Anexo I

TERMO DE REFERÊNCIA

## 1 - OBJETO

**1.1 – Aquisição de Solução de comunicação (roteadores, licenças e serviço),** visando atender às necessidades deste Tribunal Regional Eleitoral, conforme especificações descritas no presente Termo de Referência.

**1.1.1 –** Faz parte dos itens a serem adquiridos o fornecimento de Garantia "on site" de 24 (vinte e quatro) meses, iniciada a partir do recebimento definitivo pelo gestor da contratação.

## 2 – DAS ESPECIFICAÇÕES TÉCNICAS

**2.1 –** Serão ser adquiridos equipamentos conforme quantitativo e especificações mínimas a seguir descritas:

| Lote | ITEM | Especificação do material (grupo) | Quantidade |
|---|---|---|---|
| 1 | 1 | **ROTEADOR CONCENTRADOR – Código SIASG BR104620** | **2** |
| | 2 | **ROTEADOR REMOTO SD-WAN COM WI-FI INTEGRADO - Código SIASG BR104620** | **30** |
| | 3 | **PONTO DE ACESSO WI-FI - Código SIASG BR393277** | **30** |
| | 4 | **SERVIÇO DE INSTALAÇÃO E SUPORTE - Código SIASG 3840** | **1** |

**2.2** – A presente aquisição se destina a aquisição de equipamentos para composição de solução de comunicação para interligação dos Cartórios Eleitorais e do Edifício Sede do Tribunal Regional Eleitoral do Paraná, visando o bom funcionamento da solução e considerando a necessidade de integração entre os equipamentos na solução pretendida, todos devem pertencer a um lote único, de forma a garantir a integração e o bom funcionamento da solução pretendida.

**2.3 – Das especificações dos itens a serem contratados:**

**2.3.1 - Item 1 – Roteador Concentrador**

**2.3.1.1 - Características do Equipamento:**

1. Deve suportar, no mínimo, 10 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;
2. Deve suportar, no mínimo, 2 Gbps de throughput IPS;
3. Deve suportar, no mínimo, 8,5 Gbps de throughput de VPN IPSec;
4. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL ou TLS;
5. Deve suportar, no mínimo, 1 Gbps de throughput com as funcionalidades firewall, controle de aplicação, IPS e antimalware habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir;
6. Suporte a, no mínimo, 1.200.000 de conexões simultâneas;
7. Suporte a, no mínimo, 50.000 novas conexões por segundo;
8. Estar licenciado para, ou suportar sem o uso de licença adicional, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos;
9. Estar licenciado para, ou suportar sem o uso de licença adicional, 15.000 túneis de clientes VPN IPSEC simultâneos;
10. Estar licenciado para, ou suportar sem o uso de licença adicional, 500 clientes de VPN SSL simultâneos;
11. Possuir ao menos 8 interfaces 1Gbps RJ-45;
12. Possuir ao menos 2 interfaces 10Gbps;
13. Estar licenciado ou ter disponível sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
14. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
15. Possuir fonte de alimentação 100-240V AC;
16. Possuir no máximo 2 RU de altura.

#### 2.3.1.2 – Requisitos mínimos de funcionalidade:

##### 2.3.1.2.1 - Características Gerais:

1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede, ou por console de gerenciamento instalada em máquina virtual compatível com solução VMWare em uso pelo TRE-PR;
7. Os dispositivos de proteção de rede devem possuir suporte a, pelo menos, 4000 VLAN Tags 802.1q;
8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
13. Os dispositivos de proteção de rede devem suportar sFlow;
14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
15. Deve suportar NAT dinâmico (Many-to-1);
16. Deve suportar NAT dinâmico (Many-to-Many);
17. Deve suportar NAT estático (1-to-1);
18. Deve suportar NAT estático (Many-to-Many);
19. Deve suportar NAT estático bidirecional 1-to-1;
20. Deve suportar Tradução de porta (PAT);
21. Deve suportar NAT de Origem;
22. Deve suportar NAT de Destino;
23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

24. Deve poder combinar NAT de origem e NAT de destino na mesma política;
25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
26. Deve implementar o protocolo ECMP;
27. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster e estatísticas de uso das interfaces de rede;
28. Deve ser capaz de enviar logs para sistema de monitoramento externo e ser compatível com o software QRadar, utilizado pelo TRE-PR;
29. Deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2) para o protocolo IPv4;
30. Deve suportar roteamento dinâmico para o protocolo IPv6;
31. Suportar OSPF graceful restart;
32. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
33. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
34. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
35. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo em modo transparente;
36. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo em layer 3;
37. A configuração em alta disponibilidade deve sincronizar:
    a. Sessões;
    b. Configurações;
    c. NAT;
    d. QoS;
    e. Objetos de rede;
    f. Associações de Segurança das VPNs;
    g. Tabelas FIB;
38. O modo de alta disponibilidade deve possibilitar monitoração de falha de link;

39. Deve possuir suporte para criação de sistemas virtuais no mesmo appliance;
40. Deve 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;
41. Deve permitir o controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
42. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
43. O console deve suportar o gerenciamento pontos de acesso wireless. Caso a solução ofertada não possua esta funcionalidade deverá ser fornecida solução complementar, por meio de controladora virtual compatível com o ambiente VMWare do TRE-PR, para controle dos pontos de acesso conforme descrito na seção "**Controladora Wireless em Alta disponibilidade**";
44. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.

**2.3.1.2.2** - Controle por Política de Firewall

1. Deverá suportar controles por zona de segurança;
2. Deve permitir efetuar controles de políticas por porta e protocolo;
3. Deve permitir efetuar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
6. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
7. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall;
8. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução.

### 2.3.1.2.3 - Controle de Aplicações:

1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
4. 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 Skype e utilização da rede Tor;
5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
6. Deve identificar o uso de táticas evasivas via comunicações criptografadas;

7. A atualização da base de assinaturas de aplicações automaticamente;
8. Deve estar apto a limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
9. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
10. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
11. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
12. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
13. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
14. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
15. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
17. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

### 2.3.1.2.4 - Prevenção de Ameaças:

1. Para proteção do ambiente contra ataques, os dispositivos de

proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

2. Para este item a solução deve suportar o licenciamento futuro com suporte a performance do 2.3.1.1 item 5;
3. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
4. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
5. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
6. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
7. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
8. Deve permitir o bloqueio de vulnerabilidades;
9. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
10. Deverá possuir os seguintes mecanismo de inspeção de IPS:
    a. Análise para detecção de anomalias de protocolo;
    b. IP Defragmentation;
    c. Remontagem de pacotes TCP;
    d. Bloqueio de pacotes malformados;
11. Ser capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
12. Detectar e bloquear a origem de portscans;
13. Bloquear ataques efetuados por worms conhecidos;
14. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
15. Possuir assinaturas para bloqueio de ataques de buffer overflow;
16. Deverá possibilitar a criação de assinaturas customizadas pela

interface gráfica do produto;

17. Identificar e bloquear comunicação com botnets;
18. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
    a. O nome da assinatura ou do ataque;
    b. Aplicação;
    c. Usuário;
    d. origem
    e. destino da comunicação;
19. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
20. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
21. Os eventos devem identificar o país de onde partiu a ameaça;
22. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
23. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
24. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando: Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc.;
25. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
26. Mesmo sem o licenciamento deste recurso de Proteção de Ameaças, deve ser possível criar assinaturas de modo manual para tratar a inspeção até a camada 7 do modelo OSI (Aplicação);

### 2.3.1.2.5 - Filtro de URL:

1. A solução deve suportar o licenciamento futuro, com as seguintes funcionalidades;
    a. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês,

ano, dia da semana e hora);

b. Deve 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;
c. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
d. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
e. Possuir pelo menos 60 categorias de URLs;
f. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
g. Permitir a customização de página de bloqueio;
h. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
i. Além do Explicit Web Proxy, suportar proxy Web transparente;

**2.3.1.2.6 - Identificação de Usuários:**

1. Deve incluir a capacidade de 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-directory e base de dados local;
2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir

limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;

4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
7. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
8. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução.

### 2.3.1.2.7 - QoS e Traffic Shaping:

1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve 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 vídeo streaming;
2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent,

YouTube e Azureus;

6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
7. O QoS deve possibilitar a definição de tráfego com banda garantida;
8. O QoS deve possibilitar a definição de tráfego com banda máxima;
9. O QoS deve possibilitar a definição de fila de prioridade;
10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
11. Suportar modificação de valores DSCP para o Diffserv;
12. Suportar priorização de tráfego usando informação de Type of Service;
13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

### 2.3.1.2.8 - Filtro de Dados:

1. Permitir a criação de filtros para arquivos e dados pré-definidos;
2. Os arquivos devem ser identificados por extensão e tipo;
3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
6. Permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

### 2.3.1.2.9 - Geo Localização:

1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3. Deve possibilitar a criação de regiões geográficas pela interface

gráfica e criar políticas utilizando as mesmas.

**2.3.1.2.10 - VPN**

1. Suportar VPN Site-to-Site e Cliente-To-Site;
2. Suportar IPSec VPN;
3. Suportar SSL VPN;
4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Palo Alto Networks, Fortinet, SonicWall;
9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
15. Deverá manter uma conexão segura com o portal durante a sessão;
16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
17. Deve suportar agregação de túneis IPSec;

18. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec;
19. A VPN IPSec deve suportar Forward Error Correction (FEC);
20. Deve suportar TLS 1.2 em VPN SSL.

### 2.3.1.2.11 - Wireless Controller:

1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
5. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
8. 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 devem ser tunelados até o controlador wireless;
9. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
10. Deve permitir o gerenciamento de pontos de acesso conectados

remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;

11. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
12. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
13. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
15. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;
21. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
24. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
25. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

26. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
27. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
28. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
29. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
30. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
31. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
32. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
33. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
34. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

35. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
36. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
37. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
38. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
39. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
    a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
    b. Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
    c. ASLEAP;
    d. Null Probe Response / Null SSID Probe Response;
    e. Long Duration;
    f. Ataques contra Wireless Bridges;
    g. Weak WEP;
    h. Invalid MAC OUI."
40. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
41. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
42. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
43. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
44. Deve implementar autenticação administrativa através do protocolo RADIUS;

45. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
46. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
47. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
48. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
49. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
50. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
51. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
52. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal.
53. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
58. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

59. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
62. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
63. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
64. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
65. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
66. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
67. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
68. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
69. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
70. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
71. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
72. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF

ou CAD;

73. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
74. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
75. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
76. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
77. A solução deve possuir ferramentas de diagnósticos e debug;
78. A solução deve suportar comunicação com elementos externos através de APIs;
79. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo/lote;
80. Caso a solução ofertada não possua a funcionalidade "Wireless Controler" integrada, deverá ser fornecida solução complementar, por meio de controladora virtual compatível com o ambiente VMWare do TRE-PR, para controle dos pontos de acesso conforme descrito na seção "80.1" "**Controladora Wireless em Alta disponibilidade**", com licenças de funcionamento perpétuas, não sendo aceitas modalidades em Cloud.

**80.1 . Controladora Wireless em Alta Disponibilidade:**

a) Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
b) Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos. A controladora deve ser fornecida com licenciamento perpétuo e estar apta a controlar, pelo menos, 250 pontos de acesso;
c) Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;

d) A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
e) O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
f) A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
g) Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
h) 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 devem ser tunelados até o controlador wireless;
i) Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
j) Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
k) Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
l) A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

m) A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
n) A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
o) A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
p) A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
q) A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
r) A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
s) A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

t) A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;
u) A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
v) A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
w) A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
x) A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
y) A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
z) A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
aa) A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações

complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

bb) A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

cc) A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

dd) A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

ee) A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

ff) Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

gg) A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

hh) A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

ii) A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

jj) A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

kk) A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;

ll) A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);

b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;

c. ASLEAP;

d. Null Probe Response / Null SSID Probe Response;

e. Long Duration;

f. Ataques contra Wireless Bridges;

g. Weak WEP;

h. Invalid MAC OUI."

mm) A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;

nn) A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;

oo) A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;

pp) Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;

qq) Deve implementar autenticação administrativa através do protocolo RADIUS;

rr) Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

ss) Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

tt) A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;

uu) Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

vv) A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

ww) A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

xx) A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

yy) A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;

zz) A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

aaa) A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

bbb) A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

ccc) A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

ddd) A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

eee) A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;

fff) A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

ggg) Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

hhh) A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;

iii) A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispostivo conectado à rede wireless;

jjj) A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

kkk) A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

lll) A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

mmm) A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

nnn) A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

ooo) A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;

ppp) A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

qqq) A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

rrr) A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

sss) A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

ttt) A solução deve apresentar graficamente a topologia lógica da

rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

uuu) A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

vvv) A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

www) A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;

xxx) A solução deve possuir ferramentas de diagnósticos e debug;

yyy) A solução deve suportar comunicação com elementos externos através de APIs;

zzz) A solução deverá ser compatível e gerenciar os pontos de acesso deste processo.

**2.3.1.2.12 - SD-WAN:**

1. Deve implementar balanceamento de link por hash do IP de origem;
2. Deve implementar balanceamento de link por hash do IP de origem e destino;
3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;
4. Deve implementar balanceamento de link por custo configurado do link;
5. Deve suportar o balanceamento de, no mínimo, 5 links;
6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;
7. Deve 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;
8. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

9. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
10. Deve suportar Zero-Touch Provisioning;
11. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
12. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
13. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
14. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
18. Deve 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;
19. Conforme disposto no item I do artigo 15 da Lei nº 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), **os itens 1 e 2, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante**.

### 2.3.2 - Item 2 – Roteador Remoto SD-WAN com Wi-fi integrado

#### 2.3.2.1 - Características do Equipamento:

1. Deve suportar, no mínimo, 5 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;
2. Deve suportar, no mínimo, 1 Gbps de throughput IPS;
3. Deve suportar, no mínimo, 4 Gbps de throughput de VPN IPSec;
4. Deve suportar, no mínimo, 300 Mbps de throughput de VPN SSL ou TLS inspection;
5. Deve suportar, no mínimo, 800 Mbps de throughput de Controle de Aplicação;
6. Deve suportar, no mínimo, 500 Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;
7. Suporte a, no mínimo, 500.000 conexões simultâneas;
8. Suporte a, no mínimo, 30.000 novas conexões por segundo;
9. Estar licenciado para, ou suportar sem o uso de licença, 180 túneis de VPN IPSEC Site-to-Site simultâneos;
10. Estar licenciado para, ou suportar sem o uso de licença, 220 túneis de clientes VPN IPSEC simultâneos;
11. Estar licenciado para, ou suportar sem o uso de licença adicional, 180 clientes de VPN SSL simultâneos;
12. Permitir gerenciar ao menos 6 Access Points em modo túnel e 12 em modo bridge;
13. Possuir ao menos 4 interfaces 1Gbps;
14. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 2 sistemas virtuais lógicos (Contextos) por appliance;
15. Suporte a, no mínimo, 2 sistemas virtuais lógicos (Contextos) por appliance;
16. Possuir no máximo 1 RU de altura.

#### 2.3.2.1 - Requisitos Mínimos de Funcionalidade

##### 2.3.2.1.1 - Características Gerais:

1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
7. Os dispositivos de proteção de rede devem possuir suporte a, no mínimo, 200 VLAN Tags 802.1q;
8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
13. Os dispositivos de proteção de rede devem suportar sFlow;
14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
15. Deve suportar NAT dinâmico (Many-to-1);
16. Deve suportar NAT dinâmico (Many-to-Many);
17. Deve suportar NAT estático (1-to-1);
18. Deve suportar NAT estático (Many-to-Many);
19. Deve suportar NAT estático bidirecional 1-to-1;
20. Deve suportar Tradução de porta (PAT);
21. Deve suportar NAT de Origem;

22. Deve suportar NAT de Destino;
23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
24. Deve poder combinar NAT de origem e NAT de destino na mesma politica
25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66;
26. Deve implementar o protocolo ECMP;
27. Deve 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;
28. Deve ser capaz de enviar logs para sistema de monitoramento externo e ser compatível com o software QRadar, utilizado pelo TRE-PR;
29. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
30. Deve possuir proteção anti-spoofing;
31. Deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2) para IPv4;
32. Suportar OSPF graceful restart;
33. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
34. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
35. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
36. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
37. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em modo transparente;
38. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em layer 3;
39. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;
40. A configuração em alta disponibilidade deve sincronizar: Sessões;
41. A configuração em alta disponibilidade deve sincronizar:

Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

42. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
43. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
44. O modo de Alta-Disponibilidade deve possibilitar monitoração de falha de link;
45. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;
46. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
47. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
48. Efetuar controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
49. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
50. O console de administração deve suportar pelo menos inglês;
51. O console deve suportar o gerenciamento de pontos de acesso wireless;
52. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.

### 2.3.2.1.2 - Controle por Política de Firewall:

1. Deverá suportar controles por zona de segurança;
2. Efetuar controles de políticas por porta e protocolo;
3. Efetuar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4. Deve efetuar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
5. Deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública;
6. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
7. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall
8. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;
9. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web.

### 2.3.2.1.3 - Controle de Aplicações:

1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel,

facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

4. 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 Skype e utilização da rede Tor;
5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
6. Identificar o uso de táticas evasivas via comunicações criptografadas;
7. Atualizar a base de assinaturas de aplicações automaticamente;
8. Deve estar apto a limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
9. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
10. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
11. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
12. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
13. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
14. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
15. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia

utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
17. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
18. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.

**2.3.2.1.4 - Prevenção de Ameaças:**

1. Para este item a solução deve suportar o licenciamento futuro com suporte a performance do 2.3.2.1 item 6;
2. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
3. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
4. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
5. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
6. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
7. Deve permitir o bloqueio de vulnerabilidades;
8. Deve incluir proteção contra ataques de negação de serviços;
9. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
10. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise

para detecção de anomalias de protocolo;

11. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
12. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
14. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
15. Detectar e bloquear a origem de portscans;
16. Bloquear ataques efetuados por worms conhecidos;
17. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
18. Possuir assinaturas para bloqueio de ataques de buffer overflow;
19. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
20. Identificar e bloquear comunicação com botnets;
21. Registrar na console de monitoração 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;
22. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
23. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
24. Os eventos devem identificar o país de onde partiu a ameaça;
25. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
26. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
27. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por

Usuários, Grupos de usuário, origem, destino, zonas de segurança;

28. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
29. Mesmo sem o licenciamento deste recurso de Proteção de Ameaças, deve ser possível criar assinaturas de modo manual para tratar a inspeção até a camada 7 do modelo OSI (Aplicação).

### 2.3.2.1.5 - Filtro de URL:

1. Para este item a solução deve suportar o licenciamento futuro;
2. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
3. Deve 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;
4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
5. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
6. Possuir pelo menos 60 categorias de URLs;
7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
8. Permitir a customização de página de bloqueio;
9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
10. Além do Explicit Web Proxy, suportar proxy Web transparente;
11. Mesmo sem o licenciamento deste recurso, deve ser possível criar regras de filtro URL de modo manual com suporte a expressões regulares.

### 2.3.2.1.6 - Identificação de Usuários:

1. Deve incluir a capacidade de 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-directory e base de dados local;
2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
10. Prover no mínimo um token nativamente, possibilitando

autenticação de duplo fator.

### 2.3.2.1.7 - QoS e Traffic Shaping:

1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve 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 vídeo streaming;
2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
7. O QoS deve possibilitar a definição de tráfego com banda garantida;
8. O QoS deve possibilitar a definição de tráfego com banda máxima;
9. O QoS deve possibilitar a definição de fila de prioridade;
10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
11. Suportar modificação de valores DSCP para o Diffserv;
12. Suportar priorização de tráfego usando informação de Type of Service;
13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

### 2.3.2.1.8 - Filtro de Dados:

1. Permitir a criação de filtros para arquivos e dados pré-definidos;
2. Os arquivos devem ser identificados por extensão e tipo;

3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

### 2.3.2.1.9 - Geo Localização:

1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

### 2.3.2.1.10 – VPN:

1. Suportar VPN Site-to-Site e Cliente-To-Site;
2. Suportar IPSec VPN;
3. Suportar SSL VPN;
4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

9. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
15. Deverá manter uma conexão segura com o portal durante a sessão;
16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
17. Deve suportar agregação de túneis IPSec
18. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec
19. A VPN IPSec deve suportar Forward Error Correction (FEC)
20. Deve suportar TLS 1.2 em VPN SSL.

### 2.3.2.1.11 - Wireless Controller:

1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;

4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
5. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
8. 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 devem ser tunelados até o controlador wireless;
9. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
10. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
11. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
12. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

13. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
15. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com

isso permitir maior flexbilidade no design da rede wireless;

21. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
24. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
25. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
26. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
27. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
28. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
29. A solução deve suportar priorização via WMM e permitir a tradução

dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

30. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
31. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
32. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
33. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;
34. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
35. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
36. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
37. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
38. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

39. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
40. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
41. ASLEAP;
42. Null Probe Response / Null SSID Probe Response;
43. Long Duration;
44. Ataques contra Wireless Bridges;
45. Weak WEP;
46. Invalid MAC OUI."
47. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
48. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
49. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
50. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
51. Deve implementar autenticação administrativa através do protocolo RADIUS;
52. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
53. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
54. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
55. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
56. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
57. A solução deve implementar o mecanismo de mudança de

autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

58. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
59. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
60. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
61. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
62. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
63. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
64. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
65. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
66. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
67. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
68. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
69. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispostivo conectado à rede wireless;
70. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que

estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

71. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
72. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
73. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
74. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
75. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
76. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
77. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
78. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
79. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
80. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
81. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
82. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
83. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;

84. A solução deve possuir ferramentas de diagnósticos e debug;
85. A solução deve suportar comunicação com elementos externos através de APIs;
86. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;
87. Caso a solução ofertada não possua a funcionalidade “Wireless Controler” deverá ser fornecida solução complementar, por meio de controladora virtual compatível com o ambiente VMWare do TRE-PR, para controle dos pontos de acesso conforme descrito na seção “Controladora Wireless em Alta disponibilidade”, com licenças de funcionamento perpétuas, não sendo aceitas modalidades em Cloud.

**2.3.2.1.12 - SD-WAN:**

1. Deve implementar balanceamento de link por hash do IP de origem;
2. Deve implementar balanceamento de link por hash do IP de origem e destino;
3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
4. Deve implementar balanceamento de link por custo configurado do link.
5. Deve suportar o balanceamento de, no mínimo, 5 links;
6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec
7. Deve 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.
8. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
9. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde
10. Deve suportar Zero-Touch Provisioning
11. Possuir checagem do estado de saúde do Link baseando-se em

critérios mínimos de: Latência, Jitter e Perda de Pacotes

12. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado
13. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.
14. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS
15. Suportar UDP Hole Punching em arquitetura ADVPN
16. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado
17. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.
18. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN
19. Deve 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.

### 2.3.2.1.13 - Access Point:

1. O equipamento deve possuir uma antena integrada para acesso wi-fi de clientes. Se o equipamento ofertado não possuir esta antena, o atendimento a este item poderá ser composto com a entrega de um equipamento adicional para cada roteador remoto adquirido, conforme especificações do item 3 deste lote;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac em Wave2;
4. Deve suportar operação nas faixas de frequência de 2.4GHz e

5GHz;

5. Deve suportar MU-MIMO 3x3;
6. Deve possuir antenas externas no equipamento com ganho mínimo de 5dBi em 2.4GHz e 3.5dBi em 5GHz;
7. Deve suportar uma potência de transmissão de no mínimo 20 dBm;
8. Deve suportar velocidades mínimas de 1300 Mbps em 5GHz e 450 Mbps em 2.4GHz;
9. Conforme disposto no item I do artigo 15 da Lei nº 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), **os itens 1 e 2, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante**.

### 2.3.3 - Item 3 – Ponto de Acesso Wi-fi:

1. Deve ser do tipo Indoor;
2. Deverá possuir três rádios, sendo eles:
   a. O primeiro rádio deve suportar Taxa de transmissão de no mínimo 867 Mbps e ser configurável para operar em 2.4GHz e 5GHz;
   b. O segundo rádio deve suportar Taxa de transmissão de no mínimo 867 Mbps e operar em 5GHz;
   c. O terceiro rádio deve suportar Taxa de transmissão de no mínimo 400 Mbps e ser configurável para operar em 2.4GHz e 5GHz;
3. Suportar no mínimo 512 usuários associados nos rádios 1 e 2;
4. Suportar no mínimo 128 usuários associados no rádio 3;
5. Deverá possuir também um Rádio do Tipo BLE, além dos rádios explicitados acima;
6. Implementar as tecnologias 802.11 a/b/g/n/ac-W2;
7. Implementar SU-MIMO 2x2;
8. Implementar 802.11ac Wave2;
9. Implementar MU-MIMO;

10. Deve permitir que o terceiro rádio seja utilizado como analisador de espectro;
11. Implementar 802.11ac VHT 20/40/80 MHz;
12. Ter potência máxima de ao menos 24 dBm;
13. Sensibilidade RX de ao menos -86 dBm considerando tráfego em VHT40 para MCS 0;
14. Ter ao menos 6 antenas internas;
15. O ganho das antenas internas em 2.4GHz deve ser ao menos 4 dBi;
16. O ganho das antenas internas em 5GHz deve ser ao menos 5 dBi;
17. Ter 1 antena interna do tipo BLE;
18. A antena do tipo BLE deve possuir potência de ao menos 5 dBm;
19. Deve possuir 2 interfaces de rede operando em velocidades de 10/100/1000Mbps, sendo 1 com capacidade de alimentação do equipamento via PoE (PoE 802.3af);
20. Possuir interface de console;
21. Possuir local para conexão de trava Kensington;
22. Deve suportar temperatura de operação até 40 º C;
23. Implementar Transmit Beamforming (TxBF);
24. Possuir certificado WPA3;
25. Deve permitir sua implementação em modo Bridge, Mesh e Tunel;
26. O Fabricante da solução deve possuir ferramenta própria de controle de acesso à rede (NAC), permitindo que posteriormente sejam implementados serviços como Device Profiling, descoberta de rede, Políticas de Controle de Acesso, Micro-Segmentação, Endpoint Compliance e autenticação avançada com Agentes.

### 2.3.3.1 - Requisitos Mínimos de Funcionalidade

#### 2.3.3.1.1 - Características Gerais:

1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da wireless (sem fio) e que permita que as suas configurações sejam centralizadas em controlador wireless;
2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por

gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

3. Deve acompanhar licença que permita que sejam habilitadas todas as suas funcionalidades;
4. Deve identificar automaticamente o controlador wireless ao qual se conectará;
5. Deve permitir ser gerenciado remotamente através de links WAN;
6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
7. 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 devem ser tunelados até o controlador wireless;
8. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
9. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
10. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
11. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
12. Possuir funcionalidade de ajuste de potência automática de forma a extender cobertura no caso de falha de APs vizinhos gerenciados

pela mesma controladora;

13. Deve suportar mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs;
14. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
15. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede;
16. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
17. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
18. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
19. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
20. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
21. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
22. Deve implementar o padrão IEEE 802.11e;
23. Deve implementar o padrão IEEE 802.11h;
24. Implementar agregação de pacotes A-MPDU e A-MSDU no Access Point;
25. Implementar LPDC - Low Density Parity Check no Access Point;
26. Implementar (MLD) - Maximum Likelihood Demodulation no Access Point;
27. Implementar Maximum Ratio Combining (MRC) no Access Point;

28. Deve possuir indicadores luminosos (LED) para indicação de status;
29. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;
30. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
31. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
32. Suportar, através de upgrade de licenciamento, método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens Syslog;
33. Deve ser fornecido com garantia do tipo NBD para no mínimo 24 meses
34. Deve ser fornecido com kit de montagem para teto, permitindo que o Ponto de Acesso seja instalado em superfícies planas, como tetos;
35. Deve possuir certificado de homologação válido e vigente emitido pela ANATEL.

### 2.3.4 - Item 4 – Serviço de Instalação

1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;
2. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura existente e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da

CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

4. Após a instalação, a solução deverá ser monitorada de forma remota pelo prazo mínimo de 8 (oito) horas corridas, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação.

5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma remota apresentando as configurações realizadas nos equipamentos pelo prazo mínimo de 8 (oito) horas corridas;

6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. A Contratante solicitará os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços (conforme item 10.1.b do edital), sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o

resumo das configurações dos equipamentos.

a. Este relatório deve ser enviado com todas as informações em até 15 (quinze)dias após a finalização dos serviços;

8. Somente os roteadores concentradores deverão ser instalados de forma on-site nas dependências da CONTRATANTE os demais poderão ser instalados de forma remota;

9. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE.

10. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

11. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE, conforme item 10.1.a do edital;

12. As atividades deverão ser realizadas dentro do horário comercial;

13. A implantação não deverá se limitar somente as configurações aqui destacadas. Quaisquer novas funcionalidades suportadas pelos equipamentos poderão fazer parte do escopo do projeto. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE;

14. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida).

## 3 – DA ENTREGA E DO RECEBIMENTO

### 3.1 - DA ENTREGA DO OBJETO

**3.1.1 -** Todos os equipamentos entregues devem ser de uma única marca e modelo.

**3.1.1.1 -** A contratada deverá apresentar os equipamentos acondicionados conforme padrão do fabricante. A embalagem deve garantir a proteção do equipamento durante o transporte e estocagem, bem como conter a identificação do produto e demais informações que facilitem a verificação e manuseio dos mesmos.

**3.1.2 -** Deverá ser fornecida documentação completa e atualizada (manuais, termos de garantia, etc.), no idioma Português, e em quantidade necessária à instalação e à operação dos equipamentos;

**3.1.3 -** A Contratada deverá fixar nos equipamentos chapa/etiqueta com número de controle patrimonial, a ser fornecida pelo Tribunal Regional Eleitoral do Paraná juntamente com as instruções para fixação das mesmas.

**3.1.3.1 -** A fixação da etiqueta patrimonial deverá ser feita antes do início da entrega dos equipamentos ao TRE-PR. O número de controle patrimonial deverá, também, ser registrado externamente nas embalagens dos equipamentos, através de etiquetas adesivas fornecidas e confeccionadas pela Contratada.

**3.1.4 - DO LOCAL DE ENTREGA:** Os equipamentos deverão ser entregues na Seção de Rede deste Tribunal, mediante agendamento pelo telefone 41 - 3330-8628.

**3.1.4.1 -** A entrega deverá ser feita em dias úteis – segunda a sexta-feira – no horário compreendido entre as 12 e as 19 horas, podendo também ocorrer, caso o TRE julgue necessário, em sábados, domingos e feriado.

**3.1.5 – DO PRAZO DE ENTREGA:**

a) **Para os itens 01 a 03**: prazo máximo **de 40 (quarenta) dias corridos contados da assinatura do contrato**, estando incluso no valor contratado quaisquer despesas com frete e demais impostos inerentes à contratação.

b) **Para o item 4:** prazo máximo **de 60 (sessenta) dias corridos contados do recebimento dos equipamentos.**

**3.1.5.1 -** Não serão aceitas entregas de equipamentos no período de recesso deste TRE, ou seja, entre 19 de dezembro e 7 de janeiro.

**3.1.6 -** Conforme o Art. 3º, inciso III do Decreto 7174/2010[1], caso o produto seja importado, a Contratada deverá apresentar, no momento da entrega, Guia de Recolhimento de Imposto de Importação sobre os produtos a serem fornecidos, mesmo que seja em nome do seu fornecedor, evitando assim, o fornecimento de produtos com entrada ilegal no país, sob pena de não recebimento do objeto, sem prejuízo das sanções cabíveis.

**3.2 – DO RECEBIMENTO**

**3.2.1 – DO RECEBIMENTO PROVISÓRIO**

---

[1] Art. 3º, inciso III do Decreto 7.174/2010 – *"Além dos requisitos dispostos na legislação vigente, nas aquisições de bens de informática e automação, o instrumento convocatório deverá conter, obrigatoriamente:*
*III – exigência contratual de comprovação da origem dos bens importados oferecidos pelos licitantes e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto (...)"*

**3.2.1.1 -** O recebimento provisório será realizado pela Seção de Rede, no prazo máximo de 01 (um) dia.

### 3.2.2 – DO RECEBIMENTO TÉCNICO E DEFINITIVO

**3.2.2.1 -** Comissão Técnica com no mínimo 3 servidores a ser instituída pela Secretaria de Tecnologia da Informação realizará, no prazo máximo de 02 (dois) dias úteis, uma inspeção técnica dos equipamentos adquiridos para verificação da sua integridade física e cumprimento das especificações exigidas no edital e seus anexos;

**3.2.2.2 -** Para a inspeção técnica, será utilizada a documentação entregue pelo fornecedor e/ou fabricante do equipamento contendo as especificações detalhadas dos itens licitados;

**3.2.2.3 -** A inspeção técnica poderá ser realizada por amostragem, a critério da Administração. O equipamento que, a qualquer tempo durante a vigência do contrato, apresentar irregularidades ou estiver em desacordo com aquele aprovado durante a análise da amostra deverá ser substituído no prazo de até 05 (cinco) dias, contados do comunicado enviado pelo TRE-PR.

**3.2.2.4 -** Os equipamentos deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões e/ou outros problemas físicos;

**3.2.2.5 -** O equipamento testado deverá possuir todos os componentes e as mesmas características do equipamento ofertado no edital, sendo aceitos componentes e especificações superiores;

**3.2.2.6 -** Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições de funcionamento, Comissão Técnica a ser instituída pela Secretaria de Tecnologia da Informação emitirá(ão) o Atestado de Aceite Técnico e definitivo no prazo máximo informado no item 3.2.2.1.

**3.2.3.1 -** A Coordenadoria de Infraestrutura receberá e encaminhará a nota fiscal e atestado do bem no prazo máximo de 02 (dois) dias úteis

**3.2.4 -** Recebido o objeto, mas constatado qualquer defeito/irregularidade, a Contratada deverá providenciar a substituição no prazo de até 05 (cinco) dias, contados do comunicado do TRE/PR, sem quaisquer ônus.

## 4 – OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

### 4.1 – DA SUSTENTABILIDADE

**4.1.1 -** Os equipamentos a serem entregues devem estar em conformidade com as diretrizes RoHS;

**4.1.2 -** As unidades do equipamento deverão ser entregues devidamente acondicionadas em embalagens individuais adequadas, que utilizem, preferencialmente, materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e a armazenagem;

**4.1.3 -** A contratada para o fornecimento dos equipamentos, na qualidade de fabricante, importador, distribuidor ou comerciante, poderá ser solicitada a

providenciar o recolhimento e o adequado descarte do lixo tecnológico originário desta aquisição de equipamentos, entendido como aqueles produtos ou componentes eletrônicos em desuso e sujeitos a disposição final, para fins de sua destinação final ambientalmente adequada, conforme a lei 12.305/2010, artigo 33 caput, inciso VI e seus parágrafos;

**4.1.4 -** O modelo de equipamento ofertado deverá possuir a seguinte certificação: certificação emitida por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro, que ateste, conforme Instrução Normativa INMETRO nº 170/2012, a adequação em segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

**4.2 – DOS REQUISITOS DE GARANTIA**

**4.2.1 –** A garantia de funcionamento será pelo período de 24 (vinte e quatro) meses contados a partir do Recebimento Definitivo do componente, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

**4.2.1 –** Caso haja garantia adicional oferecida pelo fabricante, a Contratada deverá descrever os seus termos na Proposta Detalhada (anexo II).

**4.2.2 -** A garantia deve incluir todo e qualquer defeito decorrente de projeto, fabricação, construção, montagem, acondicionamento, transporte ou desgaste prematuro, com a substituição de peças, componentes, ajustes, reparos e correções necessárias, às expensas da contratada;

**4.2.3 -** O fornecedor não poderá, em hipótese alguma, negar-se a registrar chamadas relacionadas ao equipamento adquirido, ainda que se conclua, ao final, que a solução do incidente não seja de responsabilidade do fornecedor/fabricante;

**4.2.4 -** O prazo máximo para o primeiro atendimento dos chamados é de 02 (dois) dias úteis, contados a partir da abertura do chamado;

**4.2.5 -** O prazo máximo para a solução do problema é de 3 (três) dias úteis contados a partir do primeiro atendimento, mesmo incluindo a troca de peças e/ou componentes mecânicos ou eletrônicos;

**4.2.6 -** Em caso de substituição de peças e/ou componentes eletrônicos ou mecânicos, as peças substitutas deverão ser originais do fabricante e ter especificações iguais ou superiores às substituídas;

**4.2.7 -** As peças e componentes trocados deverão ser novos – não utilizados ou recondicionados;

**4.2.8 -** O primeiro atendimento dos chamados técnicos deverá ser presencial e feito nas dependências da sede do Tribunal Regional Eleitoral do Paraná (on site) em Curitiba, de segunda-feira a sexta-feira, no horário das 12h30m às 18h30m, por profissionais especializados:

**4.2.8.1 -** Quando não for possível a solução do problema no local, sendo necessária a remoção do equipamento, o conserto deverá ser efetivado nas dependências do laboratório da Contratada, ficando a mesma responsável pelo translado dos equipamentos e sua devolução em perfeitas condições de uso;

**4.2.9 -** A Contratada deverá manter, durante os 24 (vinte e quatro) meses de vigência da garantia, e às suas expensas, central de atendimento para abertura de chamados

técnicos pelo menos no horário das nove às dezoito horas, de segunda a sexta-feira. A central deverá ser acionada preferencialmente por e-mail. Será aceita também a disponibilização de canal para abertura de chamados técnicos por meio de serviço web da contratada;

**4.2.10 -** Na abertura do chamado técnico, a Contratada deverá fornecer um número de registro único para cada chamado;

**4.2.11 -** Considerar-se-á como recebida a solicitação de abertura do chamado técnico após o envio do e-mail (levando em consideração a data e hora do envio do e-mail) ou da abertura da ocorrência/ordem de serviço no serviço web da contratada (este último deve gerar um protocolo de atendimento com as informações de número da ordem de serviço, descrição do pedido de suporte e data e hora da abertura do chamado técnico);

**4.2.12 -** A contratada deverá entregar, obrigatoriamente, para o fiscal setorial da contratação ao final de todo atendimento realizado um laudo contendo, no mínimo, as seguintes informações:

a) Data e hora da abertura do chamado;
b) Número de registro do chamado;
c) Número do patrimônio TRE-PR do equipamento envolvido;
d) Número de série do equipamento envolvido;
e) Data e hora da chegada do técnico no local de atendimento para o primeiro atendimento;
f) Data e hora da resolução do problema, se aplicável;
g) Procedimentos realizados;
h) No caso de substituição de peças, a descrição do componente substituído.

**4.2.12.1 -** A contratada deverá encaminhar para o gestor da garantia técnica, através do e-mail rede@tre-pr.jus.br, no prazo máximo de 24 (vinte e quatro) horas após a realização dos atendimentos, uma cópia do laudo deixado com o fiscal da contratação ao final de cada visita técnica.

**4.2.13 -** A Contratada deverá encaminhar mensalmente, até o 5º (quinto) dia útil do mês subsequente, relatório de todos os chamados técnicos, atendidos ou não, realizados em sua central de atendimento no mês anterior. O relatório deverá conter, pelo menos, as seguintes informações:

a) Data e hora da abertura dos chamados;
b) Número de registro dos chamados;
c) Número do patrimônio TRE-PR dos equipamentos envolvidos;
d) Número de série dos equipamentos envolvidos;
e) Data e hora da chegada do técnico nos locais de atendimento;
f) Data e hora das resoluções dos problemas, quando aplicável;
g) No caso de substituição de peças, a descrição dos componentes substituídos.

**4.2.14 -** Caso constatado, durante a vigência do contrato, repetidos defeitos em um mesmo componente dentro do lote dos equipamentos adquiridos, principalmente na placa principal, disco rígido ou fonte de alimentação, relacionados à pré-existência de algum vício de conhecimento superveniente à data de sua aquisição, a Contratada será, a critério da Contratante, obrigada a trocar o componente de todos os equipamentos fornecidos;

**4.2.15 -** A contratada deverá, durante a vigência do contrato, prestar todas as informações solicitadas pelos gestores, esclarecendo dúvidas, inclusive, dando todo

o suporte necessário no que tange a levantamentos e estudos referentes ao objeto da contratação, no prazo máximo de 05 (cinco) dias úteis.

**4.2.16** - A instituição poderá promover, a qualquer tempo, diligência para checar a veracidade das informações prestadas pela contratada e ainda verificar por amostragem a confrontação do detalhamento das especificações técnicas do Termo de Referência com os equipamentos recebidos.

**4.2.16.1** – Constatada alguma irregularidade, a qualquer tempo, a contratada deverá saná-la no prazo máximo de 05 (cinco) dias úteis.

**4.3 – OUTRAS OBRIGAÇÕES**

**4.3.1 –** Todos os equipamentos a serem entregues deverão ser idênticos.

**4.3.2 -** Todas as funcionalidades e/ou licenciamentos descritos para os itens 1, 2 e 3 deste pregão deverão estar licenciados no modelo perpétuo, mantendo as funcionalidades descritas em operação de forma independente da vigência do contrato de garantia dos equipamentos;

**4.3.3 -** A Contratada fornecedora do equipamento deve garantir que todos os componentes do produto são novos (sem uso, reforma ou recondicionamento) e que não estarão fora de linha de fabricação durante a validade do registro de preço. Será permitida a oferta de equipamentos comprovadamente similares, pelo mesmo preço, no caso de indisponibilidade do originalmente proposto, ficando à critério da contratante o aceite ou não do equipamento ofertado.

**4.3.4 -** Todos os cabos e conectores externos necessários ao funcionamento dos equipamentos deverão ser fornecidos com comprimento de 1,5m (um metro e cinquenta centímetros). Os cabos de conexão do equipamento à rede elétrica deverão seguir o padrão NBR-14136;

**4.3.5 -** Para todos os itens de especificação serão aceitas ofertas de qualquer componente de especificação diferente da solicitada, desde que comprovadamente igual ou superior, individualmente, quanto à qualidade, o desempenho, a operacionalidade, a ergonomia ou a facilidade no manuseio do originalmente especificado – conforme o caso, e desde que não cause, direta ou indiretamente, incompatibilidade com qualquer das demais especificações, ou desvantagem nestes mesmos atributos dos demais componentes ofertados.

**4.3.6 -** É de responsabilidade da Contratada o perfeito fornecimento do objeto, devendo ser de primeira qualidade, obedecendo à garantia legal e às demais normas do Código de Defesa do Consumidor.

**4.3.7** – Apresentar a comprovação dos critérios informados nos itens 2.3.1.2.1 subitem 44, 2.3.2.1.1 subitem 52, 2.3.3.1.1 subitem 35 e item 4.1.4, todos contidos neste Termo de Referência.

**4.3.8 -** Manter durante toda a execução do contrato, as obrigações assumidas na licitação

## 5 – DAS DISPOSIÇÕES GERAIS

**5.1** - Os throughputs, capacidade de encaminhamento de informações para esta solução, devem ser comprovados por documento de domínio público do fabricante.

**5.2 -** Dúvidas poderão ser sanadas com a Seção de Rede, por meio do telefone (041) 3330-8628 no horário compreendido entre as 12h e as 19h ou pelo e-mail rede@tre-pr.jus.br