TERMO DE REFERÊNCIA

Nº 005/2024

1. OBJETO DA CONTRATAÇÃO

1.1 Contratação de empresa especializada em locação de equipamentos de conectividade e segurança de rede, para o Centro Especializado em Reabilitação – CER II Cajazeiras localizado no endereço: Rua Juscelino Kubitscheck, nº 28 – Cajazeiras XI – Salvador-BA – CEP: 41.330-500.

1.2 Equipamentos e Serviços:

- Fornecimento de Appliance de Firewall NGFW;
- Switch; e
- Access Point.

2. JUSTIFICATICA PARA CONTRATAÇÃO

2.1 A presente contratação se justifica em razão da necessidade de selecionar a melhor proposta, com base nos princípios administrativos da publicidade, moralidade, impessoalidade e eficiência, bem como nos critérios estabelecidos em regimento próprio elaborado pela CONTRATANTE, para a contratação de serviços destinados às atividades do CER II Cajazeiras, administrado pela CONTRATANTE, conforme Contrato de Gestão nº 613/2024, celebrado juntamente com o município de Salvador, por meio da Secretaria Municipal da Saúde;

2.2 A execução dos serviços acima descritos é de extrema importância e sua falta ou má execução impactam diretamente na segurança e à saúde dos pacientes, colaboradores e demais pessoas;

2.3 As ameaças, que podem ser internas ou externas, vêm aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas com múltiplas camadas de proteção, de forma a reduzir o risco, minimizando a probabilidade e os impactos de um eventual ataque cibernético;

2.4 Dentro do contexto analisado, o firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede; e

2.5 Pode-se elencar abaixo os pontos de destaque aos benefícios projetados:

2.5.1 Convergência tecnológica desejada e necessária à implementação de todos os eixos e estratégias da APAE de Salvador;

2.5.2 Alinhamento estratégico de planejamento, orientados pela APAE de Salvador;

2.5.3 Maior qualidade da infraestrutura e dos serviços de TI da APAE de Salvador;

2.5.4 Aumento do grau de satisfação dos usuários com os serviços de TI da APAE de Salvador;

2.5.5 Ampliar a visibilidade e o controle do uso da Infraestrutura e dispositivos aderente ao Plano Estratégico orientada à Governa e Políticas de Acesso; e

2.5.6 Aderência e atendimento à legislação vigente, Marco Civil da Internet e Lei Geral de Proteção de dados, LGPD.

3. CONDIÇÕES GERAIS

3.1 Fornecer, implantar, configurar, suportar e monitorar os equipamentos (Firewall, Switch e Access Point). Realizar a entrega e instalação dos equipamentos para utilização imediata, para atender as demandas da CONTRATANTE em até 20 (vinte) dias corridos da assinatura do contrato, informando em tempo hábil, qualquer motivo impeditivo que a impossibilite de assumir os serviços conforme o estabelecido;

3.2 A CONTRATADA deve comprovar expertise e capacidade técnica para realizar a instalação, configuração e monitoramento dos equipamentos;

3.3 A CONTRATADA deve ter pelo menos um especialista em seu quadro de colaboradores com certificação comprovada pelo fabricante da solução do NGFW que será oferecida;

3.4 Guardar absoluto sigilo sobre todas as informações recebidas da CONTRATANTE, as quais não poderão ser utilizadas para finalidades outras que não a do cumprimento do objeto do presente contrato; e

3.5 A CONTRATANTE poderá inspecionar regularmente o equipamento e, se constatar alguma irregularidade, notificará a CONTRATADA.

4. DA VIGÊNCIA DO CONTRATO

4.1 O Contrato celebrado com a CONTRATANTE para prestação do serviço terá o prazo de vigência de 12 (doze) meses, a contar da data da sua assinatura.

5. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

5.1 Será declarada vencedora, a melhor proposta financeira que atender as especificações técnicas.

5.2 Os preços ofertados pelas empresas interessadas em participar do processo deverão estar expressos em reais (R$) e encaminhados, impreterivelmente, até 12h do dia 27 de novembro de 2024, no seguinte endereço eletrônico: licitacao@apaesalvador.org.br, com CNPJ e assinatura juntamente com a documentação a seguir:

5.3 Não serão aceitas propostas que apresentem preços incompatíveis com os preços executados pelo mercado e pela atividade exercida.

Portfólio de Serviços Prestados

- CAT – Certificado de Acervo Técnico da Empresa ou Carta de Referência de Prestação de Serviços;
- Certificado de um profissional pela emitido pelo fabricante da solução NGFW;
- Certidão Municipal;
- Certidão Estadual;
- CND FGTS;
- Certidão de Tributos Federais e da Dívida Ativa da União;
- Certidão de Débitos Trabalhistas;
- Cronograma de Execução do Serviço (considerando início, desenvolvimento e finalização); e
- Contrato Social, com a última alteração contratual, caso haja.

6. OBRIGAÇÕES DA CONTRATADA

6.1 Atender as especificações constantes no ANEXO I;

6.2 A CONTRATADA deverá fornecer os equipamentos nas condições necessárias para uso imediato dos mesmos;

6.3 Os equipamentos devem ser novos e sem histórico de uso anterior.

6.4 Os equipamentos devem estar em produção atual, ou seja, não podem ser obsoletos ou descontinuados.

6.5 Na proposta deverá ser fornecido a marca e o modelo do(s) equipamento(s) para fins de identificação das funcionalidades;

6.6 O prazo máximo de entrega e instalação dos equipamentos será de até 20 (vinte) dias corridos, contados a partir da data de assinatura do contrato;

6.7 Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o objeto do presente Termo, nem subcontratar quaisquer das prestações a que está obrigada sem prévio consentimento, por escrito, do CONTRATANTE;

6.8 Executar os serviços com o máximo de zelo, bem como seguir rigorosamente as especificações e normas pertinentes em vigência;

6.9 Após a entrega, o CONTRATANTE realizará, por um período de até 07 (sete) dias úteis, testes em que será verificado se o link atende completamente todos os quesitos e condições do Contrato e se contempla todas as especificidades discriminadas na proposta; e

6.10 A CONTRATADA deve entregar um relatório técnico mensal até o quinto dia útil do mês subsequente assinado por um colaborador da CONTRATA.

7. OBRIGAÇÕES DA CONTRATANTE

7.1 Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir acesso de empregados, prepostos ou representantes da CONTRATADA às dependências das Unidades de Saúde relacionadas à execução dos serviços;

7.2 Disponibilizar pontos de rede para o equipamento;

7.3 Disponibilizar pontos de conexão elétrica para o equipamento; e

7.4 Promover os pagamentos avençados pelos equipamentos que estão sendo efetivamente utilizados, nas condições e prazos especificados e ora acordados.

8. GARANTIA E SUPORTE

8.1 Durante a vigência do contrato, a manutenção de hardware locado será de responsabilidade da CONTRATADA, cobrindo-se qualquer quebra que possa ocorrer, com o limite de até 24 (vinte quatros) horas para o reparo efetivo do problema, a partir da abertura do chamado, seja por e-mail ou telefone;

8.2 Substituir o equipamento, a qualquer tempo, caso se faça necessário, por motivos de reparos mecânicos;

8.3 A CONTRATADA deverá disponibilizar uma central de atendimento que será responsável pela abertura de chamados de solicitações e suporte técnico;

ANEXO I

DAS ESPECIFICAÇÕES TÉCNICAS

Firewall, COM AS SEGUINTES ESPECIFICAÇÕES MÍNIMAS

DESCRIÇÃO ITEM 1 (FIREWALL) – Quantidade 01 (um)
Equipamento para proteção por perímetro (Firewall / UTM), a ser instalado nas dependências do Centro Especializado em Reabilitação – CER II Cajazeiras, com as seguintes características:
1. A CONTRATADA deverá fornecer, instalar, configurar e manter, em regime de LOCAÇÃO, equipamento para proteção por perímetro (Firewall / UTM) para proteção do acesso ao canal de comunicação descrito neste edital; **2.** Permitir que sejam ligados no mínimo 3 links de internet de diferentes operadoras; **3.** Para garantir maior segurança, não serão aceitos computadores ou servidores com instalação de sistemas operacionais tradicionais do mercado, tais como Microsoft Windows, FreeBSD, Solaris, AIX ou GNU/Linux; **4.** Deverá possuir minimamente as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention, Controladora Wireless, Virtualização e Retenção de Log em Cloud; **5.** Firewall com capacidade mínima de processamento de 4 (quatro) Gbps; **6.** IPS com capacidade mínima de processamento de 1 (um) Gbps; **7.** Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 500 (quinhentos) Mbps; **8.** Inspeção SSL Throughput com capacidade mínima de processamento de 300 (trezentos) Mbps; **9.** VPN com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego IPSec; **10.** VPN SSL com capacidade de, pelo menos, 400 (quatrocentos) Mbps de tráfego; **11.** Deverá suportar 600.000 (seiscentos mil) conexões simultâneas; **12.** Deverão ser licenciados para suportar, pelo menos, 150 (cento e cinquenta) usuários de VPN SSL; **13.** Deverá suportar, pelo menos, 40.000 (quarenta mil) novas conexões por segundo; **14.** Deverá suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site-Site; **15.** Deverá suportar, pelo menos, 200 (duzentos) túneis de VPN Client-Site; **16.** Deverá possuir, pelo menos, 5 (cinco) interfaces RJ 45; **17.** Deverá suportar operação em modo de alta disponibilidade (cluster) e estar licenciados para operar desta forma, em modo ativo-ativo; **18.** Deverá possuir licença para número ilimitado de usuários e endereços IP; **19.** Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de UTP durante a vigência contratual; **20.** Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 9 (nove) Pontos de Acesso sem fio; **21.** Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos,9 (nove) equipamentos; **22.** Deverá ser realizado a instalação inicial do equipamento que está restrito a entrega do equipamento, conferência de itens e teste inicial de funcionamento; **23.** Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários; **24.** Deverá incluir licença para a funcionalidade de VPN SSL; **25.** Deverá incluir licença para atualização de vacina de antivírus/anti-spyware;

26. Deverá incluir licença de atualização para filtro de conteúdo Web;
27. Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas;
28. Funcionalidade de Firewall

28.1. Deverá possuir controle de acesso à internet por endereço IP de origem e destino;
28.2. Deverá possuir controle de acesso à internet por sub-rede;
28.3. Deverá suportar tags de VLAN (802.1q);
28.4. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;
28.5. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
28.6. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
28.7. Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;
28.8. Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
28.9. Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
28.10. Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
28.11. Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;
28.12. Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
28.13. Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
28.14. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;
28.15. Deverá suportar aplicações multimídia, como: H.323 e SIP;
28.16. Deverá possuir tecnologia de firewall do tipo Statefull;
28.17. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
28.18. Deverá permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;
28.19. Deverá suportar PBR – Policy Based Routing;
28.20. Deverá permitir a criação de VLANS no padrão IEEE 802.1q;
28.21. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
28.22. Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
28.23. Deverá permitir forwarding de camada 2 para protocolos não IP;
28.24. Deverá suportar forwarding multicast;
28.25. Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;
28.26. Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;
28.27. Deverá permitir o agrupamento de serviços;
28.28. Deverá permitir o filtro de pacotes sem a utilização de NAT;
28.29. Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
28.30. Deverá possuir mecanismo de anti-spoofing;
28.31. Deverá permitir criação de regras definidas pelo usuário;
28.32. Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;
28.33. Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser

associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

28.34. Deverá possuir a funcionalidade de balanceamento e contingência de links;

28.35. Deverá suportar sFlow;

28.36. O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando, ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY;

28.37. Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;

28.38. Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

28.39. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

28.40. Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

28.41. Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

28.42. Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

28.43. Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

28.44. Deverá suportar SIP, H.323 e SCCP NAT Traversal;

28.45. Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

28.46. Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

29. Funcionalidade de Traffic Shaping e Priorização de Tráfego

29.1. Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

29.2. Deverá permitir modificação de valores DSCP para o DiffServ;

29.3. Deverá permitir priorização de tráfego e suportar ToS;

29.4. Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

29.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

29.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

29.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

29.8. Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

29.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

29.10. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino; e

29.11. Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade essa conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

30. Funcionalidade de Anti-Spam de Gateway

30.1. Deverá permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

30.2. Deverá possuir filtragem de e-mail por palavras chaves;

30.3. Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

30.4. Deverá possuir, para a funcionalidade de anti-spam, o recurso de RBL;

30.5. Deverá permitir a checagem de reputação da URL no corpo da mensagem de correio eletrônico; e

30.6. Deverá ter a capacidade de permitir a criação de perfis de AntiSpam específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

31. Funcionalidade de Filtro de Conteúdo Web

31.1. Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

31.2. Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

31.3. Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

31.4. Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

31.5. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

a) Proxy anônimo;
b) Webmail;
c) Instituições de saúde;
d) Notícias;
e) Phishing;
f) Hackers;
g) Pornografia;
h) Racismo;
i) Websites pessoais; e
j) Compras.

31.6. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

31.7. Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;

31.8. Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

31.9. Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;

31.10. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

31.11. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

31.12. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores; Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

31.13. Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

31.14. Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

31.15. Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

31.16. Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

31.17. Deverá filtrar o conteúdo baseado em categorias em tempo real;

31.18. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

31.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

31.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

31.21. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;

31.22. Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

31.23. Deverá permitir o bloqueio de redirecionamento HTTP;

31.24. Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

31.25. Deverá possuir Proxy Explícito e Transparente;

31.26. Deverá implementar roteamento WCCP e ICAP; e

31.27. Deverá ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade essa conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

32. Funcionalidade de Detecção de Intrusão

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

32.2. Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

32.3. Deverá estar orientado à proteção de redes;

32.4. Deverá permitir funcionar em modo transparente, sniffer e router;

32.5. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

32.6. Deverá permitir a criação de padrões de ataque manualmente;

32.7. Deverá possuir integração à plataforma de segurança;

32.8. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

32.9. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

32.10. Deverá 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;

32.11. Deverá ter a capacidade de permitir a criação de perfis de inspeção específicos para tipos de dispositivos identificados automaticamente (funcionalidade conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;
32.12. Deverá possuir mecanismos de detecção/proteção de ataques;
32.13. Deverá possuir reconhecimento de padrões;
32.14. Deverá possuir análise de protocolos;
32.15. Deverá possuir detecção de anomalias;
32.16. Deverá possuir detecção de ataques de RPC (Remote Procedure Call);
32.17. Deverá possuir proteção contra-ataques de Windows ou NetBios;
32.18. Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
32.19. Deverá possuir proteção contra-ataques DNS (Domain Name System);
32.20. Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
32.21. Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
32.22. Deverá possuir métodos de notificação de detecção de ataques;
32.23. Deverá possuir alarmes na console de administração;
32.24. Deverá possuir alertas via correio eletrônico;
32.25. Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
32.26. Deverá ter a capacidade de resposta/logs ativa a ataques;
32.27. Deverá prover a terminação de sessões via TCP resets;
32.28. Deverá armazenar os logs de sessões;
32.29. Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
32.30. Deverá mitigar os efeitos dos ataques de negação de serviços;
32.31. Deverá permitir a criação de assinaturas personalizadas;
32.32. Deverá possuir filtros de ataques por anomalias;
32.33. Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
32.34. Deverá permitir filtros de anomalias de protocolos;
32.35. Deverá suportar reconhecimento de ataques de DoS reconnaissance, exploits e evasion;
32.36. Deverá suportar verificação de ataque na camada de aplicação;
32.37. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware; e
32.38. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

33. Funcionalidade de VPN

33.1. Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
33.2. Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
33.3. Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
33.4. Deverá possuir suporte a VPN SSL;
33.5. Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
33.6. A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
33.7. Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
33.8. A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS;
33.9. Deverá permitir a arquitetura de VPN hub and spoke; e

33.10. Deverá possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

34. Funcionalidade de Controle de Aplicações

34.1. Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

34.2. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

a) P2P;
b) Instant Messaging;
c) Web;
d) Transferência de arquivos; e
e) VoIP.

34.3. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

34.4. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

34.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

34.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

34.7. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

34.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

34.9. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

34.10. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

34.11. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

34.12. Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

34.13. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações; e

34.14. Deverá permitir criação de padrões de aplicação manualmente;

Deverá ter a capacidade de permitir a criação de perfis de controle de aplicações específicos para tipos de dispositivos identificados automaticamente (funcionalidade essa conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

35. Funcionalidade de Cache e Otimização WAN

35.1. Deverá possuir capacidade de armazenamento local;

35.2. Deverá implementar, no mínimo, as seguintes técnicas de otimização:

a) Otimização de protocolos;
b) Byte caching; e
c) Web caching.

35.3. Deverá otimizar, no mínimo, os seguintes protocolos: CIFS, FTP, HTTP, MAPI e TCP;

35.4. Deverá implementar alta disponibilidade, no mínimo, ativo-passivo;

35.5. Deverá possuir cache de páginas Web (HTTP); e

35.6. Deverá apresentar gráfico ou relatório que indique a quantidade de tráfego que está sendo otimizada, em porcentagem ou bytes.

36. Funcionalidade de DLP (Data Leak Prevention)

36.1. O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de

Informações) de gateway deverá funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

36.2. Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;

36.3. Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

36.4. Sobre o tráfego de mensageiros instantâneos, deverá inspecionar, no mínimo, os protocolos AIM, ICQ, MSN e Yahoo!;

36.5. Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

36.6. Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

36.7. Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

36.8. Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

36.9. Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

36.10. Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

36.11. Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;

36.12. Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

37. Funcionalidade de Balanceamento de Carga

37.1. Deverá permitir a criação de endereços IPs virtuais;

37.2. Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

37.3. Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

37.4. Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, First Alive e HTTP host;

37.5. Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

37.6. Deverá permitir que seja mantido o IP de origem;

37.7. Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

37.8. Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam; e

37.9. Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

38. Funcionalidade de Virtualização

38.1. Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

38.2. Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

38.3. Deverá permitir a criação de um administrador global que tenha acesso a todas

as configurações das instâncias virtuais criadas;

38.4. Deverá possuir as seguintes certificações:
a) Certificação Wi-Fi Alliance;
b) Certificação ICSA para Firewall;
c) Certificação ICSA para VPN SSL;
d) Certificação ICSA para VPN IPSec; e
e) Certificação ICSA para IPS.

38.5. O equipamento de firewall e/ou IPS deverá ter sido aprovado nos testes da NSS Labs e deverá estar na lista de recomendados.

39. Funcionalidade de SD-WAN

39.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;

39.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;

39.3. A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN;

39.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;

39.5. Solução deve ser capaz de prover Zero Touch provisioning;

39.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;

39.7. A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site;

39.8. A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15;

39.9. Reconhecimento em camada 7 totalmente segregado da camada 4;

39.10. Deve, de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino;

39.11. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

39.12. A solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

39.13. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6;

39.14. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;

39.15. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, no qual seja possível configurar um valor de Theshold para cada um destes itens, será utilizado como fator de decisão nas regras de SD-WAN;

39.16. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu Valor de Saúde melhor que o link atual;

39.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema; e

39.18. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

40. Da Atualização das Licenças

40.1. A CONTRATADA deverá prover toda e qualquer atualização ao produto durante a vigência do contrato;

40.2. Entende-se como atualização o fornecimento de qualquer evolução do produto, incluindo patchs, fixes, correções, updates, service packs e novas versões lançadas;

40.3. O fornecimento de novas versões e releases não acarretará quaisquer ônus adicionais ao CONTRATANTE durante a vigência do contrato; e

40.4. A CONTRATADA deverá informar ao CONTRATANTE toda e qualquer atualização lançada pelo Fabricante, com detalhamento técnico.

DESCRIÇÃO ITEM 2 (Switch de Acesso 48 Portas) – Quantidade estimada 02 (dois)
Equipamento computador de rede eternet, a ser instalado nas dependências do Centro Especializado em Reabilitação – CER II Cajazeiras, com, no mínimo, as seguintes características:
1. Compatível com rack padrão EIA (19") e possuir kits completos para instalação; **2.** Deverá possuir fonte de alimentação primária interna que opere com tensões de entrada entre 110 e 240 V AC e suporte frequência entre 50/60hz **3.** Deverá possuir 48 portas RJ45 10/100/1000 BaseT full-duplex para conexão de cabos de par metálico UTP com conector RJ45. Deve implementar a auto negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); **4.** Deverá possuir pelo menos 4 slots SFP+ 10GE; **5.** Deverá possuir pelo menos 24 portas PoE (802.3af/at) com PoE budget de 370W; **6.** Deverá possuir capacidade de comutação (Duplex) mínima de 176Gbps; **7.** Deverá possuir capacidade de encaminhar 260 Mpps; **8.** Deverá possuir capacidade de suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; **9.** Deve possuir tabela MAC com suporte a 32.000 endereços; **10.** Deverá implementar Flow Control baseado no padrão IEEE 802.3X; **11.** Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); **12.** Deverá possuir suporte a comutação de Jumbo Frames; **13.** Deverá possuir a capacidade de identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; **14.** Deverá possuir suporte a criação de rotas estáticas em IPv4 e IPv6; **15.** Deverá possuir o serviço de DHCP Relay; **16.** Deverá possuir suporte a IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela; **17.** Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring); **18.** Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). **19.** Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; **20.** Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; **21.** Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; **22.** Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; **23.** Deverá possuir suporte a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; **24.** Deverá possuir suporte MAC Authentication Bypass (MAB); **25.** Deve implementar RADIUS CoA (Change of Authorization); **26.** Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; **27.** Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

28. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
29. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
30. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
31. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
32. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
33. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
34. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
35. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
36. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
37. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
38. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
39. Deverá possuir Gerenciamento através de IPv4 e IPv6;
40. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; e
41. **Deve ser totalmente compatível e gerenciado pela solução de NGFW que será fornecida pela CONTRATADA ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:**
    - **41.1.** A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;
    - **41.2.** Deve operar como ponto central para automação e gerenciamento dos switches;
    - **41.3.** Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
    - **41.4.** Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
    - **41.5.** Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
    - **41.6.** Deve montar a topologia da rede de maneira automática;
    - **41.7.** Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
    - **41.8.** Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
    - **41.9.** Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
    - **41.10.** Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
    - **41.11.** Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

41.12. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
41.13. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
41.14. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
41.15. Deve ser capaz de configurar parâmetros SNMP dos switches;
41.16. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
41.17. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
41.18. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;
41.19. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
41.20. Deve prover indicadores de saúde dos elementos críticos do ambiente;
41.21. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
41.22. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede; e
41.23. Deve possuir API no formato REST.

DESCRIÇÃO ITEM 3 (Switch de Acesso 24 Portas) – Quantidade estimada 03 (três)
Equipamento comutador de rede eternet, a ser instalado nas dependências do Centro Especializado em Reabilitação – CER II Cajazeiras, com, no mínimo, as seguintes características:
1. Compatível com rack padrão EIA (19”) e possuir kits completos para instalação; **2.** Deverá possuir fonte de alimentação primária interna que opere com tensões de entrada entre 110 e 240 V AC e suporte frequência entre 50/60hz **3.** Deverá possuir 24 portas RJ45 10/100/1000 BaseT full-duplex para conexão de cabos de par metálico UTP com conector RJ45. Deve implementar a auto negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); **4.** Deverá possuir pelo menos 4 slots SFP+ 10GE; **5.** Deverá possuir pelo menos 12 portas PoE (802.3af/at) com PoE budget de 185W; **6.** Deverá possuir capacidade de comutação (Duplex) mínima de 128Gbps; **7.** Deverá possuir capacidade de encaminhar 190 Mpps; **8.** Deverá possuir capacidade de suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; **9.** Deve possuir tabela MAC com suporte a 32.000 endereços; **10.** Deverá implementar Flow Control baseado no padrão IEEE 802.3X; **11.** Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); **12.** Deverá possuir suporte a comutação de Jumbo Frames; **13.** Deverá possuir a capacidade de identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; **14.** Deverá possuir suporte a criação de rotas estáticas em IPv4 e IPv6; **15.** Deverá possuir o serviço de DHCP Relay; **16.** Deverá possuir suporte a IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela; **17.** Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring); **18.** Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). **19.** Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; **20.** Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; **21.** Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; **22.** Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; **23.** Deverá possuir suporte a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; **24.** Deverá possuir suporte MAC Authentication Bypass (MAB); **25.** Deve implementar RADIUS CoA (Change of Authorization); **26.** Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; **27.** Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

28. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
29. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
30. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
31. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
32. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
33. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
34. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
35. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
36. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
37. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
38. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
39. Deverá possuir Gerenciamento através de IPv4 e IPv6;
40. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
41. Deve ser totalmente compatível e gerenciado pela solução de NGFW que será fornecida pela CONTRATADA nesse termo ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- **41.24.** A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;
- **41.25.** Deve operar como ponto central para automação e gerenciamento dos switches;
- **41.26.** Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
- **41.27.** Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
- **41.28.** Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
- **41.29.** Deve montar a topologia da rede de maneira automática;
- **41.30.** Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
- **41.31.** Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- **41.32.** Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- **41.33.** Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- **41.34.** Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

41.35. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
41.36. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
41.37. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
41.38. Deve ser capaz de configurar parâmetros SNMP dos switches;
41.39. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
41.40. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
41.41. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;
41.42. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
41.43. Deve prover indicadores de saúde dos elementos críticos do ambiente;
41.44. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
41.45. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede; e
41.46. Deve possuir API no formato REST.

DESCRIÇÃO ITEM 4 (Access Point) – Quantidade estimada 09 (nove)
Equipamento Access Point, a ser instalado nas dependências do Centro Especializado em Reabilitação – CER II Cajazeiras, com as seguintes características:
1. Deverá possuir, ao menos, 02 (duas) interfaces de rede 10/100/1000 Base-T RJ-45; **2.** Deverá possuir, ao menos, 01 (uma) interface de console RS-232 RJ-45; **3.** Deverá possuir, ao menos 01 (um) rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; **4.** Deverá possuir, ao menos, 7 (seta) SSIDs simultâneos em cada rádio; **5.** Deverá possuir potência de transmissão de, ao menos, 21 dBm; **6.** Deverá ser compatível com a tecnologia Wi-Fi 6 **7.** Deve possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com ganhos de, no mínimo, 3 dBi para 5GHz; **8.** Deve suportar operação na temperatura de 0 a 40 °C. **9.** Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede. **10.** Deve suportar os padrões 802.11a/b/g/n/ac/ax. **11.** Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; **12.** O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; **13.** Deve possuir a tecnologia MU-MIMO com operação 2x2. **14.** Deve suportar taxas de conexão (data rate) de até 2 Gbps. **15.** Deve possuir PoE (Power over Ethernet), padrão 802.3at, possibilitando seu uso sem a necessidade de fontes de energia externas. **16.** Deve ser incluso injetor PoE capaz de suportar completa operação do equipamento; **17.** Deve suportar a criação de redes mesh; **18.** O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados via túnel seguro (com criptografia) até o controlador wireless; **19.** Deve suportar a criação de enlaces de bridge entre 02 (dois) Access Points. **20.** Em conjunto com o controlador wireless, deve suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação. **21.** Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; **22.** Deve possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais. **23.** Deve implementar UL (uplink) MU-MIMO 802.11. **24.** Deve implementar Spectrum Analyzer. **25.** Deve implementar Spatial Reuse (BSS Coloring). **26.** Deve suportar recurso de Target Wake Time (TWT); **27.** Deve possuir certificação WiFi Alliance. **28. Deve possuir homologação da ANATEL, de acordo com a Resolução número 242.**

29. **Deve ser compatível com o NGFW que será fornecido pela CONTRATADA nesse termo, ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:**
    - **29.1.** Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;
    - **29.2.** Deverá suportar monitoração e supressão de Ponto de Acesso indevido;
    - **29.3.** Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;
    - **29.4.** Deverá permitir a visualização dos clientes conectados;
    - **29.5.** Deverá prover suporte a Fast Roaming;
    - **29.6.** Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;
    - **29.7.** A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
    - **29.8.** Deverá possuir Captive Portal por SSID;
    - **29.9.** Deverá permitir configurar o bloqueio de tráfego entre SSIDs;
    - **29.10.** Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;
    - **29.11.** Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);
    - **29.12.** Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;
    - **29.13.** Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;
    - **29.14.** Deverá permitir a criação de políticas de firewall baseadas em horário;
    - **29.15.** Deverá permitir NAT nas políticas de firewall;
    - **29.16.** Deverá possibilitar definir número de clientes por SSID;
    - **29.17.** Deverá permitir e/ou bloquear o tráfego entre SSIDs;
    - **29.18.** Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;
    - **29.19.** A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;
    - **29.20.** Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;
    - **29.21.** Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;
    - **29.22.** Deve possuir mecanismo de balanceamento de tráfego/usuários entre frequências ou rádios;
    - **29.23.** Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;
    - **29.24.** Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;
    - **29.25.** Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;
    - **29.26.** Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;
    - **29.27.** Deve suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID,

utilizando-se de AES e/ou TKIP;

29.28. Deve suportar os seguintes métodos de autenticação EAP:

29.29. EAP-TLS , EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

29.30. Deve suportar 802.1x através de RADIUS;

29.31. Deve suportar filtro baseado em endereço MAC por SSID;

29.32. Deve permitir configurar parâmetros de rádio, como: banda e canal;

29.33. Deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

29.34. Deve possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

29.35. Deve possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

29.36. Deve possuir WIDS com, ao menos, os seguintes perfis:

29.36.1. Rogue/Interfering AP Detection;

29.36.2. Ad-hoc Network Detection;

29.36.3. Wireless Bridge Detection;

29.36.4. Weak WEP Detection; e

29.36.5. MAC OUI Checking.

29.37. A solução deve detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

Salvador, 19 de novembro de 2024.

Derval Freire Evangelista
Presidente da APAE Salvador