CADERNO DE TESTES PARA PROJETO WI-FI NACIONAL POLÍCIA FEDERAL

Data:		
Fabricante:		
Modelos:	**Item 1**	
	Item 2	
	Item 3	
	Item 4	
	Item 5	
	Item 6	

_____ _____

Representante Empresa Representante Polícia Federal

Teste	Tipo	Objetivo	Procedimento Básico de Teste	Resultado Esperado	Evidência	Resultado	
						Aprovado	Reprovado
Gestão							
a.1	OBRIGATÓRIO	Verificar a relação entre autenticação, IP, MAC, nome do dispositivo cliente e switch	Durante todo o período de testes habilitar a Solução de Automação ou a Solução de Autenticação para registrar, no mínimo, as conexões de dispositivios clientes, falhas de autenticação, endereços MAC e IPs, switch ou access point ou controladora utilizado, porta do switch, nome do usuário, data, hora e tipo de autenticação. No final do período de testes verificar o que foi registrado.	Possibilidade de busca por nome de usuário, endereço MAC e endereço IP. Relatório gerado em PDF e HTML.	Tela da Solução de Automação ou Solução de Autenticação mostrando uma pesquisa para cada tipo de busca. Relatórios gerados, em formato PDF.		
a.2	OBRIGATÓRIO	Coletar dados e estatísticas gerais	Verificar a coleta de dados e estatísticas gerais da rede (métricas de desempenho como vazão, perda de pacotes, carga de processadores de elementos, etc.) e geração de relatórios a partir das variáveis coletadas.	As informações coletadas devem estar disponíveis para visualização e exportação no Solução de Automação.	Telas da Solução de Automação mostrando os contadores e os gráficos. Relatórios gerados, em formato PDF. Registro de log do Syslog.		
a.3	OBRIGATÓRIO	Emissão de relatórios de inventários	Emitir relatórios de inventários. Exemplos: - Equipamentos substituídos nos últimos 30 dias. - Equipamentos instalados (com modelo, número de série, versão do firmware, etc). - Quantidade de interfaces disponíveis por equipamento, isto é, sem uso nos últimos 30 dias.	Relatórios em PDF ou HTML.	Relatórios gerados, em formato PDF.		
a.4	OBRIGATÓRIO	Localização de dispositivos clientes e access points rogues em tempo real	Carregar a planta baixa do local, posicionar os access points ativos.Conectar dois ou três dispositivos clientes na rede wireless.Ligar um access point que não esteja configurado na controladora.	Indicação da contagem de dispositivos clientes conectados à rede wireless, com indicação em qual access point cada um deles está conectado, em tempo real.Indicação da existência de um access point rogue, em tempo real.	Telas da Solução de Automação mostrando na planta baixa a localização dos access points.Telas da Solução de Automação mostrando na planta baixa a localização dos dispositivos clientes.Telas da Solução de Automação mostrando na planta baixa a localização do access point rogue.		
Autenticação							
b.1	OBRIGATÓRIO	Autenticação de dispositivo cliente através da rede wireless usando Certificado	Conectar um dispositivo cliente com certificado através da rede wireless. Gerar tráfego desse novo dispositivo cliente a um dos servidores.	Dispositivo cliente e usuário reconhecidos e autorizados a acessar a rede.	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso. Registro de log do Syslog.		

b.2	OBRIGATÓRIO	Autenticação de visitante através da rede wireless usando portal	Conectar um dispositivo cliente desconhecido através da rede wireless. Gerar tráfego desse novo dispositivo cliente a um dos servidores.	Dispositivo cliente desconhecido deve ser redirecionado para portal de autenticação. Após a autenticação, deve ser autorizado a acessar a rede.	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso. Registro de log do Syslog.		
b.3	OBRIGATÓRIO	Autenticação de dispositivo cliente através de rede wireless usando PSK	Conectar um dispositivo cliente através da rede wireless usando PSK. Gerar tráfego desse novo dispositivo cliente a um dos servidores.	Dispositivo cliente autorizado a acessar a rede	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso. Registro de log do Syslog.		
b.4	INFORMATIVO	Autenticação de dispositivo cliente através de rede wireless usando PSK com senha na Solução de Autenticação	Cadastrar senha individual para o dispositivo cliente na Solução de Autenticação. Conectar o dispositivo IoT através da rede wireless usando PSK com a senha criada. Gerar tráfego desse novo dispositivo cliente a um dos servidores.	Dispositivo cliente autorizado a acessar a rede	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso. Registro de log do Syslog.		
b.5	OBRIGATÓRIO	Autenticação de dispositivo cliente através de rede cabeada usando endereço MAC	Cadastrar endereço MAC do dispositivo cliente na Solução de Autenticação. Conectar o dispositivo cliente através da rede cabeada. Gerar tráfego desse novo dispositivo cliente a um dos servidores.	Dispositivo cliente autorizado a acessar a rede	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso. Registro de log do Syslog.		
b.6	OBRIGATÓRIO	SSID por tipo de autenticação	Configurar um SSID para dispositivos clientes que usam certificado e outro para dispositivos clientes que usam portal. Divulgar os SSIDs, conectar um dispositivo em cada um dos SSIDs.	Através de ferramenta de captura de tráfego demonstrar os dois SSIDs funcionando simultaneamente. Na controladora wireless verificar a conexão dos dispositivos com os respectivos SSIDs.	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso. Tela da controladora wireless. Tráfego capturado, em formato PCAP. Registro de log do Syslog.		
b.7	OBRIGATÓRIO	Definir a VLAN dinamicamente conforme autenticação	Em um switch fora do fabric conectar um dispositivo cliente com certificado.	Associação do dispositivo cliente à VLAN determinada pela Solução de Autenticação.	Tela da Solução de Autenticação ou Solução de Automação mostrando o acesso e a designação correta de VLAN.Registro de log do Syslog.		
b.8	OBRIGATÓRIO	Desconexão do dispositivo cliente através de solicitação	Conectar um dispositivo cliente e autenticar na Solução de Autenticação. Quando solicitado enviar comando para desconexão do dispositivo cliente.	Dispositivo cliente desconectado quando solicitado.	Tela da Solução de Autenticação ou Solução de Automação mostrando a desconexão. Registro de log do Syslog.		

b.9	OBRIGATÓRIO	Aplicação de ACL/Política de Segurança de camada 3 em rede wireless	Definir ACL/Política de Segurança restringindo ICMP e/ou Telnet. Deve ser utilizada um único SSID. Relacionar a ACL/Política de Segurança com família de dispositivo cliente (por exemplo: computador, telefone IP e IoT). Conectar dois dispositivos clientes de famílias diferentes na rede wireless. Tentar acesso ICMP e Telnet a partir de cada um dos dipositivos clientes.	Criação de ACL/Política de Segurança. Que a ACL/Política de Segurança não exista na controladora e/ou no access point, antes de conectar os dispositivos clientes. Aplicação da ACL/Política de Segurança no SSID, conforme a família de dispositivo cliente. Restrição do ICMP e/ou Telnet conforme ACL/Política de Segurança.	**Antes de conectar os dispositivos clientes:** Tela da Solução de Autenticação ou Solução de Automação com a indicação da criação das ACL/Política de Segurança. Tela da Solução de Autenticação ou Solução de Automação com a indicação que as ACL/Política de Segurança não estão configuradas na controladora e/ou access point. **Depois de conectar os dispositivos clientes:** Tela da Solução de Autenticação ou Solução de Automação com a indicação que a ACL/Política de Segurança foi configurada na controladora e/ou no access point, conforme família de dispositivo cliente. Teste ICMP e Telnet com sucesso ou não em função da ACL/Política de Segurança.		
b.10	INFORMATIVO	Alteração de ACL/Política de Segurança de camada 3 em rede wireless	Alterar uma ACL/Política de Segurança do teste anterior. Tentar acesso ICMP e Telnet a partir do dispositivo cliente envolvido.	Reflexo da alteração da ACL/Política de Segurança na configuração da controladora ou access point sem a necessidade de reset da porta. Restrição do ICMP e/ou Telnet conforme ACL/Política de Segurança.	Tela da Solução de Autenticação ou Solução de Automação com a indicação a alteração da ACL/Política de Segurança. Tela da Solução de Autenticação ou Solução de Automação com a indicação que a alteração da ACL/Política de Segurança foi refletida na controladora ou no access point, conforme família de dispositivo cliente. Teste ICMP e Telnet com sucesso ou não em função da ACL/Política de Segurança.		
b.11	OBRIGATÓRIO	Remoção de ACL/Política de Segurança de camada 3 em rede wireless	Desconexão os dispositivos clientes.	Remoção da ACL/Política de Segurança na configuração da controladora e/ou do access point.	Tela da Solução de Autenticação ou Solução de Automação com a indicação que a remoção da ACL/Política de Segurança foi refletida na controladora e/ou no access point.		
Acesso							
c.1	OBRIGATÓRIO	Verificar SSID específico de Internet	Conectar um dispositivo cliente na rede wireless no SSID de Internet. Acessar a Internet a partir do dispositivo cliente. Acessar a um servidor a partir do dispositivo cliente.	Dispositivo cliente conectado ao SSID de Internet. Dispositivo cliente consegue acessar à Internet. Dispositivo cliente não consegue acessar qualquer outro servidor.	Tela da Solução de Autenticação ou Solução de Automação com a indicação que o dispositivo cliente está no SSID de Internet. Teste ICMP com sucesso da comunicação entre o dispositivo cliente e um servidor na Internet. Teste ICMP com falha da comunicação entre o dispositivo cliente e um dos servidores.		

c.2	OBRIGATÓRIO	Separação de tráfego, conforme SSID, em conexão local ou em túnel até a controladora wireless	Configurar dois SSIDs, um para conexão local e outro para túnel até a controladora wireless.Conectar dispositivos cliente em cada um dos SSIDs.Gerar tráfego a partir dos dispositvos cliente a um servidor.	Cada um dos dispositivos clientes conectados em um dos SSIDs.Conforme o SSID o tráfego gerado sairá por conexão local no AP ou pela controladora wireless.	Tela da Solução de Autenticação ou Solução de Automação com a indicação que cada dispositivo cliente está em um SSID.Tela da Solução de Automação mostrando a configuração de saída de cada um dos SSIDs.Tráfego capturado, em formato PCAP, das interfaces aérea e cabeada.Teste ICMP com sucesso da comunicação entre os dispositivos clientes e servidores.		
c.3	OBRIGATÓRIO	Verificação das marcações do QoS em camada 2 e camada 3	Configurar marcação de QoS nas interfaces aérea e cabeada. Configurar QoS na aplicação do dispositivo cliente.	Marcações do pacote conforme configuração das interfaces aérea e cabeada.	Tela da Solução de Automação com a indicação de qual marcação de QoS para qual SSID. Tabela de compatibilidade das marcações de QoS aérea e cabeada. Tráfego capturado, em formato PCAP, das interfaces aérea e cabeada.		
c.4	INFORMATIVO	Análise da qualidade da conexão de dispositivos clientes através da rede wireless	Durante todo o período de testes habilitar a Solução de Automação para registrar as conexões de dispositivios clientes wireless e os possíveis problemas e falhas ocorridos. No final do período de testes verificar o que foi registrado.	Histórico das conexões de dispositivos clientes disponível. Indicação de possíveis problemas e falhas nas conexões de dispositivos clientes. Visualização de relatório em PDF ou HTML.	Relatório gerado, em PDF.		

OBSERVAÇÕES

RESULTADO