet dedicada) o sistema possa automaticamente utilizar o link alternativo (internet banda larga) para manter as conexões sempre ativas.

**4.3. DOS LINKS DE ACESSO DEDICADO À INTERNET**

**4.3.1.** Trata-se da prestação de serviços de acesso à Internet por meio de links dedicados com largura de banda de 100 (cem) e 300 (trezentos) Mbps e Firewall;

**4.3.2.** Os serviços fornecidos deverão ter as características técnicas conforme especificações constantes neste instrumento, atendendo, no mínimo, às seguintes características:

**4.3.2.1.** Banda simétrica;

**4.3.2.2.** Suporte a pacotes IP com MTU mínimo de 1.500 Bytes;

**4.3.2.3.** Taxas de transmissão e quantidade de links e IP's por link de acordo com a seguinte tabela:

| UNIDADE/LOCALIDADE[3] | QTDE LINKS ATIVOS | LARGURA DE BANDA (Mbps) | QTD IPv4 POR LINK |
|---|---|---|---|
| Unidade Sede - São Paulo/SP | 2 | 300 | 16 |
| Nape Alto Tietê (Mogi das Cruzes/SP) – MOGI | 1 | 100 | 1 |
| Subseção Araçatuba – ARA | 1 | 100 | 1 |
| Subseção Botucatu – BOT | 1 | 100 | 1 |
| Subseção Campinas – CAM | 1 | 100 | 1 |
| Subseção Guarulhos – GRU | 1 | 100 | 1 |
| Subseção Itapetininga – ITA | 1 | 100 | 1 |
| Subseção Marília – MAR | 1 | 100 | 1 |
| Subseção Osasco – OSA | 1 | 100 | 1 |
| Subseção Presidente Prudente – PP | 1 | 100 | 1 |
| Nape Registro – REG (AGUARDA ABERTURA)[4] | 1 | 100 | 1 |

[3] Relação de endereços das unidades disponível em: https://portal.coren-sp.gov.br/fale-conosco/enderecos/.

| UNIDADE/LOCALIDADE[3] | QTDE LINKS ATIVOS | LARGURA DE BANDA (Mbps) | QTD IPv4 POR LINK |
|---|---|---|---|
| Subseção Ribeirão Preto – RP | 1 | 100 | 1 |
| Nape Santa Cecília (São Paulo/SP) – SC | 1 | 100 | 1 |
| Nape Santo Amaro (São Paulo/SP) – AMR | 1 | 100 | 1 |
| Subseção Santo André – AND | 1 | 100 | 1 |
| Subseção Santos – SAN | 1 | 100 | 1 |
| Subseção São José do Rio Preto – SJRP | 1 | 100 | 1 |
| Subseção São José dos Campos – SJC | 1 | 100 | 1 |
| Nape Sorocaba – SOR | 1 | 100 | 1 |

**4.3.2.4.** Endereços IPv6 deverão ser fornecidos de acordo com o padrão para usuário de internet, ou seja, ranges de máscara 48 ou 56 para cada link;

**4.3.2.5.** Taxas de transferência de dados em modo simétrico (recepção = transmissão) de, pelo menos 100 ou 300 Mbps, a depender da localidade, em um único enlace ou em múltiplos enlaces agrupados, entregues no mesmo roteador. Caso os serviços sejam ofertados por meio de mais de um enlace, estes deverão estar configurados para balanceamento automático de carga e a conexão com a rede do CONTRATANTE deverá ser feita por meio de uma única porta Ethernet;

**4.3.2.6.** Os links de acesso à Internet não poderão ser compartilhados com nenhum outro cliente do prestador de serviços e deverão possuir dimensionamento correto para garantir a transmissão de dados de acordo com a velocidade estipulada neste instrumento, bem como garantir a qualidade de serviços mínima exigida;

**4.3.2.7.** A largura da banda contratada deverá estar 100% disponível para tráfego de dados entre o firewall instalado no CONTRATANTE e o roteador de serviços durante todo o período de seu funcionamento;

**4.3.2.8.** Todos os equipamentos e acessórios necessários para a ativação dos links de acesso à Internet deverão ser fornecidos pela CONTRATADA e seguirão as características técnicas dispostas neste documento;

**4.3.2.9.** O meio físico do transporte de dados deverá ser por meio de redes de fibra óptica, a serem entregues e instaladas nos locais indicados pela Contratante, ficando a Contratada responsável integralmente pelos custos de infraestrutura e de instalação das conexões;

**4.3.2.10.** A comunicação de dados não poderá ser feita por meios aéreos de comunicação (satélite ou rede sem fio) na última milha, devendo ser estas realizadas por meio terrestre;

**4.3.2.11.** Caberá à CONTRATADA prover todo o cabeamento externo necessário à disponibilização do serviço a ser fornecido até o primeiro ponto de acesso dentro das instalações do Coren-SP;

[4] Unidade com abertura planejada, porém sem data de inauguração definida. Assim sendo, a Administração virá a solicitar a contratação dos serviços em questão a partir da definição da data de inauguração definida, a ocorrer durante a vigência contratual, formalizando a ativação dos serviços por meio do envio de Ordem de Serviço (OS) à Contratada.

**4.3.2.12.** Especificamente, em relação aos links dedicados de 300 Mbps, destinados à unidade Sede do Coren-SP:

**4.3.2.12.1.** Os caminhos físicos utilizados em cada um dos links deverão estar separados entre si. Nesta situação, tanto os equipamentos (modem, roteador, etc.) quanto os meios físicos da rede de acesso deverão ser redundantes e tolerantes a falhas, isto é, cada link dedicado deverá possuir uma estrutura própria, devendo chegar ao endereço da unidade Sede do Coren-SP por caminhos distintos.

**4.3.2.12.2.** Em virtude da segurança e disponibilidade dos sistemas, acessos e serviços publicados e tendo em vista que o serviço operará em contingência ativa, os dois links contratados deverão operar em esquema de tolerância a falhas ativo/ativo, usando técnica de cluster com protocolo VRRP, de modo a garantir a alta disponibilidade do serviço de acesso à Internet. Cada equipamento deverá "ser responsável" por um dos dois ranges de IP contratados e estes equipamentos deverão ser configurados de forma que, no caso de falha em um deles, o que permanecer disponível passe a responder pelas duas faixas de IPs, (tanto pela sua própria quanto pela daquele que está indisponível). Essa configuração deverá persistir pelo tempo que o equipamento/link indisponível permanecer neste estado, devendo retornar assim que o mesmo voltar à atividade.

**4.3.2.13.** A comunicação dos links não poderá sofrer limitações de velocidade ou restrições à quantidade de dados trafegados, tais como traffic shaping;

**4.3.2.14.** Os serviços não poderão sofrer qualquer espécie de redução quanto ao tempo de conexão ou ao volume de dados trafegado (conexão ilimitada);

**4.3.2.15.** Os serviços deverão permitir modificações ou ampliações sem que estas impliquem na interrupção do restante das conexões da rede;

**4.3.2.16.** Todos os serviços de implantação dos links de acesso à internet deverão ser entregues em pleno funcionamento, nas condições técnicas estabelecidas pela Contratante. A Contratada deverá, para tanto, disponibilizar todos os equipamentos necessários à prestação dos serviços, tais como modens, roteadores e outros necessários, sem ônus para a Contratante;

**4.3.2.17.** Na execução dos serviços, a Contratada ficará responsável pelas seguintes ações, sem custos adicionais à Contratante:

**a)** Serviços de gerência proativa da rede;

**b)** Serviços de configuração dos equipamentos fornecidos;

**c)** Serviços de integração e testes de cada link fornecido;

**d)** Serviços de manutenção dos links, com substituição em caso de defeito nos equipamentos, garantindo a continuidade do serviço;

**e)** Serviços esporádicos relativos ao remanejamento de links, juntamente com os seus equipamentos;

**4.3.2.18.** A CONTRATADA se responsabilizará por eventuais adaptações nas instalações físicas nas dependências da CONTRATANTE, assim como a infraestrutura externa, para a

implantação dos serviços contratados (passagem de cabos, lançamento de cabos ou fibras ópticas, adaptação de tomadas, etc.).

**4.3.3.** Da Disponibilidade dos Serviços de Acesso à Internet:

**4.3.3.1.** Todos os serviços de link dedicado, incluindo o atendimento técnico, devem estar disponíveis no período de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, por todo o período contratado, exceto nas interrupções programadas em razão de emergências, motivadas por razões de ordem técnica ou por razões de segurança das instalações;

**4.3.3.2.** Caso haja necessidade técnica de interrupção provisória dos serviços, inclusive em função de mudança de tecnologia, a Contratada deverá comunicar o fato por escrito, com antecedência mínima de 7 (sete) dias úteis; podendo ser deferido ou não o pedido, dependendo da conveniência e interesse da Contratante, considerada a necessidade dos serviços de conexão à internet para o funcionamento das unidades administrativas e para manutenção de serviços WEB realizados pelo órgão;

**4.3.3.3.** As interrupções programadas mencionadas no subitem acima deverão ocorrer, preferencialmente, em finais de semana ou fora do horário comercial. Porém, importa destacar que, caso a Contratada exceda o período previsto, o referido serviço será considerado indisponível no tempo excedente, estando sujeito a glosas no faturamento mensal, sem prejuízo da possibilidade de aplicação de penalidades administrativas;

**4.3.3.4.** Os serviços serão considerados disponíveis desde que estejam plenamente funcionais e operacionais, atendendo a todas as especificações técnicas referentes ao respectivo serviço. Entretanto, o serviço não será considerado indisponível em razão de fatos que estejam sob a responsabilidade da Contratada;

**4.3.3.5.** Os níveis mínimos de serviços especificados pela Contratante considerarão a continuidade das atividades que dependem especificamente do acesso à internet para a qualidade no atendimento prestado aos assistidos da Contratante.

**4.3.4.** O Backbone do prestador de serviço de link dedicado deverá:

**4.3.4.1.** Possuir canais próprios e dedicados;

**4.3.4.2.** Garantido o funcionamento do serviço DNS a partir de servidores localizados nas dependências do Coren-SP, incluindo autoridade sobre as zonas diretas e reversas;

**4.3.4.3.** O serviço DNS deverá suportar o protocolo DNSSEC;

**4.3.4.4.** Possuir política de roteamento que permita trânsito nacional e internacional para a Contratante;

**4.3.4.5.** Fornecer toda a infraestrutura (ECDs, enlaces de comunicação, etc.) necessária para atender os requisitos especificados neste Termo de Referência, incluindo a configuração, manutenção e gerenciamento;

**4.3.4.6.** Fornecer o roteador para a prestação dos serviços com todos os acessórios e programas necessários à sua instalação, operação e monitoração, sendo que o roteador deverá possuir no mínimo duas interfaces Ethernet Full - Duplex (100/1000 Base- T);

**4.3.4.7.** Suportar o gerenciamento por SNMP (versões 1, 2 ou 3);

**4.3.4.8.** Suportar a coleta de estatísticas via SSFlow ou NetFlow;

**4.3.4.9.** Os protocolos SNMP, SFlow/NetFlow devem ser configurados para enviar estatísticas para sistemas internos à CONTRATANTE.

**4.3.5.** A Contratada deverá fornecer link único, não sendo aceito fornecimento de diversos links de menor velocidade com balanceamento entre eles;

**4.3.6.** Em locais que não for possível atender com fibra ótica, poderá ser atendido com IP dedicado com velocidade mínima de 50%, de acordo com a velocidade pedida para o local. Esse quantitativo não deverá ultrapassar 10% do quantitativo total de links a serem instalados considerado todo o objeto de contratação.

**4.3.7.** A Contratada deverá possuir Termo de Autorização da Agência Nacional de Telecomunicações – ANATEL, bem como o registro de suas estações;

**4.3.8.** Os serviços de acesso à internet não deverão sofrer nenhum tipo de tarifação adicional.

**4.4. DO SERVIÇO DE ANTI-DDoS PARA O LINK DE 300 MBPS**

**4.4.1.** A Contratada deverá possuir infraestrutura própria de mitigação com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional;

**4.4.2.** Entenda-se por infraestrutura própria de mitigação, a existência de equipamentos instalados no backbone da Contratada com o objetivo de bloquear o tráfego malicioso, evitando. Assim. a saturação da banda da internet e indisponibilidade dos serviços em momentos de ataques DDoS (Distributed Denial of Service);

**4.4.3.** Não serão aceitas soluções que contemplem equipamentos de mitigação no ambiente da Contratante, de forma que toda a infraestrutura de mitigação deverá ser instalada obrigatoriamente no backbone da Contratada;

**4.4.4.** A Contratada deverá possuir, pelo menos, 2 (dois) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps (quarenta gigabits por segundo);

**4.4.5.** A Contratada deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual;

**4.4.6.** O ataque deverá ser mitigado separando o tráfego legítimo do tráfego malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis. A técnica Anti-DDoS utilizada deverá ser por métrica de volumetria, não podendo haver restrições por volume de tráfego, devendo contemplar o volume total do link concentrador;

**4.4.7.** O serviço de Anti-DDoS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não;

**4.4.8.** Não deverá haver cobrança de taxa adicional por volume de mitigação de ataque nos IPs monitorados;

**4.4.9.** A Solução deverá possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

**4.4.10.** A Solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

**4.4.11.** Em eventuais ataques não detectados pela Contratada, quando identificados pela Contratante, estes deverão ser mitigados imediatamente pela Contratada após a abertura de chamado via central de suporte, sendo sempre considerado um chamado de Severidade Nível 1, devendo realizá-lo sem nenhum ônus à CONTRATANTE;

**4.4.12.** A Solução deverá manter uma lista dinâmica de endereços IPs bloqueados, retirando da lista os endereços que não enviarem mais requisições maliciosas, após um período de tempo considerado seguro pela Contratada e Contratante;

**4.4.13.** A Solução deverá implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

**4.4.13.1.** Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

**4.4.13.2.** Ataques à pilha TCP, incluindo mau uso das Flags TCP, ataques de RST e FIN, SYN FLOOD e TCP IDLE RESETS;

**4.4.13.3.** Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

**4.4.13.4.** Ataques de botnets, worms e ataques que utilizam falsificação de endereços de origem (IP Spoofing).

**4.4.14.** Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de borda da Contratada;

**4.4.15.** A Solução deverá permitir a proteção, no mínimo, todo o tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;

**4.4.16.** A Contratada deverá disponibilizar, por meio eletrônico ou portal na internet, relatórios mensais de mitigação de ataques contendo, no mínimo, horário de início de ação de mitigação, horário de sucesso da mitigação e horário do fim do ataque;

**4.4.17.** Toda a conexão entre o backbone da Contratada e os equipamentos a serem instalados por nas dependências da Contratante, serão de exclusiva responsabilidade da Contratada;

**4.4.18.** Os equipamentos fornecidos pela Contratada deverão dar suporte a serviços de registro de nomes dinâmicos;

**4.4.19.** A interface entre o sistema instalado pela Contratada e a rede/equipamentos da Contratante deverá ser feita por meio de portas de comunicação do tipo RJ-45, via padrões 802.3u ou 802.3ab, compatível com a rede existente, sendo que, no mínimo, uma porta deverá às especificações;

**4.4.20.** Deverão ser fornecidos endereços de rede correspondentes aos protocolos IPv4 e IPv6. No caso do Ipv4, deverá ser fornecido, no mínimo, 1 (um) número de endereço Ipv4 (Internet Protocol) fixo e válido. Os IPs não poderão ser traduzidos por NAT até o backbone da operadora;

**4.4.21.** Caso haja necessidade por parte do CONTRATANTE, a CONTRATADA deverá executar configurações adicionais de roteamentos em seus equipamentos para funcionamento de sistemas informatizados, como por exemplo: relógio eletrônico.

### 4.5. DOS REQUISITOS DE GERÊNCIA DE REDE

**4.5.1.** A Contratada deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, capacity planning, relatórios, tickets e de níveis de serviços.

**4.5.2.** As seguintes funcionalidades relacionadas à Gerência de Rede deverão ser atendidas pela Solução ofertada:

**4.5.2.1.** Disponibilizar a visualização de informações online (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

**4.5.2.2.** Atuar de forma proativa, antecipando os problemas na rede e garantindo o cumprimento dos SLAs estabelecidos, realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando 24 horas por dia, 7 dias por semana, todos os dias do ano;

**4.5.2.3.** Permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

**4.5.2.4.** Viabilizar a operação e administração através de uma console única, de forma que não serão aceitas soluções que possuam acessos segmentados aos módulos;

**4.5.2.5.** Dispor de escalabilidade, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

**4.5.2.6.** Permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc.;

**4.5.2.7.** Permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

**4.5.2.8.** A Solução de Gerência da Rede deverá ser 100% web sem a necessidade de instalação de clientes específicos. Logo, não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plugins nos desktops dos empregados da Contratante;

**4.5.2.9.** Realizar acesso via web padrão HTTP e possuir suporte a HTTPS, devendo ser acessível através dos principais browsers do mercado, tais como Google Chrome, Mozilla Firefox, Microsoft Edge e Safari;

**4.5.2.10.** Possuir interface em língua portuguesa;

**4.5.2.11.** Permitir a exportação das informações para relatórios em formatos comerciais;

**4.5.2.12.** Fornecer, através do portal, visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens:

**a)** Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações;

**b)** Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados.

São Paulo, de 21 de julho de 2023.

## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

| INTEGRANTE REQUISITANTE/ RESPONSÁVEL PELA ÁREA TÉCNICA (GTI) | INTEGRANTE TÉCNICO |
|---|---|
| Rafael Conceição da Silva<br>Assinado de forma digital por Rafael Conceição da Silva<br>Dados: 2023.07.24 16:44:45 -03'00'<br>**Rafael Conceição da Silva**<br>Gerente – GTI<br>Matrícula 455 | Regis de Oliveira Araujo<br>Assinado de forma digital por Regis de Oliveira Araujo<br>Dados: 2023.07.24 16:42:45 -03'00'<br>**Régis de Oliveira Araújo**<br>Analista de Segurança da Informação<br>Matrícula 1044 |
| **INTEGRANTE DA ÁREA DE APOIO ADMINISTRATIVO** | |
| Natalia Cristina da Silva Santos<br>Assinado de forma digital por Natalia Cristina da Silva Santos<br>Dados: 2023.07.24 17:02:45 -03'00'<br>**Natalia Cristina da Silva Santos**<br>Assessor II – GCC<br>Matrícula 1189 | |