Revisão 2024.10

ESPECIFICAÇÃO TÉCNICA de SOFTWARE DE GERENCIAMENTO LAN E WLAN

Características mínimas

1. Deve realizar o gerenciamento centralizado de todos os elementos da solução de LAN e WLAN, podendo ser utilizada pela CONTRATANTE como única interface gráfica de administração da solução;
2. Não serão aceitas soluções baseadas em softwares open source.
3. O sistema embarcado de gerenciamento deverá permitir instalação de forma On-Premise, ou seja, não será aceito soluções baseadas em nuvem/cloud;
4. A solução de gerência deve ser instalável e compatível com os sistemas operacionais Microsoft Windows Server ou Linux Enterprise;
5. Toda a infraestrutura de hardware para a ativação da solução de gerenciamento deve ser entregue com todos os recursos necessários para sua execução;
   5.1. Deve ser entregue os servidores/apliances em sua configuração mínima para suportar todos os requisitos descritos neste termo de referência;
   5.2. Deve ser entregue com recursos suficientes para prover redundância da plataforma em casos que ocorra a inoperância de um dos componentes que compõem a solução;
   5.3. Deve ser entregue recurso computacional suficiente para o gerenciamento unificado de, no mínimo, 30.000 dispositivos, entre switches e pontos de acesso. Será aceito o fornecimento de clusters de Servidores com appliances físicos ou virtuais da solução ofertada com, no mínimo, 10.000 dispositivos em cada instância entre switches gerenciados, access points e dispositivos de fabricantes diferentes para monitoramento por meio de SNMP, podendo cada uma das instância ter sua própria interface de administração;
   5.4. Deve ser entregue recurso computacional suficiente para, no mínimo, 100.000 autenticações simultâneas;
6. Deve oferecer suporte ao gerenciamento de forma centralizada, ou no máximo 3 instâncias, aos dispositivos, com ou sem fio, em uma única rede campus, em múltiplas localidades e múltiplas WANs.
7. Prover uma interface gráfica para gerenciar toda a solução proposta e de forma centralizada.
8. Deve possuir capacidade de gerenciamento hierárquico dos dispositivos com possibilidade de definição de grupos de equipamentos e alteração das configurações do grupo sem a necessidade de configuração individual de cada equipamento;
9. Deve suportar a construção, definição e configuração de rede baseada em GUI (Interface gráfica do usuário), suportando a utilização de templates para configuração;

10. Deve suportar o provisionamento de configurações para múltiplos cenários, como grandes ou pequenos escritórios, permitindo que os usuários parametrizem o fluxo de trabalho conforme as atribuições. Atividades podem ser executas simultaneamente em lotes de provisionamento;
11. Deve suportar a integração com ferramentas de planejamento de redes wireless (próprias ou de terceiro), permitindo que os usuários importem arquivos de planejamento de rede para visualização wireless;
12. Deve suportar tecnologias plug-and-play (PnP), incluindo métodos de implantação baseados em opção DHCP, leitura de código de barras ou e-mail, permitindo o registro e implementação de dispositivos em lote sem coleta manual de ESN;
13. Deve detectar APs e terminais não autorizados no modo WIDS/WIPS e aplicando medidas de defesa. Deve coletar estatísticas sobre APs e terminais não autorizados;
14. Deve Suportar a integração automática de dispositivos por meio de endereços IPv6 e configuração automática de LAN-WAN;
15. Deve permitir integração com sistemas que gerenciem dispositivos IoT, que se utilizarem da infraestrutura de pontos de acesso da solução, utilizando pelo menos Wifi + BLE (Bluetooth) ou Wifi + RFID.
16. Deve suportar a exibição de dashboard com informações como visão geral de recursos, estatísticas e tendências de alarme e estatísticas de tráfego, e permitir que os usuários personalizem os componentes e a formatação do dashboard conforme necessário e os definam como dashboard padrão.
17. Deve suportar políticas de QoS orientada a aplicativos de camada 7, com suporte a políticas flexíveis de acesso;
18. Deve suportar a integração com múltiplas fontes de identidade, como AD/LDAP, ou RADIUS, ou Azure AD, ou Google Cloud AD, não limitadas a estas, realizando o mapeamento de funções locais com base em atributos de conta e autorização de acesso a rede;
19. Deve permitir que os usuários possam alternar entre várias redes sem fazer login novamente;
20. A plataforma deve ser construída através de conceito multicliente ou multisite, isto é, uma única plataforma deve ser capaz de criar diversos ambientes distintos de gerenciamento, para clientes/sites finais distintos;
    20.1. Cada cliente criado deve ser único e isolado, não permitindo que a estrutura de um dos clientes possua acesso aos demais registrados na plataforma;
    20.2. Cada cliente/site deve possuir sua própria estrutura de grupos de usuários, permitindo a eles a utilização de cada um dos métodos de autenticações descritos neste termo de referência;
    20.3. A plataforma deve possuir camada de gestão de clientes/sites, onde permita da criação, edição e remoção de clientes;
    20.4. A plataforma deverá suportar, no mínimo, a criação de até 300 ambientes de gerenciamento distintos (Clientes/sites);
21. Permitir a visualização de alertas da rede, com indicação de níveis de severidade, permitindo o acesso simultâneo de, no mínimo, 5 usuários de monitoração, e o envio automático de alertas por e-mail;
22. A plataforma deve implementar adição de dispositivos de fabricantes diferentes para monitoramento por meio de SNMP.

23. Deve possuir capacidade de gerenciamento de logs interno a solução, permitindo ainda, a interconexão com servidores de syslog externo.;
24. Deve implementar busca dinâmica por usuários e dispositivos, retornando as informações específicas do usuário buscado e de sua conexão;
25. Deve permitir, através da interface gráfica, o acesso à interface CLI do equipamento, de forma segura;
26. Os componentes responsáveis pelos serviços de gerência da solução devem implementar acesso remoto administrativo através de navegador de internet (browser) padrão, com interface gráfica, utilizando o protocolo HTTPS;
27. Deve permitir a criação de perfis de administradores, criando visões administrativas independentes como, por exemplo, superusers, operators e monitors;
28. Deve ser possível criar grupos administrativos de usuários, permitindo editar quais elementos da plataforma serão acessíveis para cada grupo;
29. Deve permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados nos ativos gerenciados, a partir da plataforma de gerência;
30. Deve implementar o controle de mudanças nas configurações dos ativos gerenciados, backup de configurações e registro histórico destas implantações, permitindo o rollback das configurações através de um ponto de backup;
31. Deve realizar a atualização de software dos ativos de forma gradual (em grupos), sem causar indisponibilidade do respectivo serviço, através de agendamentos, gerando relatórios posterior do resultado da atualização;
32. Deve implementar o controle da distribuição das atualizações de software, mantendo um repositório de versões de softwares;
33. Implementar mecanismos de atribuição de TAG/LABEL/TEMPLATES para os ativos gerenciados, permitindo aplicação de configurações;
34. Deve possuir interface que detalhe o status de configurações aplicadas, informando, no mínimo, os seguintes status: Sucesso, Aplicando, Falha;
35. Permitir a configuração de servidor syslog externo, para exportar logs de operação;
36. Implementar configuração de VLANs (IEEE 802.1Q) dos ativos gerenciados;
37. Permitir o agendamento de tarefas administrativas e operacionais que devem ser executadas.
38. Implementar a monitoração de desempenho através de telemetria nos dispositivos, quando cabível com: tráfego de dados nas portas, consumo de CPU, consumo de memória, falhas de autenticação, utilização da rede por cliente.
39. Deve ser possível implementar Listas de Controle de Acesso – ACLs nos ativos gerenciados através da interface de gerenciamento;
40. Possuir arquitetura cliente-servidor ou web-based com método de conexão segura entre os ativos gerenciados e plataforma de gerenciamento através de criptografia;
41. Suportar mecanismo de Zero Touch Provisioning (ZTP), permitindo que os dispositivos que estiverem com as configurações de fábrica se registrem automaticamente na plataforma de gerenciamento a fim de obter as configurações desejadas.

42. Permitir a visualização gráfica dos equipamentos de rede gerenciados e a topologia da rede.
43. Suportar a visualização de alertas da rede em tempo real, com indicação de níveis de severidade, permitindo o acesso simultâneo de usuários de monitoração além do envio automático de alertas por e-mail;
44. Implementar monitoramento de desempenho que suporte ao menos um dos seguintes recursos: Netflow, sFlow, OpenFlow, HTTP, Netconf ou similar com gráficos.
45. Verificar e alterar o estado operacional dos equipamentos de rede, reconhecendo, pelo menos, os seguintes estados operacionais: ativo e inativo.
46. Deverá possuir ferramentas para depuração e gerenciamento como debug, trace, log de eventos.
47. Deve suportar a configuração de VXLAN com gateways centralizados e distribuídos, podendo ser implantada na camada de agregação ou na borda. Deve Suportar redes virtuais baseadas em VXLAN de Camada 2 pura sem gateways.
48. Deve Suportar implantação de rede VXLAN ou SPB sob demanda por meio de protocolos abertos, como BGP-EVPN ou IS-IS.
49. Deve suportar “wizard-based fabric network construction” e “automatic network configuration” por meio de VXLAN ou SPB na camada de overlay e orquestração automática da rede na camada de underlay / overlay conforme alteração do link de operação;
50. **Requisitos específicos para comutadores:**
    - 50.1. Deve suportar o gerenciamento de todos os modelos de switches solicitados neste termo de referência;
    - 50.2. Deve implementar a listagem das informações dos usuários conectados nas redes LAN: endereço IP, endereço MAC, tipo de dispositivo cliente e VLAN;
    - 50.3. Através da interface gráfica ou ferramenta de aplicação de scripts de configuração da solução de gerenciamento, deve ser possível a configuração, ao menos, das seguintes funcionalidades dos comutadores:
        - 50.3.1. Criação de Subnets;
        - 50.3.2. Adicionar/Remover interfaces de um grupo de LAG;
        - 50.3.3. Atribuir tipo de interface, entre hibrida, acesso ou tronco;
        - 50.3.4. Criação de rotas estáticas;
        - 50.3.5. Configuração de parâmetros de roteamento dinâmico OSPF;
        - 50.3.6. Criação e atribuição de políticas de tráfego (QoS);
        - 50.3.7. Criação e atribuição de ACL’s;
        - 50.3.8. Criação e atribuição de políticas de autenticação (802.1x, portal e MACAuthentication);
        - 50.3.9. Configuração de empilhamento entre comutadores;
        - 50.3.10. Configuração de STP (MSTP, RSTP, VBST);
51. **Requisitos específicos para pontos de acesso:**
    - 51.1. Deve suportar o gerenciamento de todos os modelos de pontos de acesso solicitados neste termo de referência;
    - 51.2. A plataforma deve prover o gerenciamento e controle de todas as funcionalidades a serem ofertadas através dos pontos de acesso registrados para os clientes finais;

51.3. Deve permitir a criação e publicação, de no mínimo, 16 SSID's por ponto de acesso;

51.4. Deve implementar a configuração, por SSID, das seguintes funcionalidades:

51.4.1. Nome de Rede SSID;

51.4.2. Modo agendado, permitindo definir dia da semana e horário para ativação e desativação;

51.4.3. Permitir a seleção de quais bandas devem ser utilizadas, entre as disponíveis, nos pontos de acesso (2.4Ghz, 5Ghz)

51.4.4. Definição de TAG's/LABEL's/TEMPLATE's para especificar quais pontos de acesso devem propagar a rede/SSID configurada;

51.4.5. Modo de encaminhamento de tráfego de usuário:

51.4.6. Permitir Configuração para servidor DHCP;

51.4.7. Deve ser possível a definição de múltiplas VLAN's, com atribuição orientada a TAG's/LABEL's/TEMPLATE's ;

51.4.8. Ocultar a publicação do SSID (SSID Hiding);

51.4.9. Isolamento de comunicação entre dispositivos clientes conectados ao mesmo SSID;

51.4.10. Definição de prioridade WMM (Wi-Fi Multimedia), com edição dos parâmetros de priorização;

51.4.11. Deve suportar, no mínimo, os seguintes métodos de autenticação:

51.4.11.1. Aberto;

51.4.11.2. Aberto com autenticação através de portal;

51.4.11.3. MAC Authentication;

51.4.11.4. Chave compartilhada, com suporte WPA 3 Enterprise;

51.4.11.5. 802.1x Authentication, com opção de seleção para servidor RADIUS interno e externo e suporte a CoA (Change of Authorization);

51.4.12. Atribuição de Rate Limiting para entrada e saída, com possibilidade de definição de intervalo de tempo o qual a função deve estar ativa;

51.4.13. Criação de filtros orientados a camada de aplicação (L7);

51.5. A plataforma deve ser capaz de gerenciar as configurações de rádio, em todas as bandas disponíveis pelo ponto de acesso, permitindo a parametrização das seguintes métricas:

51.5.1. Definição de canais de operação;

51.5.2. Potência de Transmissão (TPC);

51.5.3. Forçar a desconexão de terminais com sinal de transmissão fraco, com customização de SNR;

51.5.4. Deve possuir funcionalidade de configuração automática dos parâmetros de potência de transmissão e canal de operação, orientado a

análise do ambiente em que o ponto de acesso está fixado, procurando as configurações de melhor eficiência para o ambiente;

51.6. Deve implementar análise de espectro para deteção de ataques e interferências do ambiente e aplicar medidas de contenção automáticas WIDS/WIPS;

51.6.1. Deve possuir capacidade de mostrar em interface gráfica o resultado da análise de espectro, informando quais os tipos de deteção e contenção foram aplicadas;

51.6.2. Deve ser possível fazer buscas históricas de resultados anteriores, informando quais detecções e contenções foram realizadas em um determinado período;

51.6.3. Deve ser possível criar listas de SSID's que serão ignorados no momento da análise;

51.7. Deve ser possível listar todas as conexões ativas e históricas, informando, no mínimo, as seguintes métricas da conexão:

51.7.1. MAC Address do terminal que se conectou;

51.7.2. SSID utilizado para conexão;

51.7.3. Endereço IP obtido pelo terminal;

51.7.4. Packet Loss;

51.7.5. SNR;

51.7.6. Força da potência de conexão (RSSI);

51.7.7. Taxa negociada (Mbit/s);

51.7.8. Canal;

51.8. A plataforma deve ser capaz de apresentar as principais aplicações de camada 7 que estão sendo utilizada na rede, informando o volume de dados utilizado por cada uma delas;

52. Requisito de Autenticação;

52.1. A plataforma deve possuir, de forma integrada, ambiente de autenticação de usuários;

52.2. Permitir a autenticação para acesso dos usuários que se conectem à rede através de MAC Address, Captive Portal, 802.1x em base Local, 802.1x RADIUS e 802.1x AD/LDAP.

52.2.1. Deve estar disponível para a rede LAN e WLAN;

52.3. Implementar mecanismo de AAA para usuários da rede;

52.4. Implementar autenticação via servidor RADIUS: Authentication, Accounting.

52.5. A solução deve possuir um servidor RADIUS incorporado para autenticação 802.1x e MAC. Não será aceito como um produto separado.

52.6. Deverá possuir uma base local de autenticação;

52.7. Deverá suportar integração com uma base externa via Radius, LDAP e AD;

52.8. A solução deve permitir classificar o tipo do dispositivo (notebook, celular, tablet) e o sistema operacional do dispositivo (Windows, Linux, Mac, Android) sem a necessidade de instalar agentes.

52.9. Deve implementar a listagem das informações dos usuários conectados nas redes LAN: endereço IP, endereço MAC, tipo de dispositivo cliente e VLAN.

52.10. A plataforma deve possuir mecanismos de criação e gerenciamento de usuários guests, com as seguintes formas de autorização:

52.10.1. Concordando com termo e condições;

52.10.2. Usuário e Senha;
52.10.3. Login através de mídia social (Facebook, Google);
52.10.4. Código de Acesso;
52.10.5. Formulário de auto provisionamento com autorização automática ou através de um operador;
52.10.6. O portal visitante, que deverá suportar customizações;

52.11. O período da conta do visitante deverá ser configurado por tempo e por número de dispositivo por conta;

52.12. O modelo de licenciamento da solução para gerenciamento de convidados/visitantes deve basear-se na quantidade de dispositivos ativos simultaneamente (notebooks, celulares, tablets, etc) e deve ser na modalidade perpétua;

52.13. O licenciamento de autenticação e device proffiling deve operar em formato de pool na plataforma de gerenciamento, isto é, o somatório total das licenças deve estar disponível a utilização por qualquer ponto de acesso ou switches gerenciado;

52.14. Deve permitir a configuração, por SSID, de túnel IPSEC ou GRE;

52.15. A plataforma deve possuir suporte a integração de portais externos através de API's;

52.16. Gerar e apresentar, on-line, as informações de usuários conectados na rede, como: endereço IP, endereço MAC, tipo de dispositivo (modelo ou fabricante), VLAN, parâmetros de associação, autenticação e tempo de duração da conexão.

52.17. Deve implementar busca dinâmica por usuários e dispositivos, retornando as informações específicas do usuário autenticado buscado e de sua conexão;

CONDIÇÕES GERAIS

a) Garantia da solução de 5 anos, disponibilizada pelo fabricante ou parceiro oficial autorizado - apresentar comprovação oficial do fabricante e dos SLA;
b) Todos os componentes da solução integrados pelo fabricante do mesmo - apresentar comprovação;
c) A solução deverá ser fornecida com todas as licenças necessárias para o pleno funcionamento, na modalidade perpétua em nome da CONTRATANTE, e com atualizações durante a vigência do contrato;
d) Anexar documentação técnica detalhada oficial do fabricante, contemplando os requisitos solicitados;
e) Adicionalmente a proposta, a licitante deverá indicar, ponto a ponto, com a indicação do documento e página onde se encontra a comprovação do atendimento de cada requisito e conformidade do material proposto com a especificação exigida deste termo de referência;

TREINAMENTO NA SOLUÇÃO OFERTADA

1. Deverá ser ofertado treinamento oficial de no mínimo 20 horas para até 10 pessoas;
2. O treinamento deve ser ofertado por profissional capacitado e certificado na solução ofertada;
3. O treinamento deve contemplar a solução como um todo no intuito de capacitar a equipe para o eficiente gerenciamento da solução ofertada pela CONTRATADA, abrangendo desde a configuração inicial até a administração contínua do sistema.
4. Introdução à Solução.

4.1. Visão geral

5. Configuração Inicial:

5.1. Procedimentos passo a passo para a instalação e configurações iniciais

5.2. Configuração de parâmetros básicos.

6. Características da Solução:

6.1. Apresentação detalhada das funcionalidades oferecidas.

6.2. Destaque para recursos exclusivos e diferenciados.

7. Administração de Rede e Portas:

7.1. Exploração do painel de administração.

7.2. Configuração de VLANs e segmentação de rede.

7.3. Alocação de recursos, equipamentos.

7.4. Gerenciamento de portas e suas funcionalidades.

8. Segurança e Controle de Acesso:

8.1. Implementação de medidas de segurança.

8.2. Configuração de políticas de controle de acesso.

9. Utilização de ferramentas de monitoramento.
10. Deverá ser ofertado material de apoio, manuais detalhados, vídeos tutoriais (se necessário) e documentação técnica para referência contínua.
11. Deverá ser emitido certificado de participação no treinamento.