



PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL  
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF  
Telefone: (61) 3424-3936 - <https://www.iti.gov.br>

## LICITAÇÃO: ANEXO Nº I - REQUISITOS TECNOLÓGICOS/2020/COTIC/CGPOA

Processo nº 00100.001416/2020-79

Interessado: @interessados\_virgula\_espaco@

### ANEXO I - REQUISITOS TECNOLÓGICOS

#### 1. INTRODUÇÃO

- 1.1. Este documento consiste no descritivo técnico do Termo de Referência (SEI 0454065), item 4.7 - Requisitos Tecnológicos.

#### GRUPO 1 - SOLUÇÃO DE FIREWALL

#### 2. ITENS 1 E 2 - FIREWALLS (PERFIS 1 E 2)

##### Requisitos Gerais

- 2.1. A solução deverá ser dimensionada para operar no ambiente com os seguintes parâmetros:
- 2.1.1. 400 usuários simultâneos na instituição;
- 2.1.2. 2 dispositivos por usuário, sendo 1 em rede sem fios (ex.: 1 desktop e 1 tablet por pessoa);
- 2.1.3. Ocupar, no máximo, 2 unidades de *rack* (2Us).
- 2.2. As funcionalidades deverão ser disponíveis integralmente para os usuários e dispositivos do dimensionamento acima. Ou seja, é proibida a entrega de funcionalidades com atendimento parcial (Ex.: módulo "ABC" que atenda até 10 usuários, em vez dos 400 descritos acima);
- 2.3. Os equipamentos devem ter seu licenciamento completo e perpétuo;
- 2.3.1. No caso de funcionalidades que são comercializadas unicamente na modalidade de assinatura, o tempo da subscrição será o mesmo da garantia junto ao fabricante, contatos juntamente com os prazos do *hardware*.
- 2.4. Os equipamentos serão entregues com todos os *tranceivers*, conectorização, trilhos e demais componentes necessários para a instalação física nos *racks* e conectividade na infraestrutura de rede do ITI.
- 2.5. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia e que estejam em modo *End of Life* no ato da assinatura da ata de registro de preços, não deixando de

atender à vigência da garantia.

2.5.1. Se o equipamento ofertado não atenda a este requisito, será aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos do edital.

2.5.2. O fabricante do equipamento proposto deve possuir avaliação(ões) publicada(s) entre os anos de 2017 a 2019 pela NSS Labs, confirmando taxa de bloqueio de ataques ("efetividade de segurança") mínima de 95% (noventa e cinco por cento).

2.6. Todo e qualquer componente externo da solução (ex.: ferramenta de gerência, centralizador de *logs*, gerador de relatórios, sensor, etc) necessário para o atendimento dos requisitos técnicos deverá ser compatível com o *hypervisor VMWare*;

2.6.1. Caso haja necessidade de licenciamentos quaisquer diversos aos citados acima, como sistema gerenciador de bancos de dados (Ex.: MS SQL, Oracle), sistema operacional (Windows Server, Suse Linux, Red Hat) ou outro tipo de dependência que enseje custos, deverão ser entregues pelo fornecedor como parte da solução.

2.7. O fornecedor entregará 2 instâncias de gerenciamento de firewall, sendo:

2.7.1. Uma para o ambiente interno do ITI, com localização física dos equipamentos em 2 sites em Brasília;

2.7.2. Uma para o ambiente de assinaturas avançadas, com localização física dos equipamentos em Brasília e em Florianópolis;

### **Características físicas**

2.8. 1 interface console RJ45

2.9. Para o firewall perfil 1 (item 1):

2.9.1. No mínimo, 8 interfaces x 10/100/1000 BaseT

2.9.2. No mínimo, 2 interfaces 10G SFP+ (10G Base-SR, conectorização tipo LC);

2.10. Para o firewall perfil 2 (item 2):

2.10.1. No mínimo, 8 interfaces x 10/100/1000 BaseT;

2.11. Ao menos duas interfaces USB que podem ser utilizadas como:

2.11.1. Acesso *failover* por Modem USB;

2.11.2. Interface de *setup* inicial do *Firewall*.

2.11.3. Caso o equipamento conte com apenas uma interface USB, deverá haver disponibilidade de ao menos mais uma interface de comunicação no padrão RJ-45 para acesso de gerenciamento.

2.12. Deve ser instalado pela contratada em bastidor padrão de 19", com tamanho máximo de 1 RU e acompanhado dos respectivos Kit's de fixação.

2.12.1. A instalação consiste na colocação dos equipamentos em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos, e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de tecnologia da informação do contratante, incluindo: instalação física, conexão, configuração e integração, aplicação de licenças e atualização de firmware, se necessário;

2.12.2. A instalação abrange a aplicação das políticas definidas no serviço de configuração da solução de firewall, disponível no módulo de gerenciamento da solução, preferencialmente por meio do padrão *Zero Touch Deploy*;

- 2.12.3. A contratada deverá garantir os equipamentos, componentes, acessórios, *transceivers* e cabos de conexão (elétricos e lógicos) necessários para interligar fisicamente todos os componentes.
- 2.13. Fonte 100–240VAC, 50–60 Hz; e
- 2.14. Tomada padrão brasileiro.

## Características funcionais

A solução deve:

### Firewall

- 2.15. Suportar configurações de multi-WAN, permitindo, ao menos, 4 conexões externas com a internet simultaneamente;
- 2.16. Operar com interfaces em modo de failover;
- 2.17. Funcionalidade de failover para um modem USB diretamente conectado;
- 2.18. Configuração de um modem USB como uma interface a ser utilizada em *Failover* de WAN;
- 2.19. Interfaces externas configuradas em modo Round Robin, com pesos configuráveis;
- 2.20. Interfaces externas configuradas com a funcionalidade de “*overflow*”, permitindo o uso de links externos secundários quando o principal for excedido;
- 2.21. Realizar agregação de links (802.3ad);
- 2.22. Detecção de falha de links;
- 2.23. Suportar balanceamento de *links*;
- 2.24. Controle de banda por usuário, grupo de usuários, políticas e protocolo;
- 2.25. Controle de banda por interface;
- 2.26. Controle de banda por endereço de IP e VLAN;
- 2.27. Consumo de banda e cota de tempo por usuário;
- 2.28. Suportar sua implementação como Rounting Mode; Drop-In Mode (mesmo endereço IP em todas as interfaces) e em Transparent Bridge Mode;
- 2.29. Suportar:
  - 2.29.1. NAT estático e dinâmico;
  - 2.29.2. NAT 1:1;
  - 2.29.3. PAT;
  - 2.29.4. IPSec NAT Traversal; e
  - 2.29.5. NAT baseado em política.
- 2.30. Operar em modo de alta-disponibilidade, podendo atuar como ATIVO-PASSIVO e ATIVO-ATIVO;
- 2.31. Capacidade de fazer *load balancing* entre pelo menos 10 servidores internos com pesos distintos;
- 2.32. Suportar IPv6 nativamente;

- 2.33. Possuir capacidade de atuar como um roteador multicast para encaminhamento de tráfego multicast da origem até os destinos dentro da rede;
- 2.34. Suportar a detecção e mitigação de flood UDP;
- 2.35. Possuir mecanismo *antispoofing*;
- 2.36. Detectar e bloquear, no mínimo:
  - 2.36.1. *IP spoofing*
  - 2.36.2. *SYN flood*
  - 2.36.3. *UDP flood*
  - 2.36.4. *Port scanning*
  - 2.36.5. *ICMP flood*
  - 2.36.6. *ICMP sweep*
- 2.37. Suportar configuração de quatro zonas de segurança, sendo externa, privada, opcional (DMZ) e customizada.
- 2.38. Suportar endereçamento IP estático e dinâmico;
- 2.39. Possuir funcionalidades de DHCP relay que permitam a adição de servidores DHCP simultâneos.
- 2.40. Permitir DHCPv6 em interfaces externas.
- 2.41. Possuir no firewall de perfil 1:
  - 2.41.1. Throughput de 15 Gbps para firewall;
  - 2.41.2. Throughput de 4 Gbps para IPS;
  - 2.41.3. Throughput de 3 Gbps para UTM (combinando AV, VPN, firewall, Web Filter com *deep inspection*, antispam e IPS);
  - 2.41.4. Suportar 3.500.000 conexões simultâneas;
  - 2.41.5. Suportar um mínimo de 300 VLANs;
- 2.42. Possuir no firewall de perfil 2:
  - 2.42.1. Throughput de 8 Gbps para firewall;
  - 2.42.2. Throughput de 2 Gbps para IPS;
  - 2.42.3. Throughput de 1,5 Gbps para UTM (combinando AV, VPN, firewall, Web Filter com *deep inspection*, antispam e IPS);
  - 2.42.4. Suportar 2.000.000 conexões simultâneas;
  - 2.42.5. Suportar um mínimo de 200 VLANs;
- 2.43. O equipamento de firewall deve possuir, no mínimo, funcionalidades de: firewall, filtro de conteúdo, controle de URL, controle de aplicação, *intrusion prevention system* (IPS), antivírus de rede, controle de ameaças avançadas, antispam/phishing, SD-WAN e geração de relatórios;
  - 2.43.1. Caso haja alguma funcionalidade não disponibilizada nativamente pelo *appliance*, o licitante deverá disponibilizar a ferramenta complementar do mesmo fabricante;
- 2.44. Implementar políticas de segurança na camada de aplicação;
- 2.45. Possuir políticas na camada de aplicação pré-configuradas com proteção padrão para suportar os seguintes protocolos com inspeção de *malware*:

- 2.45.1. HTTP / HTTPS;
- 2.45.2. POP3 / POP3S;
- 2.45.3. IMAP / IMAPS;
- 2.45.4. SMTP / SMTPS;
- 2.45.5. FTP;
- 2.45.6. DNS;
- 2.45.7. SIP; e
- 2.45.8. H.323.
- 2.46. Suportar autenticação via RADIUS, SecureID, LDAP e Active Directory;
- 2.47. Suportar autenticação transparente de usuários (Single Sign On) de AD e RADIUS;
- 2.48. Suportar a configuração de regras de proxy explícito para aceitar solicitações de clientes e buscar informação em nome dos clientes;
- 2.49. Ter funcionalidade de proxy SMTP para analisar documentos com macros embutidas e o equipamento também deve possuir uma opção para remover estes macros antes de enviar o documento para seus destinatários;
- 2.50. Suportar certificados digitais autoassinados (*self-signed*) para executar *deep inspection* de pacotes via proxy SMTP sobre TLS;
- 2.51. Executar *deep content inspection* de dados em proxy HTTPS;
- 2.52. Limitar o acesso de usuários a contas Google pessoais;
- 2.53. Definir o intervalo de tempo entre tentativas de login incorretas em conexões FTP;
- 2.54. Possuir a funcionalidade de NTP server;
- 2.55. Detectar regras conflitantes;
- 2.56. Suportar DNS dinâmico dos seguintes provedores, como:
  - 2.56.1. DynDNS.org
  - 2.56.2. No-IP.com
  - 2.56.3. dynu.com
  - 2.56.4. duckdns.org
- 2.57. Possuir defesas de ataques fragmentados, permitindo que o firewall monte os pacotes fragmentados antes de encaminhá-los a redes internas;
- 2.58. Conseguir filtrar conteúdo nos protocolos mais comuns, assim como filtrar conteúdo tipo "MIME";
- 2.59. Proteger e-mails internos contra open relay. Ele deve ser capaz e ser configurado para domínios de e-mail aceitos no ambiente;
- 2.60. Permitir a configuração de limites para detecção de ataques de flood e Denial of Service (DoS) além de distributed denial of service (DDoS);
- 2.61. Suportar Protocol Anomaly Detection (PAD) para DNS e outros tipos de protocolos;
- 2.62. Suportar Server Name Indication (SNI) para configurar domínios para funcionalidades de bloqueio, inspeção ou permissão;

- 2.63. Complementar capacidades e bloqueio de CN existentes com SNI com a finalidade de bloquear domínios específicos do Google;
- 2.64. Suportar bloqueio e gerenciamento de tráfego por domínios especificados por FQDNs (Fully Qualified Domain Names) a fim de bloquear sites disponibilizados por Content Delivery Networks (CDNs);
- 2.65. Suportar o bloqueio de domínios através de *wildcard*;
- 2.66. Permitir a criação de políticas por IP utilizando *wildcard*;
- 2.67. Suportar o a configuração por política de bloqueio de conexões *inbound* e *outbound* para um país (ou conjunto de países);
- 2.68. O equipamento de firewall deve oferecer integração a mecanismos de Autenticação Forte de Múltiplo Fator (MFA) através do Protocolo Radius para as formas de VPN suportadas, sendo no mínimo SSL VPN (cliente), através da implementação PAP, L2TP (clientless) através da implementação MSCHAPv2 e IKEv2 (clientless) através da implementação EAP-MSCHAPv2;
- 2.69. O Fabricante da solução deve disponibilizar uma plataforma de abertura de chamados para suporte sem limite de número de chamados enquanto o licenciamento do dispositivo estiver válido;
- 2.70. O Fabricante deve possuir estoque de RMA dentro do Brasil a fim de agilizar a entrega de produtos em caso de falha/quebra;
- 2.71. O equipamento de firewall deve aplicar políticas granulares para restringir o tráfego de países considerados arriscados de acordo com a política de segurança da empresa contratante de acordo com o tipo de tráfego, porta, protocolo, endereço, usuário ou grupo de origem assim como destino;
- 2.72. O equipamento de firewall deve permitir outros tipos de tráfego que não ofereçam ameaças semelhantes, como DNS ou Mail para / de países que tenham certos protocolos bloqueados quando considerados perigosos pela política de segurança da empresa;
- 2.73. Permitir que o administrador de rede realize uma configuração em modo “offline” para posteriormente ser injetada ao firewall;
- 2.74. Possuir ferramenta de diagnóstico de tráfego de rede, tipo *tcpdump*;
- 2.75. Efetuar captura e *download* de pacotes no formato PCAP;
- 2.76. Suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e/ou aplicações (por exemplo, Youtube e WhatsApp);
- 2.77. A solução deve suportar *single sign-on* (SSO) para soluções RADIUS;
- 2.78. A solução deve rastrear as sessões de usuários via SSO para RADIUS;
- 2.79. A solução deve suportar o download e alteração de diferentes versões de configuração para equipamentos, possibilitando utilizar a mesma configuração para hardwares distintos e versões de SO distintas;
- 2.80. A solução deve suportar SSO redundantes;
- 2.81. Gerenciar via linha comando através de porta serial e via SSH;
- 2.82. Suportar *single sign-on* para logins via RDP.
- 2.83. Suportar via SSO diversos usuários em uma única máquina para sistemas operacionais Windows;
- 2.84. Deve suportar VPN Mobile;
- 2.85. Suportar pelo menos 250 VPNs Mobile usando IPSec;

- 2.86. Suportar ao menos 250 usuários mobile usando VPN SSL;
- 2.87. Ser compatível com clientes SSL para Windows 7, 8, 10, Mac OS, Android e iOS;
- 2.88. Suportar VPN *site-to-site*;
- 2.89. Deve suportar pelo menos 100 VPNs entre *sites* utilizando IPSec;
- 2.90. Suportar interações com outros produtos e marcas que suportem o padrão IPSec;
- 2.91. A solução deve suportar os seguintes métodos de autenticação:
  - 2.91.1. DES;
  - 2.91.2. AES 128;
  - 2.91.3. AES 192; e
  - 2.91.4. AES 256.
- 2.92. A solução deve suportar os seguintes métodos de criptografia:
  - 2.92.1. SHA-2;
  - 2.92.2. MD5;
  - 2.92.3. IKE Pre-Shared Key;
  - 2.92.4. 3rd Party Cert; e
  - 2.92.5. AES with CBC and GCM.
- 2.93. Deve suportar Dead Peer Detection (DPD);
- 2.94. Deve suportar VPN *site-to-site* e *client-to-site* com IKEv2;
- 2.95. Deve suportar Perfect Forward Secrecy (PFS) com chaves Diffie-Hellman (ou Diffie-Hellman-Merkle) em pacotes web e email;
- 2.96. Realizar VPN Failover (reestabelecer a VPN através de um segundo link em caso de falha do link primário);
- 2.97. Suportar VPN IPSEC com um throughput igual ou maior que 1 Gbps;
- 2.98. Permitir criar interfaces virtuais para VPNs e rotear tráfego utilizando VPNs *site-to-site* com protocolos de roteamento dinâmico;
- 2.99. A solução deve permitir visualizar estatísticas de VPN em interfaces virtuais, gateways e tunnel types para qualquer tipo de usuário;
- 2.100. Deve permitir visualizar mensagens de diagnóstico de VPN para ajudar a remediar e realizar o *troubleshooting* pelos administradores do sistema;
- 2.101. A solução deve suportar tuneis VPN *site-to-site* estáticos (políticas) e dinâmicas (roteadas) para *Microsoft Azure* e *AWS*; e
- 2.102. A solução deve suportar VPN em interfaces virtuais e realizar Failover entre elas.

### Web Filter

- 2.103. Ter a funcionalidade de filtro de conteúdo Web e de URL com licenciamento incluso;
- 2.104. Permitir que o filtro trabalhe por categorias, ajustado por grupos de usuário e possuir um mínimo de 120 categorias;
- 2.105. Permitir exceções no filtro de conteúdo por meio de whitelist;

- 2.106. Apresentar ao usuário uma tela de aviso indicando que a categoria do website acessado não está de acordo com as políticas da empresa, permitindo ao mesmo seguir adiante após clicar em um “aceite”;
- 2.107. Suportar customização da mensagem de bloqueio;
- 2.108. Suportar uma base de dados atualizada dinamicamente localizada na nuvem ou disponível em uma solução de máquina virtual compatível com VMWare;
- 2.109. Filtrar conteúdo em múltiplas línguas, incluindo mas não limitado a: português, inglês, alemão, espanhol, japonês, chinês tradicional e simplificado;
- 2.110. Identificar e bloquear mais de 1000 aplicações diferentes, incluindo controle granular de aplicação, como telas de login e metodologias específicas de transferência de arquivo;
- 2.111. Suportar *updates* automáticos de assinaturas de aplicação;
- 2.112. Ter capacidade de atualização *offline* de suas assinaturas de aplicação;
- 2.113. Reconhecer pelo menos as seguintes aplicações:
  - 2.113.1. active directory;
  - 2.113.2. appletalk echo;
  - 2.113.3. bittorrent;
  - 2.113.4. 4shared;
  - 2.113.5. cs game;
  - 2.113.6. call of duty;
  - 2.113.7. citrix;
  - 2.113.8. db2
  - 2.113.9. diablo3;
  - 2.113.10. dropbox;
  - 2.113.11. edonkey;
  - 2.113.12. evernote;
  - 2.113.13. emule;
  - 2.113.14. facebook;
  - 2.113.15. facebook chat;
  - 2.113.16. google drive;
  - 2.113.17. google-docs;
  - 2.113.18. gnutella;
  - 2.113.19. gmail;
  - 2.113.20. gmail chat;
  - 2.113.21. http-proxy;
  - 2.113.22. http-tunnel;
  - 2.113.23. skype;
  - 2.113.24. linked-in;
  - 2.113.25. logme in;



2.113.26. ms-rdp;  
2.113.27. mysql;  
2.113.28. msft-store;  
2.113.29. netflix;  
2.113.30. spotify;  
2.113.31. skydrive;  
2.113.32. teamviewer;  
2.113.33. twitter;  
2.113.34. vnc;  
2.113.35. youtube;  
2.113.36. oracle;  
2.113.37. kerberos;  
2.113.38. ldap;  
2.113.39. radius;  
2.113.40. itunes;  
2.113.41. dhcp;  
2.113.42. ftp;  
2.113.43. dns;  
2.113.44. wins;  
2.113.45. msrpc;  
2.113.46. ntp;  
2.113.47. snmp;  
2.113.48. rpc over http;  
2.113.49. gotomeeting;  
2.113.50. twitch.tv;  
2.113.51. vevo;  
2.113.52. webex;  
2.113.53. winamp;  
2.113.54. zoom;  
2.113.55. sftp;  
2.113.56. sql-net;  
2.113.57. vmnet;  
2.113.58. quic;  
2.113.59. cisco tdp;  
2.113.60. openvpn;  
2.113.61. tinyvpn;

- 2.113.62. dotvpn;
- 2.113.63. tor;
- 2.113.64. yammer;
- 2.113.65. fortnite;
- 2.113.66. LoL;
- 2.113.67. second life;
- 2.113.68. netscout;
- 2.113.69. whatsapp;
- 2.113.70. telegram;
- 2.113.71. klogin.
- 2.114. Suportar validação de URL com *content filtering*;
- 2.115. Disponibilizar bases de dados de *blacklists* do fabricante;
- 2.116. Bloquear tráfego vindo de IPs maliciosos reconhecidos por base de dados de blacklists disponíveis no mercado (no mínimo, a do próprio fabricante).
- 2.117. Bloquear tráfego de botnets reconhecidas por base de dados de blacklist disponíveis no mercado (no mínimo, a do próprio fabricante);
- 2.118. Suportar a filtro de aplicação no próprio hardware da solução através de subscrição inclusa por tempo integral da garantia; e
- 2.119. Suportar a configuração de exceções para filtro de aplicação.

## Antivírus

- 2.120. Ter a funcionalidade de antivírus de borda com licenciamento incluso;
- 2.121. Receber atualizações de assinaturas de antivírus automaticamente;
- 2.122. Permitir o acesso a *updates* de assinatura de manualmente e instalar estas assinaturas a partir de um ambiente *offline*;
- 2.123. Suportar a opção de quarentena para e-mails recebidos
- 2.124. Suportar *whitelists* para e-mails a fim de receber mensagens de domínios confiáveis em seu ambiente
- 2.125. Ter a capacidade de detectar e bloquear *malwares* diversos, como: spyware, *Potentially Unwanted Programs* (PUPs), trojans, bots e backdoors;
- 2.126. Ser capaz de escanear todos os arquivos comprimidos (.zip, .tar, .rar, .gzip) com pelo menos 3 níveis de compressão;
- 2.127. Ser capaz de tratar arquivos criptografados;
- 2.128. Suportar os pelo menos os protocolos: HTTP, FTP, SMTP, POP3;
- 2.129. Possuir pontuação de reputação para cada URL/IP acessado;
- 2.130. Permitir o *by-pass* da varredura do AV, com base na pontuação;
- 2.131. Permitir o bloqueio de endereços com reputação baixa devido a histórico de vírus e/ou outros tipos de *malware*. O score deve ser estipulado baseado em informação recebida por repositório do

fabricante;

- 2.132. Possuir engine de antivírus;
- 2.133. Possuir um engine de análise heurística avançada;
- 2.134. Possuir um engine de AV de inteligência artificial;
- 2.135. Desenvolver perfis de arquivos maliciosos e benignos. Esses perfis incluem comportamentos e características de arquivos para fornecer uma visão abrangente da ameaça em potencial;
- 2.136. Avaliar a ameaça em potencial;
- 2.137. Identificar uma ameaça, e bloquear o *malware* automaticamente, impedindo que a carga mal-intencionada entre em sua rede.

### Antispam

- 2.138. Ter a funcionalidade de Antispam com licenciamento incluso;
- 2.139. Possuir capacidades de Anti-Spam ativadas a partir de uma assinatura adicional no mesmo hardware, ou solução do mesmo fabricante que seja integrável com o *firewall*;
- 2.140. Trabalhar com tecnologia de anti-spam baseada em Recurrent Pattern Detection (RPD) ou similar;
- 2.141. Possuir em sua solução de anti-spam uma opção de quarentena;
- 2.142. Ser capaz de bloquear mensagens com links maliciosos;
- 2.143. Ter integração entre análise de antivírus e anti-spam (detecção e surto de vírus);
- 2.144. Possuir capacidade para bloquear spam em idiomas estrangeiros;
- 2.145. Possuir capacidade para bloquear spam baseado em texto;
- 2.146. Identificar e bloquear *e-mails* falsificados (*email spoofing*);
- 2.147. Ter integração com MS Exchange 2019 e Exchange Online (Azure);
- 2.148. Ser compatível com Zimbra.

### IPS

- 2.149. Ter a funcionalidade de IPS com licenciamento incluso;
- 2.150. Receber atualizações automáticas de assinaturas de IPS
- 2.151. Oferecer suporte para o IPS conduzir análises na camada de aplicação, definir o nível de severidade do ataque e gerar alarmes remotos para notificações de eventos
- 2.152. Oferecer suporte para bloqueio automático de fontes conhecidas de ataque
- 2.153. Suportar todos os principais protocolos: HTTP, FTP, SMTP, POP3, IMAP
- 2.154. Oferecer suporte para acessar atualizações de assinatura e, manualmente, instalar assinaturas em modo *offline*;
- 2.155. Possuir a capacidade de realizar os escaneamentos em modo FAST SCAN e FULL SCAN
- 2.156. Permitir que cada ameaça de IPS seja tratada de forma específica, de acordo com seu nível de ameaça;
- 2.157. Prevenir, no mínimo, os seguintes ataques:
  - 2.157.1. *SQL injection*;

- 2.157.2. Cross-site scripting (XSS);
- 2.157.3. Travessia de diretórios (*directory traversal*);
- 2.157.4. Execução remota de código;
- 2.157.5. *Portscans*;
- 2.157.6. *Exploits*;
- 2.157.7. *Backdoors*;
- 2.157.8. *Spoofing*;
- 2.157.9. *Flooding*;
- 2.157.10. Tráfego mal formado;
- 2.157.11. Cabeçalhos inválidos de protocolos;
- 2.157.12. Elevação de privilégios;
- 2.157.13. *Local File Inclusion*;
- 2.157.14. Buffer overflows;
- 2.157.15. Evasão de IPS:
  - 2.157.15.1. *IP Packet Fragmentation*;
  - 2.157.15.2. *Stream Segmentation*;
  - 2.157.15.3. *RPC Fragmentation*;
  - 2.157.15.4. *URL Obfuscation*;
  - 2.157.15.5. *HTML Obfuscation*;
  - 2.157.15.6. *Payload Encoding*;
  - 2.157.15.7. *FTP Evasion*; e
  - 2.157.15.8. *Layered Evasions*.
- 2.158. Permitir desativar a análise de ataques a partir de endereços/faixa de IP específicos; e
- 2.159. Permitir desativar a análise de assinaturas e protocolos.

## DLP

- 2.160. Suportar recursos de prevenção contra perda de dados (DLP)
- 2.161. Oferecer suporte DLP para iniciativas de conformidade com PCI, HIPAA e GDPR;
- 2.162. Suportar regras predefinidas de DLP para números de identidade nacionais/internacionais, dados de cartão de crédito, dados de endereço, informações pessoais identificáveis (PII) e informações sobre saúde;
- 2.163. Fornecer regras predefinidas de DLP para o Brasil;
- 2.164. Suportar atualizações de assinatura de DLP e/ou a instalação manual de assinaturas de DLP em modo *offline*;
- 2.165. Funcionar em conjunto com as demais ferramentas da solução, para mitigar ameaças.

## APT

- 2.166. Ter recurso de detecção de ameaças persistentes avançadas (APT);

- 2.167. Suportar emulação completa de sistema para detectar *malware* avançado durante o tempo de execução da execução em uma Next Generation Sandbox na nuvem para, no mínimo, 25 artefatos simultâneos;
- 2.168. Suportar APT para todos os executáveis de Windows, zip, PDF, objeto do Microsoft Office, Mac OS, Javascript e tipos de arquivo APK do Android;
- 2.169. Fornecer relatórios detalhados com análises acionáveis que identificam um arquivo como *malware*;
- 2.170. Incluir uma lista sumária de indicadores de ameaças que informam porque o arquivo foi bloqueado como *malware*.

### Firewall de DNS e Phishing

- 2.171. Ter a funcionalidade de Firewall de DNS e proteção contra *phishing* com licenciamento incluso;
- 2.172. Fornecer proteção anti-malware de blacklists de domínios por firewall de DNS
- 2.173. Fornecer filtro de conteúdo a nível de domínio
- 2.174. Prover detalhes de contexto da ameaça em cada alerta
- 2.175. Proteger o ambiente de ameaças de comando e controle e outras conexões maliciosas;
- 2.176. Utilizar bases de inteligência da solução para otimizar a proteção;
- 2.177. Permitir a comunicação individualizada e personalizada entre a vítima do ataque e o fornecedor do sistema de análise de ameaças
- 2.178. Fornecer relatórios com dados detalhados e análise aprofundada identificando o arquivo como malware

### Access Portal

- 2.179. Permitir que administradores realizem o suporte de implementação e acesso centralizado à aplicações na nuvem e recursos internos via RDP e SSH, com integração com soluções de SSO;
- 2.180. Habilitar a funcionalidade de Access Portal no mesmo hardware através de licenciamento adicional incluso;
- 2.181. Incluir no suporte a SAML no Access Portal para a integração com SSO e provedores de MFA, que atuem como identity provider (IDP);
- 2.182. Integrar a autenticação do Access Portal com mecanismos de autenticação do firewall, incluindo RADIUS

### SD-WAN

- 2.183. Ter a funcionalidade de SD-WAN com licenciamento incluso;
- 2.184. Suportar roteamento baseado por política de SD-WAN, permitindo que administradores especifiquem parâmetros para definir por qual interface certo tipo de tráfego será enviado.
- 2.185. Permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se a mesma for MPLS, internet, 4G/LTE, entre outras;
- 2.186. Ser compatível com o componente de da solução, permitindo que suas características e análises sejam realizadas nas VPNs assim como em links WAN;

- 2.187. Conter mecanismo de detecção de melhor circuito de roteamento (algoritmos de melhor caminho);
- 2.188. Possuir roteamento Baseado em Políticas e múltiplas saídas (e tipos de saídas) WANs;
- 2.189. Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem;
- 2.190. Ser configurada para realizar *failover* entre links principais e secundários caso os links utilizados ultrapassem os limites previamente definidos de *jitter*, latência e perda de pacotes;
- 2.191. Deve verificar *jitter*, latência e perda de pacotes de cada link externo com endereços distintos na internet;
- 2.192. Ser configurável via implantação *Zero-Touch Deploy*;
- 2.193. Ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico;
- 2.194. Realizar o gerenciamento de tráfego por tipo de aplicação;
- 2.195. A solução de SD-WAN UTM deve suportar atualizações automáticas de endereço IP via serviço de DNS Dinâmico
- 2.196. Suportar o monitoramento de link com *ping*, TCP e DNS;
- 2.197. Suportar o monitoramento de links VPN; e
- 2.198. Permitir a exportação de informações via Netflow.

## Gerenciamento

- 2.199. A solução será entregue com sua ferramenta de gerência de firewalls com licenciamento incluso.
- 2.199.1. Haverão duas instâncias licenciadas de gerência apartadas a serem providas pela contratada: uma com 4 firewalls do perfil 1, outra com 2 equipamentos de cada perfil.
- 2.200. Prover administração em tempo real de, no mínimo, 4 firewalls, inclusive de modelos diferentes do fabricante, através de uma única interface de gerência;
- 2.201. Suportar monitoramento em tempo real de logs de tráfego, alarmes, eventos, diagnósticos e estatísticas;
- 2.202. Enviar diversos alertas via SNMP ou email;
- 2.203. Permitir o uso de NAT para conexões via *gateway* de aplicação SNMP;
- 2.204. Permitir ser gerenciado através de múltiplos computadores simultaneamente;
- 2.205. Permitir a criação de templates para configurações de VPN;
- 2.206. Permitir a criação de templates para configurações compartilhadas entre firewalls de diversos locais remotos;
- 2.207. Suportar o agendamento para a aplicação de configurações compartilhadas de um ou diversos *firewalls* simultaneamente;
- 2.208. Suportar a função de *rollback* para configurações anteriores;
- 2.209. Permitir a edição de políticas através de Windows GUI, interface Web e CLI;
- 2.210. Suportar a configuração de acessos distintos para administradores
- 2.211. Suportar gerenciamento via Web Browser ou via cliente;
- 2.212. Suportar comparação de versões de configurações;

2.213. Possuir a capacidade de criação de políticas de firewall;

### **Relatórios e logs**

2.214. A solução será entregue com licenciamento de sua ferramenta de gerência de gráficos e geração de relatórios, do tipo *virtual appliance*, incluso.

2.215. Possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário;

2.216. Permitir a implementação de servidores externos ao firewall para centralizar os logs e relatórios;

2.217. A solução de armazenamento de logs e relatórios não deve ter custo adicional;

2.218. Permitir o envio de logs para, no mínimo, 2 servidores simultaneamente;

2.219. Criptografar a transmissão dos logs sem que seja necessária a criação de uma VPN para tal;

2.220. A solução de logs e relatórios deve possuir ao menos 90 relatórios pré-configurados, sem qualquer custo adicional;

2.221. Suportar a extração de relatórios no formato de PDF e CSV;

2.222. Possuir relatórios:

2.222.1. Executivo;

2.222.2. de *compliance* com padrões internacionais como HIPAA, PCI e GDPR;

2.222.3. de ameaças;

2.222.4. maiores consumidores de aplicações web;

2.222.5. ativos em exposição (representação de quais ativos representam maior risco na rede)

2.223. Gerar relatórios contendo dados do ultimo dia, semana ou mês, automaticamente e envia-los por e-mail e FTP

2.224. Permitir em seu dashboard o pivotamento ou aprofundamento para maiores detalhes dos logs;

2.225. Suportar o envio de todos os relatórios por e-mail para períodos específicos

2.226. Suportar acessos distintos de administração e somente leitura para acessos a logs da solução;

2.227. Ser compatível com solução VMWare;

2.228. Indicar os tipos de trafego passando pelo firewall em layout gráfico;

2.229. Prover uma visão de mapa mundi, indicando a origem e destino do trafego de aplicação, pacotes negados e eventos de ameaças (no mínimo IPS e conexões);

2.230. Possuir relatórios de IPS que detalhem as informações e CVE de cada ameaça;

2.231. Suportar a agregação de diversos firewalls a fim de criar relatórios unificados da solução;

2.232. Suportar eventos de SSO;

2.233. Apresentar os FQDNs de clientes do Firewall em relatórios por usuário;

2.234. Possuir dashboard para bloqueio de IPs de origens de ataques;

2.235. Possuir um dashboard indicando o uso de cada política, inclusive informando as políticas não utilizadas no firewall;

2.236. Possuir um *dashboard* indicando geograficamente o fluxo do tráfego do firewall, políticas acionadas assim como o IP de origem e destino do tráfego.

### 3. ITEM 3 - SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE FIREWALL (POR SITE)

3.1. Configurar a ferramenta de gerência em ambiente VMWare, preparando para aceitar os ativos da solução;

3.2. Aplicar e tornar disponíveis as políticas a serem sincronizadas com os *firewalls* da solução;

3.3. Disponibilizar acesso à contratante;

3.4. Habilitar e disponibilizar perfil de leitura e geração de relatórios gerenciais da solução;

3.5. Integrar a solução com os serviços de diretório e autenticação da CONTRATANTE;

3.6. Aplicar, no mínimo, as políticas de segurança na CONTRATANTE pertinentes ao equipamento:

3.6.1. Firewall;

3.6.2. Antispam/Antiphishing;

3.6.3. Antivírus de rede;

3.6.4. VPN;

3.6.5. Filtros de conteúdos (*web filter, app control, etc*);

3.6.6. Logs.

3.6.7. IPS;

3.6.8. APT;

3.6.9. *Firewall* de DNS;

3.6.10. Relatórios; e

3.6.11. Demais incluídas na solução.

3.7. Caso a funcionalidade ainda não exista no ambiente da CONTRATANTE, a CONTRATADA deverá estabelecer uma linha de base, a partir de regras de monitoramento (ex.: utilização do IPS em modo de detecção), antes da efetivação das regras para bloqueio;

3.8. A CONTRATADA deverá apoiar a contratante na instalação, reinstalação, configuração ou reconfiguração dos módulos adquiridos/contratados a qualquer tempo durante a garantia da solução.

#### Treinamento para os *firewalls*

3.9. Oferecer treinamento para operacionalização dos *firewalls* (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.

3.10. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.

3.11. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.

3.12. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.



#### 4. ITEM 4 - TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE FIREWALL

- 4.1. O treinamento oficial do fabricante será de, no mínimo, 40 horas, em português.
- 4.2. O treinamento será realizado preferencialmente no modelo presencial, em instalações providas pela CONTRATADA.
- 4.3. Os treinamentos só serão aceitos na modalidade à distância se:
  - 4.3.1. Por impossibilidade logística devido à pandemia de COVID-19;
  - 4.3.2. Por interesse e oportunidade da Administração.
- 4.4. Deve ser ministrado por profissional certificado pelo fabricante dos equipamentos como instrutor.
- 4.5. A ementa do curso deve abranger conteúdos que vão desde instalação, configuração, gerenciamento, operação a *troubleshooting* dos equipamentos de hardware e de softwares que compõem a solução de redes sem fios.
- 4.6. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.
- 4.7. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus à contratante.
- 4.8. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento.
- 4.9. Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.
- 4.10. Caso não haja disponibilidade para realização em Brasília, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.
- 4.11. Deverá ser fornecido certificado de conclusão oficial do fabricante da solução aos participantes.

#### GRUPO 2 - SOLUÇÃO DE REDES

#### 5. ITEM 5 - SISTEMA DE GERENCIAMENTO E CONTROLE DE ACESSO DE REDES SEM FIOS E CABEADAS

##### Requisitos Gerais

- 5.1. A solução deverá ser dimensionada para operar no ambiente com os seguintes parâmetros:
  - 5.1.1. A solução deverá operar para atender simultaneamente 400 usuários na instituição, sendo mandatória a solução permitir a autenticação destes usuários simultâneos, fornecendo, caso necessário, licenças para este processo de autenticação, conforme especificações do mecanismo de controle de acesso;
  - 5.1.2. *Access points* devem ter funcionalidade de gerenciar outros *access points*, trabalhando em modo auto controlado (*cluster*);

- 5.1.3. Licenciamento contemplando o quantitativo mínimo de 100 (cem) dispositivos de rede, por meio de licença para autenticação de usuários no servidor TACACS+ interno;
- 5.2. O(s) sistema(s) de gerência e controle de acesso da rede sem fio deverão atender as especificações, a exemplo de, e não limitado a: serviço de autenticação, ferramenta de relatórios, software de gestão e inventário de ativos, sistema de prevenção de intrusões em redes sem fios (Wireless Intrusion Prevention System - WIPS). Caso necessário, a fim de atender aos requisitos, poderá o fornecedor entregar controladora física ou virtual.
- 5.2.1. Os equipamentos devem ter seu licenciamento completo e perpétuo;
- 5.2.2. Os eventuais módulos adicionais providos para o atendimento das especificações técnicas serão do mesmo fabricante, por questão de integração e compatibilidade completa da solução.
- 5.2.3. As licenças entregues deverão ser bidirecionais sempre que aplicável. Ou seja, caso haja necessidade de que o fornecedor entregue a licença "ABC" na controladora e a "XYZ" no *access point* para o funcionamento adequado da funcionalidade, ambas serão entregues.
- 5.3. A gerência da rede wireless será provida na forma de solução virtualizada (*virtual appliance*), compatível com o *hypervisor* VMWare;
- 5.4. As funcionalidades deverão ser disponíveis integralmente para os usuários e dispositivos do dimensionamento acima. Ou seja, é proibida a entrega de funcionalidades com atendimento parcial (Ex.: módulo "ABC" que atenda até 10 usuários, em vez dos 400 descritos acima);
- 5.5. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia e que estejam em modo *End of Life* no ato da assinatura da ata de registro de preços, não deixando de atender à vigência da garantia.
- 5.5.1. Se o equipamento ofertado não atenda a este requisito, será aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos do edital.
- 5.6. Todo e qualquer componente da solução (ex.: ferramenta de gerência, centralizador de *logs*, gerador de relatórios, sensor, etc) necessário para o atendimento dos requisitos técnicos deverá ser compatível com o *hypervisor* VMWare;
- 5.6.1. Caso haja necessidade de licenciamentos quaisquer diversos aos citados acima, como sistema gerenciador de bancos de dados (Ex.: MS SQL, Oracle), sistema operacional (Windows Server, Suse Linux, Red Hat) ou outro tipo de dependência que enseje custos, deverão ser entregues pelo fornecedor como parte da solução.

### **Análise de perfil de dispositivo**

- 5.7. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 5.8. Deve categorizar os dispositivos em pelo menos 3 níveis:
- 5.8.1. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);
- 5.8.2. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);
- 5.8.3. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);
- 5.9. Deve ser capaz de gerar gráficos das categorias separando os dispositivos conforme suas características;
- 5.10. Deve suportar a coleta de informações, para classificação, usando no mínimo:
- 5.10.1. DHCP;

- 5.10.2. HTTP User-Agent;
- 5.10.3. MAC OUI;
- 5.10.4. ActiveSync plugin;
- 5.10.5. SNMP;
- 5.10.6. Subnet Scanner;
- 5.10.7. IF-MAP;
- 5.10.8. MDM;
- 5.10.9. TCP Fingerprinting.
- 5.11. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;
- 5.12. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 5.13. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:
  - 5.13.1. Agente proprietário;
  - 5.13.2. HTTP User-Agent;
  - 5.13.3. SNMP;
  - 5.13.4. DHCP;
  - 5.13.5. MAC OUI.
- 5.14. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

#### **Controle de acesso de dispositivos e usuários**

- 5.15. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:
  - 5.15.1. Microsoft Active Directory;
  - 5.15.2. Diretórios LDAP;
  - 5.15.3. PostgreSQL;
  - 5.15.4. MSSQL;
  - 5.15.5. Servidores de Token;
  - 5.15.6. Lista interna estática de hosts.
- 5.16. Deve suportar "Single Sign-on" (SSO) através de SAML;
- 5.17. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
  - 5.17.1. Atributos do usuário autenticado;
  - 5.17.2. Hora do dia, dia da semana;
  - 5.17.3. Tipo de dispositivo utilizado;
  - 5.17.4. Localização do usuário;

- 5.17.5. Tipo de autenticação utilizada.
- 5.18. Deve permitir a visualização de todas informações relativas a cada transação e autenticação, a solução deverá trazer no mínimo as seguintes informações:
  - 5.18.1. Data e Hora;
  - 5.18.2. Mac Address do dispositivo;
  - 5.18.3. Classificação do dispositivo;
  - 5.18.4. Usuário;
  - 5.18.5. Método de autenticação utilizado;
  - 5.18.6. Fonte de autenticação utilizada para validação;
  - 5.18.7. Perfil de acesso aplicado;
  - 5.18.8. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);
  - 5.18.9. Informações de resposta da solução para o elemento de rede;
  - 5.18.10. Alertas em caso de falha;
- 5.19. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:
  - 5.19.1. Lista com últimos Alertas do sistema;
  - 5.19.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Autenticações Web;
  - 5.19.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;
  - 5.19.4. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;
  - 5.19.5. Últimas falhas de autenticação;
  - 5.19.6. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:
    - 5.19.6.1. Saudáveis (dentro das políticas estabelecidas);
    - 5.19.6.2. Não saudáveis (que estão fora das políticas estabelecidas);
  - 5.19.7. Lista com as últimas autenticações;
  - 5.19.8. Lista com as últimas autenticações com sucesso;
  - 5.19.9. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;
- 5.20. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;
- 5.21. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 5.22. Deve suportar autenticações via OAuth2 e Facebook;
- 5.23. Deve possuir, no mínimo, recursos integrados de AAA: RADIUS e TACACS+;
- 5.24. Deve possuir suporte aos seguintes recursos:
  - 5.24.1. RADIUS;
  - 5.24.2. RADIUS CoA;

- 5.24.3. TACACS+;
- 5.24.4. Web authentication;
- 5.24.5. SAML;
- 5.24.6. EAP-TLS;
- 5.24.7. MAC address authentication (dispositivos sem suporte a 801X);
- 5.25. Deve suportar verificação de vulnerabilidade através de varredura de portas;
- 5.26. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;
- 5.27. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
- 5.28. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;
- 5.29. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- 5.30. Deve possuir suporte a administração através de IPv6;
- 5.31. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;
- 5.32. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
- 5.33. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
- 5.34. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;
- 5.35. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha.

### **Software de gerência/controladora WLAN**

- 5.36. Solução local (*appliance virtual*), responsável pelas seguintes funções na rede sem fio: administração, configuração e gerenciamento completo centralizado dos pontos de acesso *wifi* também descritos na solução.
- 5.37. A controladora/ software de gerência deverá ser do mesmo fabricante do ponto de acesso a fim de garantir uma perfeita interoperabilidade.
- 5.38. Seja por meio da controladora ou por meio do software de gerenciamento, deve ser fornecida solução que comporte o gerenciamento de no mínimo 50 (cinquenta) pontos de acesso e gerenciar no mínimo 800 (oitocentos) usuários simultâneos.
- 5.39. Deverá ser fornecido o licenciamento para gerenciamento de 20 pontos de acesso, conforme quantitativo de Access points exigidos;
- 5.40. Caso a licitante esteja fornecendo controladora, e seja necessária uma expansão futura das capacidade da controladora WLAN (física ou virtual), o licenciamento para gerenciamento dos pontos de acesso deverá ser reaproveitado, adicionando a diferença de licença dos novos quantitativos exigidos de pontos de acesso e licenciamento/troca de hardware para comportar o aumento de capacidade de gerenciamento das controladoras.

- 5.41. Oferecer recursos de mobilidade entre VLANs para *roaming* de camada 2;
- 5.42. Implementar *roaming* (deslocamento) baseado nos protocolos IEEE 802.11r, 802.11k e 802.11v;
- 5.43. A Controladora WLAN poderá estar diretamente e/ou remotamente conectada aos Ponto de Acesso Sem Fio por ela gerenciadas, inclusive via roteamento nível 3 da camada OSI;
- 5.44. Se a Controladora WLAN falhar, os *access points* relacionados deverão se associar a uma Controladora WLAN alternativa de forma automática, não permitindo que a rede sem fio se torne inoperante;
- 5.45. Deve realizar o *upgrade* de *softwares* dos pontos de acesso *wifi*.
- 5.46. Deve implementar agendamento automático de upgrades de firmware dos Access Points (APs).
- 5.47. Deve efetuar backups automáticos das configurações e arquivos.
- 5.48. Deve disponibilizar uma console de gerenciamento web acessível através de protocolo HTTPS, compatível com os principais browsers do mercado (Firefox e Chrome).

#### **Requisitos de autenticação de usuários e visitantes (captive portal)**

- 5.49. Caso seja necessário componente externo à controladora, ele deverá ser baseado nas mesmas características de virtualização e licenciamento descritas acima, devendo ser do mesmo fabricante da solução ofertada;
- 5.50. Deve ser capaz de ocultar o rótulo de identificação (SSID) de redes;
- 5.51. Deve permitir a limitação de banda para uma rede;
- 5.52. Deve disponibilizar pelo menos 03 (três) níveis de acesso à Console de Gerenciamento Web, sendo:
  - 5.52.1. Administrador: acesso de leitura e escrita às configurações para o gerenciamento do sistema.
  - 5.52.2. Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações.
  - 5.52.3. Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede Wi-Fi.
- 5.53. Deve permitir a criação de múltiplas redes distintas e segregadas, mas administradas na mesma console.
- 5.54. Deve permitir que as contas de usuários visitantes sejam armazenadas internamente na solução, não havendo necessidade de criação de usuários temporários em bases externas;
- 5.55. Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA;
  - 5.55.1. Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes.
  - 5.55.2. Este mecanismo deve permitir ainda que o cliente visitante crie a sua própria conta de usuário, cuja validação deve ser realizada por meio de mensagem a ser enviada ao visitante durante o cadastro.
  - 5.55.3. No caso de a solução gerar um usuário e/ou senha automaticamente, estes dados devem ser informados ao visitante através de e-mail, SMS, ou captive portal.

- 5.55.4. Todo o processo deve ser realizado sem a intervenção do administrador da solução que controla a solução wireless (self-service).
- 5.56. Deve possuir captive portal web de autenticação do tipo splash page.
- 5.56.1. Caso não haja possibilidade de integração, serão aceitas soluções integradas com outros softwares de acesso, do mesmo fabricante, sem custos extras ao ITI.
- 5.57. A solução deve suportar no mínimo os seguintes métodos de autenticação:
  - 5.57.1. WEP
  - 5.57.2. WPA
  - 5.57.3. WPA2-PSK
  - 5.57.4. WPA2-Enterprise with 802.1X
  - 5.57.5. WPA3
  - 5.57.6. EAP-TLS
  - 5.57.7. Autenticação por *MAC address* (para dispositivos não compatíveis com o padrão 802.1x).
- 5.58. Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;
- 5.59. Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de *sponsorship*;
- 5.60. Deve permitir o gerenciamento das credenciais de visitantes;
- 5.61. Deve permitir a configuração de contas de usuários visitantes com prazo de validade e largura de banda;
- 5.62. Deve realizar o caching de endereço MAC dos usuários visitantes;
- 5.63. Deve permitir o login automático de usuários que realizem o auto-registro;
- 5.64. Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;
- 5.65. Deve permitir a criação de token de acesso;
- 5.66. Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;
- 5.67. Deve permitir autenticação através de social login nativa na solução;
- 5.68. Implantar o padrão 802.1x.
- 5.69. A ferramenta deverá fornecer servidor RADIUS e servidor TACACS+ para o serviço de AAA;
- 5.70. A ferramenta deverá implementar mecanismos de análise de dispositivos, caracterizando o tipo do dispositivo e infraestrutura com critérios pre definidos (device fingerprint);

#### **Requisitos de gerenciamento e controle de acesso do ambiente**

- 5.71. A controladora deve permitir a visualização de um conjunto de informações de análise dos Access Points que fazem parte da rede wireless, disponibilizando pelo menos as seguintes informações:
  - 5.71.1. Relação dos Access Points conectados, disponibilizando no mínimo as informações de Nome, MAC Address, Modelo de equipamento e endereço IP.
  - 5.71.2. Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;

- 5.71.3. Quantidade de dispositivos conectados em cada Access Point, volume de dados utilizado, tempo de disponibilidade e SSIDs.
- 5.71.4. Localização dos Access Points em planta baixa inserida no sistema, incorporando informações sobre os equipamentos gerenciados.
- 5.72. Deve dispor de alarmes e eventos acerca das configurações dos pontos de acesso para auditoria;
- 5.73. Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede wireless, disponibilizando pelo menos os dados abaixo especificados:
  - 5.73.1. Endereço IP, MAC Address, Hostname, Usuário;
  - 5.73.2. Sistema Operacional do dispositivo utilizado;
  - 5.73.3. Tempo de conexão;
  - 5.73.4. Informação do SSID e Ponto de Acesso utilizados;
  - 5.73.5. Gráficos ou Dados de utilização dos Usuários;
  - 5.73.6. Últimos alertas do sistema;
  - 5.73.7. Informações de destinos acessados.
- 5.74. Deve possibilitar o agrupamento dos Access Point suportando a criação e o gerenciamento de grupos de Access Point simultâneos.
- 5.75. Deve guardar os logs por um período de no mínimo 3 (três) meses ou suportar envio dos logs no formato Syslog;
- 5.76. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- 5.77. Possuir suporte a MIB II, conforme RFC 1213.

## 6. ITEM 6 - SISTEMA DE GERENCIAMENTO E CONTROLE DE ACESSO DE REDES CABEADAS

### Requisitos Gerais

- 6.1. A solução deverá ser dimensionada para operar no ambiente com os seguintes parâmetros:
  - 6.1.1. A solução deverá operar para atender simultaneamente 20 (vinte) usuários na instituição, sendo mandatória a solução permitir a autenticação destes usuários simultâneos, fornecendo, caso necessário, licenças para este processo de autenticação, conforme especificações do mecanismo de controle de acesso;
  - 6.1.2. Licenciamento contemplando o quantitativo mínimo de 30 (trinta) dispositivos de rede, por meio de licença para autenticação de usuários no servidor TACACS+ interno;
- 6.2. O(s) sistema(s) de gerência e controle de acesso da rede sem fio deverão atender as especificações, a exemplo de, e não limitado a: serviço de autenticação, ferramenta de relatórios, software de gestão e inventário de ativos, sistema de controle de acesso a redes. Caso necessário, a fim de atender aos requisitos, poderá o fornecedor entregar controladora física ou virtual.
  - 6.2.1. Os equipamentos devem ter seu licenciamento completo e perpétuo;



- 6.2.2. Os eventuais módulos adicionais providos para o atendimento das especificações técnicas serão do mesmo fabricante, por questão de integração e compatibilidade completa da solução.
- 6.2.3. As licenças entregues deverão ser bidirecionais sempre que aplicável. Ou seja, caso haja necessidade de que o fornecedor entregue a licença "ABC" na controladora e a "XYZ" no *access point* para o funcionamento adequado da funcionalidade, ambas serão entregues.
- 6.3. A gerência da rede wireless será provida na forma de solução virtualizada (*virtual appliance*), compatível com o *hypervisor* VMWare;
- 6.4. As funcionalidades deverão ser disponíveis integralmente para os usuários e dispositivos do dimensionamento acima. Ou seja, é proibida a entrega de funcionalidades com atendimento parcial (Ex.: módulo "ABC" que atenda até 10 usuários, em vez dos 400 descritos acima);
- 6.5. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia e que estejam em modo *End of Life* no ato da assinatura da ata de registro de preços, não deixando de atender à vigência da garantia.
- 6.5.1. Se o equipamento ofertado não atenda a este requisito, será aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos do edital.
- 6.6. Todo e qualquer componente da solução (ex.: ferramenta de gerência, centralizador de *logs*, gerador de relatórios, sensor, etc) necessário para o atendimento dos requisitos técnicos deverá ser compatível com o *hypervisor* VMWare;
- 6.6.1. Caso haja necessidade de licenciamentos quaisquer diversos aos citados acima, como sistema gerenciador de bancos de dados (Ex.: MS SQL, Oracle), sistema operacional (Windows Server, Suse Linux, Red Hat) ou outro tipo de dependência que enseje custos, deverão ser entregues pelo fornecedor como parte da solução.

### **Análise de perfil de dispositivo**

- 6.7. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 6.8. Deve categorizar os dispositivos em pelo menos 3 níveis:
- 6.8.1. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);
- 6.8.2. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);
- 6.8.3. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);
- 6.9. Deve ser capaz de gerar gráficos das categorias separando os dispositivos conforme suas características;
- 6.10. Deve suportar a coleta de informações, para classificação, usando no mínimo:
- 6.10.1. DHCP;
- 6.10.2. HTTP User-Agent;
- 6.10.3. MAC OUI;
- 6.10.4. ActiveSync plugin;
- 6.10.5. SNMP;
- 6.10.6. Subnet Scanner;
- 6.10.7. IF-MAP;

- 6.10.8. MDM;
- 6.10.9. TCP Fingerprinting.
- 6.11. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;
- 6.12. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 6.13. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:
  - 6.13.1. Agente proprietário;
  - 6.13.2. HTTP User-Agent;
  - 6.13.3. SNMP;
  - 6.13.4. DHCP;
  - 6.13.5. MAC OUI.
- 6.14. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

#### **Controle de acesso de dispositivos e usuários**

- 6.15. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:
  - 6.15.1. Microsoft Active Directory;
  - 6.15.2. Diretórios LDAP;
  - 6.15.3. PostgreSQL;
  - 6.15.4. MSSQL;
  - 6.15.5. Servidores de Token;
  - 6.15.6. Lista interna estática de hosts.
- 6.16. Deve suportar "Single Sign-on" (SSO) através de SAML;
- 6.17. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
  - 6.17.1. Atributos do usuário autenticado;
  - 6.17.2. Hora do dia, dia da semana;
  - 6.17.3. Tipo de dispositivo utilizado;
  - 6.17.4. Localização do usuário;
  - 6.17.5. Tipo de autenticação utilizada.
- 6.18. Deve permitir a visualização de todas informações relativas a cada transação e autenticação, a solução deverá trazer no mínimo as seguintes informações:
  - 6.18.1. Data e Hora;
  - 6.18.2. Mac Address do dispositivo;
  - 6.18.3. Classificação do dispositivo;

- 6.18.4. Usuário;
- 6.18.5. Método de autenticação utilizado;
- 6.18.6. Fonte de autenticação utilizada para validação;
- 6.18.7. Perfil de acesso aplicado;
- 6.18.8. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);
- 6.18.9. Informações de resposta da solução para o elemento de rede;
- 6.18.10. Alertas em caso de falha;
- 6.19. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:
  - 6.19.1. Lista com últimos Alertas do sistema;
  - 6.19.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Autenticações Web;
  - 6.19.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;
  - 6.19.4. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;
  - 6.19.5. Últimas falhas de autenticação;
  - 6.19.6. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:
    - 6.19.6.1. Saudáveis (dentro das políticas estabelecidas);
    - 6.19.6.2. Não saudáveis (que estão fora das políticas estabelecidas);
  - 6.19.7. Lista com as últimas autenticações;
  - 6.19.8. Lista com as últimas autenticações com sucesso;
  - 6.19.9. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;
- 6.20. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;
- 6.21. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 6.22. Deve suportar autenticações via OAuth2 e Facebook;
- 6.23. Deve possuir, no mínimo, recursos integrados de AAA: RADIUS e TACACS+;
- 6.24. Deve possuir suporte aos seguintes recursos:
  - 6.24.1. RADIUS;
  - 6.24.2. RADIUS CoA;
  - 6.24.3. TACACS+;
  - 6.24.4. Web authentication;
  - 6.24.5. SAML;
  - 6.24.6. EAP-TLS;
  - 6.24.7. MAC address authentication (dispositivos sem suporte a 801X);
- 6.25. Deve suportar verificação de vulnerabilidade através de varredura de portas;

- 6.26. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;
- 6.27. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
- 6.28. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;
- 6.29. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- 6.30. Deve possuir suporte a administração através de IPv6;
- 6.31. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;
- 6.32. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
- 6.33. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
- 6.34. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;
- 6.35. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha.

## 7. **ITEM 7 - ACCESS POINT**

- 7.1. Deve implementar, no mínimo, as tecnologias 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax, compatíveis as frequências de rádio 2,4Ghz e 5Ghz com irradiação omnidirecional, com as seguintes características:
  - 7.1.1. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;
  - 7.1.2. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
  - 7.1.3. 802.11n (2.4GHz): 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)
  - 7.1.4. 802.11n (5GHz): 6.5 to 600 (MCS0 to MVC31, HT20 to HT40)
  - 7.1.5. IEEE 802.11ac: 6,5 a 860 Mbps (MCS0 a MCS9, NSS=1 a 2 e VHT20 a VHT80);
  - 7.1.6. 802.11ax: 3,6 a 570 Mbps em 2,4 GHz;
  - 7.1.7. 802.11ax: 3.6 a 4,803 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160)
  - 7.1.8. Deve possuir integração ZIGBEE e rádio bluetooth BLE 5.0 para utilização em serviços de localização com maior precisão. Não se faz necessária a entrega do software de localização, ficando a cargo da infraestrutura a compatibilidade e recurso disponíveis para futuras aquisições de software;
- 7.2. Implementar DFS (Dynamic Frequency Selection) para otimização do espectro de rádio frequência;
- 7.3. Implementar TWT (Target Wake Time);
- 7.4. Deverá conter todas as licenças necessárias para utilização conjunta das funcionalidades descritas na controladora, como: firewall, WIPS, autenticação, gerenciamento, relatórios e quaisquer outras

para atendimento pleno dos requisitos da solução;

- 7.5. Deverão ser fornecidos pontos de acesso Wi-Fi idênticos, novos e sem uso anterior;
- 7.6. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta;
- 7.7. Deve ser apresentado certificado válido fornecido pela Wi-Fi Alliance na categoria Wi-Fi CERTIFIED 6 na data do pregão contendo, no mínimo, as funcionalidades:
  - 7.7.1. DL OFDMA;
  - 7.7.2. UL OFDMA;
  - 7.7.3. DL MU-MIMO; e
  - 7.7.4. Target Wake Time (TWT).
- 7.8. A configuração dos seus parâmetros operacionais, o gerenciamento das políticas de segurança e de radiofrequência devem ser gerenciadas pela solução;
- 7.9. Deve possuir garantia de no mínimo 60 (sessenta) meses, pelo fabricante ou CONTRATADA.
- 7.10. Deve possibilitar a fixação do equipamento em teto e parede. Devem ser fornecidos todos os acessórios necessários para que possa ser feita a fixação.
- 7.11. Não deve haver restrição de licença que limite o número de usuários por Ponto de Acesso.
- 7.12. O modelo do equipamento ofertado deve possuir, na data da entrega da proposta, homologação junto à ANATEL.
- 7.13. Deve possuir no mínimo 01 (uma) porta Ethernet 2.5 multigigabit Ethernet BASE-T autosense, UTP RJ45;
- 7.14. Deve permitir ser alimentado através da tecnologia PoE.
  - 7.14.1. Caso o aparelho seja compatível apenas com o padrão PoE+, a contratada deverá fornecer, sem custos adicionais, todos os recursos para o perfeito funcionamento do aparelho, como: injetores compatíveis com o modelo do *access point* ofertado (bivolt), cabos de força e de dados Cat6a e adaptadores.
- 7.15. Deverá ser fornecida e instalada a versão mais recente do software interno do ponto de acesso Wi-Fi.
- 7.16. Deve possuir captive portal web de autenticação do tipo splash page local ou em conjunto com a ferramenta de gerência.
- 7.17. Deve implementar recursos de *firewall*.
- 7.18. Deve suportar, no mínimo, 200 usuários conectados/autenticados por rádio.
- 7.19. Deve localmente ou em conjuntos com a solução de controladora wireless, implementar análise de espectro de RF em 2.4GHz e 5GHz para identificação de outros pontos de acesso intrusos e não autorizados (rogues), além de interferências no canal habilitado no ponto de acesso e nos demais canais configurados na rede Wi-Fi. A análise de espectro deve ser realizada de forma simultânea ao atendimento dos clientes do ponto de acesso, sem que estes sejam desconectados.
- 7.20. Deve localmente ou em conjunto com a solução de controladora wireless, realizar o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.
- 7.21. Ajustar automaticamente os canais 802.11 e realizar a detecção de interferências e reajustar os parâmetros de Rádio Frequência visando evitar problemas de cobertura e performance.
- 7.22. Deve permitir, simultaneamente, usuários configurados, no mínimo, nos padrões IEEE 802.11a, 802.11n, 801.11ac e 802.11ax;

- 7.23. Deve operar nas frequências de 2.4GHz e 5GHz;
- 7.24. Deve Operar com DFS (802.11h) e OFDMA;
- 7.25. Deve implementar protocolo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).
- 7.26. Ser compatível com os padrões WMM e 802.1p para priorização de tráfego.
- 7.27. Deve possuir capacidade para operação em modo "repetidor", permitindo a comunicação entre pontos de acesso Wi-Fi sem a necessidade de cabeamento adicional permitindo desta forma o atendimento de usuários em locais isolados da localidade.
- 7.28. Deve possuir cliente DHCP, para configuração automática do endereço IP.
- 7.29. Deve permitir a conexão à rede de usuários em IPv4, IPv6 e suportar dual-stack (clientes IPv4 e IPv6 no mesmo ponto de acesso Wi-Fi).
- 7.30. Deve possuir a capacidade de criação de no mínimo 12 (doze) SSIDs.
- 7.31. Permitir habilitar e desabilitar a divulgação do SSID.
- 7.32. Deverá possuir mecanismo de rádio com suporte à MIMO 4x4, com 4 *Spatial Streams*, no mínimo para o rádio de 5GHz;
- 7.33. Possuir LED's indicativos do estado de operação e da atividade do rádio;
- 7.34. O software interno e os arquivos de configuração devem ser armazenados em memória não-volátil, permitindo a sua atualização via solução de controladora wireless.
- 7.35. Permitir o uso do protocolo de autenticação IEEE 802.1X para no mínimo EAP-TLS e EAP-PEAP.
- 7.36. Deve ser compatível com WPA.
- 7.37. Deve implementar WPA2 com AES.
- 7.38. Deve ser compatível com o padrão IEEE 802.11i.
- 7.39. Deve implementar WPA3 Enterprise.
- 7.40. Deve permitir a implantação de VLANs segundo o padrão IEEE 802.1Q;
- 7.41. Deve permitir a configuração de no mínimo 8 (oito) VLANs.
- 7.42. Deve implementar a técnica de direcionamento de banda, permitindo que clientes com suporte a faixa de frequência de 5 GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5 GHz.
- 7.43. Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol) em modo cliente.
- 7.44. Deve implementar o envio de eventos por meio do protocolo Syslog.
- 7.45. Deve implementar controle de limite de uso de banda.

## **8. ITEM 8 - SERVIÇO DE CONFIGURAÇÃO DO SISTEMA DE GERENCIAMENTO E CONTROLE DE ACESSO DE REDES SEM FIOS E CABEADAS)**

- 8.1. A instalação será feita em qualquer um dos prédios de lotação da contratante em Brasília;
- 8.2. A contratada deverá executar Site Survey via software ou Indoor no prédio da contratante, conforme solicitação, podendo ser solicitada inspeção física do ambiente.

- 8.3. A instalação dos Ponto de Acesso Sem Fio deverá ser posterior a este Site Survey, apoiada por software adequado, que indique:
- 8.3.1. O melhor posicionamento dos dispositivos para a maximização da cobertura do sinal de radiofrequência nos espectros 802.11 a/b/g/n/ac/ax;
- 8.3.2. A quantidade exata de pontos de acesso a serem instalados por ambiente;
- 8.3.3. As zonas de interferência;
- 8.3.4. A frequência a ser utilizada por cada ponto de acesso;
- 8.3.5. As áreas de cobertura;
- 8.3.6. As taxas de transmissão ou faixas de níveis de recepção de sinal de RF em desenho colorido.
- 8.4. A potência mínima aceita para o dimensionamento do quantitativo de *access points* é de -65 dBm.
- 8.4.1. A instalação não será aceita se houver pontos de sombras ou com sinal fraco nas instalações da contratada.
- 8.5. A empresa licitante interessada deverá solicitar as plantas de referência do prédio para endereço eletrônico [cotic@iti.gov.br](mailto:cotic@iti.gov.br) e realizar *site survey* preditivo, a fim de estimar a qualidade do sinal e quantitativo de equipamentos propostos;
- 8.5.1. O *site survey* preditivo fará parte da proposta de preços para a solução de *wifi*, tendo o sinal mínimo de -65dBm;
- 8.5.2. Por questões de eventuais mudanças nos *layouts* das salas, a CONTRATADA deverá realizar novo levantamento durante o planejamento da implantação;
- 8.6. As atividades contempladas pelo serviço de instalação incluem: planejamento, instalação física e configuração lógica dos pontos de acesso e da controladora wireless;
- 8.7. Deverá ser elaborado pela contratada um plano de implantação contendo todo o detalhamento de implantação dos produtos;
- 8.8. O plano deverá contemplar o diagrama lógico da rede com todos os equipamentos envolvidos na solução e as configurações lógicas que serão realizadas em cada equipamento e software;
- 8.9. A CONTRATADA deverá criar e disponibilizar o cronograma das atividades para aprovação da CONTRATANTE;
- 8.10. Deverá configurar na contratada redes ao menos:
- 8.10.1. Rede para usuários internos, utilizando o algoritmo WPA2 com a base de autenticação ou certificados digitais, a critério da CONTRATANTE;
- 8.10.2. Rede para dispositivos corporativos, autenticado utilizando certificados digitais;
- 8.10.3. Rede para visitantes, utilizando cadastro do cidadão via registro local.
- 8.11. Configurar o portal de acesso (captive portal) de visitantes e elaborar manuais de utilização para o cadastrador de usuários e para o usuário final.
- 8.12. Para a rede cabeada, os equipamentos serão configurados e implantados para gerenciar os ativos corporativos mediante autenticação forte, postura (conformidade) com rede segregada para quarentena, 802.1x dos *switches*, habilitação dos dashboards de monitoramento, implantação do serviço TACACS da solução e da CA (se aplicável).

## Treinamento para o sistema de controle de acessos

8.13. Oferecer treinamento para operacionalização do sistema de controle de acesso para redes sem fios e cabeadas (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.

8.14. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.

8.15. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.

8.16. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

## **9. ITEM 9 - SERVIÇO DE CONFIGURAÇÃO DO SISTEMA DE GERENCIAMENTO E CONTROLE DE ACESSO DE REDES CABEADAS)**

9.1. Para a rede cabeada, os equipamentos serão configurados e implantados para gerenciar os ativos corporativos mediante autenticação forte, postura (conformidade) com rede segregada para quarentena, 802.1x dos *switches*, habilitação dos dashboards de monitoramento, implantação do serviço TACACS da solução e da CA (se aplicável).

### **Treinamento para o sistema de controle de acessos**

9.2. Oferecer treinamento para operacionalização do sistema de controle de acesso para redes sem fios e cabeadas (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.

9.3. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.

9.4. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.

9.5. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

## **10. ITEM 10 - TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE CONTROLE DE ACESSO**

10.1. O treinamento oficial do fabricante do sistema de controle de acesso (sem fios e cabeada) será de, no mínimo, 40 horas, em português.

10.2. O treinamento será realizado preferencialmente no modelo presencial, em instalações providas pela CONTRATADA.

10.3. Os treinamentos só serão aceitos na modalidade à distância se:

10.3.1. Por impossibilidade logística devido à pandemia de COVID-19;

10.3.2. Por interesse e oportunidade da Administração.



- 10.4. Deve ser ministrado por profissional certificado pelo fabricante dos equipamentos como instrutor.
- 10.5. A ementa do curso deve abranger conteúdos que vão desde instalação, configuração, gerenciamento, operação a *troubleshooting* dos equipamentos de hardware e de softwares que compõem a solução de redes sem fios.
- 10.6. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.
- 10.7. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus à CONTRATANTE.
- 10.8. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento.
- 10.9. Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.
- 10.10. Caso não haja disponibilidade para realização em Brasília, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.
- 10.11. Deverá ser fornecido certificado de conclusão oficial do fabricante da solução aos participantes.

## 11. ITEM 11 - SWITCHES CORE

### Características gerais

- 11.1. Deverão ser fornecidos 2 (dois) equipamentos para compor o *Cluster* da camada *core*;
- 11.2. Deve possuir no mínimo 48 portas 1/10GbE padrão SFP/SFP+;
- 11.2.1. Todas as portas óticas deverão conter *tranceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 11.3. Deve possuir no mínimo 4 portas 40 GbE padrão QSFP+;
- 11.3.1. Deve ser entregue com cabos do tipo DAC de no mínimo 1 metro de comprimento de 40Gbps de velocidade de conexão suficientes para todas as portas 40GbE dos equipamentos;
- 11.4. Caso a solução utilize KeepAlive, deve ser entregue com 01(um) cabo adicional do tipo DAC de no mínimo 3 metros de comprimento de 10Gbps de velocidade de conexão;
- 11.5. Qualquer que seja o equipamento ofertado, mesmo que este possua número superior de portas exigidas, deverá ter todas as portas de comunicação (downlink e uplink) habilitadas e licenciadas.
- 11.6. Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento.
- 11.7. A arquitetura deve permitir "Cluster" de Switches (par de switches) em que dois (02) switches interligados operem em conjunto.
- 11.8. Deve implementar a solução de MC-LAG (Multi Chassis Link Aggregation Group) ou tecnologia semelhante que possibilite funcionalidade idêntica, em que mesmo havendo conexões entre diferentes equipamentos pertencentes ao mesmo par de switches, seja disponibilizado somente um único caminho

lógico e agregado de comunicação, eliminando desta forma a necessidade do uso do protocolo STP (Spanning Tree Protocol).

- 11.8.1. Não serão aceitas soluções em condição de empilhamento ou em cascadeamento;
- 11.9. O par de switches deve operar em alta-disponibilidade e possibilitar o upgrade de software sem que haja a parada do ambiente, com a mudança de tráfego entre os switches, caso necessário;
- 11.10. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 11.11. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 11.12. Deverá ser fornecido um jogo de manuais originais dos equipamentos fornecidos, preferencialmente em língua portuguesa, contendo informações sobre as suas características técnicas, configurações, programação, montagem, instalação, manutenção, operação e gerenciamento de todas as funcionalidades fornecidas. Toda documentação dos equipamentos fornecidos será fornecida tanto na forma impressa como também em mídia digital, na forma de arquivos eletrônicos;
- 11.13. Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior;
- 11.14. Todas as versões de sistema operacional ou software armazenado no equipamento deverão ser fornecidos nos releases mais atualizados, adequadas às necessidades requeridas nesta especificação, fornecidas se disponíveis na mídia CD-ROM. Durante a vigência da garantia / suporte técnico será prevista a atualização do Sistema Operacional do equipamento dentro da mesma versão por outra mais atualizada visando manter o equipamento atualizado e livre de bugs, falhas de segurança etc;
- 11.15. Deverão ser fornecidos todos os softwares, cabos de força e lógicos, conectores, adaptadores, acessórios de fixação, necessários para o pleno funcionamento do equipamento;
- 11.16. Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante;
- 11.17. Todos os equipamentos e seus acessórios deverão estar na embalagem original do fabricante. Todos os acessórios básicos que acompanham os equipamentos deverão ser fornecidos;
- 11.18. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19";
- 11.19. Operar nas temperaturas de 0 a 40 °C;
- 11.20. Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima do chassi, e redundância n+1 instalada- 01(uma) fonte extra de redundância;

### **Desempenho**

- 11.21. Deve possuir capacidade de comutação de, no mínimo, 2 Tbps;
- 11.22. Deve possuir capacidade de encaminhamento de, no mínimo, 900 MPPS;

### **Disponibilidade**

- 11.23. Deve possuir interface de Console Serial ou USB;
- 11.24. Deve possuir uma porta para gerenciamento out-of-band com conector RJ-45;

11.25. Deve implementar 803ad Agregação de Links com mínimo de 54 grupos de 8 portas;

11.26. Deve possuir buffers de, no mínimo, 16MB;

### Switching

11.27. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

11.28. Deve implementar funcionalidade que permita a detecção de falhas de uplink;

11.29. Deve implementar, no mínimo, 4.000(quatro mil) VLANs, conforme padrão IEEE 801q;

11.30. Deve implementar os seguintes padrões IEEE 801D, 801W, 801S, 801P

11.31. Deve Implementar JUMBO FRAME (mínimo de 9k) em todas as interfaces Gigabit Ethernet

11.32. Tabela de endereços MAC com capacidade para no mínimo 80.000 endereços MAC;

11.33. Deve implementar LLDP (IEEE 801ab)

11.34. Deve implementar o padrão IEEE801AK

11.35. Deve implementar MRVP

11.36. Deve implementar PVST+, RPVST+ ou protocolo compatível;

11.37. Deve implementar MSTP (IEEE 801s) com suporte a 64 instâncias;

11.38. Suportar tabela para pelo menos 90.000 hosts IPV4 e 45.000 Hosts IPV6.

### Roteamento

11.39. Deve possuir tabela de roteamento com no mínimo 13.000 rotas IPv4 e 3.000 rotas IPv6;

11.40. Deve implementar roteamento estático;

11.41. Deve Implementar roteamento OSPFv2 e OSPFv3;

11.42. Deve implementar roteamento OSPFv2 NSSA;

11.43. Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro;

11.44. Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 8 grupos;

11.45. Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado;

11.46. Deve implementar BGP;

11.47. Deve implementar PRB (Policy Based Routing)

11.48. Deve implementar VRRP (Virtual Router Redundancy Protocol);

11.49. Deve implementar DHCP Client e DHCP Relay

11.50. Deve suportar VRF (Virtual Routing and Forwarding) até 3 VRFs Routing

11.51. Deve implementar VRF Ipv4 e Ipv6;

11.52. Deve implementar funcionalidade que especifica o número máximo de entradas no ARP;

11.53. Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de “down”

**Multicast**

- 11.54. Deve implementar PIM-SM;
- 11.55. Deve implementar IGMP nas versões v1 e v2 e Snooping
- 11.56. Deve implementar MLD Snooping;

**Software Defined Networking**

- 11.57. Deve possuir tecnologia que permite a separação do plano de dados (encaminhamento de pacotes) e do plano de controle;
- 11.58. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
- 11.59. Deve ser totalmente programável em REST API
- 11.60. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
- 11.61. Deve possuir interface REST API e scripting via Python;
- 11.62. Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta similar, podendo ser composto por hardware ou software adicional;

**QoS**

- 11.63. Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado;
- 11.64. Deve implementar rate-limiting;
- 11.65. Deve suportar espelhamento de portas;
- 11.66. Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ;
- 11.67. Deve suportar no mínimo, 8 (oito) filas de prioridade por porta.

**Segurança**

- 11.68. Deve implementar ACL's Ipv4 e Ipv6;
- 11.69. Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch;
- 11.70. Deve suportar RADIUS/TACACS+.

**Gerenciamento**

- 11.71. Deve suportar duas imagens de software na memória flash (IOS, Firmware);
- 11.72. Deve possuir capacidade de armazenar múltiplos arquivos de configuração;
- 11.73. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 11.74. Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração

- 11.75. Deve implementar SNMP v1, v2c e v3;
- 11.76. Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP
- 11.77. Deve suportar Self Signed Certificate Management
- 11.78. Deve suportar SSH v2
- 11.79. Deve Suportar AAA (TACACS+ & RADIUS)
- 11.80. Deve implementar CLI com gerência por meio de linhas de comando;

## 12. **ITEM 12 - SWITCH TOPO DE RACK 48 PORTAS**

### **Características gerais**

- 12.1. Deve possuir no mínimo 48 portas 1/10GbE padrão UTP Base-T;
- 12.2. Deve possuir no mínimo 4 portas 40 GbE padrão QSFP+;
- 12.2.1. Deve ser entregue com cabos do tipo DAC de no mínimo 3 metros de comprimento de 40Gbps de velocidade de conexão suficientes para todas as portas 40GbE dos equipamentos;
- 12.3. Qualquer que seja o equipamento ofertado, mesmo que este possua número superior de portas exigidas, deverá ter todas as portas de comunicação (downlink e uplink) habilitadas e licenciadas.
- 12.4. Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento
- 12.5. A arquitetura deve permitir "Cluster" de Switches (par de switches) em que dois (02) switches interligados operem em conjunto. Deve implementar a solução de MC-LAG (Multi Chassis Link Aggregation Group) ou tecnologia semelhante que possibilite funcionalidade idêntica, em que mesmo havendo conexões entre diferentes equipamentos pertencentes ao mesmo par de switches, seja disponibilizado somente um único caminho lógico e agregado de comunicação, eliminando desta forma a necessidade do uso do protocolo STP (Spanning Tree Protocol). Não serão aceitas soluções em condição de empilhamento ou em cascadeamento;
- 12.6. Caso opere em cluster, deverá o par de switches operar em alta-disponibilidade e possibilitar o upgrade de software sem que haja a parada do ambiente, com a mudança de tráfego entre os switches, caso necessário;
- 12.7. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19";
- 12.8. Operar nas temperaturas de 0 a 40 °C;
- 12.9. Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima do chassi, e redundância n+1 instalada- 01(uma) fonte extra de redundância;
- 12.10. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 12.11. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 12.12. Deverá ser fornecido um jogo de manuais originais dos equipamentos fornecidos, preferencialmente em língua portuguesa, contendo informações sobre as suas características técnicas, configurações, programação, montagem, instalação, manutenção, operação e gerenciamento de todas as

funcionalidades fornecidas. Toda documentação dos equipamentos fornecidos será fornecida tanto na forma impressa como também em mídia digital, na forma de arquivos eletrônicos;

12.13. Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior;

12.14. Todas as versões de sistema operacional ou software armazenado no equipamento deverão ser fornecidos nos releases mais atualizados, adequadas às necessidades requeridas nesta especificação, fornecidas se disponíveis na mídia CD-ROM. Durante a vigência da garantia / suporte técnico será prevista a atualização do Sistema Operacional do equipamento dentro da mesma versão por outra mais atualizada visando manter o equipamento atualizado e livre de bugs, falhas de segurança etc;

12.15. Deverão ser fornecidos todos os softwares, cabos de força e lógicos, conectores, adaptadores, acessórios de fixação, necessários para o pleno funcionamento do equipamento;

12.16. Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante;

12.17. Todos os equipamentos e seus acessórios deverão estar na embalagem original do fabricante. Todos os acessórios básicos que acompanham os equipamentos deverão ser fornecidos;

### **Desempenho**

12.18. Deve possuir capacidade de comutação de, no mínimo, 2 Tbps;

12.19. Deve possuir capacidade de encaminhamento de, no mínimo, 900 MPPS;

### **Disponibilidade**

12.20. Deve possuir interface de Console Serial ou USB;

12.21. Deve possuir uma porta para gerenciamento out-of-band com conector RJ-45;

12.22. Deve implementar 803ad Agregação de Links com mínimo de 54 grupos de 8 portas;

12.23. Deve possuir buffers de, no mínimo, 16MB;

### **Switching**

12.24. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

12.25. Deve implementar funcionalidade que permita a detecção de falhas de uplink;

12.26. Deve implementar, no mínimo, 4.000(quatro mil) VLANs, conforme padrão IEEE 801q;

12.27. Deve implementar os seguintes padrões IEEE 801D, 801W, 801S, 801P

12.28. Deve Implementar JUMBO FRAME (mínimo de 9k) em todas as interfaces Gigabit Ethernet

12.29. Tabela de endereços MAC com capacidade para no mínimo 80.000 endereços MAC;

12.30. Deve implementar LLDP (IEEE 801ab)

12.31. Deve implementar o padrão IEEE801AK

12.32. Deve implementar MRVP

- 12.33. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 12.34. Deve implementar MSTP (IEEE 801s) com suporte a 64 instâncias;
- 12.35. Suportar tabela para pelo menos 90.000 hosts IPV4 e 45.000 Hosts IPV6

### **Roteamento**

- 12.36. Deve possuir tabela de roteamento com no mínimo 13.000 rotas IPv4 e 3.000 rotas IPv6;
- 12.37. Deve implementar roteamento estático;
- 12.38. Deve Implementar roteamento OSPFv2 e OSPFv3;
- 12.39. Deve implementar roteamento OSPFv2 NSSA;
- 12.40. Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro;
- 12.41. Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 8 grupos;
- 12.42. Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado;
- 12.43. Deve implementar BGP;
- 12.44. Deve implementar PRB (Policy Based Routing);
- 12.45. Deve implementar VRRP (Virtual Router Redundancy Protocol);
- 12.46. Deve implementar DHCP Client e DHCP Relay
- 12.47. Deve suportar VRF (Virtual Routing and Forwarding) até 3 VRFs Routing
- 12.48. Deve implementar VRF Ipv4 e Ipv6;
- 12.49. Deve implementar funcionalidade que especifica o número máximo de entradas no ARP;
- 12.50. Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de “down”

### **Multicast**

- 12.51. Deve implementar PIM-SM;
- 12.52. Deve implementar IGMP nas versões v1 e v2 e Snooping
- 12.53. Deve implementar MLD Snooping ;

### **Software Defined Networking**

- 12.54. Deve possuir tecnologia que permite a separação do plano de dados (encaminhamento de pacotes) e do plano de controle;
- 12.55. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
- 12.56. Deve ser totalmente programável em REST API
- 12.57. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão

ser fornecidas;

12.58. Deve possuir interface REST API e scripting via Python;

12.59. Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta similar, podendo ser composto por hardware ou software adicional;

## QoS

12.60. Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado;

12.61. Deve implementar rate-limiting;

12.62. Deve suportar espelhamento de portas;

12.63. Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ;

12.64. Deve suportar no mínimo, 8 (oito) filas de prioridade por porta;

## Segurança

12.65. Deve implementar ACL's Ipv4 e Ipv6;

12.66. Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch;

12.67. Deve suportar RADIUS/TACACS+ servers.

## Gerenciamento

12.68. Deve suportar duas imagens de software na memória flash (IOS, Firmware);

12.69. Deve possuir capacidade de armazenar múltiplos arquivos de configuração;

12.70. Deve implementar sFlow (IPv4 e IPv6) ou similar;

12.71. Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração

12.72. Deve implementar SNMP v1, v2c e v3;

12.73. Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP;

12.74. Deve suportar Self Signed Certificate Management;

12.75. Deve suportar SSH v2;

12.76. Deve Suportar AAA (TACACS+ & RADIUS);

12.77. Deve implementar CLI com gerência por meio de linhas de comando;

## 13. ITEM 13 - SWITCH DE ACESSO 48 PORTAS

### Características Gerais

13.1. Deve possuir 48 (quarenta e oito) portas POE+ 10/100/1000Mbps do tipo RJ45;



- 13.2. Deve possuir 4 (quatro) portas 1/10Gbps SFP+;
- 13.2.1. Todas as portas óticas deverão conter *tranceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 13.2.2. O fornecedor deverá entregar 4 *patch cords* óticos padrão OM4 compatíveis, de 3 (três) metros cada;
- 13.3. Deve implementar IEEE 802.3az para as portas 10/100/1000Mbps.

### Desempenho

- 13.4. Deve possuir capacidade de comutação de, no mínimo, 176Gbps;
- 13.5. Deve possuir capacidade de encaminhamento de, no mínimo, 110MPPS;

### Disponibilidade

- 13.6. Deve possuir uma interface de console USB;
- 13.7. Deve suportar empilhamento de no mínimo 8 (oito) switches;
- 13.8. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;
- 13.9. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;
- 13.10. Deve possuir buffers de, no mínimo, 6 MB;

### Switching

- 13.11. Deve suportar a agregação de links entre diferentes membros da pilha;
- 13.12. Deve possuir no mínimo 15.000 endereços MAC;
- 13.13. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 13.14. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
- 13.15. Deve implementar no mínimo 2000 VLANs simultaneamente;
- 13.16. Deve implementar MVRP (Multiple VLAN Registration Protocol);
- 13.17. Deve implementar LLDP (IEEE 802.1ab);
- 13.18. Deve implementar LLDP-MED;
- 13.19. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 13.20. Deve implementar MSTP (IEEE 802.1s);
- 13.21. Deve implementar túneis VxLAN (VTEP).

### Roteamento

- 13.22. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
- 13.23. Deve implementar roteamento estático;
- 13.24. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);

- 13.25. Deve implementar RIPng;
- 13.26. Deve implementar OSPF;
- 13.27. Deve implementar OSPFv3;
- 13.28. Deve implementar Policy-based Routing;
- 13.29. Deve implementar VRRP;
- 13.30. Deve implementar VRRPv3;
- 13.31. Deve implementar servidor DHCP;
- 13.32. Deve implementar DHCP snooping (IPv4 e IPv6);
- 13.33. Deve implementar DHCP relay (IPv4 e IPv6);
- 13.34. Deve implementar Gateway mDNS, com suporte a Apple Bonjour

### **Multicast**

- 13.35. Deve implementar PIM-SM;
- 13.36. Deve implementar PIM-DM;
- 13.37. Deve implementar MLD snooping;
- 13.38. Deve implementar IGMP v3.

### **Software Defined Networking**

- 13.39. Deve implementar OpenFlow 1.3 ou superior;
- 13.40. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
- 13.41. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
- 13.42. Deve implementar 16 instâncias de OpenFlow;
- 13.43. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
- 13.44. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
- 13.45. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
- 13.46. Deve suportar no mínimo 16.000 regras openflow;
- 13.47. Deve possuir interface REST API;
- 13.48. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
- 13.49. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

### **QoS**

- 13.50. Deve implementar controle de broadcast;
- 13.51. Deve implementar rate limiting para pacotes ICMP;
- 13.52. Deve implementar rate limiting para tráfego broadcast e multicast;
- 13.53. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
- 13.54. Deve suportar espelhamento de portas;
- 13.55. Deve suportar espelhamento de tráfego para um switch remoto.

## **Segurança**

- 13.56. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
- 13.57. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
- 13.58. Deve implementar 802.1x;
- 13.59. Deve implementar autenticação baseada em web;
- 13.60. Deve implementar autenticação baseada em endereço MAC;
- 13.61. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
- 13.62. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 13.63. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 13.64. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 13.65. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

## **Gerenciamento**

- 13.66. Deve implementar NTP com autenticação MD5;
- 13.67. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
- 13.68. Deve suportar duas imagens de software na flash;
- 13.69. Deve suportar múltiplos arquivos de configuração na flash;
- 13.70. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
- 13.71. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 13.72. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem

necessidade de instalação de nenhum software ou dispositivo on-site;

- 13.73. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
- 13.74. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 13.75. Deve possuir interface web para configuração;
- 13.76. Deve implementar TR-69 (CPE WAN Management Protocol) ou similar;
- 13.77. Deve suportar diagnóstico de transceivers ópticos;
- 13.78. Deve implementar Syslog sobre TLS ou similar;
- 13.79. Deve implementar Secure SFTP (SFTP);
- 13.80. Deve implementar SNMP v1/v2/v3;
- 13.81. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
- 13.82. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 13.83. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
- 13.84. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

## Licenciamento

- 13.85. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 13.86. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

## 14. ITEM 14 - SWITCH DE ACESSO 48 PORTAS MULTIGIGABIT

### Características Gerais

- 14.1. Deve possuir, no mínimo, 48 (quarenta e oito) portas POE+ 10/100/1000Mbps do tipo RJ45 (Base-T)
  - 14.1.1. No mínimo 8 (oito) portas serão padrão Ethernet Base-T com capacidade de fluxo Multigigabit (IEEE 802.3bz) 1/2.5/5GBaseT ports PoE+;
  - 14.1.2. Caso não seja possível as portas Multigigabit dentre as 48 portas acima, poderá ser entregue slot adicional para este fim.
- 14.2. As portas padrão Gigabit Ethernet devem possuir a funcionalidade de transmissão de energia via cabo Ethernet (Power over Ethernet).
- 14.3. Possuir no mínimo 2 (duas) portas SFP+.
  - 14.3.1. Poderão também serem entregues mediante modulo adicional, caso necessário.
  - 14.3.2. Todas as portas óticas deverão conter *tranceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;

14.3.3. O fornecedor deverá entregar 2 *patch cords* óticos padrão OM4 compatíveis, de 3 (três) metros cada;

14.4. Deve implementar IEEE 802.3az para as portas 10/100/1000Mbps.

### **Desempenho**

14.5. Deve possuir capacidade de comutação de, no mínimo, 200Gbps;

14.6. Deve possuir capacidade de encaminhamento de, no mínimo, 100MPPS;

### **Disponibilidade**

14.7. Deve possuir uma interface de console USB;

14.8. Deve suportar empilhamento de no mínimo 8 (oito) switches;

14.9. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;

14.10. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;

14.11. Deve possuir buffers de, no mínimo, 6 MB;

### **Switching**

14.12. Deve suportar a agregação de links entre diferentes membros da pilha;

14.13. Deve possuir no mínimo 15.000 endereços MAC;

14.14. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

14.15. Deve implementar funcionalidade que permita a detecção de falhas de uplink;

14.16. Deve implementar no mínimo 2000 VLANs simultaneamente;

14.17. Deve implementar MVRP (Multiple VLAN Registration Protocol);

14.18. Deve implementar LLDP (IEEE 802.1ab);

14.19. Deve implementar LLDP-MED;

14.20. Deve implementar PVST+, RPVST+ ou protocolo compatível;

14.21. Deve implementar MSTP (IEEE 802.1s);

14.22. Deve implementar túneis VxLAN (VTEP).

### **Roteamento**

14.23. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;

14.24. Deve implementar roteamento estático;

14.25. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);

14.26. Deve implementar RIPv6;

14.27. Deve implementar OSPF;

14.28. Deve implementar OSPFv3;

14.29. Deve implementar Policy-based Routing;

- 14.30. Deve implementar VRRP;
- 14.31. Deve implementar VRRPv3;
- 14.32. Deve implementar servidor DHCP;
- 14.33. Deve implementar DHCP snooping (IPv4 e IPv6);
- 14.34. Deve implementar DHCP relay (IPv4 e IPv6);
- 14.35. Deve implementar Gateway mDNS, com suporte a Apple Bonjour;

### **Multicast**

- 14.36. Deve implementar PIM-SM;
- 14.37. Deve implementar PIM-DM;
- 14.38. Deve implementar MLD snooping;
- 14.39. Deve implementar IGMP v3.

### **Software Defined Networking**

- 14.40. Deve implementar OpenFlow 1.3 ou superior;
- 14.41. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
- 14.42. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
- 14.43. Deve implementar 16 instâncias de OpenFlow;
- 14.44. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
- 14.45. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
- 14.46. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
- 14.47. Deve suportar no mínimo 16.000 regras openflow;
- 14.48. Deve possuir interface REST API;
- 14.49. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
- 14.50. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

### **QoS**

- 14.51. Deve implementar controle de broadcast;
- 14.52. Deve implementar rate limiting para pacotes ICMP;
- 14.53. Deve implementar rate limiting para tráfego broadcast e multicast;
- 14.54. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;

- 14.55. Deve suportar espelhamento de portas;
- 14.56. Deve suportar espelhamento de tráfego para um switch remoto.

## **Segurança**

- 14.57. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
- 14.58. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
- 14.59. Deve implementar 802.1x;
- 14.60. Deve implementar autenticação baseada em web;
- 14.61. Deve implementar autenticação baseada em endereço MAC;
- 14.62. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
- 14.63. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 14.64. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 14.65. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 14.66. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

## **Gerenciamento**

- 14.67. Deve implementar NTP com autenticação MD5;
- 14.68. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
- 14.69. Deve suportar duas imagens de software na flash;
- 14.70. Deve suportar múltiplos arquivos de configuração na flash;
- 14.71. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
- 14.72. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 14.73. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
- 14.74. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
- 14.75. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 14.76. Deve possuir interface web para configuração;

- 14.77. Deve implementar TR-69 (CPE WAN Management Protocol) ou similar;
- 14.78. Deve suportar diagnóstico de transceivers ópticos;
- 14.79. Deve implementar Syslog sobre TLS ou similar;
- 14.80. Deve implementar Secure SFTP (SFTP);
- 14.81. Deve implementar SNMP v1/v2/v3;
- 14.82. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
- 14.83. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 14.84. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
- 14.85. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

### Licenciamento

- 14.86. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 14.87. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

## 15. ITEM 15 - SWITCH DE ACESSO 24 PORTAS

### Características Gerais

- 15.1. Deve possuir 24 (vinte e quatro) portas POE+ 10/100/1000Mbps do tipo RJ45;
- 15.2. Deve possuir 4 (quatro) portas 1/10Gbps SFP+;
- 15.2.1. Todas as portas óticas deverão conter *tranceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 15.2.2. O fornecedor deverá entregar 4 *patch cords* óticos padrão OM4 compatíveis, sendo 2 unidades de 3 (três) metros e 2 unidades de 5 (cinco) metros;
- 15.3. Deve implementar IEEE 802.3az para as portas 10/100/1000Mbps;
- 15.4. Deverá ser fornecido um jogo de manuais originais dos equipamentos fornecidos, preferencialmente em língua portuguesa, contendo informações sobre as suas características técnicas, configurações, programação, montagem, instalação, manutenção, operação e gerenciamento de todas as funcionalidades fornecidas. Toda documentação dos equipamentos fornecidos será fornecida tanto na forma impressa como também em mídia digital, na forma de arquivos eletrônicos;
- 15.5. Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante;



- 15.6. Todos os equipamentos e seus acessórios deverão estar na embalagem original do fabricante. Todos os acessórios básicos que acompanham os equipamentos deverão ser fornecidos.

### **Desempenho**

- 15.7. Deve possuir capacidade de comutação de, no mínimo, 56Gbps;  
15.8. Deve possuir capacidade de encaminhamento de, no mínimo, 40MPPS;

### **Disponibilidade**

- 15.9. Deve possuir uma interface de console USB;  
15.10. Deve suportar empilhamento de no mínimo 8 (oito) switches;  
15.11. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;  
15.12. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;  
15.13. Deve possuir buffers de, no mínimo, 6 MB;

### **Switching**

- 15.14. Deve suportar a agregação de links entre diferentes membros da pilha;  
15.15. Deve possuir no mínimo 15.000 endereços MAC;  
15.16. Deve implementar funcionalidade que permita a detecção de links unidirecionais;  
15.17. Deve implementar funcionalidade que permita a detecção de falhas de uplink;  
15.18. Deve implementar no mínimo 2000 VLANs simultaneamente;  
15.19. Deve implementar MVRP (Multiple VLAN Registration Protocol);  
15.20. Deve implementar LLDP (IEEE 802.1ab);  
15.21. Deve implementar LLDP-MED;  
15.22. Deve implementar PVST+, RPVST+ ou protocolo compatível;  
15.23. Deve implementar MSTP (IEEE 802.1s);  
15.24. Deve implementar túneis VxLAN (VTEP).

### **Roteamento**

- 15.25. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;  
15.26. Deve implementar roteamento estático;  
15.27. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);  
15.28. Deve implementar RIPng;  
15.29. Deve implementar OSPF;  
15.30. Deve implementar OSPFv3;  
15.31. Deve implementar Policy-based Routing;  
15.32. Deve implementar VRRP;

- 15.33. Deve implementar VRRPv3;
- 15.34. Deve implementar servidor DHCP;
- 15.35. Deve implementar DHCP snooping (IPv4 e IPv6);
- 15.36. Deve implementar DHCP relay (IPv4 e IPv6);
- 15.37. Deve implementar Gateway mDNS, com suporte a Apple Bonjour

### **Multicast**

- 15.38. Deve implementar PIM-SM;
- 15.39. Deve implementar PIM-DM;
- 15.40. Deve implementar MLD snooping;
- 15.41. Deve implementar IGMP v3.

### **Software Defined Networking**

- 15.42. Deve implementar OpenFlow 1.3 ou superior;
- 15.43. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
- 15.44. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
- 15.45. Deve implementar 16 instâncias de OpenFlow;
- 15.46. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
- 15.47. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
- 15.48. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
- 15.49. Deve suportar no mínimo 16.000 regras openflow;
- 15.50. Deve possuir interface REST API;
- 15.51. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
- 15.52. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

### **QoS**

- 15.53. Deve implementar controle de broadcast;
- 15.54. Deve implementar rate limiting para pacotes ICMP;
- 15.55. Deve implementar rate limiting para tráfego broadcast e multicast;
- 15.56. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
- 15.57. Deve suportar espelhamento de portas;

- 15.58. Deve suportar espelhamento de tráfego para um switch remoto.

### **Segurança**

- 15.59. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
- 15.60. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
- 15.61. Deve implementar 802.1x;
- 15.62. Deve implementar autenticação baseada em web;
- 15.63. Deve implementar autenticação baseada em endereço MAC;
- 15.64. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
- 15.65. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 15.66. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 15.67. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 15.68. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

### **Gerenciamento**

- 15.69. Deve implementar NTP com autenticação MD5;
- 15.70. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
- 15.71. Deve suportar duas imagens de software na flash;
- 15.72. Deve suportar múltiplos arquivos de configuração na flash;
- 15.73. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
- 15.74. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 15.75. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
- 15.76. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
- 15.77. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 15.78. Deve possuir interface web para configuração;
- 15.79. Deve implementar TR-69 (CPE WAN Management Protocol) ou similar;

- 15.80. Deve suportar diagnóstico de transceivers ópticos;
- 15.81. Deve implementar Syslog sobre TLS ou similar;
- 15.82. Deve implementar Secure SFTP (SFTP);
- 15.83. Deve implementar SNMP v1/v2/v3;
- 15.84. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
- 15.85. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 15.86. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
- 15.87. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

#### **Licenciamento**

- 15.88. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 15.89. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

#### **Treinamento para os switches**

- 15.90. Oferecer treinamento para operacionalização dos *switches* (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.
- 15.91. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.
- 15.92. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.
- 15.93. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

#### **16. ITEM 16 - TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE SWITCHES**

- 16.1. O treinamento oficial do fabricante será de, no mínimo, 40 horas, em português.
- 16.2. O treinamento será realizado preferencialmente no modelo presencial, em instalações providas pela CONTRATADA.
- 16.3. Os treinamentos só serão aceitos na modalidade à distância se:
  - 16.3.1. Por impossibilidade logística devido à pandemia de COVID-19;
  - 16.3.2. Por interesse e oportunidade da Administração.
- 16.4. Deve ser ministrado por profissional certificado pelo fabricante dos equipamentos como instrutor.

- 16.5. A ementa do curso deve abranger conteúdos que vão desde instalação, configuração, gerenciamento, operação a *troubleshooting* dos equipamentos de hardware e de softwares que compõem a solução de redes sem fios.
- 16.6. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.
- 16.7. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus à contratante.
- 16.8. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento.
- 16.9. Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.
- 16.10. Caso não haja disponibilidade para realização em Brasília, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.
- 16.11. Deverá ser fornecido certificado de conclusão oficial do fabricante da solução aos participantes.

### GRUPO 3 - REDE DE ARMAZENAMENTO

#### 17. ITEM 17 - SWITCH FIBRE CHANNEL

##### Características físicas

- 17.1. Possuir altura máxima de 1 RU (Rack Units);
- 17.2. Suportar, no mínimo, 24 (vinte e quatro) portas de 8/16 Gigabit Fibre Channel, padrão SFP+ com conectores LC;
- 17.2.1. Todas as portas equipamento entregue devem ser licenciadas para uso e acompanharem com os respectivos *transceivers*, conectorização, trilhos e demais componentes necessários para a instalação física nos *racks* e conectividade na infraestrutura de rede do ITI;
- 17.3. Deve possuir no mínimo 4 portas 10 GbE padrão SFP+ para uplink;
- 17.3.1. Serão aceitos equipamentos com padrões de velocidades maiores (ex.: QSFP+), desde que metade do quantitativo das portas acompanhe os respectivos cabos do tipo *breakout* para compatibilização com o padrão SFP+, e a outra metade acompanhe cabos DAC de 3 metros compatíveis com a porta de *uplink* do equipamento entregue;
- 17.4. Possuir fontes redundantes em configuração *grid* N+N, *hot-swappable*, operando entre 100-240V AC nominal ( $\pm 10\%$  variação no intervalo) e 60Hz nominal, com cabeamento incluso;
- 17.5. Possuir ventiladores *hot-swappable* com gerenciamento integrado de temperatura e potência;
- 17.6. Possuir porta gerenciamento "out-of-band" 10/100/1000, permitindo um gerenciamento remoto;
- 17.7. Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.
- 17.8. O switch deverá estar em conformidade com a norma IEC 60950 (*Safety of Information Technology Equipment Including Electrical Business Equipment*), para segurança do usuário contra incidentes

elétricos e combustão dos materiais elétricos.

17.9. O switch e seus acessórios deverão estar acondicionados em embalagens com caixa e calços de proteção especialmente desenvolvidos para suportar o empilhamento e as vibrações.

17.10. Garantia do equipamento e sistema operacional de 60 meses.

### **Características operacionais**

17.11. Possuir capacidade de atualização não-disruptiva de software, *In-Service Software Upgrade* (ISSU);

17.12. Possuir capacidade de armazenamento de mais de uma versão de software no switch;

17.13. Possuir comutação e restabelecimento de processos de forma a manter o status e consistência das conexões (*stateful process restart/failover*);

17.14. Possuir capacidade de interligação entre chassis equivalentes através de canais de alta disponibilidade e desempenho;

17.15. Permitir a criação de ambientes independentes e isolados logicamente, dentro do switch.

17.16. Cada ambiente de SAN Virtualizado deve possuir as funcionalidades de zoneamento e os serviços nativos ao *Fabric* totalmente isolados, sendo independentes como uma SAN tradicional;

17.17. Suportar a criação de no mínimo 32 (trinta e dois) SANs Virtuais;

17.18. Possuir capacidade de configuração de *zones* em SAN Virtual, pelos seguintes critérios: N\_Port World Wide Name (nWWN), N\_Port FC-ID;

17.19. Possuir capacidade de configurar privilégios de leitura e escrita em um *zone* (*read-only zoning*);

17.20. Suportar modo NPIV ou Access Gateway;

17.21. Suportar os tipos de porta Fibre Channel básicos: E, F, FL;

17.22. Suportar os tipos de porta Fibre Channel avançados: TE, SD, ST;

17.23. Possuir a funcionalidade de espelhamento de tráfego em uma porta local (SPAN) ou em switch remoto (RSPAN), podendo ser configurada em qualquer porta FC, de qualquer módulo, permitindo que o tráfego de uma interface possa ser enviado para um analisador de protocolo externo;

17.24. Ter a capacidade de verificar o caminho de encaminhamento de um pacote na rede SAN (*FC trace route*);

17.25. Ter a capacidade de verificar o tempo de resposta de um dispositivo na rede SAN (*FC Ping*);

17.26. Suportar ao envio de informações ao um servidor externo, Syslog;

17.27. Possuir estatísticas por interface de utilização e erros;

17.28. Possuir roteamento de tráfego entre SANs Virtuais diferentes;

### **Desempenho e escalabilidade**

17.29. O Chassi deve suportar tráfego máximo sustentado em todas as 24 portas à 16 Gbps Fibre Channel ou sem *oversubscription* nas portas;

17.30. Permitir a criação de até 24 *port-channels* por chassi;

17.31. Permitir a criação de até 24 Inter-Switch Link (ISL) por chassi;

## Gerenciamento

- 17.32. Possuir ferramenta gráfica baseada em HTML5 para gerenciamento, provisionamento, configuração, monitoração, análise de eventos, verificação de conectividade, visualização de dispositivos e mapeamento dinâmico da topologia da SAN;
- 17.33. Permitir a visualização de representações gráficas dos equipamentos on-line, mostrando o estado operacional das portas, permitindo inclusive a configuração e monitoramento em tempo real.
- 17.34. A ferramenta deve exibir a topologia da rede. A descoberta dos equipamentos e suas interligações deve ser feita obrigatoriamente de forma automática, permitindo também sua customização manual.
- 17.35. Permitir a configuração de diferentes perfis de usuários do sistema, criando regras como administrador, operador e apenas leitura.
- 17.36. O software de gerência deve prover detecção de falhas em tempo real, além de oferecer relatórios e regras de tratamento de alarmes pré-configuradas para ações de intervenção.
- 17.37. Suportar a implementação de alta disponibilidade através de sistema ativo-standby com banco de dados compartilhado;
- 17.38. Deve possuir integrações nativas com outras ferramentas de gerência com o VMware vCenter 6.x;
- 17.39. Deve permitir a criação de *Dashboards* customizados para visualização imediata das principais informações do Fabric SAN;

## Segurança

- 17.40. Possuir autenticação, autorização e registro das operações dos administradores;
- 17.41. Suportar RADIUS e TACACS+;
- 17.42. Implementar controle de acesso baseado em regras configuráveis ("Role-Based Access Control" – RBAC);
- 17.43. Possuir gerenciamento via SNMPv3 com criptografia baseada no algoritmo AES;
- 17.44. Suportar SSHv2 (Secure Shell Protocol version 2);
- 17.45. Suportar SFTP (Security FTP) para proteção na transferência de arquivos;
- 17.46. Implementar listas de controle de Acesso (ACLs);
- 17.47. Possuir isolamento total entre os múltiplos *Fabrics* através de SANs Virtuais;
- 17.48. Possuir zoneamento baseado em hardware (Hardware-enforced zoning);
- 17.49. Possuir zonas independentes por SAN Virtual;
- 17.50. Possuir capacidade de fazer a associação fixa entre um determinado dispositivo identificável via World Wide Name e uma porta do Director (*Port Security*);
- 17.51. Possuir capacidade de garantir comunicação segura entre switches SAN, somente habilitando equipamentos previamente autorizada via configuração (*Fabric Binding*);

## Treinamento para os switches fibre channel

17.52. Oferecer treinamento para operacionalização dos switches fibre channel (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.

17.53. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.

17.54. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.

17.55. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.



Documento assinado eletronicamente por **Giordanno Azevedo Costa Martins, Integrante Técnico**, em 04/11/2020, às 13:07, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

Nº de Série do Certificado: 48033346914305620050757767996



Documento assinado eletronicamente por **Roberto Wagner de Carvalho Araújo, Integrante Requisitante**, em 04/11/2020, às 13:15, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

Nº de Série do Certificado: 1287494053113912491



A autenticidade deste documento pode ser conferida no site [https://sei.iti.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0454066** e o código CRC **24A9C689**.