

## **ANEXO A – TERMO DE REFERÊNCIA**

### **ESPECIFICAÇÕES TÉCNICAS DETALHADAS**

#### **1. ITEM 01 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW – TIPO I**

- 1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 1.2. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.
- 1.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.
- 1.4. Deve possuir e estar licenciado durante a vigência contratual de 36 (trinta e seis meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais.
- 1.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.
- 1.6. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.
- 1.7. Deve possuir IPS com capacidade mínima de processamento de 8 (oito) Gbps.
- 1.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 5 (cinco) Gbps contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 1.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 6 (seis) Gbps.
- 1.10. Deve possuir VPN com capacidade de, pelo menos, 35 (trinta e cinco) Gbps de tráfego IPSec.
- 1.11. Deve suportar 10.000.000 (dez milhões mil) conexões simultâneas.
- 1.12. Deve suportar, pelo menos, 390.000 (Trezentos e noventa mil) novas conexões por segundo.
- 1.13. Deve suportar, pelo menos, 1.900 (mil e novecentos) túneis de VPN Site-Site.
- 1.14. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 1.15. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 1.16. Deve possuir, pelo menos, 04 (quatro) interfaces SFP 1GE.
- 1.17. Deve possuir, pelo menos, 04 (quatro) interfaces RJ 45 5GE.
- 1.18. Deve possuir, pelo menos, 04 (quatro) interfaces RJ 45 1GE.
- 1.19. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade

e estar licenciados para operar desta forma.

- 1.20. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 60 (sessenta) equipamentos.
- 1.21. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 120 (cento e vinte) equipamentos.
- 1.22. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 1.23. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

#### **1.24. FUNCIONALIDADES DE FIREWALL**

- 1.24.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 1.24.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 1.24.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 1.24.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 1.24.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 1.24.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 1.24.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 1.24.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 1.24.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 1.24.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 1.24.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 1.24.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 1.24.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 1.24.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 1.24.15. Deve suportar o encaminhamento de tráfego multicast.
- 1.24.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 1.24.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;

- 1.24.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 1.24.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 1.24.20. Suportar OSPF gracefulrestart;
- 1.24.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 1.24.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 1.24.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 1.24.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 1.24.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 1.24.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 1.24.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
- 1.24.28. Drop sem notificação do bloqueio ao usuário;
- 1.24.29. Drop com notificação do bloqueio ao usuário;
- 1.24.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 1.24.31. TCP-Reset para o cliente;
- 1.24.32. TCP-Reset para o server ou para os dois lados da conexão.
- 1.24.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 1.24.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 1.24.35. Deve oferecer suporte ao protocolo SIP.
- 1.24.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 1.24.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 1.24.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 1.24.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 1.24.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.

- 1.24.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 1.24.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 1.24.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 1.24.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 1.24.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.24.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 1.24.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 1.24.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 1.24.49. Realizar Traffic Shaping para a solução de segurança
- 1.24.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 1.24.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 1.24.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 1.24.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 1.24.54. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 1.24.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 1.24.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 1.24.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 1.24.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 1.24.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 1.24.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 1.24.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 1.24.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.

- 1.24.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 1.24.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 1.24.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 1.24.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 1.24.67. Funcionar com tradução de porta (PAT);
- 1.24.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 1.24.69. Implementar e suportar NAT64 e NAT46;
- 1.24.70. Implementar NAT66
- 1.24.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 1.24.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 1.24.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 1.24.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 1.24.75. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 1.24.76. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 1.24.77. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 1.24.78. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 1.24.79. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.
- 1.25. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**
- 1.25.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 1.25.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 1.25.3. Deve permitir priorização de tráfego e suportar ToS.
- 1.25.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 1.25.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

- 1.25.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 1.25.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 1.25.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 1.25.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 1.25.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

#### **1.26. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

- 1.26.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 1.26.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 1.26.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 1.26.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 1.26.5. Deve permitir a criação de categorias personalizadas.
- 1.26.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 1.26.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 1.26.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 1.26.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 1.26.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 1.26.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 1.26.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 1.26.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 1.26.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 1.26.15. Permitir a criação de categorias de URLs customizadas;
- 1.26.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;

- 1.26.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 1.26.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 1.26.19. Permitir a customização de página de bloqueio;
- 1.26.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 1.26.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 1.26.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.26.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 1.26.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 1.26.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 1.26.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 1.26.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 1.26.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 1.26.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 1.26.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 1.26.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 1.26.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 1.26.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 1.26.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 1.26.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.

- 1.26.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 1.26.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 1.26.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 1.26.39. Deve possuir Proxy Explícito e Transparente.
- 1.26.40. Deve implementar roteamento WCCP e ICAP.

#### **1.27. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**

- 1.27.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 1.27.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 1.27.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 1.27.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 1.27.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 1.27.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 1.27.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 1.27.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 1.27.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 1.27.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 1.27.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 1.27.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 1.27.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 1.27.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 1.27.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 1.27.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica

de Servidores Web.

- 1.27.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 1.27.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 1.27.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 1.27.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 1.27.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 1.27.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 1.27.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;
- 1.27.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 1.27.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 1.27.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 1.27.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 1.27.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 1.27.29. Identificar, alertar e bloquear comunicação com botnets;
- 1.27.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 1.27.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 1.27.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 1.27.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 1.27.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 1.27.35. Identificar nos eventos o país de onde partiu a ameaça;
- 1.27.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;

- 1.27.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 1.27.38. Deve possuir alarmes na console de administração.
- 1.27.39. Deve possuir alertas via correio eletrônico.
- 1.27.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 1.27.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 1.27.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 1.27.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 1.27.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

#### **1.28. FUNCIONALIDADE DE VPN**

- 1.28.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 1.28.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
- 1.28.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 1.28.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 1.28.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 1.28.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 1.28.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 1.28.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 1.28.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 1.28.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 1.28.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 1.28.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 1.28.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 1.28.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 1.28.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 1.28.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.

- 1.28.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.

**1.29. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 1.29.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 1.29.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 1.29.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 1.29.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 1.29.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 1.29.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 1.29.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 1.29.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 1.29.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 1.29.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 1.29.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 1.29.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 1.29.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 1.29.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 1.29.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 1.29.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE,

baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

- 1.29.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 1.29.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 1.29.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 1.29.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 1.29.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 1.29.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 1.29.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 1.29.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 1.29.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 1.29.26. Deve permitir criação de padrões de aplicação manualmente.
- 1.29.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 1.29.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 1.29.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 1.29.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encryptado” e aplicações VOIP que utilizam criptografia proprietária;

#### **1.30. FUNCIONALIDADE DE SD-WAN**

- 1.30.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 1.30.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com gestão, orquestração e plano de controle SD-WAN baseados em nuvem.
- 1.30.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 1.30.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

- 1.30.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 1.30.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 1.30.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 1.30.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 1.30.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 1.30.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 1.30.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 1.30.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 1.30.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 1.30.14. Passivo: uso do tráfego real para as medições;
- 1.30.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 1.30.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 1.30.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 1.30.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 1.30.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- 1.30.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 1.30.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 1.30.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).

- 1.30.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 1.30.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 1.30.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 1.30.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 1.30.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 1.30.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 1.30.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

#### **1.31. FUNCIONALIDADE DE CONTROLADORA WIRELESS**

- 1.31.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
- 1.31.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
- 1.31.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido.
- 1.31.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+.
- 1.31.5. Deverá permitir a visualização dos clientes conectados.
- 1.31.6. Deverá prover suporte a Fast Roaming.
- 1.31.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
- 1.31.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.
- 1.31.9. Deverá possuir Captive Portal por SSID.
- 1.31.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs.
- 1.31.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou

TKIP.

1.31.12. Deverá suportar os seguintes métodos de autenticação EAP:

1.31.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.

1.31.13. Deverá suportar 802.1x através de RADIUS.

1.31.14. Deverá suportar filtro baseado em endereço MAC por SSID.

1.31.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal.

1.31.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.

1.31.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.

1.31.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).

1.31.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

1.31.19.1. Rogue/Interfering AP Detection;

1.31.19.2. Ad-hoc Network Detection;

1.31.19.3. Wireless Bridge Detection;

1.31.19.4. Weak WEP Detection;

1.31.19.5. MAC OUI Checking.

1.31.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID.

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

1.31.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário.

1.31.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs.

1.31.24. Deverá permitir a criação de políticas de traffic shaping.

1.31.25. Deverá permitir a criação de políticas de firewall baseadas em horário.

1.31.26. Deverá permitir NAT nas políticas de firewall.

1.31.27. Deverá possibilitar definir número de clientes por SSID.

1.31.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs.

1.31.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha.

1.31.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.

- 1.31.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados.
- 1.31.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
- 1.31.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
- 1.31.34. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 1.31.35. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 1.31.36. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
- 1.31.37. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso.
- 1.31.38. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.39. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
- 1.31.40. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.41. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.42. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.43. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.44. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.45. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 1.31.46. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede.

## **2. ITEM 02 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW – TIPO II**

- 2.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 2.2. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.
- 2.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.
- 2.4. Deve possuir e estar licenciado durante a vigência contratual de 36 (trinta e seis meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais.
- 2.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 2.6. Deve possuir firewall com capacidade mínima de processamento de 27 (vinte e sete) Gbps.
- 2.7. Deve possuir IPS com capacidade mínima de processamento de 4(quatro) Gbps.
- 2.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2 (dois) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 2.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 2 (dois) Gbps.
- 2.10. Deve possuir VPN com capacidade de, pelo menos, 24 (vinte e quatro) Gbps de tráfego IPsec.
- 2.11. Deve suportar 2.500.000 (dois milhões e quinhentos mil) conexões simultâneas.
- 2.12. Deve suportar, pelo menos, 120.000 (cento e vinte mil) novas conexões por segundo.
- 2.13. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 2.14. Deve suportar, pelo menos, 2000 (dois mil) túneis de VPN Client-Site.
- 2.15. Deve possuir, pelo menos, 2 (duas) interfaces SFP+ 10GE.
- 2.16. Deve possuir, pelo menos, 8 (oito) interfaces RJ45 1GE.
- 2.17. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.
- 2.18. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 20 (vinte) equipamentos.
- 2.19. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 60 (sessenta) equipamentos.
- 2.20. Deve ser compatível com a Solução de Gerência Centralizada NGFW
- 2.21. Deve ser compatível com a Solução Centralizada de Armazenamento de Logs e Relatórios
- 2.22. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

- 2.23. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês

**2.24. FUNCIONALIDADES DE FIREWALL**

- 2.24.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 2.24.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 2.24.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 2.24.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 2.24.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 2.24.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 2.24.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 2.24.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 2.24.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 2.24.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 2.24.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 2.24.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 2.24.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 2.24.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 2.24.15. Deve suportar o encaminhamento de tráfego multicast.
- 2.24.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 2.24.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 2.24.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.24.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 2.24.20. Suportar OSPF gracefulrestart;
- 2.24.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.24.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).

- 2.24.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 2.24.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 2.24.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 2.24.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 2.24.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
- 2.24.28. Drop sem notificação do bloqueio ao usuário;
- 2.24.29. Drop com notificação do bloqueio ao usuário;
- 2.24.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 2.24.31. TCP-Reset para o cliente;
- 2.24.32. TCP-Reset para o server ou para os dois lados da conexão.
- 2.24.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 2.24.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 2.24.35. Deve oferecer suporte ao protocolo SIP.
- 2.24.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 2.24.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 2.24.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 2.24.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 2.24.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 2.24.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 2.24.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 2.24.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 2.24.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 2.24.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo

granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- 2.24.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 2.24.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 2.24.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 2.24.49. Realizar Traffic Shaping para a solução de segurança
- 2.24.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 2.24.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 2.24.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 2.24.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 2.24.54. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 2.24.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 2.24.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 2.24.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 2.24.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 2.24.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 2.24.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 2.24.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 2.24.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 2.24.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 2.24.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 2.24.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 2.24.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 2.24.67. Funcionar com tradução de porta (PAT);

- 2.24.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 2.24.69. Implementar e suportar NAT64 e NAT46;
- 2.24.70. Implementar NAT66
- 2.24.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 2.24.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 2.24.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 2.24.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 2.24.75. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 2.24.76. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 2.24.77. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 2.24.78. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 2.24.79. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

## **2.25. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 2.25.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 2.25.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 2.25.3. Deve permitir priorização de tráfego e suportar ToS.
- 2.25.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 2.25.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 2.25.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 2.25.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 2.25.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 2.25.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e

destino.

- 2.25.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

## **2.26. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

- 2.26.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 2.26.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 2.26.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 2.26.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 2.26.5. Deve permitir a criação de categorias personalizadas.
- 2.26.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 2.26.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 2.26.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 2.26.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 2.26.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 2.26.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 2.26.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 2.26.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 2.26.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 2.26.15. Permitir a criação de categorias de URLs customizadas;
- 2.26.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 2.26.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 2.26.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 2.26.19. Permitir a customização de página de bloqueio;
- 2.26.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de

dados local;

- 2.26.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 2.26.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.26.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 2.26.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 2.26.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 2.26.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 2.26.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 2.26.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 2.26.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 2.26.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 2.26.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 2.26.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 2.26.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 2.26.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 2.26.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 2.26.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 2.26.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 2.26.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 2.26.39. Deve possuir Proxy Explícito e Transparente.
- 2.26.40. Deve implementar roteamento WCCP e ICAP.

## **2.27. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**

- 2.27.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 2.27.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 2.27.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 2.27.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 2.27.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 2.27.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 2.27.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 2.27.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 2.27.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 2.27.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 2.27.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 2.27.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 2.27.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 2.27.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 2.27.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 2.27.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 2.27.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 2.27.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 2.27.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 2.27.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.

- 2.27.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 2.27.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 2.27.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;
- 2.27.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 2.27.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 2.27.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 2.27.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.27.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.27.29. Identificar, alertar e bloquear comunicação com botnets;
- 2.27.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.27.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.27.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 2.27.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 2.27.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 2.27.35. Identificar nos eventos o país de onde partiu a ameaça;
- 2.27.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 2.27.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 2.27.38. Deve possuir alarmes na console de administração.
- 2.27.39. Deve possuir alertas via correio eletrônico.
- 2.27.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 2.27.41. Deve ter a capacidade de resposta/logs ativa a ataques.

- 2.27.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 2.27.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 2.27.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

## **2.28. FUNCIONALIDADE DE VPN**

- 2.28.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 2.28.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
- 2.28.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 2.28.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 2.28.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 2.28.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.28.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 2.28.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 2.28.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 2.28.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 2.28.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 2.28.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.28.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 2.28.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 2.28.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 2.28.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 2.28.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.

## **2.29. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 2.29.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;

- 2.29.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 2.29.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 2.29.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 2.29.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 2.29.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 2.29.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 2.29.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 2.29.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 2.29.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 2.29.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 2.29.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 2.29.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 2.29.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 2.29.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 2.29.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 2.29.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 2.29.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 2.29.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory,

reconhecendo grupos de usuários cadastrados.

- 2.29.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 2.29.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 2.29.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 2.29.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 2.29.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 2.29.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 2.29.26. Deve permitir criação de padrões de aplicação manualmente.
- 2.29.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 2.29.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 2.29.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 2.29.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária;

## **2.30. FUNCIONALIDADE DE SD-WAN**

- 2.30.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 2.30.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com gestão, orquestração e plano de controle SD-WAN baseados em nuvem.
- 2.30.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 2.30.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 2.30.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 2.30.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 2.30.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.

- 2.30.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 2.30.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 2.30.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 2.30.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 2.30.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 2.30.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 2.30.14. Passivo: uso do tráfego real para as medições;
- 2.30.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 2.30.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 2.30.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 2.30.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 2.30.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- 2.30.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 2.30.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 2.30.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 2.30.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 2.30.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 2.30.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou

automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;

- 2.30.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 2.30.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 2.30.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 2.30.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

## **2.31. FUNCIONALIDADE DE CONTROLADORA WIRELESS**

- 2.31.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
- 2.31.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
- 2.31.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido.
- 2.31.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+.
- 2.31.5. Deverá permitir a visualização dos clientes conectados.
- 2.31.6. Deverá prover suporte a Fast Roaming.
- 2.31.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
- 2.31.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.
- 2.31.9. Deverá possuir Captive Portal por SSID.
- 2.31.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs.
- 2.31.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP.
- 2.31.12. Deverá suportar os seguintes métodos de autenticação EAP:
  - 2.31.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.
- 2.31.13. Deverá suportar 802.1x através de RADIUS.
- 2.31.14. Deverá suportar filtro baseado em endereço MAC por SSID.
- 2.31.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal.

- 2.31.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.
- 2.31.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.
- 2.31.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).
- 2.31.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:
  - 2.31.19.1. Rogue/Interfering AP Detection;
  - 2.31.19.2. Ad-hoc Network Detection;
  - 2.31.19.3. Wireless Bridge Detection;
  - 2.31.19.4. Weak WEP Detection;
  - 2.31.19.5. MAC OUI Checking.
- 2.31.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID.
- 2.31.21. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.
- 2.31.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário.
- 2.31.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs.
- 2.31.24. Deverá permitir a criação de políticas de traffic shaping.
- 2.31.25. Deverá permitir a criação de políticas de firewall baseadas em horário.
- 2.31.26. Deverá permitir NAT nas políticas de firewall.
- 2.31.27. Deverá possibilitar definir número de clientes por SSID.
- 2.31.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs.
- 2.31.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha.
- 2.31.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 2.31.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados.
- 2.31.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
- 2.31.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
- 2.31.34. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 2.31.35. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.

- 2.31.36. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
- 2.31.37. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso.
- 2.31.38. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.39. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
- 2.31.40. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.41. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.42. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.43. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.44. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.45. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 2.31.46. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede.

### **3. ITEM 03 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW – TIPO III**

- 3.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 3.2. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.
- 3.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

- 3.4. Deve possuir e estar licenciado durante a vigência contratual de 36 (trinta e seis meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais.
- 3.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 3.6. Deve possuir firewall com capacidade mínima de processamento de 4 (quatro) Gbps.
- 3.7. Deve possuir IPS com capacidade mínima de processamento de 2 (dois) Gbps.
- 3.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1 (um) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 3.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1(um) Gbps.
- 3.10. Deve possuir VPN com capacidade de, pelo menos, 4(quatro) Gbps de tráfego IPSec.
- 3.11. Deve suportar 700.000 (setecentos mil) conexões simultâneas.
- 3.12. Deve suportar, pelo menos, 80.000 (oitenta mil) novas conexões por segundo.
- 3.13. Deve suportar, pelo menos, 180 (cento e oitenta) túneis de VPN Site-Site.
- 3.14. Deve suportar, pelo menos, 240 (duzentos e quarenta) túneis de VPN Client-Site.
- 3.15. Deve possuir, pelo menos, 5 (cinco) interfaces RJ45 1GE.
- 3.16. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.
- 3.17. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 8 (oito) equipamentos.
- 3.18. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 8 (oito) equipamentos.
- 3.19. Deve ser compatível com a Solução de Segurança Cibernética Distribuída NGFW dos TIPOS "I, II e III"
- 3.20. Deve ser compatível com a Solução de Logs e Relatoria.
- 3.21. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 3.22. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

### **3.23. FUNCIONALIDADES DE FIREWALL**

- 3.23.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 3.23.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 3.23.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.

- 3.23.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 3.23.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 3.23.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 3.23.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 3.23.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 3.23.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 3.23.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 3.23.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 3.23.12. Deve suportar o encaminhamento de tráfego multicast.
- 3.23.13. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 3.23.14. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 3.23.15. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 3.23.16. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 3.23.17. Suportar OSPF gracefulrestart;
- 3.23.18. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 3.23.19. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 3.23.20. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 3.23.21. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 3.23.22. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 3.23.23. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 3.23.24. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
- 3.23.25. Drop sem notificação do bloqueio ao usuário;
- 3.23.26. Drop com notificação do bloqueio ao usuário;
- 3.23.27. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;

- 3.23.28. TCP-Reset para o cliente;
- 3.23.29. TCP-Reset para o server ou para os dois lados da conexão.
- 3.23.30. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 3.23.31. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 3.23.32. Deve oferecer suporte ao protocolo SIP.
- 3.23.33. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 3.23.34. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 3.23.35. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 3.23.36. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 3.23.37. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 3.23.38. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 3.23.39. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 3.23.40. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 3.23.41. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 3.23.42. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 3.23.43. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 3.23.44. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 3.23.45. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 3.23.46. Realizar Traffic Shaping para a solução de segurança
- 3.23.47. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 3.23.48. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 3.23.49. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de

prioridade;

- 3.23.50. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 3.23.51. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 3.23.52. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 3.23.53. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 3.23.54. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 3.23.55. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 3.23.56. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 3.23.57. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 3.23.58. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 3.23.59. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 3.23.60. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 3.23.61. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 3.23.62. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 3.23.63. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 3.23.64. Funcionar com tradução de porta (PAT);
- 3.23.65. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 3.23.66. Implementar e suportar NAT64 e NAT46;
- 3.23.67. Implementar NAT66
- 3.23.68. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 3.23.69. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 3.23.70. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 3.23.71. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 3.23.72. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

- 3.23.73. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 3.23.74. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 3.23.75. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 3.23.76. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

### **3.24. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 3.24.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 3.24.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 3.24.3. Deve permitir priorização de tráfego e suportar ToS.
- 3.24.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 3.24.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 3.24.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 3.24.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 3.24.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 3.24.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 3.24.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

### **3.25. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

- 3.25.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 3.25.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 3.25.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 3.25.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 3.25.5. Deve permitir a criação de categorias personalizadas.

- 3.25.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 3.25.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 3.25.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 3.25.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 3.25.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 3.25.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 3.25.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 3.25.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 3.25.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 3.25.15. Permitir a criação de categorias de URLs customizadas;
- 3.25.16. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 3.25.17. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 3.25.18. Permitir a customização de página de bloqueio;
- 3.25.19. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 3.25.20. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 3.25.21. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 3.25.22. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 3.25.23. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 3.25.24. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 3.25.25. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP

e LDAP/AD;

- 3.25.26. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 3.25.27. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 3.25.28. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 3.25.29. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 3.25.30. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 3.25.31. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 3.25.32. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 3.25.33. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 3.25.34. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 3.25.35. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 3.25.36. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 3.25.37. Deve possuir Proxy Explícito e Transparente.
- 3.25.38. Deve implementar roteamento WCCP e ICAP.

### **3.26. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**

- 3.26.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 3.26.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 3.26.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 3.26.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 3.26.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 3.26.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 3.26.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 3.26.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.

- 3.26.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 3.26.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 3.26.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 3.26.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 3.26.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 3.26.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 3.26.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 3.26.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 3.26.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 3.26.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 3.26.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 3.26.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 3.26.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 3.26.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 3.26.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;
- 3.26.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 3.26.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 3.26.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 3.26.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 3.26.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

- 3.26.29. Identificar, alertar e bloquear comunicação com botnets;
- 3.26.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 3.26.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 3.26.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 3.26.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 3.26.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 3.26.35. Identificar nos eventos o país de onde partiu a ameaça;
- 3.26.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 3.26.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 3.26.38. Deve possuir alarmes na console de administração.
- 3.26.39. Deve possuir alertas via correio eletrônico.
- 3.26.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 3.26.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 3.26.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 3.26.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 3.26.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

### **3.27. FUNCIONALIDADE DE VPN**

- 3.27.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 3.27.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
- 3.27.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 3.27.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 3.27.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 3.27.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e

v2);

- 3.27.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 3.27.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 3.27.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 3.27.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 3.27.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 3.27.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 3.27.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 3.27.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 3.27.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 3.27.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 3.27.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSEC estabelecidos.

### **3.28. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 3.28.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 3.28.2. Atualizar a base de assinaturas de aplicações automaticamente;
- 3.28.3. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 3.28.4. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 3.28.5. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 3.28.6. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 3.28.7. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 3.28.8. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 3.28.9. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 3.28.10. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;

- 3.28.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensagens instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 3.28.12. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 3.28.13. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 3.28.14. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 3.28.15. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 3.28.16. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 3.28.17. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 3.28.18. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 3.28.19. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 3.28.20. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 3.28.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 3.28.22. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 3.28.23. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 3.28.24. Deve permitir criação de padrões de aplicação manualmente.
- 3.28.25. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 3.28.26. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 3.28.27. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária;

### **3.29. FUNCIONALIDADE DE SD-WAN**

- 3.29.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.

- 3.29.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com gestão, orquestração e plano de controle SD-WAN baseados em nuvem.
- 3.29.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 3.29.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 3.29.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 3.29.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 3.29.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 3.29.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 3.29.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 3.29.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 3.29.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 3.29.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 3.29.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 3.29.14. Passivo: uso do tráfego real para as medições;
- 3.29.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 3.29.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 3.29.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 3.29.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 3.29.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

- 3.29.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 3.29.21. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 3.29.22. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 3.29.23. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 3.29.24. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 3.29.25. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 3.29.26. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 3.29.27. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 3.29.28. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

### **3.30. FUNCIONALIDADE DE CONTROLADORA WIRELESS**

- 3.30.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
- 3.30.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
- 3.30.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido.
- 3.30.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+.
- 3.30.5. Deverá permitir a visualização dos clientes conectados.
- 3.30.6. Deverá prover suporte a Fast Roaming.
- 3.30.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
- 3.30.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de

gerência.

- 3.30.9. Deverá possuir Captive Portal por SSID.
- 3.30.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs.
- 3.30.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP.
- 3.30.12. Deverá suportar os seguintes métodos de autenticação EAP:
  - 3.30.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.
- 3.30.13. Deverá suportar 802.1x através de RADIUS.
- 3.30.14. Deverá suportar filtro baseado em endereço MAC por SSID.
- 3.30.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal.
- 3.30.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.
- 3.30.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.
- 3.30.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).
- 3.30.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:
  - 3.30.19.1. Rogue/Interfering AP Detection;
  - 3.30.19.2. Ad-hoc Network Detection;
  - 3.30.19.3. Wireless Bridge Detection;
  - 3.30.19.4. Weak WEP Detection;
  - 3.30.19.5. MAC OUI Checking.
- 3.30.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID.
- 3.30.21. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.
- 3.30.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário.
- 3.30.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs.
- 3.30.24. Deverá permitir a criação de políticas de traffic shaping.
- 3.30.25. Deverá permitir a criação de políticas de firewall baseadas em horário.
- 3.30.26. Deverá permitir NAT nas políticas de firewall.
- 3.30.27. Deverá possibilitar definir número de clientes por SSID.
- 3.30.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs.

- 3.30.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha.
- 3.30.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 3.30.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados.
- 3.30.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
- 3.30.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
- 3.30.34. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 3.30.35. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 3.30.36. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
- 3.30.37. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso.
- 3.30.38. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 3.30.39. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
- 3.30.40. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 3.30.41. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora.
- 3.30.42. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 3.30.43. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 3.30.44. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora.
- 3.30.45. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a

Controladora.

- 3.30.46. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede.

#### **4. ITEM 04 – ATIVO DE REDE WIRED – TIPO I**

##### **4.1. INFORMAÇÕES GERAIS E GARANTIA**

- 4.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI.

- 4.1.2. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.

##### **4.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

- 4.2.1. Deve possuir 32 (trinta e duas ) interfaces do tipo 1000Base-T/2500Base -T para conexão de cabos de par metálico UTP com concetor R-45.

- 4.2.2. Deve possuir 16 (dezesseis) interfaces do tipo 1000Base-T/2500Base -T/5000Base-T para conexão de cabos de par metálico UTP com concetor R-45.

- 4.2.3. Adicionalmente, deve possuir 8 (oito) slots SFP28 para conexão de fibras ópticas do tipo 25GBase-X operando em 25GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.

- 4.2.4. Deve operar com latência igual ou inferior à 1us (microsegundo).

- 4.2.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.

- 4.2.6. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.

- 4.2.7. Deve ser fornecido com fonte de alimentação interna redundante com capacidade para operar em tensões de 110V e 220V.

- 4.2.8. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.

- 4.2.9. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).

- 4.2.10. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.

- 4.2.11. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash.

##### **4.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO**

- 4.3.1. Deve possuir capacidade de comutação de pelo menos 700 Gbps e ser capaz de encaminhar até 1000 Mpps (milhões de pacotes por segundo).

- 4.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.

- 4.3.3. Deve possuir tabela MAC com suporte a 60.000 endereços.

- 4.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.

- 4.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
- 4.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
- 4.3.7. Deve suportar a comutação de Jumbo Frames.
- 4.4. SPANNING TREE E RECURSOS DE PROTEÇÃO
  - 4.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
  - 4.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
  - 4.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
  - 4.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
  - 4.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
  - 4.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
  - 4.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 4.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2
  - 4.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
  - 4.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
  - 4.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
  - 4.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
  - 4.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
  - 4.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
  - 4.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
  - 4.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
  - 4.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o

protocolo ARP.

- 4.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.

#### 4.6. CAPACIDADES DE CAMADA 3

- 4.6.1. Deve suportar Multi-Chassis Link Aggregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica.
- 4.6.2. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos.
- 4.6.3. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
- 4.6.4. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
- 4.6.5. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.
- 4.6.6. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ).
- 4.6.7. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
- 4.6.8. Deve suportar o protocolo PTP (Precision Time Protocol).

#### 4.7. AUTENTICAÇÃO, ACESSO E SEGURANÇA

- 4.7.1. Deve implementar serviço de DHCP Server e DHCP Relay.
- 4.7.2. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
- 4.7.3. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 4.7.4. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 4.7.5. Deve suportar autenticação por MAC Authentication Bypass (MAB).
- 4.7.6. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 4.7.7. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 4.7.8. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.

- 4.7.9. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 4.7.10. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
- 4.7.11. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
- 4.7.12. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.
- 4.8. GEREciamento E MONITORAMENTO
- 4.8.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
- 4.8.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 4.8.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
- 4.8.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 4.8.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 4.8.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 4.8.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 4.8.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 4.8.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).
- 4.8.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 4.8.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 4.8.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
- 4.8.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 4.8.14. Deve possuir uma ferramenta de captura de pacotes que auxilie na identificação de problemas na rede. Essa ferramenta deve permitir o uso de filtros para selecionar o tráfego a ser capturado e possibilitar a exportação dos pacotes em formato .pcap, para posterior análise no software Wireshark.
- 4.8.15. Deve implementar Netflow, sFlow ou similar.
- 4.8.16. Deve suportar configuração e monitoramento por meio de REST API.
- 4.8.17. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI” e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

- 4.8.17.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
- 4.8.17.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
- 4.8.17.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
- 4.8.17.4. Deve operar como ponto central para automação e gerenciamento dos switches.
- 4.8.17.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
- 4.8.17.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
- 4.8.17.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
- 4.8.17.8. Deve montar a topologia da rede de maneira automática.
- 4.8.17.9. Deve ser capaz de configurar os switches da rede.
- 4.8.17.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 4.8.17.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 4.8.17.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
- 4.8.17.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
- 4.8.17.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 4.8.17.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 4.8.17.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 4.8.17.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 4.8.17.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 4.8.17.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.

- 4.8.17.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 4.8.17.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 4.8.17.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 4.8.17.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 4.8.17.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 4.8.17.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 4.8.17.26. Deve possuir API no formato REST.

## **5. ITEM 05 – ATIVO DE REDE WIRED – TIPO II**

### **5.1. INFORMAÇÕES GERAIS E GARANTIA**

- 5.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI.
- 5.1.2. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.

### **5.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

- 5.2.1. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector R-45.
- 5.2.2. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.
- 5.2.3. Deve operar com latência igual ou inferior à 1us (microsegundo).
- 5.2.4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.
- 5.2.5. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.
- 5.2.6. Deve ser fornecido com fonte de alimentação interna redundante com capacidade para operar em tensões de 110V e 220V.
- 5.2.7. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.
- 5.2.8. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).
- 5.2.9. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.
- 5.2.10. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash.

### **5.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO**

- 5.3.1. Deve possuir capacidade de comutação de pelo menos 120 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo).
- 5.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.
- 5.3.3. Deve possuir tabela MAC com suporte a 16.000 endereços.
- 5.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.
- 5.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
- 5.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
- 5.3.7. Deve suportar a comutação de Jumbo Frames.
- 5.4. **SPANNING TREE E RECURSOS DE PROTEÇÃO**
- 5.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 5.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
- 5.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
- 5.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
- 5.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
- 5.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
- 5.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 5.5. **GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2**
- 5.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
- 5.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
- 5.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
- 5.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
- 5.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.

- 5.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
- 5.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
- 5.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
- 5.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
- 5.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.
- 5.6. CAPACIDADES DE CAMADA 3
- 5.6.1. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica.
- 5.6.2. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos.
- 5.6.3. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
- 5.6.4. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
- 5.6.5. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF.
- 5.6.6. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ).
- 5.6.7. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
- 5.6.8. Deve suportar o protocolo PTP (Precision Time Protocol).
- 5.7. AUTENTICAÇÃO, ACESSO E SEGURANÇA
- 5.7.1. Deve implementar serviço de DHCP Server e DHCP Relay.
- 5.7.2. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
- 5.7.3. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 5.7.4. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 5.7.5. Deve suportar autenticação por MAC Authentication Bypass (MAB).

- 5.7.6. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 5.7.7. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 5.7.8. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
- 5.7.9. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 5.7.10. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
- 5.7.11. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
- 5.7.12. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.
- 5.8. GERENCIAMENTO E MONITORAMENTO
  - 5.8.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
  - 5.8.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
  - 5.8.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
  - 5.8.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
  - 5.8.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
  - 5.8.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
  - 5.8.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
  - 5.8.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
  - 5.8.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).
  - 5.8.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
  - 5.8.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
  - 5.8.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
  - 5.8.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
  - 5.8.14. Deve possuir uma ferramenta de captura de pacotes que auxilie na identificação de problemas na rede. Essa ferramenta deve permitir o uso de filtros para selecionar o tráfego a ser capturado e possibilitar a exportação dos pacotes em formato .pcap, para posterior análise no software Wireshark.

- 5.8.15. Deve implementar Netflow, sFlow ou similar.
- 5.8.16. Deve suportar configuração e monitoramento por meio de REST API.
- 5.8.17. Deve ser compatível e gerenciado pelos ITENS 01, 02,03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI” e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- 5.8.17.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
  - 5.8.17.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
  - 5.8.17.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
  - 5.8.17.4. Deve operar como ponto central para automação e gerenciamento dos switches.
  - 5.8.17.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
  - 5.8.17.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
  - 5.8.17.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
  - 5.8.17.8. Deve montar a topologia da rede de maneira automática.
  - 5.8.17.9. Deve ser capaz de configurar os switches da rede.
  - 5.8.17.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
  - 5.8.17.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
  - 5.8.17.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
  - 5.8.17.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
  - 5.8.17.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
  - 5.8.17.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
  - 5.8.17.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
  - 5.8.17.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede

através de análise DPI (Deep Packet Inspection).

- 5.8.17.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 5.8.17.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 5.8.17.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 5.8.17.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 5.8.17.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 5.8.17.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 5.8.17.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 5.8.17.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 5.8.17.26. Deve possuir API no formato REST.

## **6. ITEM 06 – ATIVO DE REDE WIRED – TIPO III**

### **6.1. INFORMAÇÕES GERAIS E GARANTIA**

- 6.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI.
- 6.1.2. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.

### **6.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

- 6.2.1. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45.
- 6.2.2. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.
- 6.2.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.
- 6.2.4. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.
- 6.2.5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V.
- 6.2.6. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.
- 6.2.7. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).
- 6.2.8. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.

6.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO

- 6.3.1. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo).
- 6.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.
- 6.3.3. Deve possuir tabela MAC com suporte a 30.000 endereços.
- 6.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.
- 6.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
- 6.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
- 6.3.7. Deve suportar a comutação de Jumbo Frames.

6.4. SPANNING TREE E RECURSOS DE PROTEÇÃO

- 6.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 6.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
- 6.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
- 6.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
- 6.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
- 6.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
- 6.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).

6.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2

- 6.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
- 6.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
- 6.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
- 6.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
- 6.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos

seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.

- 6.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
- 6.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
- 6.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
- 6.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
- 6.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.

#### 6.6. AUTENTICAÇÃO, ACESSO E SEGURANÇA

- 6.6.1. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
- 6.6.2. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 6.6.3. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 6.6.4. Deve suportar autenticação por MAC Authentication Bypass (MAB).
- 6.6.5. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 6.6.6. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 6.6.7. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
- 6.6.8. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 6.6.9. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
- 6.6.10. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
- 6.6.11. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.

#### 6.7. GERENCIAMENTO E MONITORAMENTO

- 6.7.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
- 6.7.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 6.7.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço

MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.

- 6.7.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 6.7.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 6.7.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 6.7.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 6.7.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 6.7.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).
- 6.7.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 6.7.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 6.7.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
- 6.7.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 6.7.14. Deve ser capaz de realizar testes nas interfaces para diagnosticar falhas físicas em cabos UTP (par trançado) conectados ao switch.
- 6.7.15. Deve suportar configuração e monitoramento por meio de REST API.
- 6.7.16. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI”, e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
  - 6.7.16.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
  - 6.7.16.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
  - 6.7.16.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
  - 6.7.16.4. Deve operar como ponto central para automação e gerenciamento dos switches.
  - 6.7.16.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
  - 6.7.16.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
  - 6.7.16.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
  - 6.7.16.8. Deve montar a topologia da rede de maneira automática.

- 6.7.16.9. Deve ser capaz de configurar os switches da rede.
- 6.7.16.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 6.7.16.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 6.7.16.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
- 6.7.16.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
- 6.7.16.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 6.7.16.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 6.7.16.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 6.7.16.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 6.7.16.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 6.7.16.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 6.7.16.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 6.7.16.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 6.7.16.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 6.7.16.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 6.7.16.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 6.7.16.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 6.7.16.26. Deve possuir API no formato REST.

## **7. ITEM 07 – ATIVO DE REDE WIRED TIPO IV**

### **7.1. INFORMAÇÕES GERAIS E GARANTIA**

- 7.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI.

- 7.1.2. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.
- 7.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE
  - 7.2.1. Deve possuir 24 (vinte e quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE.
  - 7.2.2. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.
  - 7.2.3. Deve operar com latência igual ou inferior à 1us (microsegundo).
  - 7.2.4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.
  - 7.2.5. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.
  - 7.2.6. Deve ser fornecido com fonte de alimentação interna redundante com capacidade para operar em tensões de 110V e 220V.
  - 7.2.7. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.
  - 7.2.8. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).
  - 7.2.9. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.
  - 7.2.10. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash.
- 7.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO
  - 7.3.1. Deve possuir capacidade de comutação de pelo menos 120 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo).
  - 7.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.
  - 7.3.3. Deve possuir tabela MAC com suporte a 30.000 endereços.
  - 7.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.
  - 7.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
  - 7.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
  - 7.3.7. Deve suportar a comutação de Jumbo Frames.
- 7.4. SPANNING TREE E RECURSOS DE PROTEÇÃO
  - 7.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
  - 7.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.

- 7.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
- 7.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
- 7.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
- 7.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
- 7.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 7.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2
  - 7.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
  - 7.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
  - 7.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
  - 7.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
  - 7.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
  - 7.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
  - 7.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
  - 7.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
  - 7.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
  - 7.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.
- 7.6. CAPACIDADES DE CAMADA 3
  - 7.6.1. Deve suportar Multi-Chassis Link Aggregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica.
  - 7.6.2. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos.

- 7.6.3. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
- 7.6.4. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
- 7.6.5. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF.
- 7.6.6. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ).
- 7.6.7. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
- 7.6.8. Deve suportar o protocolo PTP (Precision Time Protocol).
- 7.7. AUTENTICAÇÃO, ACESSO E SEGURANÇA
  - 7.7.1. Deve implementar serviço de DHCP Server e DHCP Relay.
  - 7.7.2. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
  - 7.7.3. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
  - 7.7.4. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
  - 7.7.5. Deve suportar autenticação por MAC Authentication Bypass (MAB).
  - 7.7.6. Deve implementar suporte a RADIUS CoA (Change of Authorization).
  - 7.7.7. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
  - 7.7.8. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
  - 7.7.9. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
  - 7.7.10. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
  - 7.7.11. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
  - 7.7.12. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.
- 7.8. GERENCIAMENTO E MONITORAMENTO
  - 7.8.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.

- 7.8.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 7.8.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
- 7.8.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 7.8.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 7.8.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 7.8.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 7.8.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 7.8.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).
- 7.8.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 7.8.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 7.8.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
- 7.8.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 7.8.14. Deve possuir uma ferramenta de captura de pacotes que auxilie na identificação de problemas na rede. Essa ferramenta deve permitir o uso de filtros para selecionar o tráfego a ser capturado e possibilitar a exportação dos pacotes em formato .pcap, para posterior análise no software Wireshark.
- 7.8.15. Deve implementar Netflow, sFlow ou similar.
- 7.8.16. Deve suportar configuração e monitoramento por meio de REST API.
- 7.8.17. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 04, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI”, e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
  - 7.8.17.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
  - 7.8.17.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
  - 7.8.17.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
  - 7.8.17.4. Deve operar como ponto central para automação e gerenciamento dos switches.
  - 7.8.17.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.

- 7.8.17.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
- 7.8.17.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
- 7.8.17.8. Deve montar a topologia da rede de maneira automática.
- 7.8.17.9. Deve ser capaz de configurar os switches da rede.
- 7.8.17.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 7.8.17.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 7.8.17.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
- 7.8.17.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
- 7.8.17.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 7.8.17.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 7.8.17.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 7.8.17.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 7.8.17.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 7.8.17.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 7.8.17.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 7.8.17.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 7.8.17.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 7.8.17.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 7.8.17.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 7.8.17.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 7.8.17.26. Deve possuir API no formato REST.

## **8. ITEM 08 – ATIVO DE REDE WIRED POE TIPO I**

### **8.1. INFORMAÇÕES GERAIS E GARANTIA**

8.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI.

8.1.2. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.

### **8.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

8.2.1. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45.

8.2.2. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.

8.2.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.

8.2.4. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.

8.2.5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V.

8.2.6. Deve implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget mínimo de 360W.

8.2.7. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.

8.2.8. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).

8.2.9. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.

### **8.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO**

8.3.1. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo).

8.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.

8.3.3. Deve possuir tabela MAC com suporte a 30.000 endereços.

8.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.

8.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).

8.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).

8.3.7. Deve suportar a comutação de Jumbo Frames.

### **8.4. SPANNING TREE E RECURSOS DE PROTEÇÃO**

- 8.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 8.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
- 8.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
- 8.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
- 8.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
- 8.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
- 8.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 8.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2
  - 8.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
  - 8.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
  - 8.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
  - 8.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
  - 8.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
  - 8.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
  - 8.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
  - 8.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
  - 8.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
  - 8.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.
- 8.6. AUTENTICAÇÃO, ACESSO E SEGURANÇA
  - 8.6.1. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.

- 8.6.2. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 8.6.3. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 8.6.4. Deve suportar autenticação por MAC Authentication Bypass (MAB).
- 8.6.5. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 8.6.6. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 8.6.7. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
- 8.6.8. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 8.6.9. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
- 8.6.10. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
- 8.6.11. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.
- 8.7. GERENCIAMENTO E MONITORAMENTO
- 8.7.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
- 8.7.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 8.7.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
- 8.7.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 8.7.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 8.7.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 8.7.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 8.7.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 8.7.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).
- 8.7.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 8.7.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 8.7.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o

switch Deve gerar log de evento e enviar trap SNMP.

- 8.7.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 8.7.14. Deve ser capaz de realizar testes nas interfaces para diagnosticar falhas físicas em cabos UTP (par trançado) conectados ao switch.
- 8.7.15. Deve suportar configuração e monitoramento por meio de REST API.
- 8.7.16. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 E 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI”, e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
  - 8.7.16.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
  - 8.7.16.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
  - 8.7.16.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
  - 8.7.16.4. Deve operar como ponto central para automação e gerenciamento dos switches.
  - 8.7.16.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
  - 8.7.16.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
  - 8.7.16.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
  - 8.7.16.8. Deve montar a topologia da rede de maneira automática.
  - 8.7.16.9. Deve ser capaz de configurar os switches da rede.
  - 8.7.16.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
  - 8.7.16.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
  - 8.7.16.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
  - 8.7.16.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
  - 8.7.16.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
  - 8.7.16.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard,

Root Guard e BPDU Guard.

- 8.7.16.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 8.7.16.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 8.7.16.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 8.7.16.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 8.7.16.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 8.7.16.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 8.7.16.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 8.7.16.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 8.7.16.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 8.7.16.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 8.7.16.26. Deve possuir API no formato REST.

## **9. ITENS 09 – ATIVO DE REDE WIRED POE TIPO II**

### **9.1. INFORMAÇÕES GERAIS E GARANTIA**

- 9.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI.
- 9.1.2. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.

### **9.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

- 9.2.1. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45.
- 9.2.2. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.
- 9.2.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.
- 9.2.4. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.
- 9.2.5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V.

- 9.2.6. Deve implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget mínimo de 180W.
- 9.2.7. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.
- 9.2.8. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).
- 9.2.9. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.
- 9.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO
- 9.3.1. Deve possuir capacidade de comutação de pelo menos 120 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo).
- 9.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.
- 9.3.3. Deve possuir tabela MAC com suporte a 30.000 endereços.
- 9.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.
- 9.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
- 9.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
- 9.3.7. Deve suportar a comutação de Jumbo Frames.
- 9.4. SPANNING TREE E RECURSOS DE PROTEÇÃO
- 9.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 9.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
- 9.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
- 9.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
- 9.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
- 9.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
- 9.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 9.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2
- 9.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch deve aplicar descarte de pacotes ou limitar a taxa de transmissão.

- 9.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
- 9.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
- 9.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
- 9.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
- 9.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
- 9.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
- 9.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
- 9.5.9. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.
- 9.5.10. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
- 9.6. AUTENTICAÇÃO, ACESSO E SEGURANÇA
  - 9.6.1. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
  - 9.6.2. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
  - 9.6.3. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
  - 9.6.4. Deve suportar autenticação por MAC Authentication Bypass (MAB).
  - 9.6.5. Deve implementar suporte a RADIUS CoA (Change of Authorization).
  - 9.6.6. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
  - 9.6.7. Em caso de indisponibilidade dos servidores RADIUS, o switch deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
  - 9.6.8. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
  - 9.6.9. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
  - 9.6.10. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
  - 9.6.11. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.

## 9.7. GERENCIAMENTO E MONITORAMENTO

- 9.7.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
- 9.7.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 9.7.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
- 9.7.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 9.7.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 9.7.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 9.7.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 9.7.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 9.7.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).
- 9.7.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 9.7.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 9.7.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
- 9.7.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 9.7.14. Deve ser capaz de realizar testes nas interfaces para diagnosticar falhas físicas em cabos UTP (par trançado) conectados ao switch.
- 9.7.15. Deve suportar configuração e monitoramento por meio de REST API.
- 9.7.16. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI”, e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
  - 9.7.16.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
  - 9.7.16.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
  - 9.7.16.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
  - 9.7.16.4. Deve operar como ponto central para automação e gerenciamento dos switches.

- 9.7.16.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
- 9.7.16.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
- 9.7.16.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
- 9.7.16.8. Deve montar a topologia da rede de maneira automática.
- 9.7.16.9. Deve ser capaz de configurar os switches da rede.
- 9.7.16.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 9.7.16.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 9.7.16.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
- 9.7.16.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
- 9.7.16.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 9.7.16.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 9.7.16.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 9.7.16.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 9.7.16.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 9.7.16.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 9.7.16.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 9.7.16.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 9.7.16.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 9.7.16.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 9.7.16.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 9.7.16.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

9.7.16.26. Deve possuir API no formato REST.

## **10. ITEM 10 - ATIVO DE REDE WIRELESS - INDOOR**

### **10.1. INFORMAÇÕES GERAIS E GARANTIA**

10.1.1. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.

10.1.2. Deve atender aos padrões 802.11a, 802.11b, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.11X, 802.3af, 802.3at, 802.3bt, 802.3az, 802.1Q, 802.11u, 802.11w, 802.11bz.

10.1.3. Deve suportar operação na temperatura de 0 a 40 °C.

### **10.2. INTERFACES E CONECTIVIDADE FÍSICA**

10.2.1. Deve possuir, ao menos, 01 (uma) interfaces de rede 100/1000/2500/5000 Base-T RJ-45.

10.2.2. Deve possuir, ao menos, 01 (uma) interface de console RS-232 RJ-45.

10.2.3. Deve suportar PoE (Power over Ethernet), permitindo funcionamento completo sem fonte de alimentação externa via porta Ethernet.

10.2.4. Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede.

### **10.3. RECURSOS DE RÁDIO E ANTENAS**

10.3.1. Deve possuir capacidade tri-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio.

10.3.2. Deve possuir a tecnologia MU-MIMO com operação 2x2.

10.3.3. Deve possuir, ao menos 01 rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento.

10.3.4. Deve possuir suas antenas internas ao equipamento.

10.3.5. Deve possuir potência de transmissão de, ao menos, 21 dBm para cada uma das três bandas.

10.3.6. Deve suportar taxas de transmissão (data rate) de até 5.0 Gbps.

10.3.7. Deve implementar UL (uplink) MU-MIMO e DL (downlink) MU-MIMO.

10.3.8. Deve implementar Spatial Reuse (BSS Coloring).

10.3.9. Deve implementar Spectrum Analyzer.

10.3.10. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem em todas as frequências disponíveis no equipamento.

10.3.11. O ponto de acesso deve capaz de realizar varredura contínua em segundo plano, em todas as bandas disponíveis no equipamento, sem prejuízo ao fornecimento de acesso nas mesmas bandas. Caso o ponto de acesso não possua tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação.

### **10.4. FUNCIONALIDADES E OPERAÇÃO**

- 10.4.1. Deve suportar ao menos 8 SSIDs por rádio.
- 10.4.2. Deve suportar os modos de operação bridge, tunnel e mesh para os SSIDs.
- 10.4.3. Deve permitir a desativação opcional dos LEDs indicadores de status.
- 10.4.4. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID.
- 10.4.5. Deve possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais.
- 10.4.6. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve poder ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados via túnel seguro (com criptografia) até o controlador wireless.
- 10.4.7. Deve suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação.
- 10.4.8. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI”. e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- 10.5. GERENCIAMENTO CENTRALIZADO
  - 10.5.1. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
  - 10.5.2. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
  - 10.5.3. Deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.
  - 10.5.4. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 10.6. AUTENTICAÇÃO E SEGURANÇA
  - 10.6.1. Deve suportar os modos de segurança WPA2 e WPA3 por SSID, com uso dos algoritmos de criptografia compatíveis.
  - 10.6.2. Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.
  - 10.6.3. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+.
  - 10.6.4. Deve suportar filtro baseado em endereço MAC por SSID.
  - 10.6.5. Deverá possuir Captive Portal por SSID.
  - 10.6.6. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manuais, que possam ser enviadas por e-mail ou SMS aos usuários, com capacidade de definição de horário da expiração da senha.
  - 10.6.7. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 10.7. MONITORAMENTO, VISIBILIDADE E CONTROLE DE ACESSO

- 10.7.1. Deverá permitir a visualização dos clientes conectados.
- 10.7.2. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
- 10.7.3. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).
- 10.7.4. Deve possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.
- 10.7.5. Deve possuir WIDS com, ao menos, os seguintes perfis:
  - 10.7.5.1. Rogue/Interfering AP Detection.
  - 10.7.5.2. Ad-hoc Network Detection.
  - 10.7.5.3. Wireless Bridge Detection.
  - 10.7.5.4. Weak WEP Detection.
  - 10.7.5.5. MAC OUI Checking.
- 10.7.6. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 10.8. OTIMIZAÇÃO E INTELIGÊNCIA DE RÁDIO FREQUÊNCIA (RF)
  - 10.8.1. Deve permitir configurar parâmetros de rádio, como: banda e canal.
  - 10.8.2. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
  - 10.8.3. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre dois Access Points gerenciados.
  - 10.8.4. Deve possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
  - 10.8.5. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
  - 10.8.6. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas mesmas frequências. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.
  - 10.8.7. A solução deve detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.
  - 10.8.8. Deverá prover suporte a Fast Roaming.
- 10.9. CONTROLE DE TRÁFEGO, QOS E POLÍTICAS
  - 10.9.1. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
  - 10.9.2. Deverá permitir e/ou bloquear o tráfego entre SSIDs.

- 10.9.3. Deverá possibilitar definir número de clientes por SSID.
- 10.9.4. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
- 10.9.5. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 10.9.6. Deverá permitir a criação de políticas de firewall baseadas em horário.
- 10.9.7. Deverá permitir NAT nas políticas de firewall.

## **11. ITEM 11 - ATIVO DE REDE WIRELESS – OUTDOOR**

### **11.1. INFORMAÇÕES GERAIS E GARANTIA**

- 11.1.1. Deve possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses.
- 11.1.2. Deve atender aos padrões 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.11Q, 802.11X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bt, 802.3bz.
- 11.1.3. Deve suportar operação na temperatura de 0 a 50 °C.
- 11.1.4. Deve possuir certificação para ambientes externos IP67.

### **11.2. INTERFACES E CONECTIVIDADE FÍSICA**

- 11.2.1. Deve possuir, ao menos, 02 (duas) interfaces de rede 100/1000 Base-T RJ-45.
- 11.2.2. Deve possuir, ao menos, 01 (uma) interface de console RS-232 RJ-45.
- 11.2.3. Deve suportar PoE (Power over Ethernet), permitindo funcionamento completo sem fonte de alimentação externa via qualquer porta Ethernet.
- 11.2.4. Deve ser incluso injetor PoE capaz de suportar completa operação do equipamento.
- 11.2.5. Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede.

### **11.3. RECURSOS DE RÁDIO E ANTENAS**

- 11.3.1. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
- 11.3.2. Deve possuir a tecnologia MU-MIMO com operação 4x4.
- 11.3.3. Deve possuir, ao menos 01 rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento.
- 11.3.4. Deve possuir antenas externas ao equipamento.
- 11.3.5. Deve possuir potência de transmissão de, ao menos, 24 dBm para cada uma das bandas.
- 11.3.6. Deve suportar taxas de transmissão (data rate) de até 2.0 Gbps.
- 11.3.7. Deve implementar UL (uplink) MU-MIMO e DL (downlink) MU-MIMO.
- 11.3.8. Deve implementar Spatial Reuse (BSS Coloring).

- 11.3.9. Deve implementar Spectrum Analyzer.
- 11.3.10. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem em todas as frequências disponíveis no equipamento.
- 11.3.11. O ponto de acesso deve capaz de realizar varredura contínua em segundo plano, em todas as bandas disponíveis no equipamento, sem prejuízo ao fornecimento de acesso nas mesmas bandas. Caso o ponto de acesso não possua tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação.
- 11.4. FUNCIONALIDADES E OPERAÇÃO
- 11.4.1. Deve suportar ao menos 8 SSIDs por rádio.
- 11.4.2. Deve suportar os modos de operação bridge, tunnel e mesh para os SSIDs.
- 11.4.3. Deve permitir a desativação opcional dos LEDs indicadores de status.
- 11.4.4. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID.
- 11.4.5. Deve possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais.
- 11.4.6. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve poder ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados via túnel seguro (com criptografia) até o controlador wireless.
- 11.4.7. Deve suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação.
- 11.4.8. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II, III, IV, V e VI”. e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- 11.4.8.1. Gerenciamento Centralizado
- 11.4.8.1.1. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 11.4.8.1.2. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
- 11.4.8.1.3. Deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.
- 11.4.8.1.4. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 11.4.8.2. Autenticação e Segurança
- 11.4.8.2.1. Deve suportar os modos de segurança WPA2 e WPA3 por SSID, com uso dos algoritmos de criptografia compatíveis.
- 11.4.8.2.2. Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.
- 11.4.8.2.3. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS

ou TACACS+.

- 11.4.8.2.4. Deve suportar filtro baseado em endereço MAC por SSID.
- 11.4.8.2.5. Deverá possuir Captive Portal por SSID.
- 11.4.8.2.6. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manuais, que possam ser enviadas por e-mail ou SMS aos usuários, com capacidade de definição de horário da expiração da senha.
- 11.4.8.2.7. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 11.4.8.3. Monitoramento, Visibilidade e Controle de Acesso
  - 11.4.8.3.1. Deverá permitir a visualização dos clientes conectados.
  - 11.4.8.3.2. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
  - 11.4.8.3.3. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).
  - 11.4.8.3.4. Deve possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.
  - 11.4.8.3.5. Deve possuir WIDS com, ao menos, os seguintes perfis:
    - 11.4.8.3.5.1. Rogue/Interfering AP Detection.
    - 11.4.8.3.5.2. Ad-hoc Network Detection.
    - 11.4.8.3.5.3. Wireless Bridge Detection.
    - 11.4.8.3.5.4. Weak WEP Detection.
    - 11.4.8.3.5.5. MAC OUI Checking.
  - 11.4.8.3.6. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 11.4.8.4. Otimização e Inteligência de Rádio Frequência (RF)
  - 11.4.8.4.1. Deve permitir configurar parâmetros de rádio, como: banda e canal.
  - 11.4.8.4.2. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
  - 11.4.8.4.3. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre dois Access Points gerenciados.
  - 11.4.8.4.4. Deve possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
  - 11.4.8.4.5. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
  - 11.4.8.4.6. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de

interferências provenientes de equipamentos não-WiFi e que operem nas mesmas frequências. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.

- 11.4.8.4.7. A solução deve detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.
- 11.4.8.4.8. Deverá prover suporte a Fast Roaming.
- 11.4.8.5. Controle de Tráfego, QOS e Políticas
  - 11.4.8.5.1. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
  - 11.4.8.5.2. Deverá permitir e/ou bloquear o tráfego entre SSIDs.
  - 11.4.8.5.3. Deverá possibilitar definir número de clientes por SSID.
  - 11.4.8.5.4. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
  - 11.4.8.5.5. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
  - 11.4.8.5.6. Deverá permitir a criação de políticas de firewall baseadas em horário.
  - 11.4.8.5.7. Deverá permitir NAT nas políticas de firewall.

## **12. ITEM 12 – SOLUÇÃO DE SEGURANÇA DE ENDPOINT – EPP TIPO I**

### **12.1. REQUISITOS GERAIS**

- 12.1.1. Deve permitir a instalação, gerenciamento e atualização das funcionalidades de 500 (quinhentos) endpoints durante toda a vigência contratual de 36 (trinta e seis) meses.
- 12.1.2. O modelo de licenciamento deve ser baseado no número de endpoints registrados no console central de gerenciamento do mesmo fabricante.
- 12.1.3. O licenciamento deve incluir, no mínimo, as seguintes funcionalidades: recursos de acesso baseado em Zero Trust (ZTNA), antivírus (AV), proteção contra ransomware e exploits, firewall de aplicações, inventário de software, controle de dispositivos USB e proteção avançada contra ameaças por meio de sandboxing em nuvem.
- 12.1.4. Deve permitir o gerenciamento remoto dos clientes de segurança por meio de um console centralizado fornecido pelo próprio fabricante.
- 12.1.5. Deve permitir a realização de backup do arquivo de configuração.
- 12.1.6. Os clientes de segurança devem ser capazes de enviar logs para o console central de gerenciamento.
- 12.1.7. Deve ser capaz de registrar logs (diário de eventos) referentes às funcionalidades instaladas e configuradas.
- 12.1.8. Deve permitir a definição dos níveis de log, incluindo: emergência, alerta, crítico, erro, aviso, depuração e informações.
- 12.1.9. Deve suportar, no mínimo, os seguintes níveis de log: emergência, alerta, crítico, erro, aviso e

informativo.

- 12.1.10. Deve permitir a ativação seletiva de logs para os seguintes módulos: VPN, antivírus, atualizações, sandboxing, comunicação com segurança cooperativa, filtro web e verificação de vulnerabilidades.
- 12.1.11. Deve permitir a exportação dos logs para fora do cliente de segurança.
- 12.1.12. Os clientes de segurança devem permitir configuração local por meio de arquivos no formato XML (eXtensible Markup Language).
- 12.1.13. Deve oferecer funcionalidade de Zero Trust Applied, com túneis criptografados automáticos que validam o acesso a aplicativos por sessão, com base em avaliação de postura do endpoint.
- 12.1.14. Os clientes de segurança devem suportar integração com tecnologias de sandboxing, ao menos do mesmo fabricante.
- 12.1.15. Deve permitir o controle de acesso a dispositivos removíveis, possibilitando monitorar, permitir ou bloquear conexões via USB.
- 12.1.16. A Solução deve oferecer agente de logon único.
- 12.1.17. Deve possuir a capacidade de desabilitar serviços de proxy para fins de depuração.
- 12.1.18. Deve ser compatível, no mínimo, com os seguintes sistemas operacionais: Microsoft Windows 7, 8, 8.1, 10 (32 e 64 bits) e 11 (64 bits). Windows Server 2012 ou superior. macOS 10.14 ou superior. Android 5.0 ou superior. e Linux Ubuntu 16.04 ou superior.
- 12.1.19. Deve disponibilizar interface gráfica para o usuário final, com suporte aos idiomas português, inglês e espanhol.
- 12.2. FUNCIONALIDADES DE ANÁLISE COOPERATIVA
  - 12.2.1. Deverá ser capaz de integrar a uma estrutura cooperativa para compartilhar informações e receber atualizações de assinaturas dinâmicas.
  - 12.2.2. Deverá suportar o envio de logs para um analisador central de logs, onde os índices de compromissos do cliente (IoC) seja processado (taxas de confirmação)
  - 12.2.3. Deverá suportar receber atualizações de assinaturas dinâmicas da solução de proteção avançada de ameaças (ATP) ou sandboxing
  - 12.2.4. Deverá ser disponibilizado uma ferramenta que permita a aplicação de políticas diferentes, independente do cliente estar conectado ou não à rede corporativa.
  - 12.2.5. Deverá permitir ficar em quarentena no console central ou em algum outro componente que faça parte da solução de segurança cooperativa.
- 12.3. FUNCIONALIDADES DE ANTIVÍRUS
  - 12.3.1. O cliente de segurança deverá ter a capacidade de inspecionar arquivos executáveis, bibliotecas e drivers quanto a vírus.
  - 12.3.2. O cliente de segurança deverá ser capaz de verificar atualizações de assinatura automaticamente
  - 12.3.3. O cliente de segurança deverá ser capaz de enviar arquivos para inspeção nos sistemas Sandboxing do mesmo fabricante.

- 12.3.4. O cliente de segurança deverá ser capaz de bloquear os canais de comunicação usados por hackers ou atacantes.
- 12.3.5. O cliente de segurança deverá notificar localmente quando um vírus é detectado
- 12.3.6. O cliente de segurança deverá permitir que o usuário inicie uma verificação sob demanda
- 12.3.7. O cliente de segurança deverá permitir que a verificação de vírus seja iniciada automaticamente regularmente
- 12.3.8. O cliente de segurança deverá permitir a visualização dos arquivos em quarentena
- 12.3.9. Deverá permitir a configuração do perfil antivírus a partir do console central do mesmo fabricante
- 12.3.10. Deverá ter uma solução de proteção contra malware baseada em nuvem. Essa proteção deve ser capaz de gerar uma soma de verificação do arquivo acessado e consultar a nuvem se essa soma de verificação corresponder a uma nova ameaça.
- 12.3.11. A ferramenta de proteção baseada em nuvem NÃO deverá enviar o arquivo inteiro ou seus metadados. SOMENTE a soma de verificação
- 12.3.12. A ferramenta de proteção baseada em nuvem deverá analisar apenas arquivos de alto risco, como, entre outros, documentos do Word, Excel, PDF e DLL.
- 12.3.13. Deverá ter uma solução de Anti-Exploit, que protege o endpoint de ameaças em tempo real, observando o comportamento de aplicativos populares, incluindo os leitores do Office, Internet Explorer, Chrome, Firefox, Java, Java, Flash e PDF. Etc
- 12.3.14. Deverá ser capaz de enviar arquivos para uma solução de proteção avançada de ameaças (ATP) (ou sandboxing) antes de ser acessado.
- 12.3.15. Deverá suportar sandbox localmente ou através de uma solução em nuvem
- 12.3.16. Deverá ser capaz de bloquear o acesso ao arquivo até que o sandbox dê um veredicto
- 12.3.17. Caso um arquivo seja marcado como malicioso pela Sandbox, o mesmo deverá ser mantido em quarentena.
- 12.4. FUNCIONALIDADES DE FIREWALL DE APLICATIVOS
  - 12.4.1. O cliente de segurança deverá suportar perfis de Controle de Aplicativos, criados centralmente no console de gerenciamento do mesmo fabricante.
  - 12.4.2. O fabricante deverá permitir que os clientes de segurança façam consultas on-line sobre a categoria de um determinado aplicativo a ser usado na política de controle de acesso
  - 12.4.3. Deve possuir pelo menos 4000 aplicativos reconhecidos em sua base para que possam ser usados nas regras de controle de acesso dos clientes de segurança
- 12.5. FUNCIONALIDADES DE VPN IPSEC
  - 12.5.1. Deverá permitir que o usuário crie novas VPNs IPSEC.
  - 12.5.2. Deverá permitir que várias VPNs IPSEC sejam definidas simultaneamente.
  - 12.5.3. Deverá permitir a autenticação usando nome de usuário e senha.

- 12.5.4. Deverá permitir a autenticação usando certificados digitais.
- 12.5.5. Deverá permitir a seleção dos modos Principal e Agressivo.
- 12.5.6. Deverá permitir a configuração do DHCP por IPSec.
- 12.5.7. Deverá permitir o uso do NAT Traversal.
- 12.5.8. Deverá permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14).
- 12.5.9. Deverá permitir configurações de expiração de chave IKE.
- 12.5.10. Deverá suportar IKEv1 e IKEv2.
- 12.5.11. Deverá permitir o uso do Perfect Forward Secrecy.
- 12.5.12. Deverá permitir a autenticação de dois fatores fornecida pelo mesmo fabricante.
- 12.6. FUNCIONALIDADES DE GERENCIAMENTO CENTRALIZADO
  - 12.6.1. O console de gerenciamento centralizado deverá ser entregue sem custo.
  - 12.6.2. Deverá permitir a adição de clientes adicionando licenças.
  - 12.6.3. Deverá ter interface gráfica de gerenciamento.
  - 12.6.4. Deverá ter funcionalidade de backup.
  - 12.6.5. Deverá permitir a criação de usuários de diferentes perfis administrativos.
  - 12.6.6. Deverá permitir importar informações do Active Directory usando LDAP.
  - 12.6.7. Deverá permitir registro manual da estação através de um uso de uma senha.
  - 12.6.8. Deverá permitir a criação de grupos de clientes para facilitar o gerenciamento.
  - 12.6.9. Deverá permitir que a configuração do cliente mediante a definições em XML.
  - 12.6.10. Deverá permitir que as configurações de perfil sejam importadas em um dispositivo de firewall do mesmo fabricante.
  - 12.6.11. Deverá permitir a configuração de diferentes grupos e perfis para facilitar a administração.
  - 12.6.12. Deverá permitir a configuração de antivírus, filtro da web, controle de aplicativos, verificador de vulnerabilidades e perfis de VPN.
  - 12.6.13. Deverá permitir a proteção em tempo real.
  - 12.6.14. Deverá permitir que a configuração de pesquisas de vírus e vulnerabilidades em uma base agendada.
  - 12.6.15. Deverá permitir verificação completa e verificação rápida.
  - 12.6.16. Deverá permitir que o usuário configure VPNs localmente.
  - 12.6.17. Deverá permitir que o usuário desconecte uma VPN.
  - 12.6.18. Deverá permitir a conexão VPN antes do login.

- 12.6.19. Deverá permitir conexão VPN automática.
- 12.6.20. Deverá suportar o uso específico ou geral para VPN IPSec (pelo menos):
- 12.6.21. Deverá suportar o uso de certificados ou usuário e senha para autenticação.
- 12.6.22. Deverá suportar o uso de certificados no cartão inteligente.
- 12.6.23. Deverá suportar o bloqueio de tráfego IPv6.
- 12.6.24. Deverá suportar à opção para o usuário acessar a configuração do cliente por senha.
- 12.6.25. Deverá ser capaz de enviar logs para um sistema de log externos do mesmo fabricante.
- 12.6.26. Deverá permitir a instalação do certificado digital no cliente.
- 12.6.27. Deverá permitir ativar as funcionalidades de Logon Único.
- 12.6.28. Deverá ter informações disponíveis sobre: Número de dispositivos gerenciados, Versão do sistema operacional, Perfil aplicado, Usuário, Versão de assinatura do antivírus.
- 12.6.29. Status do cliente de segurança: Registrado ou não registrado.
- 12.6.30. Deverá conter informações sobre o sistema operacional no qual o cliente está instalado.
- 12.6.31. Deverá informar o perfil de segurança criado e / ou aplicado.
- 12.6.32. Deverá informar os recursos de segurança aplicados: antivírus, filtro da web, VPN, firewall de aplicativo.
- 12.6.33. Deverá permitir habilitar ou desabilitar os recursos antivírus, filtro da web, VPN, firewall de aplicativo nos terminais gerenciados.
- 12.6.34. Deverá ser capaz de fazer um inventário do software instalado em cada nó de extremidade.
- 12.6.35. Deverá permitir a implantação automática de clientes de terminal de acordo com a OU do MS AD ou grupos do MS AD.
- 12.6.36. Deverá permitir a manutenção de várias instâncias de instaladores com recursos diferentes (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.).
- 12.6.37. Deverá permitir a implantação de equipamentos que NÃO pertencem ao active directory (AD).
- 12.6.38. Deverá permitir que regras de conformidade deficientes impeçam que um cliente mal configurado se conecte a redes críticas.
- 12.6.39. Deverá ser capaz de ser acessado através da administração WEB.
- 12.6.40. Deverá ter um painel em que possa verificar rapidamente o status de integridade dos clientes.
- 12.6.41. Deverá lidar com listas centralizadas de quarentena de arquivos.
- 12.6.42. Deverá poder aplicar políticas aos terminais de acordo com os grupos, para que os clientes pertencentes a esse grupo tenham a mesma política.
- 12.6.43. Deverá poder aplicar políticas aos terminais de acordo com o usuário pertencente ao grupo, tornando mais granular à aplicação da política.

- 12.6.44. Deverá poder atribuir configurações dinamicamente quando os clientes forem movidos dos grupos.
- 12.6.45. As políticas de terminal devem atribuir perfis de proteção aos terminais. Esses perfis devem ser uma maneira de implantar uma configuração exclusiva de: malware, sandboxing, webfilter, firewall de aplicativos, VPN, verificação de vulnerabilidades e configurações do sistema (por exemplo, logfiels).
- 12.6.46. Os usuários administradores devem poder sincronizar com o AD, para permitir o login com as mesmas credenciais
- 12.6.47. Deverá ser capaz de definir funções administrativas.
- 12.6.48. Deverá suportar fazer backup / restaurar configurações do console, configuração do servidor, políticas de terminal etc.
- 12.7. FUNCIONALIDADES DE PROVISIONAMENTO DE CLIENTES.
- 12.7.1. O fabricante deverá fornecer um portal para baixar a segurança do cliente e permitir a instalação local.
- 12.7.2. Deverá ser compatível com a instalação via Microsoft Active Directory.
- 12.7.3. O console de gerenciamento central deverá poder instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft.
- 12.7.4. Deverá suportar criação de várias versões de pacotes de instalação para serem associadas a grupos do Microsoft Active Directory.
- 12.8. VISIBILIDADE
- 12.8.1. Deverá fornecer informações da estação de trabalho, no mínimo e não se limitando a: Nome completo, Telefone, E-mail, Informações pessoais obtidas minimamente de (entrada manual, linkedin, google, Sistema operacional e / ou salesforce), status do cliente, Nome do host, etiqueta de host.
- 12.8.2. Deverá suportar upload de uma foto ou avatar para identificação rápida do usuário
- 12.8.3. Deverá relatar de maneira rápida e rápida, se fizer parte de um ambiente de segurança cooperativo.
- 12.8.4. Deverá relatar rapidamente o nível de vulnerabilidade da estação de trabalho.
- 12.8.5. Deverá ter um sistema de notificação pop-up.
- 12.8.6. Deverá ter uma lista de notificações atuais e anteriores.
- 12.8.7. As notificações devem incluir: eventos AV, eventos ATP, eventos de comunicação, eventos de filtro da web e eventos do sistema.
- 12.8.8. Deverá fornecer informações sobre a vulnerabilidade, patches, versões afetadas etc., bem como o CVE correspondente.
- 12.8.9. Deverá fornecer uma lista de aplicativos bloqueados.
- 12.8.10. Caso o cliente fique em quarentena, deverá ser capaz de informar ao usuário e notificar o gerenciamento.
- 12.8.11. Deverá suportar a exibição de uma lista de explorações detectadas.
- 12.8.12. Deverá permitir exibir uma lista de aplicativos protegidos contra exploração.

12.8.13. Deverá fornecer uma lista de arquivos em quarentena.

12.8.14. Deverá ser possível visualizar os resultados da análise ATP.

#### 12.9. ANÁLISE DE VULNERABILIDADE

12.9.1. O cliente de segurança deverá ter um módulo de pesquisa de vulnerabilidades integrado e permitir o gerenciamento central no console do mesmo fabricante.

12.9.2. Deverá permitir que o usuário inicie uma análise de vulnerabilidade sob demanda.

12.9.3. As vulnerabilidades encontradas devem ser exibidas localmente com um link para visualizar informações de um banco de dados na Internet. deverá ter pelo menos: nome, gravidade e detalhes.

12.9.4. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas.

12.9.5. Links de acesso a informações complementares devem ser fornecidos, por exemplo, links para a página do fabricante onde as características da vulnerabilidade são detalhadas.

12.9.6. Deverá permitir a aplicação automática de patches.

12.9.7. Deverá detalhar quais correções requerem instalação manual.

12.9.8. A verificação de vulnerabilidades deverá ser permitida de maneira ordenada e autônoma a partir do console central.

12.9.9. Deverá verificar as vulnerabilidades antes de aplicar patches.

#### 12.10. FUNCIONALIDADES DE FILTRO DE CONTEÚDO WEB

12.10.1. Deverá permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante.

12.10.2. O fabricante deverá fazer consultas on-line com o cliente de segurança sobre a categoria de um determinado site (por exemplo, interesse geral, tecnologia, hackers, pornografia etc.) para aplicar a política de controle de acesso à Internet.

12.10.3. O cliente de segurança deverá suportar regras estáticas de acesso à Internet com base em expressões regulares.

12.10.4. Para um determinada URL, os acessos devem ser: permitir, bloquear, alertar ou monitorar.

12.10.5. Deverá configurar o filtro de URL fornecido pelo fabricante com pelo menos as seguintes ações:

12.10.6. Bloquear, avisar, permitir e monitorar.

12.10.7. Deverá configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as seguintes ações: Bloquear ou permitir.

### 13. ITEM 13 – SOLUÇÃO DE SEGURANÇA DE ENDPOINT – EPP TIPO II

#### 13.1. REQUISITOS GERAIS

13.1.1. Deve permitir a instalação, gerenciamento e atualização das funcionalidades de 25 (vinte e cinco) endpoints durante toda a vigência contratual de 36 (trinta e seis) meses.

- 13.1.2. O modelo de licenciamento deve ser baseado no número de endpoints registrados no console central de gerenciamento do mesmo fabricante.
- 13.1.3. O licenciamento deve incluir, no mínimo, as seguintes funcionalidades: recursos de acesso baseado em Zero Trust (ZTNA), antivírus (AV), proteção contra ransomware e exploits, firewall de aplicações, inventário de software, controle de dispositivos USB e proteção avançada contra ameaças por meio de sandboxing em nuvem.
- 13.1.4. Deve permitir o gerenciamento remoto dos clientes de segurança por meio de um console centralizado fornecido pelo próprio fabricante.
- 13.1.5. Deve permitir a realização de backup do arquivo de configuração.
- 13.1.6. Os clientes de segurança devem ser capazes de enviar logs para o console central de gerenciamento.
- 13.1.7. Deve ser capaz de registrar logs (diário de eventos) referentes às funcionalidades instaladas e configuradas.
- 13.1.8. Deve permitir a definição dos níveis de log, incluindo: emergência, alerta, crítico, erro, aviso, depuração e informações.
- 13.1.9. Deve suportar, no mínimo, os seguintes níveis de log: emergência, alerta, crítico, erro, aviso e informativo.
- 13.1.10. Deve permitir a ativação seletiva de logs para os seguintes módulos: VPN, antivírus, atualizações, sandboxing, comunicação com segurança cooperativa, filtro web e verificação de vulnerabilidades.
- 13.1.11. Deve permitir a exportação dos logs para fora do cliente de segurança.
- 13.1.12. Os clientes de segurança devem permitir configuração local por meio de arquivos no formato XML (eXtensible Markup Language).
- 13.1.13. Deve oferecer funcionalidade de Zero Trust Applied, com túneis criptografados automáticos que validam o acesso a aplicativos por sessão, com base em avaliação de postura do endpoint.
- 13.1.14. Os clientes de segurança devem suportar integração com tecnologias de sandboxing, ao menos do mesmo fabricante.
- 13.1.15. Deve permitir o controle de acesso a dispositivos removíveis, possibilitando monitorar, permitir ou bloquear conexões via USB.
- 13.1.16. A Solução deve oferecer agente de logon único.
- 13.1.17. Deve possuir a capacidade de desabilitar serviços de proxy para fins de depuração.
- 13.1.18. Deve ser compatível, no mínimo, com os seguintes sistemas operacionais: Microsoft Windows 7, 8, 8.1, 10 (32 e 64 bits) e 11 (64 bits). Windows Server 2012 ou superior. macOS 10.14 ou superior. Android 5.0 ou superior. e Linux Ubuntu 16.04 ou superior.
- 13.1.19. Deve disponibilizar interface gráfica para o usuário final, com suporte aos idiomas português, inglês e espanhol.
- 13.2. FUNCIONALIDADES DE ANÁLISE COOPERATIVA
- 13.2.1. Deverá ser capaz de integrar a uma estrutura cooperativa para compartilhar informações e receber atualizações de assinaturas dinâmicas.

- 13.2.2. Deverá suportar o envio de logs para um analisador central de logs, onde os índices de compromissos do cliente (IoC) seja processado (taxas de confirmação)
- 13.2.3. Deverá suportar receber atualizações de assinaturas dinâmicas da solução de proteção avançada de ameaças (ATP) ou sandboxing.
- 13.2.4. Deverá ser disponibilizado uma ferramenta que permita a aplicação de políticas diferentes, independente do cliente estar conectado ou não à rede corporativa.
- 13.2.5. Deverá permitir ficar em quarentena no console central ou em algum outro componente que faça parte da solução de segurança cooperativa.
- 13.3. FUNCIONALIDADES DE ANTIVIRUS
  - 13.3.1. O cliente de segurança deverá ter a capacidade de inspecionar arquivos executáveis, bibliotecas e drivers quanto a vírus.
  - 13.3.2. O cliente de segurança deverá ser capaz de verificar atualizações de assinatura automaticamente
  - 13.3.3. O cliente de segurança deverá ser capaz de enviar arquivos para inspeção nos sistemas Sandboxing do mesmo fabricante.
  - 13.3.4. O cliente de segurança deverá ser capaz de bloquear os canais de comunicação usados por hackers ou atacantes.
  - 13.3.5. O cliente de segurança deverá notificar localmente quando um vírus é detectado
  - 13.3.6. O cliente de segurança deverá permitir que o usuário inicie uma verificação sob demanda
  - 13.3.7. O cliente de segurança deverá permitir que a verificação de vírus seja iniciada automaticamente regularmente
  - 13.3.8. O cliente de segurança deverá permitir a visualização dos arquivos em quarentena
  - 13.3.9. Deverá permitir a configuração do perfil antivírus a partir do console central do mesmo fabricante
  - 13.3.10. Deverá ter uma solução de proteção contra malware baseada em nuvem. Essa proteção deve ser capaz de gerar uma soma de verificação do arquivo acessado e consultar a nuvem se essa soma de verificação corresponder a uma nova ameaça.
  - 13.3.11. A ferramenta de proteção baseada em nuvem NÃO deverá enviar o arquivo inteiro ou seus metadados. SOMENTE a soma de verificação
  - 13.3.12. A ferramenta de proteção baseada em nuvem deverá analisar apenas arquivos de alto risco, como, entre outros, documentos do Word, Excel, PDF e DLL.
  - 13.3.13. Deverá ter uma solução de Anti-Exploit, que protege o endpoint de ameaças em tempo real, observando o comportamento de aplicativos populares, incluindo os leitores do Office, Internet Explorer, Chrome, Firefox, Java, Java, Flash e PDF. Etc
  - 13.3.14. Deverá ser capaz de enviar arquivos para uma solução de proteção avançada de ameaças (ATP) (ou sandboxing) antes de ser acessado.
  - 13.3.15. Deverá suportar sandbox localmente ou através de uma solução em nuvem
  - 13.3.16. Deverá ser capaz de bloquear o acesso ao arquivo até que o sandbox dê um veredicto

13.3.17. Caso um arquivo seja marcado como malicioso pela Sandbox, o mesmo deverá ser mantido em quarentena.

#### 13.4. FUNCIONALIDADES DE FIREWALL DE APLICATIVOS

13.4.1. O cliente de segurança deverá suportar perfis de Controle de Aplicativos, criados centralmente no console de gerenciamento do mesmo fabricante.

13.4.2. O fabricante deverá permitir que os clientes de segurança façam consultas on-line sobre a categoria de um determinado aplicativo a ser usado na política de controle de acesso

13.4.3. Deve possuir pelo menos 4000 aplicativos reconhecidos em sua base para que possam ser usados nas regras de controle de acesso dos clientes de segurança

#### 13.5. FUNCIONALIDADES DE VPN IPSEC

13.5.1. Deverá permitir que o usuário crie novas VPNs IPSEC.

13.5.2. Deverá permitir que várias VPNs IPSEC sejam definidas simultaneamente.

13.5.3. Deverá permitir a autenticação usando nome de usuário e senha.

13.5.4. Deverá permitir a autenticação usando certificados digitais.

13.5.5. Deverá permitir a seleção dos modos Principal e Agressivo.

13.5.6. Deverá permitir a configuração do DHCP por IPSec.

13.5.7. Deverá permitir o uso do NAT Traversal.

13.5.8. Deverá permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14).

13.5.9. Deverá permitir configurações de expiração de chave IKE.

13.5.10. Deverá suportar IKEv1 e IKEv2.

13.5.11. Deverá permitir o uso do Perfect Forward Secrecy.

13.5.12. Deverá permitir a autenticação de dois fatores fornecida pelo mesmo fabricante.

#### 13.6. FUNCIONALIDADES DE GERENCIAMENTO CENTRALIZADO

13.6.1. O console de gerenciamento centralizado deverá ser entregue sem custo.

13.6.2. Deverá permitir a adição de clientes adicionando licenças.

13.6.3. Deverá ter interface gráfica de gerenciamento.

13.6.4. Deverá ter funcionalidade de backup.

13.6.5. Deverá permitir a criação de usuários de diferentes perfis administrativos.

13.6.6. Deverá permitir importar informações do Active Directory usando LDAP.

13.6.7. Deverá permitir registro manual da estação através de um uso de uma senha.

13.6.8. Deverá permitir a criação de grupos de clientes para facilitar o gerenciamento.

- 13.6.9. Deverá permitir que a configuração do cliente mediante a definições em XML.
- 13.6.10. Deverá permitir que as configurações de perfil sejam importadas em um dispositivo de firewall do mesmo fabricante.
- 13.6.11. Deverá permitir a configuração de diferentes grupos e perfis para facilitar a administração.
- 13.6.12. Deverá permitir a configuração de antivírus, filtro da web, controle de aplicativos, verificador de vulnerabilidades e perfis de VPN.
- 13.6.13. Deverá permitir a proteção em tempo real.
- 13.6.14. Deverá permitir que a configuração de pesquisas de vírus e vulnerabilidades em uma base agendada.
- 13.6.15. Deverá permitir verificação completa e verificação rápida.
- 13.6.16. Deverá permitir que o usuário configure VPNs localmente.
- 13.6.17. Deverá permitir que o usuário desconecte uma VPN.
- 13.6.18. Deverá permitir a conexão VPN antes do login.
- 13.6.19. Deverá permitir conexão VPN automática.
- 13.6.20. Deverá suportar o uso específico ou geral para VPN IPSec (pelo menos):
- 13.6.21. Deverá suportar o uso de certificados ou usuário e senha para autenticação.
- 13.6.22. Deverá suportar o uso de certificados no cartão inteligente.
- 13.6.23. Deverá suportar o bloqueio de tráfego IPv6.
- 13.6.24. Deverá suportar a opção para o usuário acessar a configuração do cliente por senha.
- 13.6.25. Deverá ser capaz de enviar logs para um sistema de log externos do mesmo fabricante.
- 13.6.26. Deverá permitir a instalação do certificado digital no cliente.
- 13.6.27. Deverá permitir ativar as funcionalidades de Logon Único.
- 13.6.28. Deverá ter informações disponíveis sobre: Número de dispositivos gerenciados, Versão do sistema operacional, Perfil aplicado, Usuário, Versão de assinatura do antivírus.
- 13.6.29. Status do cliente de segurança: Registrado ou não registrado.
- 13.6.30. Deverá conter informações sobre o sistema operacional no qual o cliente está instalado.
- 13.6.31. Deverá informar o perfil de segurança criado e / ou aplicado.
- 13.6.32. Deverá informar os recursos de segurança aplicados: antivírus, filtro da web, VPN, firewall de aplicativo.
- 13.6.33. Deverá permitir habilitar ou desabilitar os recursos antivírus, filtro da web, VPN, firewall de aplicativo nos terminais gerenciados.
- 13.6.34. Deverá ser capaz de fazer um inventário do software instalado em cada nó de extremidade.
- 13.6.35. Deverá permitir a implantação automática de clientes de terminal de acordo com a OU do MS AD ou

grupos do MS AD.

- 13.6.36. Deverá permitir a manutenção de várias instâncias de instaladores com recursos diferentes (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.).
- 13.6.37. Deverá permitir a implantação de equipamentos que NÃO pertencem ao active directory (AD).
- 13.6.38. Deverá permitir que regras de conformidade deficientes impeçam que um cliente mal configurado se conecte a redes críticas.
- 13.6.39. Deverá ser capaz de ser acessado através da administração WEB.
- 13.6.40. Deverá ter um painel em que possa verificar rapidamente o status de integridade dos clientes.
- 13.6.41. Deverá lidar com listas centralizadas de quarentena de arquivos.
- 13.6.42. Deverá poder aplicar políticas aos terminais de acordo com os grupos, para que os clientes pertencentes a esse grupo tenham a mesma política.
- 13.6.43. Deverá poder aplicar políticas aos terminais de acordo com o usuário pertencente ao grupo, tornando mais granular a aplicação da política.
- 13.6.44. Deverá poder atribuir configurações dinamicamente quando os clientes forem movidos dos grupos.
- 13.6.45. As políticas de terminal devem atribuir perfis de proteção aos terminais. Esses perfis devem ser uma maneira de implantar uma configuração exclusiva de: malware, sandboxing, webfilter, firewall de aplicativos, VPN, verificação de vulnerabilidades e configurações do sistema (por exemplo, logfiels).
- 13.6.46. Os usuários administradores devem poder sincronizar com o AD, para permitir o login com as mesmas credenciais
- 13.6.47. Deverá ser capaz de definir funções administrativas.
- 13.6.48. Deverá suportar fazer backup / restaurar configurações do console, configuração do servidor, políticas de terminal etc.
- 13.7. FUNCIONALIDADES DE PROVISIONAMENTO DE CLIENTES.
  - 13.7.1. O fabricante deverá fornecer um portal para baixar a segurança do cliente e permitir a instalação local.
  - 13.7.2. Deverá ser compatível com a instalação via Microsoft Active Directory.
  - 13.7.3. O console de gerenciamento central deverá poder instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft.
  - 13.7.4. Deverá suportar criação de várias versões de pacotes de instalação para serem associadas a grupos do Microsoft Active Directory.
- 13.8. VISIBILIDADE
  - 13.8.1. Deverá fornecer informações da estação de trabalho, no mínimo e não se limitando a: Nome completo, Telefone, E-mail, Informações pessoais obtidas minimamente de (entrada manual, linkedin, google, Sistema operacional e / ou salesforce), status do cliente, Nome do host, etiqueta de host.
  - 13.8.2. Deverá suportar upload de uma foto ou avatar para identificação rápida do usuário
  - 13.8.3. Deverá relatar de maneira rápida e rápida, se fizer parte de um ambiente de segurança cooperativo.

- 13.8.4. Deverá relatar rapidamente o nível de vulnerabilidade da estação de trabalho.
- 13.8.5. Deverá ter um sistema de notificação pop-up.
- 13.8.6. Deverá ter uma lista de notificações atuais e anteriores.
- 13.8.7. As notificações devem incluir: eventos AV, eventos ATP, eventos de comunicação, eventos de filtro da web e eventos do sistema.
- 13.8.8. Deverá fornecer informações sobre a vulnerabilidade, patches, versões afetadas etc., bem como o CVE correspondente.
- 13.8.9. Deverá fornecer uma lista de aplicativos bloqueados.
- 13.8.10. Caso o cliente fique em quarentena, deverá ser capaz de informar ao usuário e notificar o gerenciamento.
- 13.8.11. Deverá suportar a exibição de uma lista de explorações detectadas.
- 13.8.12. Deverá permitir exibir uma lista de aplicativos protegidos contra exploração.
- 13.8.13. Deverá fornecer uma lista de arquivos em quarentena.
- 13.8.14. Deverá ser possível visualizar os resultados da análise ATP.
- 13.9. ANÁLISE DE VULNERABILIDADE
  - 13.9.1. O cliente de segurança deverá ter um módulo de pesquisa de vulnerabilidades integrado e permitir o gerenciamento central no console do mesmo fabricante.
  - 13.9.2. Deverá permitir que o usuário inicie uma análise de vulnerabilidade sob demanda.
  - 13.9.3. As vulnerabilidades encontradas devem ser exibidas localmente com um link para visualizar informações de um banco de dados na Internet. deverá ter pelo menos: nome, gravidade e detalhes.
  - 13.9.4. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas.
  - 13.9.5. Links de acesso a informações complementares devem ser fornecidos, por exemplo, links para a página do fabricante onde as características da vulnerabilidade são detalhadas.
  - 13.9.6. Deverá permitir a aplicação automática de patches.
  - 13.9.7. Deverá detalhar quais correções requerem instalação manual.
  - 13.9.8. A verificação de vulnerabilidades deverá ser permitida de maneira ordenada e autônoma a partir do console central.
  - 13.9.9. Deverá verificar as vulnerabilidades antes de aplicar patches.
- 13.10. FUNCIONALIDADES DE FILTRO DE CONTEÚDO WEB
  - 13.10.1. Deverá permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante.
  - 13.10.2. O fabricante deverá fazer consultas on-line com o cliente de segurança sobre a categoria de um determinado site (por exemplo, interesse geral, tecnologia, hackers, pornografia etc.) para aplicar a

política de controle de acesso à Internet.

13.10.3. O cliente de segurança deverá suportar regras estáticas de acesso à Internet com base em expressões regulares.

13.10.4. Para um determinada URL, os acessos devem ser: permitir, bloquear, alertar ou monitorar.

13.10.5. Deverá configurar o filtro de URL fornecido pelo fabricante com pelo menos as seguintes ações:

13.10.6. Bloquear, avisar, permitir e monitorar.

13.10.7. Deverá configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as seguintes ações: Bloquear ou permitir.

#### **14. ITEM 14 – SOLUÇÃO DE LOGS E RELATORIA TIPO I**

14.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer.

14.2. Deverá possuir a capacidade de receber pelo menos 50 GB de logs diários, atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 36 (trinta e seis) meses.

14.3. Deverá suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções

14.4. Deverá possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.

14.5. Deverá permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.

14.6. Deverá suportar SNMP versão 2 e 3

14.7. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.

14.8. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.

14.9. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH

14.10. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP

14.11. Deverá possuir autenticação de usuários para acesso à plataforma via Radius

14.12. Deverá possuir autenticação de usuários para acesso à plataforma via TACACS +

14.13. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico

14.14. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.

14.15. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico

14.16. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.

- 14.17. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- 14.18. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
- 14.19. Deverá possuir mecanismos de apagamento automático para logs antigos.
- 14.20. Deverá permitir importação e exportação de relatórios;
- 14.21. Deverá ter a capacidade de criar relatórios no formato HTML;
- 14.22. Deverá ter a capacidade de criar relatórios em formato PDF;
- 14.23. Deverá ter a capacidade de criar relatórios no formato XML;
- 14.24. Deverá ter a capacidade de criar relatórios no formato CSV;
- 14.25. Deverá permitir exportar os logs no formato CSV;
- 14.26. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- 14.27. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- 14.28. Deverá ter relatórios predefinidos.
- 14.29. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução
- 14.30. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.
- 14.31. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.
- 14.32. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
- 14.33. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
- 14.34. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
- 14.35. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- 14.36. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- 14.37. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- 14.38. Deverá permitir o envio por e-mail relatórios automaticamente.
- 14.39. Deverá permitir que o relatório seja enviado por email ao destinatário específico.
- 14.40. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- 14.41. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- 14.42. Deverá permitir o uso de filtros nos relatórios.

- 14.43. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- 14.44. Deverá permitir especificar o idioma dos relatórios criados
- 14.45. Deverá gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- 14.46. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- 14.47. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- 14.48. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
- 14.49. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- 14.50. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
- 14.51. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
- 14.52. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
- 14.53. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- 14.54. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
- 14.55. Deverá permitir visualizar em tempo real os logs recebidos.
- 14.56. Deverá permitir o encaminhamento de log no formato syslog.
- 14.57. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).
- 14.58. Deverá gerar alertas de eventos a partir de logs recebidos
- 14.59. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal
- 14.60. Deverá permitir a integração ao sistema de tickets do ServiceNow
- 14.61. Deverá permitir o suporte a logs na nuvem pública do Amazon S3
- 14.62. Deverá permitir o suporte a logs na nuvem pública do Microsoft Azure
- 14.63. Permitir o suporte aos registros de nuvem pública do Google Cloud
- 14.64. Suportar o padrão SAML para autenticação do usuário administrador
- 14.65. Deverá possuir relatório de conformidade com o PCI DSS;

- 14.66. Deverá possuir um relatório de uso do aplicativo SaaS
- 14.67. Deverá possuir um relatório de prevenção de perda de dados (DLP)
- 14.68. Deverá possuir um relatório de VPN
- 14.69. Deverá possuir um relatório IPS (Intruder Prevention System)
- 14.70. Deverá possuir um relatório de reputação do cliente
- 14.71. Deverá possuir um relatório de análise de segurança do usuário
- 14.72. Deverá possuir um relatório de análise de ameaças cibernéticas
- 14.73. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança
- 14.74. Deverá possuir um relatório de tráfego DNS
- 14.75. Deverá possuir um relatório de tráfego de e-mail
- 14.76. Deverá possuir um relatório dos 10 principais aplicativos usados na rede
- 14.77. Deverá possuir um relatório dos 10 principais sites usados na rede
- 14.78. Deverá possuir um relatório de uso de mídia social

## **15. ITEM 15 – SOLUÇÃO DE AUTENTICAÇÃO**

### **15.1. CARACTERÍSTICAS E FUNCIONALIDADES GERAIS**

- 15.1.1. A solução poderá ser entregue em appliance ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, no caso de solução virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será CONTRATANTE.
- 15.1.2. Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.
- 15.1.3. Deve ser compatível e integrável com itens “01”, “02”, “03”, “24”, “25” e “26”, deste termo.
- 15.1.4. Deve ser compatível Solução de Logs e Relatoria.
- 15.1.5. Deve possuir licenciamento para 1000 (mil) usuários locais.
- 15.1.6. Deve possuir licenciamento para suportar 50 (cinquenta) grupos de usuários,
- 15.1.7. Deve possuir licenciamento para suportar 150 (cento e cinquenta) dispositivos NAS gerenciados.
- 15.1.8. Deve possuir licenciamento para suportar 500 (quinhentos) certificados de usuários.
- 15.1.9. Deve possuir licenciamento para suportar 500 (quinhentos) tokens.

### **15.2. REQUISITOS GERAIS:**

- 15.2.1. Deve possuir interface gráfica de administração via Web (HTTPS);
- 15.2.2. Deve possuir interface de administração via linha de comando (CLI) por telnet, SSH ou console serial;

- 15.2.3. Deve permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;
- 15.2.4. Deve efetuar a gerência centralizada de usuários;
- 15.3. FUNCIONALIDADES:
  - 15.3.1. O equipamento Deve enviar e-mails aos usuários ou administradores do mesmo para o controle de usuários, segundo as seguintes opções:
  - 15.3.2. Administradores: reset de senha, aprovação de novos usuários, autenticação de segundo fator (token);
  - 15.3.3. Usuários: reset de senha, auto registro, autenticação de segundo fator (token);
  - 15.3.4. Deve ter capacidade de enviar e-mails com seu próprio servidor SMTP ou integrar-se com servidor de correio eletrônico externo para envio das mensagens aos usuários ou administradores;
  - 15.3.5. O equipamento Deve suportar a criação de usuários na sua base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
  - 15.3.6. Deve suportar a criação de grupos de usuários que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
  - 15.3.7. A solução Deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
  - 15.3.8. A solução Deve funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
  - 15.3.9. Deve ter capacidade de integrar-se com servidores externos LDAP e RADIUS, permitindo assim centralizar em um único equipamento a autenticação dos usuários e dispositivos;
  - 15.3.10. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO (Single Sign On), onde se utilizarão as mesmas credenciais que o usuário utiliza ao autenticar-se no domínio em seu computador pessoal;
  - 15.3.11. Deve permitir definir lista de usuários do SSO que serão ignorados, evitando assim interferência de contas de serviços, tais como antivírus ou scripts via GPO;
  - 15.3.12. Deve prover um portal web para o auto registro dos usuários, de forma com que ele possa ingressar em um portal e registrar seus dados. Após o usuário efetuar o registro, o administrador Deve receber um e-mail para aprovar ou negar o mesmo antes que ele seja ativado;
  - 15.3.13. A geração dos usuários na base de dados local Deve ser feita das seguintes formas:
  - 15.3.14. O administrador poderá definir uma senha no momento de geração do usuário;
  - 15.3.15. O equipamento poderá gerar uma senha aleatória e enviá-la automaticamente ao usuário;
  - 15.3.16. Não definir senha ao usuário para que o mesmo utilize apenas seu token;
  - 15.3.17. Deve permitir que o usuário possua formas de recuperar sua senha através de um correio eletrônico ou pergunta de segurança, que poderão ser configuráveis pelo usuário;
  - 15.3.18. Deve permitir que se configure o número mínimo de caracteres e complexidade mínima da senha, permitindo forçar letras maiúsculas e números, para todos os usuários que sejam cadastrados na base de dados local;

- 15.3.19. Deve permitir criar políticas de bloqueio automático de um usuário após uma quantidade de falhas de autenticação, evitando assim ataques de força bruta contra o usuário;
- 15.3.20. Deve permitir a atualização do firmware via interface gráfica;
- 15.3.21. Deve permitir efetuar o backup completo da solução, incluindo configuração de rotas, interfaces, endereços IP, base de usuários, grupos e tokens. Tal arquivo Deve permitir recuperar o equipamento diretamente via interface gráfica;
- 15.3.22. Deve indicar, na interface gráfica, o estado da licença, versão de firmware, consumo de CPU, memória e disco, quantidade de usuários criados e licenciados;
- 15.3.23. Deve suportar ajuste de data e horário via NTP;
- 15.3.24. Deve suportar SNMP v1, v2 e v3, permitindo consultar MIB própria e envio de traps.
- 15.4. ADMINISTRAÇÃO DE TOKENS:
  - 15.4.1. A solução Deve ser baseada em sementes, através da qual poderá realizar a administração e sincronização de tokens;
  - 15.4.2. Deve funcionar como gerência e repositório de tokens que proporcionará a autenticação de dois fatores, que poderão ser adicionados incrementalmente conforme a necessidade, sem a necessidade de troca de licença ou hardware;
  - 15.4.3. Deve poder sincronizar os tokens para o correto funcionamento dos mesmos;
  - 15.4.4. Deve permitir desassociar um token de um usuário e associá-lo a outro, quando existirem altas ou baixas de usuários, permitindo assim o reaproveitamento do mesmo;
  - 15.4.5. Deve permitir associar os tokens aos usuários criados localmente na base de dados;
  - 15.4.6. Deve possuir opções de tokens físicos e móveis, este último instalável nos sistemas Android e iPhone;
- 15.5. LDAP INTERNO:
  - 15.5.1. A solução Deve conter um LDAP interno que permita ser configurado de uma forma hierárquica, para a correta administração por grupos ou unidades organizacionais dos usuários locais;
  - 15.5.2. Deve gerar o CN (Common Name) dos usuários para a integração com os dispositivos que o requeiram;
  - 15.5.3. Deve gerar a árvore hierárquica dos grupos de usuários que se configurem na solução.
- 15.6. AUTENTICAÇÃO 802.1X:
  - 15.6.1. Deve integrar-se ao protocolo 802.1x para efetuar autenticação de dispositivos e usuários na rede;
  - 15.6.2. Deve suportar as seguintes implementações:
    - 15.6.2.1. EAP-TTLS;
    - 15.6.2.2. PEAP;
    - 15.6.2.3. EAP-GTC;
  - 15.6.3. A solução Deve nativamente, sem o redirecionamento para equipamentos de terceiros, proporcionar a integração e autenticação de switches segundo os requisitos do 802.1x.

- 15.6.4. A solução Deve nativamente, sem o redirecionamento para equipamentos de terceiros, proporcionar a integração de clientes finais para oferecer autenticação 802.1x. Por exemplo, um cliente que utilize Windows poderá configurar seu equipamento para o suporte 802.1x.
- 15.7. AUTENTICAÇÃO BASEADA NO ENDEREÇO MAC:
- 15.7.1. A solução Deve permitir autenticação baseada no endereço MAC do equipamento do usuário, permitindo assim integrar-se com equipamentos de rede que não suportem 802.1x.
- 15.8. CERTIFICADOS:
- 15.8.1. Deve proporcionar a administração de certificados digitais, sua emissão e revogação;
- 15.8.2. 1.8.2. Deve atuar como Autoridade Certificadora (CA);
- 15.8.3. Deve criar e assinar certificados X.509 para utilização em servidores e VPNs;
- 15.8.4. Deve permitir a distribuição dos certificados via SCEP.
- 15.9. AUTENTICAÇÃO OAUTH
- 15.9.1. Deve suportar OAUTH, permitindo integração ao G Suite e outras plataformas;
- 15.9.2. Deverá garantir o suporte à integração de diretórios de usuários existentes na conta do Google GSuite atualmente em utilização. Esta solução deverá disponibilizar funcionalidade de SSO (Entrada Única), permitindo o uso das mesmas credenciais da base de dados do GSuite para autenticação na rede corporativa;
- 15.9.3. Permitir autenticação de usuários visitantes por método de validação com base em credenciais de mídias sociais: Facebook, Twitter, LinkedIn, Google, pelo menos;
- 15.10. RELATÓRIOS E REGISTRO DE EVENTOS:
- 15.10.1. Deve gerar registros dos eventos que os usuários de sua base de dados local realizem com suas contas, possibilitando a auditoria
- 16. ITEM 16 – MODULO TRANSCEIVER – TIPO I**
- 16.1. Deve possuir porta duplex 01 Gbps;
- 16.2. Deve suportar distâncias de até 100 metros utilizando fibra multimodo;
- 16.3. Deve ser compatível com fibras ópticas multimodo;
- 16.4. Deve ser do compatível com o item “ATIVOS DE REDE WIRED TIPO I, II, III, IV, V e VI”
- 16.5. Deve ser do compatível com o item “ATIVOS DE REDE WIRED – POE TIPO I, II e III”
- 16.6. Deve ser do compatível com o item “Solução De Segurança Cibernética Distribuída NGFW – Tipo I, II, III, IV, V e VI”
- 17. ITEM 17 – MODULO TRANSCEIVER – TIPO II**
- 17.1. Deve possuir porta duplex 10 Gbps;
- 17.2. Deve suportar distâncias de até 10 Km utilizando fibra monomodo;

- 17.3. Deve ser compatível com fibras ópticas monomodo;
- 17.4. Deve ser do compatível com o item “ATIVOS DE REDE WIRED TIPO I, II, III, IV, V e VI”
- 17.5. Deve ser do compatível com o item “ATIVOS DE REDE WIRED – POE TIPO I, II E III”
- 17.6. Deve ser do compatível com o item “Solução De Segurança Cibernética Distribuída NGFW – Tipo I, II, III, IV, V e VI”

**18. ITEM 18 – SOLUÇÃO DE SEGURANÇA DECOY/HONEYPOT**

- 18.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMWare vSphere ESXi 5.1, 5.5 ou 6.0 and later, KVM, Hyper-V, AWS. AZURE. No caso de solução virtualizada a responsabilidade pelo fornecimento de servidor/hardware com licenciamento necessário será da CONTRATANTE.
- 18.2. Deve possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 36 (trinta e seis ) meses.
- 18.3. Poderá ser entregue em equipamento único ou com composição de equipamentos para atender as funcionalidades exigidas.
- 18.4. Deve suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
- 18.5. Deve ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.
- 18.6. Deve ser compatível Solução de Logs e Relatoria.
- 18.7. Deve suportar ter a capacidade mínima de 05 VM de honeypot;
- 18.8. Deve estar licenciado para no mínimo 05 VLAN's;
- 18.9. Deve possuir 01 (dois) licenciamento incluso de Windows 7 ou Windows 10.
- 18.10. Deve possuir licenciamento pelo período de 36 (trinta e seis) meses para as funcionalidades de Deception Decoys, AV, IPS, e Web Filtering;
- 18.11. Deve suportar a seguinte combinação:
- 18.12. Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 ou superior
  - 18.12.1. Linux, VPN Server
  - 18.12.2. Medical (PACS, Infusion pump), ERP
  - 18.12.3. IoT, SAP and/or SCADA
- 18.13. Deve suportar os seguintes serviços:
  - 18.13.1. SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, TCP port listener
- 18.14. Deve ser capaz de criar uma rede de máquinas virtuais que se comportam como dispositivos reais a fim de atrair invasores e monitorar suas atividades na rede.

- 18.15. Deve ser capaz de monitorar as ações de atacantes que tentem violar as máquinas virtuais.
- 18.16. Deve analisar as ações dos invasores ao tentarem invadir as máquinas virtuais.
- 18.17. Deve ser capaz de simular serviços, aplicativos ou usuários nas máquinas virtuais a fim de simular um ambiente corporativo real.
- 18.18. Deve possibilitar a instalação de pacote ou script em endpoints reais que simulem interação com os serviços das máquinas virtuais a fim de influenciar o comportamento dos atacantes aumentando a superfície de engano.
- 18.19. O administrador deve ser capaz de monitorar ataques através de incidentes, lista de ataques e por representação visual da rede mostrando endpoints, máquinas virtuais do dispositivo e ataques em andamento.
- 18.20. O sistema deve ser capaz de demonstrar o número de incidentes por tipo de serviço abrangendo minimamente os seguintes: SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST e IEC104.
- 18.21. Deve suportar a criação de perfis de administrador para controlar os privilégios de acesso do aos recursos do sistema. Ao criar uma conta de administrador deve ser atribuído um perfil à conta;
- 18.22. Deve possuir minimamente os seguintes perfis de administrador: super admin – tendo acesso a todas as funcionalidades e read only – tendo acesso somente leitura. Adicionalmente deve possibilitar a criação e customização de perfis administrativos;
- 18.23. Deve suportar a autenticação remota de administradores usando servidores RADIUS e LDAP;
- 18.24. Deve ser capaz de ser implantado em redes do tipo offline ou air-gapped
- 18.25. Deve permitir inserir a licença de uso do equipamento mesmo em redes do tipo offline ou air-gapped
- 18.26. Deve ser capaz de atualizar o firmware mesmo em redes do tipo offline ou air-gapped;
- 18.27. Deve ser capaz de atualizar o módulo de segurança mesmo em redes do tipo offline ou air-gapped;
- 18.28. Deve ser capaz de armazenar Log no próprio equipamento ou integrar com um servidor remoto de armazenamento de log;
- 18.29. Deve suportar servidor de log remoto do tipo syslog e CEF.
- 18.30. Deve possuir dashboard que mostre informações dos seguintes itens:
- 18.31. Informações do sistema como: Hostname, versão do firmware e usuário conectado no momento;
- 18.32. Número de incidente e eventos com seus níveis de severidade por intervalo de tempo;
- 18.33. Número de decoy implementado;
- 18.34. Performance de CPU e RAM;
- 18.35. Informação de uso de disco;
- 18.36. Widget de Top attack;
- 18.37. Deve ser capaz de customizar o dashboard;

- 18.38. Deve ser capaz de atualizar o firmware via interface gráfica;
- 18.39. Deve ser capaz de realizar o backup e restore via interface gráfica;
- 18.40. Deve ser capaz de configurar rotas (camada 3 OSI);
- 18.41. Deve suportar configuração de cliente DNS;
- 18.42. Deve suportar configuração de IPv4 e IPv6;
- 18.43. Deve ser capaz de criar diferentes perfis de conta de administrador do sistema;
- 18.44. Deve ser capaz de integrar com servidor LDAP e Radius;
- 18.45. Deve suportar a importação de certificados CA;
- 18.46. Deve suportar a configuração de cliete de e-mail para envio de alertas;
- 18.47. Deve ser capaz de escolher o nível de severidade do alerta que será enviado;
- 18.48. Deve suportar SNMP V1, V2 e V3;
- 18.49. Deve suportar conexão com a base de dados do fabricante para atualizar informações de segurança;
- 18.50. Deve suportar integração com sistema de detecção de malware
- 18.51. Deve suportar integração com SandBox
- 18.52. Deve suportar integração com NGFW do mesmo fabricante ou de terceiros;
- 18.53. Quando integrado com solução de NGFW deve permitir:
  - 18.53.1. Quarentenar dispositivos;
  - 18.53.2. Exibir o status de IP bloqueado;
  - 18.53.3. Exportar arquivo IOC no formato CSV ou STIX;
  - 18.53.4. Mitigar e isolar de forma automática endpoint infectado para prevenir ataques ou movimentação lateral na rede;
- 18.54. Deve ser capaz de listar os incidentes detectados com no mínimo a informação de: severidade, protocolo, tipo, IP do invasor, IP da vítima, ID do Decoy, usuário invasor, porta de origem do ataque, data e hora do ataque;
- 18.55. Deve ser capaz de gerar relatórios em PDF ou CSV;
- 18.56. Deve ser capaz de listar os ataques detectados com as informações de severidade, data e hora, informação do IP do atacante;
- 18.57. Deve ser capaz de montar uma representação da rede em forma de mapa contendo informação do endpoint, decoy e ataque;
- 18.58. Deve ser capaz de classificar o nível de risco dos incidentes e eventos;
- 18.59. Deve ser capaz de informar a quantidade de eventos e incidentes que ocorreram em uma faixa de tempo;

- 18.60. Deve ser capaz de listar pelo menos o top 5 atacantes;
- 18.61. Deve ser capaz de listar o número de incidente por serviço de forma gráfica;
- 18.62. Deve ser capaz de implantar VMs Decoy na rede, para monitorar e ajudar a entender as ações de um atacante ao obter acesso não autorizado ao Decoy;
- 18.63. Deve ser capaz de implementar decoy customizado (custom image);
- 18.64. Deve suportar importação de imagem ISO;
- 18.65. Deve ser capaz de customizar o recuso de CPU, Memória e Armazenamento da VM-decoy;

**19. ITEM 19 – SOLUÇÃO DE GERÊNCIA CENTRALIZADA NGFW**

- 19.1. A solução poderá ser entregue em appliance ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, KVM, no caso de solução virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será da CONTRATANTE.
- 19.2. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período da vigência contratual.
- 19.3. Deve possuir licença para gerenciar de forma centralizada de no mínimo 50 dispositivos.
- 19.4. Deve garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
- 19.5. Deve possuir definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 19.6. Deve gerar alertas automáticos via e-mail e snmp;
- 19.7. Deve monitorar a performance e Status dos links conectados a Solução de Segurança dos links de Internet;
- 19.8. Deve possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema prevenção a intrusão (IPS – intrusion prevention system), antivírus, pontos de acesso sem fio e de filtro de URL;
- 19.9. Deve permitir usar palavras chaves ou cores para facilitar identificação de regras;
- 19.10. Deve permitir localizar quais regras um objeto (ex. Computador, serviço, etc.) Está sendo utilizado;
- 19.11. Deve atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
- 19.12. Deve permitir criação de regras que fiquem ativas em horário definido;
- 19.13. Deve permitir criação de regras com data de expiração;
- 19.14. Deve permitir realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva;
- 19.15. Deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso.

- 19.16. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- 19.17. Deve garantir que todos os componentes da Solução de Segurança dos Links de Internet sejam controlados de forma centralizada, utilizando apenas um servidor de gerência;
- 19.18. Deve garantir que os dispositivos de segurança sejam visualizados na operação integrada da rede através de geolocalização, e integrados com uma aplicação de mapas online (google maps, bing maps ou outra equivalente);
- 19.19. Deve possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
- 19.20. Deve permitir ao administrador transferir os backups para um servidor SFTP;
- 19.21. Deve realizar a função de gerência em um equipamento exclusivo, não exercendo outras funções (como firewall);
- 19.22. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada;
- 19.23. Deve permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários locais, de bases externas LDAP e RADIUS.
- 19.24. Deve suportar e realizar a sincronização do relógio interno dos equipamentos da solução via protocolo NTP;
- 19.25. Deve gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- 19.26. Deve permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;
- 19.27. Deve permitir criar os objetos que serão utilizados nas políticas, de forma centralizada.

## **20. ITEM 20 – INJETOR DE ENERGIA PARA ATIVO DE REDE WIRELESS – INDOOR**

- 20.1. Deve possuir garantia período de 12 (doze) meses
- 20.2. Deve possuir interfaces RJ45 de 1Gbps.
- 20.3. Deve suportar padrões IEEE 802.3af, 802.3at;
- 20.4. Deve suportar tensões de entrada 100-240vac;
- 20.5. Deve suportar tensão de saída de 50v dc;
- 20.6. Deve possuir POE Power Budget de 30w;
- 20.7. Deve ser compatível e do mesmo fabricante do “ATIVOS DE REDE WIRELESS INDOOR” deste edital;

## **21. ITEM 21 – SERVIDOR RACK PARA APLICAÇÕES VIRTUALIZADAS**

- 21.1. Deve ser fornecido o servidor com garantia do fabricante de 36 (trinta e seis) meses, devendo possuir as seguintes especificações:

**21.1.1. Características de Servidor**

- 21.1.1.1. Deve compatível com rack e possuir no máximo 2U de tamanho.
- 21.1.1.2. Deve possuir placa-mãe compatível com 2 (dois) processadores da família Intel® Xeon® Scalable de 3ª Geração
- 21.1.1.3. Deve possuir mínimo de 2 (duas) portas 1GbE LOM (LAN on Motherboard)
- 21.1.1.4. Deve possuir Interface de gerenciamento remoto dedicada, compatível com o padrão IPMI 2.0, com funcionalidades de controle de energia, acesso ao console (KVM over IP) e montagem de mídia virtual (Virtual Media) sem dependência de sistema operacional. Ex: iDRAC 9 Enterprise ou similar.
- 21.1.1.5. Deve possuir 2 (duas) fontes de alimentação redundantes (1+1), hot-plug, com potência mínima de 600W e certificação de eficiência 80 Plus Platinum ou superior.
- 21.1.1.6. Deve possuir Kit de trilhos deslizantes para instalação em rack padrão 19 polegadas, com braço de gerenciamento de cabos.

**21.1.2. Características do processador**

- 21.1.2.1. Deve possuir 01 (um) processador Intel® Xeon® Silver 4314 ou superior
- 21.1.2.2. Deve possuir no mínimo de 16 (dezesesseis) núcleos físicos
- 21.1.2.3. Deve possuir no mínimo de 32 (trinta e duas) threads
- 21.1.2.4. Deve possuir no mínimo frequência Base (Clock) de 2.4 GHz

**21.1.3. Características de Memória RAM**

- 21.1.3.1. Deve possuir no mínimo 64 GB (sessenta e quatro) de memória ram
- 21.1.3.2. Deve ser compatível com DDR4 RDIMM (Registered DIMM) com ECC (Error Correcting Code)

**21.1.4. Armazenamento**

- 21.1.4.1. Deve possuir no mínimo 01 (um) disco SSD de no mínimo 500 GB
- 21.1.4.2. Deve possuir no mínimo 02 (dois) discos SAS ou SATA de 2 TB Cada.

**22. ITEM 22 – UNIDADE DE SERVIÇOS TÉCNICOS**

- 22.1. Cada Unidade de Serviço Técnicos (UST) corresponderá à 2h (duas horas) de profissional especializado nas plataformas ofertadas. O serviço deve ser prestado pelo próprio fabricante (Professional Services) ou pela empresa contratada.
- 22.2. Atividades: assessement; desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; tuning; hardening; otimização; troubleshooting; updates; upgrades; provas de conceito; ensaios de contingência; customização de consultas de relatórios; treinamentos “hands on”; análise de vulnerabilidades; criação e manutenção de regras de segurança e redes; participação em comitês de segurança para esclarecimentos; documentação “as built”; documentação para rollout;
- 22.3. Os perfis dos profissionais/atividades definidas seguirão o padrão de perfis indicados por metodologias de projetos, como PMBOK. Abaixo, um detalhamento sobre os perfis de profissionais e o escopo de cada um de seus papéis:

- 22.4. Arquitetura: definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais; propor melhorias; definir controles e monitoramento do ambiente, sugerindo métricas, thresholds e indicadores de acompanhamento; apoio no planejamento, execução e avaliação de mudanças;
- 22.5. Implementação: Levantamento de dados, execução das implantações incluindo configuração customizada, integração, migrações e testes, adaptações código, criação de infraestrutura, orientação, documentação, etc;
- 22.6. Gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço
- 22.7. Suporte: Atendimento a incidentes de suporte realizando análises, troubleshooting, diagnósticos; realizando ajustes e otimização configurações; analisando e aplicando patches, fixes e updates, aplicando testes e realizando ensaios; monitorando o ambiente;
- 22.8. As atividades deverão ser prestadas na modalidade on-site, exceto quando expressamente autorizado pela Contratante;
- 22.9. Dinâmica de contratação:
- 22.9.1. A Contratante contratará a quantidade de Unidades de Serviços Técnicos estimadas para consumo pelo período desejado durante a vigência do contrato. Emitirá nota(s) de empenho para adquirir vouchers para quantidade de Unidades de Serviços Técnicos estimados para o período correspondente.
- 22.9.2. A Contratada deve entregar os vouchers relativos à quantidade de Unidades de Serviços contratadas, que poderão ser consumidos pela Contratante ao longo do período do contrato, de acordo com sua necessidade.
- 22.9.3. A Contratante consultará a Contratada para calcular a quantidade de Unidades de Serviços Técnicos necessárias para realizar a atividade pretendida e emitirá Ordem de Serviço para a Contratada prestar os serviços. E, ao final dos serviços, contabilizará o consumo das Unidades de Serviços Técnico utilizadas;
- 22.9.4. O prazo máximo para início das atividades pela Contratada será de 10 (dez) dias;
- 22.9.5. As contabilizações de UST serão feitas individualmente para cada profissional alocado;
- 22.9.6. As UST executadas fora do expediente comercial por solicitação deste órgão, serão contabilizadas em dobro;
- 22.9.7. A Contratada deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;
- 22.9.8. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;
- 22.9.9. Para o controle da execução dos serviços será utilizado a Unidade de medida UST (Unidade de Serviço

Técnico). A UST consiste na “moeda” usada para dimensionar todas as atividades que serão demandadas pela CONTRATANTE, no escopo de cada Ordem de Serviço. A contratação será em volume de UST por atividade e a licitação resultará na oferta do valor de uma UST que irá representar o esforço combinado de profissionais envolvidos, variando a complexidade e prioridade da atividade.

**23. ITEM 23 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW – TIPO IV**

- 23.1. Solução baseada em appliance, fornecida na modalidade Infraestrutura como Serviço (IaaS). Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 23.2. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.
- 23.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.
- 23.4. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais.
- 23.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.
- 23.6. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.
- 23.7. Deve possuir IPS com capacidade mínima de processamento de 8 (oito) Gbps.
- 23.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 5 (cinco) Gbps contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 23.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 6 (seis) Gbps.
- 23.10. Deve possuir VPN com capacidade de, pelo menos, 35 (trinta e cinco) Gbps de tráfego IPSec.
- 23.11. Deve suportar 10.000.000 (dez milhões mil) conexões simultâneas.
- 23.12. Deve suportar, pelo menos, 390.000 (Trezentos e noventa mil) novas conexões por segundo.
- 23.13. Deve suportar, pelo menos, 1.900 (mil e novecentos) túneis de VPN Site-Site.
- 23.14. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 23.15. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 23.16. Deve possuir, pelo menos, 04 (quatro) interfaces SFP 1GE.
- 23.17. Deve possuir, pelo menos, 04 (quatro) interfaces RJ 45 5GE.
- 23.18. Deve possuir, pelo menos, 04 (quatro) interfaces RJ 45 1GE.
- 23.19. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

- 23.20. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 60 (sessenta) equipamentos.
- 23.21. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 120 (cento e vinte) equipamentos.
- 23.22. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 23.23. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

#### **23.24. FUNCIONALIDADES DE FIREWALL**

- 23.24.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 23.24.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 23.24.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 23.24.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 23.24.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 23.24.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 23.24.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 23.24.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 23.24.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 23.24.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 23.24.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 23.24.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 23.24.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 23.24.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 23.24.15. Deve suportar o encaminhamento de tráfego multicast.
- 23.24.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 23.24.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 23.24.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

- 23.24.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 23.24.20. Suportar OSPF gracefulrestart;
- 23.24.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 23.24.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 23.24.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 23.24.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 23.24.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 23.24.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 23.24.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
- 23.24.28. Drop sem notificação do bloqueio ao usuário;
- 23.24.29. Drop com notificação do bloqueio ao usuário;
- 23.24.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 23.24.31. TCP-Reset para o cliente;
- 23.24.32. TCP-Reset para o server ou para os dois lados da conexão.
- 23.24.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 23.24.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 23.24.35. Deve oferecer suporte ao protocolo SIP.
- 23.24.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 23.24.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 23.24.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 23.24.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 23.24.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 23.24.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.

- 23.24.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 23.24.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 23.24.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS+.
- 23.24.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 23.24.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 23.24.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 23.24.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 23.24.49. Realizar Traffic Shaping para a solução de segurança
- 23.24.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 23.24.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 23.24.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 23.24.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 23.24.54. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 23.24.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 23.24.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 23.24.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 23.24.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 23.24.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 23.24.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 23.24.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 23.24.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior

controle sobre a rede interna e prevenindo ataques de IP spoofing.

- 23.24.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 23.24.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 23.24.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 23.24.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 23.24.67. Funcionar com tradução de porta (PAT);
- 23.24.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 23.24.69. Implementar e suportar NAT64 e NAT46;
- 23.24.70. Implementar NAT66
- 23.24.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 23.24.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 23.24.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 23.24.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 23.24.75. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 23.24.76. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 23.24.77. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 23.24.78. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 23.24.79. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

## **23.25. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 23.25.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 23.25.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 23.25.3. Deve permitir priorização de tráfego e suportar ToS.
- 23.25.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

- 23.25.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 23.25.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 23.25.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 23.25.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 23.25.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 23.25.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

#### **23.26. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

- 23.26.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 23.26.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 23.26.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 23.26.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 23.26.5. Deve permitir a criação de categorias personalizadas.
- 23.26.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 23.26.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 23.26.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 23.26.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 23.26.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 23.26.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 23.26.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 23.26.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 23.26.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de

URL;

- 23.26.15. Permitir a criação de categorias de URLs customizadas;
- 23.26.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 23.26.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 23.26.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 23.26.19. Permitir a customização de página de bloqueio;
- 23.26.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 23.26.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 23.26.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 23.26.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 23.26.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 23.26.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 23.26.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 23.26.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 23.26.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 23.26.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 23.26.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 23.26.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 23.26.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 23.26.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a

execução dos serviços de filtragem de conteúdo Web.

- 23.26.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 23.26.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 23.26.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 23.26.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 23.26.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 23.26.39. Deve possuir Proxy Explícito e Transparente.
- 23.26.40. Deve implementar roteamento WCCP e ICAP.

### **23.27. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**

- 23.27.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 23.27.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 23.27.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 23.27.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 23.27.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 23.27.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 23.27.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 23.27.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 23.27.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 23.27.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 23.27.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 23.27.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 23.27.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);

- 23.27.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 23.27.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 23.27.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 23.27.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 23.27.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 23.27.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 23.27.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 23.27.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 23.27.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 23.27.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;
- 23.27.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 23.27.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 23.27.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 23.27.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 23.27.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 23.27.29. Identificar, alertar e bloquear comunicação com botnets;
- 23.27.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 23.27.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 23.27.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 23.27.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de

pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

- 23.27.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 23.27.35. Identificar nos eventos o país de onde partiu a ameaça;
- 23.27.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 23.27.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 23.27.38. Deve possuir alarmes na console de administração.
- 23.27.39. Deve possuir alertas via correio eletrônico.
- 23.27.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 23.27.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 23.27.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 23.27.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 23.27.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

## **23.28. FUNCIONALIDADE DE VPN**

- 23.28.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 23.28.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
- 23.28.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 23.28.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 23.28.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 23.28.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 23.28.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 23.28.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 23.28.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 23.28.10. Realizar atribuição de DNS nos clientes remotos de VPN;

- 23.28.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 23.28.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 23.28.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 23.28.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 23.28.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 23.28.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 23.28.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.

### **23.29. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 23.29.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 23.29.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 23.29.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 23.29.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 23.29.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 23.29.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 23.29.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 23.29.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 23.29.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 23.29.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 23.29.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 23.29.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;

- 23.29.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 23.29.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 23.29.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 23.29.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 23.29.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 23.29.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 23.29.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 23.29.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 23.29.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 23.29.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 23.29.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 23.29.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 23.29.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 23.29.26. Deve permitir criação de padrões de aplicação manualmente.
- 23.29.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 23.29.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 23.29.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 23.29.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;

### **23.30. FUNCIONALIDADE DE SD-WAN**

- 23.30.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 23.30.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com gestão, orquestração e plano de controle SD-WAN baseados em nuvem.
- 23.30.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 23.30.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 23.30.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 23.30.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 23.30.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 23.30.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 23.30.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 23.30.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 23.30.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 23.30.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 23.30.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 23.30.14. Passivo: uso do tráfego real para as medições;
- 23.30.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 23.30.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 23.30.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.

- 23.30.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 23.30.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- 23.30.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 23.30.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 23.30.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 23.30.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 23.30.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 23.30.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 23.30.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 23.30.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 23.30.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 23.30.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

### **23.31. FUNCIONALIDADE DE CONTROLADORA WIRELESS**

- 23.31.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
- 23.31.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
- 23.31.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido.
- 23.31.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou

TACACS+.

23.31.5. Deverá permitir a visualização dos clientes conectados.

23.31.6. Deverá prover suporte a Fast Roaming.

23.31.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.

23.31.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.

23.31.9. Deverá possuir Captive Portal por SSID.

23.31.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs.

23.31.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP.

23.31.12. Deverá suportar os seguintes métodos de autenticação EAP:

23.31.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.

23.31.13. Deverá suportar 802.1x através de RADIUS.

23.31.14. Deverá suportar filtro baseado em endereço MAC por SSID.

23.31.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal.

23.31.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.

23.31.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.

23.31.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).

23.31.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

23.31.19.1. Rogue/Interfering AP Detection;

23.31.19.2. Ad-hoc Network Detection;

23.31.19.3. Wireless Bridge Detection;

23.31.19.4. Weak WEP Detection;

23.31.19.5. MAC OUI Checking.

23.31.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID.

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

- 23.31.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário.
- 23.31.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs.
- 23.31.24. Deverá permitir a criação de políticas de traffic shaping.
- 23.31.25. Deverá permitir a criação de políticas de firewall baseadas em horário.
- 23.31.26. Deverá permitir NAT nas políticas de firewall.
- 23.31.27. Deverá possibilitar definir número de clientes por SSID.
- 23.31.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs.
- 23.31.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha.
- 23.31.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 23.31.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados.
- 23.31.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
- 23.31.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
- 23.31.34. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 23.31.35. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 23.31.36. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
- 23.31.37. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso.
- 23.31.38. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 23.31.39. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
- 23.31.40. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.

- 23.31.41. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora.
- 23.31.42. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 23.31.43. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 23.31.44. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora.
- 23.31.45. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 23.31.46. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede.

23.32.

**24. ITEM 24 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW – TIPO V**

- 24.1. Solução baseada em appliance, fornecida na modalidade Infraestrutura como Serviço (IaaS). Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 24.2. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.
- 24.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.
- 24.4. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais.
- 24.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 24.6. Deve possuir firewall com capacidade mínima de processamento de 27 (vinte e sete) Gbps.
- 24.7. Deve possuir IPS com capacidade mínima de processamento de 4(quatro) Gbps.
- 24.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2 (dois) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 24.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 2 (dois) Gbps.

- 24.10. Deve possuir VPN com capacidade de, pelo menos, 24 (vinte e quatro) Gbps de tráfego IPSec.
- 24.11. Deve suportar 2.500.000 (dois milhões e quinhentos mil) conexões simultâneas.
- 24.12. Deve suportar, pelo menos, 120.000 (cento e vinte mil) novas conexões por segundo.
- 24.13. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 24.14. Deve suportar, pelo menos, 2000 (dois mil) túneis de VPN Client-Site.
- 24.15. Deve possuir, pelo menos, 2 (duas) interfaces SFP+ 10GE.
- 24.16. Deve possuir, pelo menos, 8 (oito) interfaces RJ45 1GE.
- 24.17. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.
- 24.18. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 20 (vinte) equipamentos.
- 24.19. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 60 (sessenta) equipamentos.
- 24.20. Deve ser compatível com a Solução de Gerência Centralizada NGFW
- 24.21. Deve ser compatível com a Solução Centralizada de Armazenamento de Logs e Relatórios
- 24.22. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 24.23. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês

#### **24.24. FUNCIONALIDADES DE FIREWALL**

- 24.24.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 24.24.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 24.24.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 24.24.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 24.24.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 24.24.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 24.24.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 24.24.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 24.24.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;

- 24.24.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 24.24.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 24.24.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 24.24.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 24.24.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 24.24.15. Deve suportar o encaminhamento de tráfego multicast.
- 24.24.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 24.24.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 24.24.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 24.24.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 24.24.20. Suportar OSPF gracefulrestart;
- 24.24.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 24.24.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 24.24.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 24.24.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 24.24.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 24.24.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 24.24.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
- 24.24.28. Drop sem notificação do bloqueio ao usuário;
- 24.24.29. Drop com notificação do bloqueio ao usuário;
- 24.24.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 24.24.31. TCP-Reset para o cliente;
- 24.24.32. TCP-Reset para o server ou para os dois lados da conexão.
- 24.24.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

- 24.24.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 24.24.35. Deve oferecer suporte ao protocolo SIP.
- 24.24.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 24.24.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 24.24.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 24.24.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 24.24.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 24.24.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 24.24.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 24.24.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 24.24.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS+.
- 24.24.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 24.24.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 24.24.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 24.24.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 24.24.49. Realizar Traffic Shaping para a solução de segurança
- 24.24.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 24.24.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 24.24.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 24.24.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);

- 24.24.54. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 24.24.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 24.24.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 24.24.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 24.24.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 24.24.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 24.24.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 24.24.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 24.24.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 24.24.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 24.24.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 24.24.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 24.24.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 24.24.67. Funcionar com tradução de porta (PAT);
- 24.24.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 24.24.69. Implementar e suportar NAT64 e NAT46;
- 24.24.70. Implementar NAT66
- 24.24.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 24.24.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 24.24.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 24.24.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 24.24.75. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 24.24.76. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes

formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

- 24.24.77. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 24.24.78. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 24.24.79. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

#### **24.25. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 24.25.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 24.25.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 24.25.3. Deve permitir priorização de tráfego e suportar ToS.
- 24.25.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 24.25.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 24.25.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 24.25.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 24.25.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 24.25.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 24.25.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

#### **24.26. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

- 24.26.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 24.26.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 24.26.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 24.26.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 24.26.5. Deve permitir a criação de categorias personalizadas.
- 24.26.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

- 24.26.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 24.26.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 24.26.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 24.26.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 24.26.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 24.26.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 24.26.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 24.26.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 24.26.15. Permitir a criação de categorias de URLs customizadas;
- 24.26.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 24.26.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 24.26.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 24.26.19. Permitir a customização de página de bloqueio;
- 24.26.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 24.26.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 24.26.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 24.26.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 24.26.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 24.26.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP

em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

- 24.26.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 24.26.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 24.26.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 24.26.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 24.26.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 24.26.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 24.26.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 24.26.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 24.26.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 24.26.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 24.26.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 24.26.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 24.26.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 24.26.39. Deve possuir Proxy Explícito e Transparente.
- 24.26.40. Deve implementar roteamento WCCP e ICAP.

#### **24.27. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**

- 24.27.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 24.27.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 24.27.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 24.27.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 24.27.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

- 24.27.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 24.27.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 24.27.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 24.27.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 24.27.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 24.27.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 24.27.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 24.27.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 24.27.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 24.27.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 24.27.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 24.27.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 24.27.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 24.27.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 24.27.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 24.27.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 24.27.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 24.27.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;
- 24.27.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 24.27.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 24.27.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;

- 24.27.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 24.27.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 24.27.29. Identificar, alertar e bloquear comunicação com botnets;
- 24.27.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 24.27.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 24.27.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 24.27.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 24.27.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 24.27.35. Identificar nos eventos o país de onde partiu a ameaça;
- 24.27.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 24.27.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 24.27.38. Deve possuir alarmes na console de administração.
- 24.27.39. Deve possuir alertas via correio eletrônico.
- 24.27.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 24.27.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 24.27.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 24.27.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 24.27.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

## **24.28. FUNCIONALIDADE DE VPN**

- 24.28.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 24.28.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;

- 24.28.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 24.28.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 24.28.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 24.28.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 24.28.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 24.28.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 24.28.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 24.28.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 24.28.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 24.28.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 24.28.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 24.28.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 24.28.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 24.28.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 24.28.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSEC estabelecidos.

#### **24.29. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 24.29.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 24.29.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 24.29.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 24.29.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 24.29.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja,

não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

- 24.29.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 24.29.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 24.29.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 24.29.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 24.29.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 24.29.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 24.29.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensagens instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 24.29.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 24.29.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 24.29.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 24.29.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 24.29.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 24.29.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 24.29.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 24.29.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 24.29.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 24.29.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários

do serviço de diretório LDAP.

- 24.29.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 24.29.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 24.29.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 24.29.26. Deve permitir criação de padrões de aplicação manualmente.
- 24.29.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 24.29.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 24.29.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 24.29.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária;

#### **24.30. FUNCIONALIDADE DE SD-WAN**

- 24.30.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 24.30.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com gestão, orquestração e plano de controle SD-WAN baseados em nuvem.
- 24.30.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 24.30.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 24.30.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 24.30.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 24.30.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 24.30.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 24.30.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 24.30.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

- 24.30.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 24.30.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 24.30.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 24.30.14. Passivo: uso do tráfego real para as medições;
- 24.30.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 24.30.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 24.30.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 24.30.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 24.30.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- 24.30.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 24.30.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 24.30.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 24.30.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 24.30.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 24.30.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 24.30.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;

- 24.30.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 24.30.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 24.30.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

#### **24.31. FUNCIONALIDADE DE CONTROLADORA WIRELESS**

- 24.31.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.
- 24.31.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
- 24.31.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido.
- 24.31.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+.
- 24.31.5. Deverá permitir a visualização dos clientes conectados.
- 24.31.6. Deverá prover suporte a Fast Roaming.
- 24.31.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
- 24.31.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.
- 24.31.9. Deverá possuir Captive Portal por SSID.
- 24.31.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs.
- 24.31.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP.
- 24.31.12. Deverá suportar os seguintes métodos de autenticação EAP:
- 24.31.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.
- 24.31.13. Deverá suportar 802.1x através de RADIUS.
- 24.31.14. Deverá suportar filtro baseado em endereço MAC por SSID.
- 24.31.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal.
- 24.31.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.
- 24.31.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.

- 24.31.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).
- 24.31.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:
  - 24.31.19.1. Rogue/Interfering AP Detection;
  - 24.31.19.2. Ad-hoc Network Detection;
  - 24.31.19.3. Wireless Bridge Detection;
  - 24.31.19.4. Weak WEP Detection;
  - 24.31.19.5. MAC OUI Checking.
- 24.31.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID.
- 24.31.21. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.
- 24.31.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário.
- 24.31.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs.
- 24.31.24. Deverá permitir a criação de políticas de traffic shaping.
- 24.31.25. Deverá permitir a criação de políticas de firewall baseadas em horário.
- 24.31.26. Deverá permitir NAT nas políticas de firewall.
- 24.31.27. Deverá possibilitar definir número de clientes por SSID.
- 24.31.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs.
- 24.31.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha.
- 24.31.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 24.31.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados.
- 24.31.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
- 24.31.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
- 24.31.34. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 24.31.35. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 24.31.36. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional,

uso de banda, potência do sinal e relação sinal/ruído.

- 24.31.37. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso.
- 24.31.38. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.39. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora.
- 24.31.40. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.41. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.42. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.43. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.44. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.45. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 24.31.46. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede.

## **25. ITEM 25 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW – TIPO VI**

- 25.1. Solução baseada em appliance, fornecida na modalidade Infraestrutura como Serviço (IaaS). Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 25.2. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.
- 25.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e

integração, desde que ocupem até 2U, no máximo.

- 25.4. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais.
- 25.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 25.6. Deve possuir firewall com capacidade mínima de processamento de 4 (quatro) Gbps.
- 25.7. Deve possuir IPS com capacidade mínima de processamento de 2 (dois) Gbps.
- 25.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1 (um) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 25.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1(um) Gbps.
- 25.10. Deve possuir VPN com capacidade de, pelo menos, 4(quatro) Gbps de tráfego IPSec.
- 25.11. Deve suportar 700.000 (setecentos mil) conexões simultâneas.
- 25.12. Deve suportar, pelo menos, 80.000 (oitenta mil) novas conexões por segundo.
- 25.13. Deve suportar, pelo menos, 180 (cento e oitenta) túneis de VPN Site-Site.
- 25.14. Deve suportar, pelo menos, 240 (duzentos e quarenta) túneis de VPN Client-Site.
- 25.15. Deve possuir, pelo menos, 5 (cinco) interfaces RJ45 1GE.
- 25.16. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.
- 25.17. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 8 (oito) equipamentos.
- 25.18. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 8 (oito) equipamentos.
- 25.19. Deve ser compatível com a Solução de Segurança Cibernética Distribuída NGFW dos TIPOS "I, II e III"
- 25.20. Deve ser compatível com a Solução de Logs e Relatoria.
- 25.21. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 25.22. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

#### **25.23. FUNCIONALIDADES DE FIREWALL**

- 25.23.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 25.23.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 25.23.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados),

roteador, proxy explícito e sniffer.

- 25.23.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 25.23.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 25.23.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 25.23.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 25.23.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 25.23.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 25.23.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 25.23.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 25.23.12. Deve suportar o encaminhamento de tráfego multicast.
- 25.23.13. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 25.23.14. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 25.23.15. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 25.23.16. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 25.23.17. Suportar OSPF gracefulrestart;
- 25.23.18. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 25.23.19. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 25.23.20. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 25.23.21. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 25.23.22. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 25.23.23. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 25.23.24. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
- 25.23.25. Drop sem notificação do bloqueio ao usuário;
- 25.23.26. Drop com notificação do bloqueio ao usuário;

- 25.23.27. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 25.23.28. TCP-Reset para o cliente;
- 25.23.29. TCP-Reset para o server ou para os dois lados da conexão.
- 25.23.30. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 25.23.31. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 25.23.32. Deve oferecer suporte ao protocolo SIP.
- 25.23.33. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 25.23.34. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 25.23.35. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 25.23.36. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 25.23.37. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 25.23.38. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 25.23.39. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 25.23.40. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 25.23.41. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS+.
- 25.23.42. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 25.23.43. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 25.23.44. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 25.23.45. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 25.23.46. Realizar Traffic Shaping para a solução de segurança
- 25.23.47. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;

- 25.23.48. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 25.23.49. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 25.23.50. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 25.23.51. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 25.23.52. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 25.23.53. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 25.23.54. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 25.23.55. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 25.23.56. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 25.23.57. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 25.23.58. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 25.23.59. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 25.23.60. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 25.23.61. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 25.23.62. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 25.23.63. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 25.23.64. Funcionar com tradução de porta (PAT);
- 25.23.65. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 25.23.66. Implementar e suportar NAT64 e NAT46;
- 25.23.67. Implementar NAT66
- 25.23.68. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 25.23.69. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 25.23.70. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.

- 25.23.71. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 25.23.72. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 25.23.73. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 25.23.74. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 25.23.75. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 25.23.76. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

#### **25.24. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 25.24.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 25.24.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 25.24.3. Deve permitir priorização de tráfego e suportar ToS.
- 25.24.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 25.24.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 25.24.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 25.24.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 25.24.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 25.24.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 25.24.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

#### **25.25. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

- 25.25.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 25.25.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 25.25.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites

peçoais, Compras.

- 25.25.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 25.25.5. Deve permitir a criação de categorias personalizadas.
- 25.25.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 25.25.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 25.25.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 25.25.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 25.25.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 25.25.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 25.25.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 25.25.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 25.25.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 25.25.15. Permitir a criação de categorias de URLs customizadas;
- 25.25.16. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 25.25.17. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 25.25.18. Permitir a customização de página de bloqueio;
- 25.25.19. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 25.25.20. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 25.25.21. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 25.25.22. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;

- 25.25.23. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 25.25.24. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 25.25.25. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 25.25.26. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 25.25.27. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 25.25.28. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 25.25.29. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 25.25.30. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 25.25.31. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 25.25.32. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 25.25.33. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 25.25.34. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 25.25.35. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 25.25.36. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 25.25.37. Deve possuir Proxy Explícito e Transparente.
- 25.25.38. Deve implementar roteamento WCCP e ICAP.

## **25.26. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**

- 25.26.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 25.26.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 25.26.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 25.26.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 25.26.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças

- detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 25.26.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 25.26.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 25.26.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 25.26.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 25.26.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 25.26.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 25.26.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 25.26.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 25.26.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 25.26.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 25.26.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 25.26.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 25.26.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 25.26.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 25.26.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 25.26.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 25.26.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 25.26.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;
- 25.26.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 25.26.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

- 25.26.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 25.26.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 25.26.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 25.26.29. Identificar, alertar e bloquear comunicação com botnets;
- 25.26.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 25.26.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 25.26.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 25.26.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 25.26.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 25.26.35. Identificar nos eventos o país de onde partiu a ameaça;
- 25.26.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 25.26.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 25.26.38. Deve possuir alarmes na console de administração.
- 25.26.39. Deve possuir alertas via correio eletrônico.
- 25.26.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 25.26.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 25.26.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 25.26.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 25.26.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

## **25.27. FUNCIONALIDADE DE VPN**

- 25.27.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;

- 25.27.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
- 25.27.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 25.27.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 25.27.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 25.27.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 25.27.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 25.27.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 25.27.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 25.27.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 25.27.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 25.27.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 25.27.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 25.27.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 25.27.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 25.27.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 25.27.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.

## **25.28. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 25.28.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 25.28.2. Atualizar a base de assinaturas de aplicações automaticamente;
- 25.28.3. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 25.28.4. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 25.28.5. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;

- 25.28.6. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 25.28.7. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 25.28.8. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 25.28.9. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 25.28.10. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 25.28.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensagens instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 25.28.12. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 25.28.13. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 25.28.14. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 25.28.15. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 25.28.16. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 25.28.17. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 25.28.18. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 25.28.19. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 25.28.20. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 25.28.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 25.28.22. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 25.28.23. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 25.28.24. Deve permitir criação de padrões de aplicação manualmente.

- 25.28.25. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 25.28.26. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 25.28.27. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encryptado” e aplicações VOIP que utilizam criptografia proprietária;

## **25.29. FUNCIONALIDADE DE SD-WAN**

- 25.29.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 25.29.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com gestão, orquestração e plano de controle SD-WAN baseados em nuvem.
- 25.29.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 25.29.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 25.29.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 25.29.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 25.29.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 25.29.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 25.29.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 25.29.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 25.29.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 25.29.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 25.29.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 25.29.14. Passivo: uso do tráfego real para as medições;
- 25.29.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o

método ativo.

- 25.29.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 25.29.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 25.29.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 25.29.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- 25.29.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 25.29.21. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 25.29.22. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 25.29.23. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 25.29.24. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 25.29.25. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 25.29.26. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 25.29.27. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 25.29.28. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

## **25.30. FUNCIONALIDADE DE CONTROLADORA WIRELESS**

- 25.30.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante.

- 25.30.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless.
- 25.30.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido.
- 25.30.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+.
- 25.30.5. Deverá permitir a visualização dos clientes conectados.
- 25.30.6. Deverá prover suporte a Fast Roaming.
- 25.30.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF.
- 25.30.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência.
- 25.30.9. Deverá possuir Captive Portal por SSID.
- 25.30.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs.
- 25.30.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP.
- 25.30.12. Deverá suportar os seguintes métodos de autenticação EAP:
  - 25.30.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA.
- 25.30.13. Deverá suportar 802.1x através de RADIUS.
- 25.30.14. Deverá suportar filtro baseado em endereço MAC por SSID.
- 25.30.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal.
- 25.30.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast.
- 25.30.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs.
- 25.30.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue).
- 25.30.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:
  - 25.30.19.1. Rogue/Interfering AP Detection;
  - 25.30.19.2. Ad-hoc Network Detection;
  - 25.30.19.3. Wireless Bridge Detection;
  - 25.30.19.4. Weak WEP Detection;
  - 25.30.19.5. MAC OUI Checking.

- 25.30.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID.
- 25.30.21. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm.
- 25.30.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário.
- 25.30.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs.
- 25.30.24. Deverá permitir a criação de políticas de traffic shaping.
- 25.30.25. Deverá permitir a criação de políticas de firewall baseadas em horário.
- 25.30.26. Deverá permitir NAT nas políticas de firewall.
- 25.30.27. Deverá possibilitar definir número de clientes por SSID.
- 25.30.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs.
- 25.30.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha.
- 25.30.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada.
- 25.30.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados.
- 25.30.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points.
- 25.30.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios.
- 25.30.34. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless.
- 25.30.35. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica.
- 25.30.36. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído.
- 25.30.37. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso.
- 25.30.38. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.39. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo

tráfego seja tunelado até a Controladora.

- 25.30.40. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.41. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.42. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.43. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.44. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.45. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora.
- 25.30.46. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede.

## **26. ITEM 26 – ATIVO DE REDE WIRED – TIPO V**

### **26.1. INFORMAÇÕES GERAIS E GARANTIA**

- 26.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI.
- 26.1.2. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses.

### **26.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

- 26.2.1. Deve possuir 32 (trinta e duas ) interfaces do tipo 1000Base-T/2500Base -T para conexão de cabos de par metálico UTP com concetor R-45.
- 26.2.2. Deve possuir 16 (dezesseis) interfaces do tipo 1000Base-T/2500Base -T/5000Base-T para conexão de cabos de par metálico UTP com concetor R-45.
- 26.2.3. Adicionalmente, deve possuir 8 (oito) slots SFP28 para conexão de fibras ópticas do tipo 25GBase-X operando em 25GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.
- 26.2.4. Deve operar com latência igual ou inferior à 1us (microsegundo).
- 26.2.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.
- 26.2.6. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.

- 26.2.7. Deve ser fornecido com fonte de alimentação interna redundante com capacidade para operar em tensões de 110V e 220V.
- 26.2.8. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.
- 26.2.9. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).
- 26.2.10. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.
- 26.2.11. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash.
- 26.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO
  - 26.3.1. Deve possuir capacidade de comutação de pelo menos 700 Gbps e ser capaz de encaminhar até 1000 Mpps (milhões de pacotes por segundo).
  - 26.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.
  - 26.3.3. Deve possuir tabela MAC com suporte a 60.000 endereços.
  - 26.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.
  - 26.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
  - 26.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
  - 26.3.7. Deve suportar a comutação de Jumbo Frames.
- 26.4. SPANNING TREE E RECURSOS DE PROTEÇÃO
  - 26.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
  - 26.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
  - 26.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
  - 26.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
  - 26.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
  - 26.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
  - 26.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 26.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2

- 26.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
- 26.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
- 26.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
- 26.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
- 26.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
- 26.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
- 26.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
- 26.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
- 26.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
- 26.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.
- 26.6. CAPACIDADES DE CAMADA 3
  - 26.6.1. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica.
  - 26.6.2. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos.
  - 26.6.3. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
  - 26.6.4. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo.
  - 26.6.5. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF.
  - 26.6.6. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ).
  - 26.6.7. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
  - 26.6.8. Deve suportar o protocolo PTP (Precision Time Protocol).

## 26.7. AUTENTICAÇÃO, ACESSO E SEGURANÇA

- 26.7.1. Deve implementar serviço de DHCP Server e DHCP Relay.
- 26.7.2. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
- 26.7.3. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 26.7.4. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 26.7.5. Deve suportar autenticação por MAC Authentication Bypass (MAB).
- 26.7.6. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 26.7.7. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 26.7.8. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
- 26.7.9. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 26.7.10. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
- 26.7.11. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
- 26.7.12. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.

## 26.8. GERENCIAMENTO E MONITORAMENTO

- 26.8.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
- 26.8.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 26.8.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
- 26.8.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 26.8.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 26.8.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 26.8.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 26.8.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 26.8.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).

- 26.8.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 26.8.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 26.8.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
- 26.8.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 26.8.14. Deve possuir uma ferramenta de captura de pacotes que auxilie na identificação de problemas na rede. Essa ferramenta deve permitir o uso de filtros para selecionar o tráfego a ser capturado e possibilitar a exportação dos pacotes em formato .pcap, para posterior análise no software Wireshark.
- 26.8.15. Deve implementar Netflow, sFlow ou similar.
- 26.8.16. Deve suportar configuração e monitoramento por meio de REST API.
- 26.8.17. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II e III” e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- 26.8.17.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
- 26.8.17.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
- 26.8.17.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
- 26.8.17.4. Deve operar como ponto central para automação e gerenciamento dos switches.
- 26.8.17.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
- 26.8.17.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
- 26.8.17.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
- 26.8.17.8. Deve montar a topologia da rede de maneira automática.
- 26.8.17.9. Deve ser capaz de configurar os switches da rede.
- 26.8.17.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 26.8.17.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 26.8.17.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.

- 26.8.17.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
- 26.8.17.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 26.8.17.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 26.8.17.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 26.8.17.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 26.8.17.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 26.8.17.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 26.8.17.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 26.8.17.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 26.8.17.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 26.8.17.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 26.8.17.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 26.8.17.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 26.8.17.26. Deve possuir API no formato REST.

## **27. ITEM 27 – ATIVO DE REDE WIRED – TIPO VI**

### **27.1. INFORMAÇÕES GERAIS E GARANTIA**

- 27.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI.
- 27.1.2. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses.

### **27.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

- 27.2.1. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45.
- 27.2.2. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.

- 27.2.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.
- 27.2.4. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.
- 27.2.5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V.
- 27.2.6. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.
- 27.2.7. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).
- 27.2.8. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.
- 27.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO
- 27.3.1. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo).
- 27.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.
- 27.3.3. Deve possuir tabela MAC com suporte a 30.000 endereços.
- 27.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.
- 27.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).
- 27.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
- 27.3.7. Deve suportar a comutação de Jumbo Frames.
- 27.4. SPANNING TREE E RECURSOS DE PROTEÇÃO
- 27.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 27.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
- 27.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
- 27.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
- 27.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
- 27.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
- 27.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).

## 27.5. GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2

- 27.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch Deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
- 27.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
- 27.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
- 27.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
- 27.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
- 27.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
- 27.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
- 27.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
- 27.5.9. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o protocolo ARP.
- 27.5.10. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.

## 27.6. AUTENTICAÇÃO, ACESSO E SEGURANÇA

- 27.6.1. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
- 27.6.2. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 27.6.3. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 27.6.4. Deve suportar autenticação por MAC Authentication Bypass (MAB).
- 27.6.5. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 27.6.6. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 27.6.7. Em caso de indisponibilidade dos servidores RADIUS, o switch Deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
- 27.6.8. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 27.6.9. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.

27.6.10. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.

27.6.11. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.

## 27.7. GERENCIAMENTO E MONITORAMENTO

27.7.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.

27.7.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).

27.7.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.

27.7.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

27.7.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.

27.7.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.

27.7.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.

27.7.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.

27.7.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).

27.7.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.

27.7.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.

27.7.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.

27.7.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.

27.7.14. Deve ser capaz de realizar testes nas interfaces para diagnosticar falhas físicas em cabos UTP (par trançado) conectados ao switch.

27.7.15. Deve suportar configuração e monitoramento por meio de REST API.

27.7.16. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II e III”, e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

27.7.16.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.

27.7.16.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.

- 27.7.16.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
- 27.7.16.4. Deve operar como ponto central para automação e gerenciamento dos switches.
- 27.7.16.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
- 27.7.16.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
- 27.7.16.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
- 27.7.16.8. Deve montar a topologia da rede de maneira automática.
- 27.7.16.9. Deve ser capaz de configurar os switches da rede.
- 27.7.16.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 27.7.16.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 27.7.16.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
- 27.7.16.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.
- 27.7.16.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 27.7.16.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 27.7.16.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 27.7.16.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 27.7.16.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 27.7.16.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 27.7.16.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 27.7.16.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 27.7.16.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 27.7.16.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.

27.7.16.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.

27.7.16.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

27.7.16.26. Deve possuir API no formato REST.

## **28. ITEM 28 – ATIVO DE REDE WIRED POE TIPO III**

### **28.1. INFORMAÇÕES GERAIS E GARANTIA**

28.1.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI.

28.1.2. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses.

### **28.2. ESPECIFICAÇÕES FÍSICAS E DE HARDWARE**

28.2.1. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45.

28.2.2. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior.

28.2.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial.

28.2.4. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos.

28.2.5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V.

28.2.6. Deve implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget mínimo de 180W.

28.2.7. Deve possuir LEDs indicadores para cada interface de rede, com sinalização de atividade e velocidade.

28.2.8. Deve suportar montagem em rack padrão 19 polegadas e ser fornecido com os acessórios necessários (ex: orelhas ou kits de fixação).

28.2.9. Deve suportar operação em temperatura ambiente de pelo menos 0°C a 40°C.

### **28.3. CAPACIDADE DE COMUTAÇÃO E DESEMPENHO**

28.3.1. Deve possuir capacidade de comutação de pelo menos 120 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo).

28.3.2. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q.

28.3.3. Deve possuir tabela MAC com suporte a 30.000 endereços.

28.3.4. Deve implementar Flow Control baseado no padrão IEEE 802.3x.

28.3.5. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X).

- 28.3.6. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP).
- 28.3.7. Deve suportar a comutação de Jumbo Frames.
- 28.4. **SPANNING TREE E RECURSOS DE PROTEÇÃO**
  - 28.4.1. Deve implementar os protocolos Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
  - 28.4.2. Deve suportar, no mínimo, 15 (quinze) instâncias de Multiple Spanning Tree.
  - 28.4.3. Deve oferecer funcionalidade equivalente ao PortFast ou Edge Port, permitindo que portas de acesso entrem diretamente no estado "Forwarding" do Spanning Tree assim que detectada uma conexão física.
  - 28.4.4. Deve implementar mecanismo de proteção da "root bridge" do Spanning Tree.
  - 28.4.5. Deve permitir a suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em portas configuradas para encaminhamento rápido (conforme o padrão IEEE 802.1w). Caso um BPDU seja recebido, deve ser possível desabilitar automaticamente essa porta.
  - 28.4.6. Deve implementar mecanismo conhecido como Loop Guard, capaz de identificar loops de rede, desativar automaticamente a interface afetada e gerar alerta do evento.
  - 28.4.7. Deve possuir funcionalidade para detecção de flapping, identificando interfaces com variação constante de status operacional. A interface deve ser automaticamente desabilitada caso exceda o número de alterações configurado dentro de um intervalo de tempo definido (em segundos).
- 28.5. **GERENCIAMENTO DE TRÁFEGO E SEGURANÇA DE CAMADA 2**
  - 28.5.1. Deve possuir controle de tráfego broadcast, multicast e unicast por porta. Quando o limite configurado for excedido, o switch deve aplicar descarte de pacotes ou limitar a taxa de transmissão.
  - 28.5.2. Deve permitir o espelhamento de tráfego (port mirroring) de uma porta para outra dentro do mesmo switch.
  - 28.5.3. Deve suportar IGMP snooping para controle de tráfego de multicast.
  - 28.5.4. Deve ser capaz de identificar automaticamente telefones IP conectados às portas e associá-los à VLAN de voz previamente definida.
  - 28.5.5. Deve suportar a criação de listas de controle de acesso (ACLs) para filtragem de tráfego, com base nos seguintes critérios: endereços IP de origem e destino, endereços MAC de origem e destino, campo CoS (Class of Service) e VLAN ID.
  - 28.5.6. Deve permitir a configuração de períodos específicos (dias e horários) para a aplicação das ACLs.
  - 28.5.7. Deve implementar mecanismos de priorização de tráfego com base nos valores de CoS definidos no cabeçalho Ethernet (IEEE 802.1p).
  - 28.5.8. Deve oferecer, no mínimo, 8 (oito) filas de priorização de QoS por porta.
  - 28.5.9. Deve implementar DHCP Snooping, permitindo bloquear respostas de servidores DHCP não autorizados, prevenindo conflitos e acessos indevidos.
  - 28.5.10. Deve possuir mecanismo de proteção contra ataques do tipo Man-in-the-Middle que explorem o

protocolo ARP.

## 28.6. AUTENTICAÇÃO, ACESSO E SEGURANÇA

- 28.6.1. Deve implementar controle de acesso por porta com suporte ao padrão IEEE 802.1X, permitindo atribuição dinâmica de VLANs com base em atributos fornecidos via protocolo RADIUS.
- 28.6.2. Deve permitir autenticação IEEE 802.1X de múltiplos dispositivos por porta, comutando exclusivamente o tráfego dos dispositivos autenticados.
- 28.6.3. Deve suportar, no mínimo, a autenticação simultânea de 15 (quinze) dispositivos por porta utilizando o protocolo IEEE 802.1X.
- 28.6.4. Deve suportar autenticação por MAC Authentication Bypass (MAB).
- 28.6.5. Deve implementar suporte a RADIUS CoA (Change of Authorization).
- 28.6.6. Deve incluir mecanismo para monitoramento da disponibilidade dos servidores RADIUS.
- 28.6.7. Em caso de indisponibilidade dos servidores RADIUS, o switch deve ser capaz de provisionar automaticamente uma VLAN de fallback para os dispositivos conectados às portas com 802.1X habilitado, evitando interrupções no acesso à rede.
- 28.6.8. Deve implementar suporte a Guest VLAN, destinada a dispositivos que não realizarem autenticação nas portas com 802.1X ativado.
- 28.6.9. Deve operar em modo de monitoramento (monitor mode) para autenticação 802.1X, permitindo testes de autenticação sem alterar o estado ou configuração da interface.
- 28.6.10. Deve autenticar dispositivos conectados via 802.1X mesmo quando estes estiverem ligados por meio da interface de um telefone IP.
- 28.6.11. Deve suportar autenticação RADIUS e contabilização (RADIUS Accounting) também sobre redes IPv6.

## 28.7. GERENCIAMENTO E MONITORAMENTO

- 28.7.1. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos por porta. Ao atingir esse limite, o switch Deve registrar o evento em log.
- 28.7.2. Deve permitir a customização do tempo (em segundos) em que um endereço MAC aprendido dinamicamente permanece na tabela MAC (MAC Table).
- 28.7.3. Deve ser capaz de registrar logs de eventos nas seguintes situações: aprendizado de novo endereço MAC, movimentação de MAC entre interfaces e remoção de MAC da interface.
- 28.7.4. Deve suportar sincronização de horário utilizando os protocolos NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).
- 28.7.5. Deve permitir o envio de mensagens de log para servidor externo via protocolo Syslog.
- 28.7.6. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3.
- 28.7.7. Deve suportar acesso remoto via CLI utilizando o protocolo SSH, tanto em IPv4 quanto em IPv6.
- 28.7.8. Deve suportar acesso remoto via interface web segura, utilizando o protocolo HTTPS.
- 28.7.9. Deve permitir upload de arquivos e atualização de firmware diretamente pela interface web (HTTPS).

- 28.7.10. Deve permitir a criação de perfis administrativos com diferentes níveis de permissão para gerenciamento e configuração do switch.
- 28.7.11. Deve suportar autenticação administrativa utilizando os protocolos RADIUS e TACACS+.
- 28.7.12. Deve possuir mecanismo para detecção de conflitos de endereço IP na rede. Em caso de conflito, o switch Deve gerar log de evento e enviar trap SNMP.
- 28.7.13. Deve suportar os protocolos LLDP e LLDP-MED, conforme padrão IEEE 802.1ab, para descoberta automática de dispositivos na rede.
- 28.7.14. Deve ser capaz de realizar testes nas interfaces para diagnosticar falhas físicas em cabos UTP (par trançado) conectados ao switch.
- 28.7.15. Deve suportar configuração e monitoramento por meio de REST API.
- 28.7.16. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03, 24, 25 e 26 “SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW TIPO I, II e III” , e ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- 28.7.16.1. Deve ser capaz, em conjunto com a controladora, de implementar e orquestrar políticas de segurança baseadas em microsegmentação, controlando a comunicação lateral entre usuários e endpoints na rede.
- 28.7.16.2. Deve permitir, em conjunto com a controladora, a criação de automações que executem ações com base em eventos detectados na rede, como quarentena de dispositivos, isolamento de endpoints e aplicação ou ajuste de políticas de segurança, de forma totalmente automatizada.
- 28.7.16.3. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo interrupção do serviço mediante a falha de um elemento.
- 28.7.16.4. Deve operar como ponto central para automação e gerenciamento dos switches.
- 28.7.16.5. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches.
- 28.7.16.6. Deve possuir interface gráfica para configuração, administração e monitoração dos switches.
- 28.7.16.7. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede.
- 28.7.16.8. Deve montar a topologia da rede de maneira automática.
- 28.7.16.9. Deve ser capaz de configurar os switches da rede.
- 28.7.16.10. Deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente para todos os switches gerenciados.
- 28.7.16.11. Deve permitir, por meio da interface gráfica, a aplicação da VLAN nativa (untagged) e das VLANs permitidas (tagged) nas interfaces dos switches.
- 28.7.16.12. Deve permitir, por meio da interface gráfica, a aplicação de políticas de Qualidade de Serviço (QoS) nas interfaces dos switches.
- 28.7.16.13. Deve permitir, por meio da interface gráfica, a aplicação de políticas de segurança com autenticação 802.1X nas interfaces dos switches.

- 28.7.16.14. Deve permitir, por meio da interface gráfica, a aplicação de mecanismos de segurança, como o DHCP Snooping, nas interfaces dos switches.
- 28.7.16.15. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard.
- 28.7.16.16. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede.
- 28.7.16.17. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection).
- 28.7.16.18. Deve ser capaz de configurar parâmetros SNMP dos switches.
- 28.7.16.19. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente.
- 28.7.16.20. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas.
- 28.7.16.21. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches.
- 28.7.16.22. A solução deve apresentar graficamente informações sobre disponibilidade dos switches.
- 28.7.16.23. Deve prover indicadores de saúde dos elementos críticos do ambiente.
- 28.7.16.24. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários.
- 28.7.16.25. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.
- 28.7.16.26. Deve possuir API no formato REST.

## **29. ITEM 29 – SOLUÇÃO DE LOGS E RELATORIA TIPO II**

- 29.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer.
- 29.2. Deverá possuir a capacidade de receber pelo menos 50 GB de logs diários, atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 12 (doze) meses.
- 29.3. Deverá suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
- 29.4. Deverá possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.
- 29.5. Deverá permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.
- 29.6. Deverá suportar SNMP versão 2 e 3

- 29.7. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
- 29.8. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.
- 29.9. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
- 29.10. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP
- 29.11. Deverá possuir autenticação de usuários para acesso à plataforma via Radius
- 29.12. Deverá possuir autenticação de usuários para acesso à plataforma via TACACS +
- 29.13. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico
- 29.14. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
- 29.15. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico
- 29.16. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- 29.17. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- 29.18. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
- 29.19. Deverá possuir mecanismos de apagamento automático para logs antigos.
- 29.20. Deverá permitir importação e exportação de relatórios;
- 29.21. Deverá ter a capacidade de criar relatórios no formato HTML;
- 29.22. Deverá ter a capacidade de criar relatórios em formato PDF;
- 29.23. Deverá ter a capacidade de criar relatórios no formato XML;
- 29.24. Deverá ter a capacidade de criar relatórios no formato CSV;
- 29.25. Deverá permitir exportar os logs no formato CSV;
- 29.26. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- 29.27. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- 29.28. Deverá ter relatórios predefinidos.
- 29.29. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução
- 29.30. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.
- 29.31. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.

- 29.32. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
- 29.33. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
- 29.34. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
- 29.35. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- 29.36. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- 29.37. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- 29.38. Deverá permitir o envio por e-mail relatórios automaticamente.
- 29.39. Deverá permitir que o relatório seja enviado por email ao destinatário específico.
- 29.40. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- 29.41. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- 29.42. Deverá permitir o uso de filtros nos relatórios.
- 29.43. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- 29.44. Deverá permitir especificar o idioma dos relatórios criados
- 29.45. Deverá gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- 29.46. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- 29.47. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- 29.48. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
- 29.49. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- 29.50. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
- 29.51. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
- 29.52. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
- 29.53. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.

- 29.54. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
- 29.55. Deverá permitir visualizar em tempo real os logs recebidos.
- 29.56. Deverá permitir o encaminhamento de log no formato syslog.
- 29.57. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).
- 29.58. Deverá gerar alertas de eventos a partir de logs recebidos
- 29.59. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal
- 29.60. Deverá permitir a integração ao sistema de tickets do ServiceNow
- 29.61. Deverá permitir o suporte a logs na nuvem pública do Amazon S3
- 29.62. Deverá permitir o suporte a logs na nuvem pública do Microsoft Azure
- 29.63. Permitir o suporte aos registros de nuvem pública do Google Cloud
- 29.64. Suportar o padrão SAML para autenticação do usuário administrador
- 29.65. Deverá possuir relatório de conformidade com o PCI DSS;
- 29.66. Deverá possuir um relatório de uso do aplicativo SaaS
- 29.67. Deverá possuir um relatório de prevenção de perda de dados (DLP)
- 29.68. Deverá possuir um relatório de VPN
- 29.69. Deverá possuir um relatório IPS (Intruder Prevention System)
- 29.70. Deverá possuir um relatório de reputação do cliente
- 29.71. Deverá possuir um relatório de análise de segurança do usuário
- 29.72. Deverá possuir um relatório de análise de ameaças cibernéticas
- 29.73. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança
- 29.74. Deverá possuir um relatório de tráfego DNS
- 29.75. Deverá possuir um relatório de tráfego de e-mail
- 29.76. Deverá possuir um relatório dos 10 principais aplicativos usados na rede
- 29.77. Deverá possuir um relatório dos 10 principais sites usados na rede
- 29.78. Deverá possuir um relatório de uso de mídia social

### **30. ITEM 30 – SERVIÇO CONTÍNUO DE GERENCIAMENTO E SUPORTE EM SEGURANÇA CIBERNÉTICA**

#### **30.1. SERVIÇOS E OPERAÇÃO**

- 30.1.1. A Contratada deverá alocar um profissional especializado, para execução de serviços que envolvem atividades de Cibersegurança, devendo ser prestadas de maneira contínua para apoiar os processos de trabalho e atividades pontuais para atender a necessidades de Cibersegurança e Conectividade da

Contratante, pelo período de 12 (doze) meses, conforme as necessidades da Contratante.

### 30.2. CONDIÇÕES INICIAIS PARA INÍCIO DO SERVIÇO

30.2.1. A prestação de serviço deverá ser iniciada após a emissão da Ordem de Serviço pela Contratante, a qual será enviada somente após a entrega do Termo de Homologação da instalação correspondente.

### 30.3. MODELO DE EXECUÇÃO

30.3.1. A execução do contrato seguirá metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada, a contratante caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços.

30.3.2. O profissional deverá receber todas as demandas sob as responsabilidades apresentadas pela Contratante, providenciando sua inspeção, conferência, classificação e prestação de contas.

30.3.3. Os profissionais deverão estudar os projetos, bem como todos os documentos que o complementarem, fornecidos pela Contratante, para execução das atividades de rotina, não se admitindo, em qualquer hipótese, alegação de desconhecimento dos mesmos.

30.3.4. Os serviços envolvem todas as atividades de rotina, configurações, programações, atendimento às demandas apresentadas pelo Contratante.

30.3.5. A execução do contrato seguirá metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada, a contratante caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A contratada deverá disponibilizar um Gerente do Projeto, que deverá supervisionar toda atividade dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela Contratante.

30.3.6. Os serviços deverão ser realizados nas dependências da Contratante, utilizando-se de equipamentos e infraestrutura com capacidade operacional.

30.3.7. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima 3 anos, na implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares a apresentadas pela Contratante.

30.3.8. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela Contratante, providenciando sua inspeção, conferência, classificação e prestação de contas.

30.3.9. Os profissionais deverão estudar os projetos, bem como todos os documentos que o complementarem, fornecidos pela Contratante, para execução das atividades de rotina, não se admitindo, em qualquer hipótese, alegação de desconhecimento dos mesmos.

30.3.10. Todos os encargos sociais e seguros em geral, necessários na execução das atividades exercidas pelos profissionais da Contratada, inclusive durante o transporte dos profissionais a serviço da Contratante, são de responsabilidade exclusiva da Contratada.

30.3.11. A Contratada deverá realizar regularmente os exames de saúde dos seus empregados, na forma da lei, assim como arcar com todas as despesas decorrentes de transporte, alimentação, inclusive seguro de vida contra o risco de acidentes de trabalho e outras especificadas nos dissídios ou convenções coletivas.

30.3.12. Cada prestador de serviço deverá apresentar-se uniformizado, com fardamento padrão fornecido pela Contratada, portando crachá de identificação.

- 30.3.13. Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente dos serviços objeto deste contrato.
- 30.3.14. Responder perante a Contratante pela conduta, frequência, pontualidade e assiduidade de seus empregados e efetuar as substituições daqueles que venham a se ausentar do serviço, por motivo justificado ou não, sem nenhum ônus para a Contratante, bem como comunicar à Contratante, antecipadamente, todo e qualquer afastamento, substituição ou inclusão de qualquer um dos seus empregados vinculados à execução do presente contrato.
- 30.3.15. Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pelo Contratante, atendendo prontamente às observações e exigências que lhe forem solicitadas.
- 30.3.16. Arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado à Contratante e terceiros, por sua culpa, ou em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência da CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência.
- 30.4.     **FORMA DE PAGAMENTO**
- 30.4.1. Os serviços serão pagos mensalmente, de acordo com o número de analistas contratados pela CONTRATADA.