5 ITENS OBRIGATÓRIOS PARA TESTE DE CONFORMIDADE

5.1 Cluster de Firewall Tipo 1

5.1.4 INTERFACES

5.1.4.1 Possuir no mínimo 08 (oito) interfaces 10 Gigabit SFP+

5.1.4.2 Possuir no mínimo 02 (duas) interfaces 40 Gigabit QSFP+ (ou superior);

5.1.4.3 Possuir no mínimo 04 (quatro) interfaces RJ45 de no mínimo 1 Gigabit;

5.1.5 TROUGHPUT

5.1.5.1 Possuir throughput de no mínimo 9 (Nove) Gbps de tráfego real por nó do cluster com as funcionalidades de segurança habilitadas (Firewall,IPS, Logging, Controle de Aplicação,Proteção contra Malware);

5.1.5.2 Possuir no mínimo 9,5(Nove e cinco décimos) Gbps de throughput para VPN IPsec;

5.1.6 CONEXÕES

5.1.6.1 Permitir no mínimo 150.000 (cento e cinquenta mil) novas conexões por segundo por nó do cluster;

5.1.6.2 Permitir no mínimo 4.000.000 (quatro milhões) conexões simultâneas por nó do cluster;

5.1.7 HARDWARE:

5.1.7.1 Possuir unidade de armazenamento interno redundante configurada em RAID-1 de no mínimo 240 GB cada, do tipo memória Flash ou SSD;

5.1.7.8 Possuir alimentação elétrica a partir de no mínimo 2 (duas) fontes independentes, redundantes e hot-swappable, capazes de operar entre 110-240VAC, 60 Hz, por reconhecimento automático do nível de tensão;

5.1.8 ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA:

5.1.8.4 Deve realizar monitoramento de falha de link;

5.2 Solução de Segurança Tipo 2

5.2.2 INTERFACES

5.2.2.1 Possuir no mínimo 08 (oito) interfaces Gigabit RJ45;

5.2.2.2 Possuir no mínimo 01(uma) interface console;

5.2.3 TROUGHPUT

5.2.3.1 Possuir no mínimo 900 (novecentos) Mbps de tráfego real com as funcionalidades de segurança habilitadas (Firewall, IPS, Logging, Controle de Aplicação, Proteção contra Malware);

5.2.3.2 Possuir no mínimo 1,5(Um e cinco décimos) Gbps de troughput para Ipsec VPN;

5.2.4 CONEXÕES

5.2.4.1 Permitir no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;

5.2.4.2 Permitir no mínimo 200.000 (duzentas mil) conexões simultâneas;

5.2.5 HARDWARE:

5.2.5.2 Possuir unidade de armazenamento interna de no mínimo 120 GB, capaz de armazenar todo o software, configuração e logs

5.2.5.3 Possuir alimentação elétrica a partir de no mínimo 2 (duas) fontes independentes e redundantes, capazes de operar entre 110-240VAC, 60 Hz;

5.3 Funcionalidades gerais para Solução de Segurança Tipo 1, Tipo 2

5.3.1 CARACTERISTICAS GERAIS

5.3.1.1 Deve implementar:

5.3.1.1.1 Firewall

5.3.1.1.2 NAT

5.3.1.1.3 URL Filtering,

5.3.1.1.4 Aplication Control;

5.3.1.1.5 Anti-bot;

5.3.1.1.6 Anti-Virus;

5.3.1.1.7 SSL Inspection;

5.3.1.1.8 IDS/IPS;

5.3.1.1.9 SDWAN;

5.3.1.1.10 VPN site-to-site;

5.3.1.4 Implementar interface gráfica Web segura, utilizando o protocolo HTTPS ou Console do próprio fabricante;

5.3.1.6 Implementar interface CLI segura através do protocolo SSH;

5.3.1.9 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;

5.3.1.10 A solução de permitir armazenar os backups localmente, bem como transferi-los para um servidor remoto;

5.3.1.11 Habilidade de realizar upgrade remotamente;

5.3.1.14 A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária dos logs localmente no appliance de segurança;

5.3.2 POLÍTICAS DE FIREWALL

5.3.2.18 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;

5.3.2.20 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;

5.3.2.21 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;

5.3.2.23 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;

5.3.3 SDWAN

5.3.3.2 A solução deverá ser capaz de balancear cargas entre dois links distintos;

5.3.3.3 Deverá implementar a criação de tuneis criptografados de forma dinâmica entre os sites;

5.3.3.5 Deverá implementar controle tráfego por aplicação;

5.3.3.6 Deverá suportar, no mínimo, 3 (três) links de WAN;

5.3.3.9 Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

5.3.3.10 Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;

5.3.3.11 Os dispositivos remotos devem suportar a funcionalidade de ZTP (Zero Touch Provisioning) para que assim, inseridos nas estruturas remotas, possam buscar automaticamente por suas configurações, com o objetivo de facilitar a instalação nas unidades remotas ou a troca de um dispositivo defeituoso;

5.3.3.12 Gerenciamento centralizado e implantação Zero Touch;

5.3.4 ACESSO REMOTO - VPN:

5.3.4.10 Deverá ser capaz de monitorar todos os usuários remotos logados;

5.3.4.11 Deverá ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado;

5.3.4.12 Deve incluir gerenciamento centralizado de VPNs, com a possibilidade de estabelecimento de VPNs com vários peers remotos ao mesmo tempo;

5.3.4.13 Clientes IPSec do mesmo fabricante devem estar disponíveis para pelo menos Windows 10 (64 bits);

5.3.5 CONTROLE DE APLICAÇÕES WEB E FILTRO URL:

5.3.5.1 A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança, que permita a criação de políticas de liberação ou bloqueio;

5.3.5.2 A solução deve ser capaz de identificar qualquer tipo de aplicação, em até camada 7, independente de porta e protocolo;

5.3.5.3 A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na mesma console de gerenciamento;

5.3.5.5 Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos de usuários;

5.3.5.6 Deve possibilitar a inspeção de tráfego criptografado HTTPS (Inbound/Outbund);

5.3.5.8 A solução deve ser capaz de criar regras com mais de uma categoria;

5.3.5.9 Deve possibilitar a permissão ou bloqueio de aplicações ou URLs por pelo menos os seguintes critérios:

5.3.5.9.1 Aplicação da Web;

5.3.5.9.2 Categorias;

5.3.5.9.3 Nível de risco;

5.3.5.9.4 IP/Range de IPs/Redes;

5.3.5.9.5 Usuários;

5.3.5.9.6 Diferentes grupos de usuários;

5.3.5.10 Aplicações que sejam passiveis a técnicas de evasão por malwares e uso excessivo de banda (EX:ultrasurf, torrent, dropbox e file sharing);

5.3.5.11 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários ou grupos do AD;

5.3.5.12 A solução deve fornecer uma forma para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

5.3.5.13 Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e no módulo de gerência;

5.3.5.14 Deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

5.3.5.15 Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas, sendo possível executar esta tarefa através da interface de gerência GUI ou WEB, ou, através de ticket direto com o fabricante;

5.3.6 IDENTIFICAÇÃO DE USUÁRIOS:

5.3.6.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório;

5.3.6.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.3.6.3 A identificação do usuário registrado no Microsoft Active Directory deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

5.3.7 SISTEMA DE PREVENÇÃO DE INTRUSÃO - IPS:

5.3.7.1 Deve possuir módulo de IPS integrado no próprio appliance, sem a necessidade de uso de quaisquer interfaces externas, para proteção do ambiente contra ataques, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança;

5.3.7.2 A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações;

5.3.7.3 O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

5.3.7.4 Possuir proteções de segurança, informações como: código CVE, severidade, e tipo de ação que a mesma irá executar;

5.3.7.18 A solução deve possuir inspeção de tráfego HTTPS sendo possível criar bypass para sites evitando qualquer tipo de quebra de sigilo de informações pessoais;

5.3.7.22 A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

5.3.8 ANTI-MALWARE:

5.3.8.1 Possuir módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de segurança e integrado à gerência centralizada de administração, monitoração e logs;

5.3.8.2 A solução deve possuir nuvem proprietária inteligente do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

5.3.8.4 A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

5.3.8.6 A solução Antibot deve possuir mecanismo de detecção em multicamadas que inclui, reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação e assinaturas;

5.3.8.9 A solução deve possuir na própria interface de gerência, gráfico contendo informações em tempo real sobre as atividades recentes de malwares detectados na solução;

5.3.8.10 Deve possuir engine onde faça Mitigação DNS, sendo ela possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso;

5.3.8.11 Deve ser capaz de inspecionar o tráfego criptografado SSL;

5.3.8.12 Deve ser capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;

5.3.8.13 Deve permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);

5.3.9 AMEAÇAS AVANÇADAS PERSISTENTES - APT:

5.3.9.1 Deverá prover as funcionalidades de inspeção de tráfego de entrada de malwares não conhecidos (dia zero) ou do tipo APT (Advanced Persistent Threat) com filtro de ameaças avançadas e análise de execução em tempo real;

5.3.9.2 A solução deve ser capaz de inspecionar o tráfego criptografado SSL;

5.3.9.5 Implementar atualização da base de dados da rede de inteligência de forma automática;

5.3.9.6 A solução deve implementar a emulação, detecção ou bloqueio de qualquer malware e/ou código malicioso detectado;

5.3.9.7 Toda análise deverá ser realizada de forma interna em Appliance do próprio fabricante ou nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

5.3.9.9 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador para solicitar a análise;

5.3.9.11 Toda a análise ou bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real;

5.3.9.12 Implementar mecanismo de exceção, permitindo a criação de regras por sub-rede e endereço IP;

5.3.9.13 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de estatísticas das ameaças;

5.4 Solução de Gerenciamento e Controle do Firewall

5.4.1 A solução deve ser do mesmo fabricante dos demais itens ofertados no Lote 01;

5.4.2 A solução deve ser capaz de gerenciar todos os equipamentos de Segurança de forma centralizada;

5.4.3 A solução deve ser responsável pela concentração dos logs e emissão de relatórios;

5.4.5 O gerenciamento de políticas será realizado em um único ponto centralizado;

5.4.6 Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos;

5.4.8 Caso a Solução de Gerenciamento Centralizada torne-se indisponível, todos os seus gateways gerenciados devem continuar funcionando normalmente, permitindo a administração, operação e total controle sobre cada gateway enquanto a gerência continuar indisponível;

5.4.9 A Solução de Gerenciamento Centralizada deve permitir a instalação de políticas individuais (somente para 1 gateway), para um grupo de gateways e para todos os seus gateways gerenciados, não sendo aceito soluções com aplicações de apenas uma das opções;

5.4.10 Possibilitar a execução das seguintes tarefas: criação e administração de políticas de firewall e controle de aplicação; criação e administração de políticas de IPS, antivírus e anti-spyware; criação e administração de políticas de conteúdo Web e filtro de URL; monitoração de logs; ferramentas de investigação de logs; debugging; troubleshooting; visualização de eventos; dashboards; captura de pacotes;

5.4.11 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, anti-malware) e URLs analisadas pelo firewall;

5.4.12 Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar onde, na base de regras, está sendo utilizado determinado objeto de rede;

5.4.13 Caso haja a necessidade de instalação de algum software para a administração da solução, o mesmo deve ser compatível com o Microsoft Windows 11;

5.4.14 Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

5.4.15 Deve registrar logs de auditoria referente as ações dos usuários administradores;

5.4.16 A solução deve possuir registro de todas as alterações realizadas em uma política de segurança, por um determinado administrador, permitindo a identificação do responsável pela mudança, contendo registros de autoria, data e origem;

5.4.17 Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou não conformes;

5.4.18 Suportar acesso baseado em perfil de usuário com as permissões de visualizar e modificar;

5.4.19 Deverá possuir validação da política avisando quando houver regras que ofusquem ou conflitem com outras regras;

5.4.20 A solução deve possuir "hit"/volume de regras para identificar possíveis melhorias na performance reordenando as mesmas;

5.4.21 Deve possuir visualização de log em tempo próximo ao real;

5.4.22 A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos;

5.4.39 Solução deve incluir monitoramento gráfico que fornece uma maneira fácil monitorar o status de gateways, apresentando os seguintes status:

5.4.39.1 Versão do sistema operacional;

5.4.39.2 Informações de utilização de CPU dos gateways gerenciados;

5.4.39.3 Informações de conexões concorrentes dos gateways gerenciados;

5.4.40 Alertar quando um membro estiver desconectado do cluster;

5.4.42 Suportar rollback de configuração para a última configuração salva e do sistema operacional para a última versão local;

5.6 Ponto de Acesso sem fio Tipo 1

5.6.2.1 Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

5.6.2.2 Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

5.6.2.3 Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (podendo ser utilizado cabo de segurança com chave ou similar);

5.6.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;

5.6.2.6 Deve possuir um ou mais Leds indicadores de estado de operação;

5.6.2.7 Não deve possuir antenas aparentes, que sejam rosqueáveis, evitando a remoção das antenas;

5.6.3 CONEXÃO E REDE:

5.6.3.1 Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior;

5.6.3.2 Suportar VLANs conforme o padrão IEEE 802.1Q;

5.6.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

5.6.4 SEGURANÇA:

5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.6.6 Implementar chave de compartilhada exclusiva (Exemplo: PPSK, Identity PSK, ePSK, MPSK, DPSK ou similiar do fabricante)

5.6.7 RÁDIO:

5.6.7.1 Fluxo 2.4Ghz e 5Ghz: no mínimo 2x2

5.6.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

5.6.7.8 Capacidade de implementar no mínimo 16 SSID;

5.6.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

5.6.7.10 Deve possuir capacidade de selecionar automaticamente o canal de transmissão;

5.6.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

5.6.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento da conexão por meio do rádio Wi-Fi com outros pontos de acesso;

5.6.7.15 Deve implementar recurso de Target Wake Time (TWT);

5.6.7.17 Deve suportar BSS Coloring;

5.7 Ponto de Acesso sem fio Tipo 2

5.7.2 HARDWARE:

5.7.2.1 Possuir capacidade de montagem em parede, teto e mastro, devendo ser fornecidos todos os acessórios necessários para estas montagens;

5.7.2.2 Deve acompanhar kit para montagem em parede, o kit deve ter recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (podendo ser utilizado cabo de segurança com chave ou similar);

5.7.2.4 Possui grau de proteção mínimo IP67, outdoor;

5.7.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;

5.7.2.7 Deve possuir um ou mais Leds indicadores de estado de operação;

5.7.3 CONEXÃO E REDE:

5.7.3.1 Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior;

5.7.3.2 Suportar VLANs confirme o padrão IEEE 802.1Q;

5.7.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

5.7.4 SEGURANÇA:

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.7.6 Implementar chave de compartilhada exclusiva (Exemplo: PPSK, Identity PSK, ePSK, MPSK, DPSK ou similar do fabricante)

5.7.7 RÁDIO:

5.7.7.1 Fluxo 5Ghz: 4x4

5.7.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

5.7.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

5.7.7.10 Deve possuir capacidade de selecionar automaticamente o canal de transmissão;

5.7.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

5.7.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento da conexão por meio do rádio Wi-Fi com outros pontos de acesso;

5.7.7.15 Deve implementar recurso de Target Wake Time (TWT);

5.7.7.17 Deve suportar BSS Coloring;

5.8 Switch Tipo 01

5.8.1 Possuir capacidade de fornecer alimentação PoE 802.3af, 802.3at ou 802.3bt;

5.8.2 Deve possuir capacidade de energizar no mínimo 2 Access Point Tipo 2 e 10 Access Point Tipo 1 ou 12 Access Point Tipo 1 simultaneamente;

5.8.3 O Switch deve ser capaz de alimentar os Acces Points Tipo 1 sem a necessidade de componentes adicionais;

5.8.5 Possuir no mínimo 24(vinte e quatro) PoE portas Gigabit RJ45;

5.8.6 Possuir no mínimo 4(quatro) portas SFP 1 Gbps ou superior;

5.8.8 Possuir Leds indicativos de funcionamento da fonte de alimentação e status das portas;

5.8.9 Deve ocupar 1U do Rack;

5.8.15 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência;

5.8.17 Implementar gerenciamento HTTPS;

5.8.18 Suportar autenticação em servidores RADIUS ou TACACS;

5.8.22. Implementar LLDP e LLDP-MED;

5.8.24. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

5.8.26. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;

5.8.28 Implementar IEEE 802.1x para autenticação do usuário, permitindo à associação dinâmica do usuário a determinada VLAN;

5.8.29 Deverá estar licenciado para a gerência e controle do item Solução de gerenciamento e controle;

5.9 Switch Tipo 02

5.9.2 Possuir no mínimo 24 portas 10/100/1000 Base-T;

5.9.3 Possuir no mínimo 4(quatro) portas SFP 1 Gbps ou superior;

5.9.5 Possuir Leds indicativos de funcionamento da fonte de alimentação e status das portas;

5.9.6 Deve ocupar 1U do Rack;

5.9.12 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência;

5.9.14 Implementar gerenciamento HTTPS;

5.9.15 Suportar autenticação em servidores RADIUS ou TACACS;

5.9.19. Implementar LLDP e LLDP-MED;

5.9.21. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

5.9.23. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;

5.10 Solução de Gerenciamento e Controle dos APs e Switches

5.10.2 A solução deve ser do mesmo fabricante dos demais itens ofertados no Lote 02;

5.10.4 A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única;

5.10.6 A comunicação entre a solução de Gerenciamento e os Access Points/Switchs deve ser criptografada;

5.10.8 A alta disponibilidade da rede sem fio será mantida pela arquitetura definida, não permitindo que a rede sem fio se torne inoperante em caso de falha na solução de gerenciamento;

5.10.9. A solução deverá ser compatível com VMware 6.7;

5.10.12 Deve permitir que as configurações sejam aplicadas em vários pontos de acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de acesso individualmente.

5.10.13 Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF).

5.10.14 Permitir a visualização de alertas da rede sem fio em tempo real.

5.10.15 Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador.

5.10.16 Deverá implementar disponibilidade de SSID baseado em dia da semana/hora;

5.10.17 Monitorar o desempenho da rede wireless;

5.10.18 A falha de comunicação entre o sistema de Gerenciamento e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso;

5.10.19 Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

5.10.20 Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede de acordo com as condições de RF;

5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;

5.10.22 Deve permitir ao administrador visualizar e monitorar o mapa de cobertura da rede sem fio;

5.10.24 Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso;

5.10.25 Deverá ser capaz de provisionar remotamente novos dispositivos em estado padrão de fábrica para estado totalmente provisionado;

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

5.10.27 Implementar controle de acesso de usuário administrativo por HTTPS. Deve ainda implementar perfis de acesso diferenciados por usuário ou grupo de usuários;

5.10.28 Gerenciar de forma centralizada a autenticação de usuários;

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.1 Usuário e senha definidos pelo administrador;

5.10.30.2 LDAP;

5.10.30.3 Implementar pelo menos duas formas de autenticação que permita que o usuário obtenha acesso a rede sem a necessidade de usuário ou senha previamente cadastrados. Exemplo: Google, Office365, Facebook, Instagram, Linkedin, Twitter;

5.10.32 Implementar Radius relay, de forma a permitir integração com servidor Radius externos;

5.10.33 Permitir a customização de página de autenticação de usuários, com inclusão de textos e logotipo;

5.10.36 Identificar usuários e dispositivo conectados e permitir a visualização de, no mínimo:

5.10.36.1 Nome usuário conectado;

5.10.36.2 Endereço MAC;

5.10.36.3 Status da autenticação;

5.10.36.4 Horário de início da sessão ou Tempo de conexão;

5.10.36.5 Sistema Operacional do dispositivo a qual está associado;

5.13 Transceiver 1000Base-SX

5.13.1 Tipo: MiniGbic SPF 1000Base-SX

5.13.2 Deve ser compatível com os switches ofertados;

5.13.3 Conector padrão LC-duplex;

5.14 Transceiver 1000Base-LX

5.14.1 Tipo: MiniGbic SPF 1000Base-LX

5.14.2 Deve ser compatível com os switches ofertados;

5.14.3 Conector padrão LC-duplex;