Aula 07 | Ameaças, segmentação e contramedidas

Proteção da WLAN corporativa, visitantes e validação de isolamento

IDENTIFICAÇÃO	INFORMAÇÕES
UC09	Planejar e implementar a segurança em redes sem fio
Aula / turma	07 de 09 · TSC03 · 4 horas (240 minutos)
Material	Material do aluno • PDF / editável
Professor	Msc Arlindo Batista Xavier Filho

1. Situação-problema: Centro Horizonte

Na Aula 06, a equipe justificou WPA2/WPA3 e mecanismos de autenticação. Mesmo com senha forte, um visitante conectado à WLAN não deve alcançar os arquivos internos. O Centro Horizonte dispõe de uma rede de colaboradores já funcional (192.168.50.0/24), recebe visitantes diariamente e utiliza um pequeno servidor de gestão. O desafio é implantar uma rede convidada separada e demonstrar que a política funciona.

Pergunta norteadora: uma rede de visitantes protegida por WPA2, mas com acesso livre aos servidores corporativos, pode ser considerada segura?

2. Objetivos de aprendizagem e indicadores

- Reconhecer ameaças wireless: AP não autorizado, evil twin, desautenticação indevida, configurações legadas e movimento lateral.
- Distinguir isolamento de clientes, separação lógica por VLAN e bloqueio de tráfego por ACL/firewall.
- Configurar uma WLAN corporativa e uma WLAN de visitantes em segmentos distintos num laboratório autorizado.
- Verificar a política de acesso por testes positivos, testes negativos e registro de evidências.
- Produzir um parecer com limitações do simulador e medidas adicionais para ambiente real.

Indicadores PC 316: I1 (plano de segurança), I2 (interligação conforme infraestrutura), I3 (configuração de APs e clientes) e I4 (diagnóstico e testes).

3. Roteiro do encontro — 240 minutos

Momento	Tempo	Produção
Acolhimento e problema	20 min	Mapa de riscos do Centro Horizonte
Análise técnica e demonstração	40 min	Matriz ameaça × proteção
Laboratório Packet Tracer	90 min	VLANs, DHCP, ACL e testes
Desafio técnico aplicado	70 min	Parecer, evidências, proposta de melhoria
Síntese e avaliação formativa	20 min	Quiz, checklist e autoavaliação

4. Ameaças wireless: o que observar?

Risco ou ameaça	Possível efeito	Resposta defensiva
AP não autorizado (rogue)	Ponto conectado à infraestrutura sem controle	Inventário, inspeção, WIDS/WIPS quando disponível
Evil twin	SSID imitado induz associação indevida	Validar rede, certificados e políticas de clientes
Desautenticação forjada	Interrupção ou reconexões inesperadas	PMF quando suportado; logs e investigação
Senha compartilhada / legado	Acesso indevido e governança fraca	WPA3 ou WPA2-AES, credenciais adequadas e migração
Movimento lateral	Visitante tenta alcançar ativos internos	VLANs, ACL/firewall e isolamento por cliente

Importante: PMF protege determinados quadros robustos de gerenciamento, não impede toda interferência ou indisponibilidade. Um SSID separado sem regras de rede também não comprova isolamento.

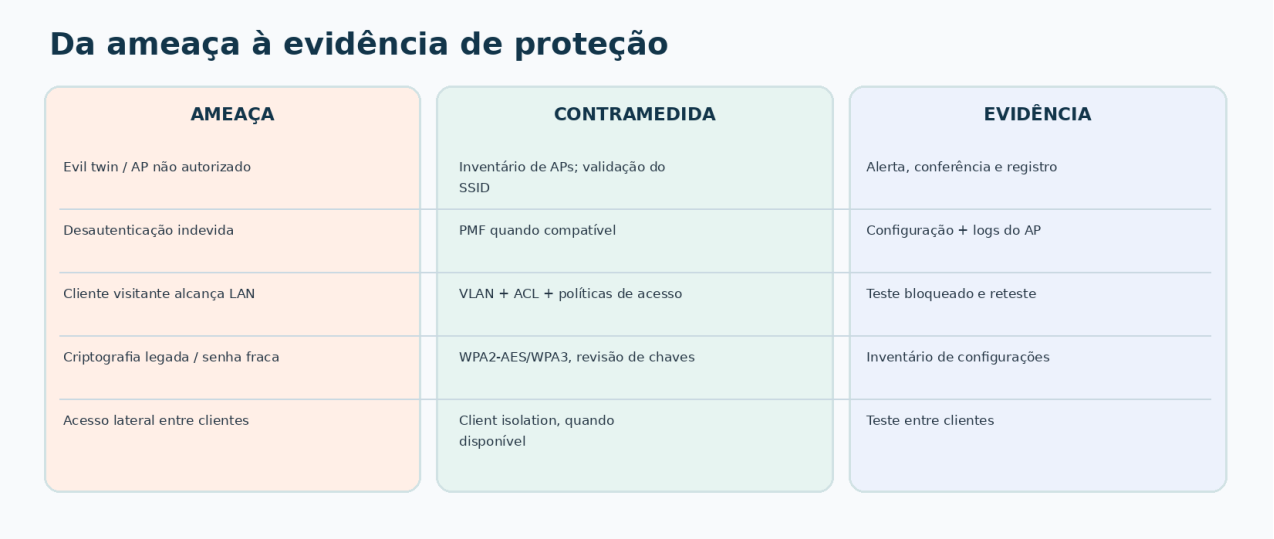


Figura 7.1 — O controle deve estar ligado a uma evidência que possa ser verificada.

5. Segmentação: três mecanismos distintos

- SSID: nome lógico do serviço wireless; por si só não impõe barreira de acesso a outros sistemas.
- VLAN: separa domínios de camada 2; duas VLANs podem comunicar-se se existir roteamento entre elas.
- ACL ou firewall: estabelece o que cada origem pode alcançar. As ACLs clássicas do laboratório são sem estado (stateless).
- Isolamento de clientes: quando o AP oferece esse recurso, restringe comunicação direta entre estações do mesmo serviço; não substitui controle entre VLANs.

A segurança real deve também considerar administração do AP, firmware, inventário, autenticação, logs, DNS/DHCP e processos para visitantes e incidentes.

6. Laboratório orientado — 90 minutos

ATENÇÃO: topologia exclusivamente simulada. A versão do Packet Tracer e os equipamentos podem apresentar nomes ou capacidades diferentes. Não acessar redes de terceiros. Não usar senhas reais. Salvar cópia da Aula 05 antes de modificar endereços e interligações.

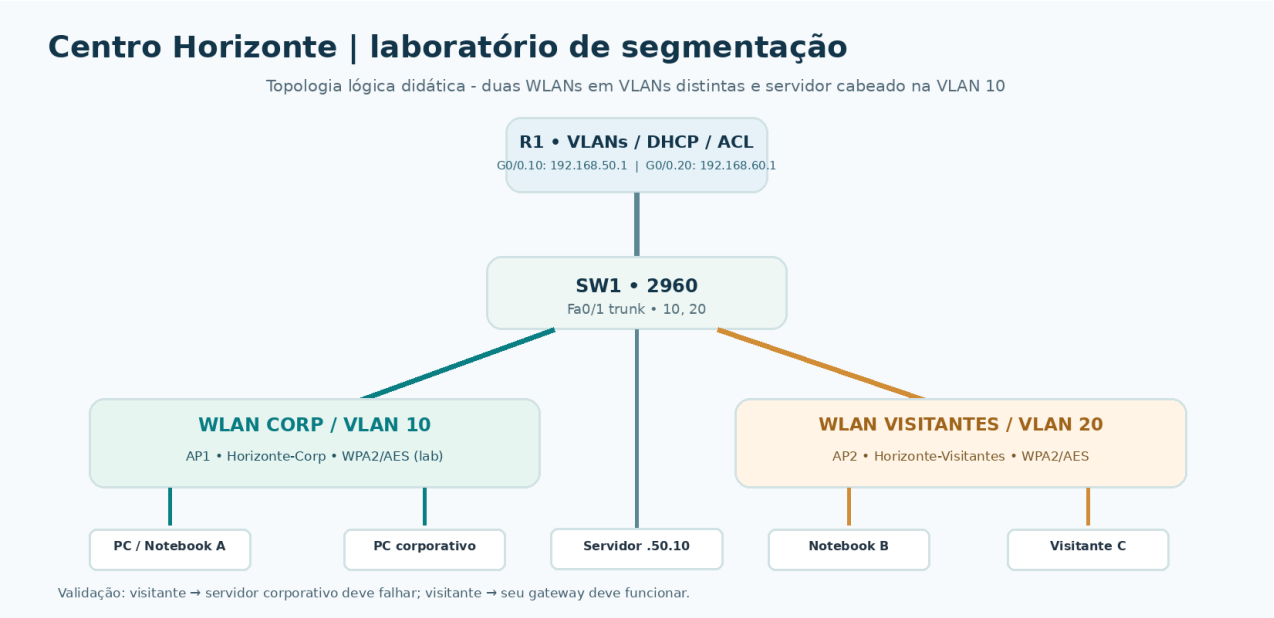


Figura 7.2 — Dois equipamentos wireless simulados em portas de acesso distintas, sem pressupor multi-SSID no WRT300N.

Elemento	Endereço / função

R1 G0/0.10, VLAN 10	192.168.50.1/24 · gateway corporativo
R1 G0/0.20, VLAN 20	192.168.60.1/24 · gateway visitantes
SW1 Fa0/1	Trunk 802.1Q até R1 · VLANs 10 e 20
SW1 Fa0/2 e Fa0/3	Portas access VLAN 10 / VLAN 20
SW1 Fa0/4	Servidor interno em access VLAN 10
AP1 / AP2	SSID Horizonte-Corp / Horizonte-Visitantes
Servidor interno	192.168.50.10/24 · gateway 192.168.50.1
Clientes	DHCP separado em cada VLAN

6.1 Etapas de implementação

1. 0–15 min — Clone o .pkt da Aula 05; adicione outro AP/WRT300N em simulação e conecte AP1 à Fa0/2 e AP2 à Fa0/3 usando as portas LAN, se utilizar WRT300N. Desative o DHCP nos dois WRT300N.
2. 15–30 min — Crie VLANs 10 e 20 no switch 2960; configure Fa0/1 em trunk e Fa0/2/Fa0/3 em modo access (ver comandos no quadro).
3. 30–45 min — Configure subinterfaces 802.1Q e dois pools DHCP em R1. Use a interface física G0/0, ajustando apenas se o modelo possuir outro nome.
4. 45–60 min — Configure SSIDs separados, WPA2-Personal/AES com credenciais fictícias quando disponível, conecte clientes e obtenha endereços de cada pool.
5. 60–75 min — Aplique a ACL VISITANTES_IN na entrada de G0/0.20. Registre um teste anterior à ACL, aplique a política e repita.
6. 75–90 min — Salve o .pkt e registre: IP/máscara/gateway, ping do visitante a 192.168.60.1 (permitido) e ping a 192.168.50.10 (bloqueado); teste corporativo ao servidor (permitido).

6.2 Configuração de referência (roteiro técnico)

SW1 / Cisco 2960 (portas de exemplo):

```
enable
configure terminal
vlan 10
 name CORP
vlan 20
 name VISITANTES
interface fastEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
interface fastEthernet0/2
 switchport mode access
 switchport access vlan 10
interface fastEthernet0/3
 switchport mode access
 switchport access vlan 20
interface fastEthernet0/4
 switchport mode access
 switchport access vlan 10
end
show vlan brief
show interfaces trunk
```

R1 / roteador 2911 (subinterfaces e DHCP de exemplo):

```
enable
configure terminal
interface gigabitEthernet0/0
 no shutdown
interface gigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.50.1 255.255.255.0
interface gigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.60.1 255.255.255.0
ip dhcp excluded-address 192.168.50.1 192.168.50.30
ip dhcp excluded-address 192.168.60.1 192.168.60.30
ip dhcp pool CORP
```

```
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
ip dhcp pool VISITANTES
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.1
ip access-list extended VISITANTES_IN
 deny ip 192.168.60.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip 192.168.60.0 0.0.0.255 any
interface gigabitEthernet0/0.20
 ip access-group VISITANTES_IN in
end
show ip interface brief
show ip access-lists
show ip dhcp binding
```

Se o AP/WRT exigir IP de gerência estático, atribua um endereço livre do respectivo segmento (por exemplo, AP1 192.168.50.2 e AP2 192.168.60.2), sem habilitar DHCP nos APs. No WRT300N, conecte pelo lado LAN e não pela porta Internet/WAN. O laboratório não simula navegação real à Internet.

7. Evidências e interpretação

Teste	Antes da ACL	Depois da ACL
Visitante → 192.168.60.1	Deve responder	Deve responder
Visitante → 192.168.50.10	Pode responder se roteável	Deve falhar
Corporativo → 192.168.50.10	Deve responder	Deve responder
Visitante para outro visitante	Dependente do AP	Depende de client isolation, não desta ACL

Não confunda um ping que falha com comprovação isolada de segurança. Registre a configuração, confirme endereçamento e verifique se o serviço de destino estava ativo antes do bloqueio. As ACLs didáticas são stateless; regras de retorno exigem planejamento apropriado.

8. Desafio aplicado — 70 minutos

O cliente quer liberar somente serviços públicos para visitantes, impedir acesso à rede corporativa e registrar tentativas suspeitas. Em equipes, elabore uma política mínima de acesso para funcionários, visitantes e equipamentos IoT. Explique por que dois SSIDs sem segmentação efetiva não resolvem o problema.

- Elabore a matriz: perfil → rede/VLAN → recurso permitido → recurso proibido → evidência.
- Escolha três riscos da matriz de ameaças e justifique contramedidas e limitações.
- Registre capturas/saídas dos comandos, um teste permitido e um bloqueado, com interpretação técnica.
- Liste verificações a realizar em equipamento real: PMF, client isolation, RADIUS, alertas/WIDS, logs, firmware e política de incidentes.

9. Entrega, reflexão e autoavaliação — 20 minutos

Entregar no Teams: arquivo TSC03_UC09_A07_EquipeXX.pkt (criado na prática), relatório TXT exportado pelo portal ou DOCX, matriz de acesso e pelo menos três evidências comentadas. Não incluir senhas de produção ou dados pessoais de terceiros.

- O teste demonstrou qual regra?
- Houve evidência positiva (permitido) e negativa (bloqueado)?
- Que proteção não foi validada no Packet Tracer?
- A proposta é repetível por outra equipe?

Referências essenciais

NIST. SP 800-153 (2012), csrc.nist.gov/pubs/sp/800/153/final. CISA. A Guide to Securing Networks for Wi-Fi. Cisco. Wireless VLANs. Links completos disponíveis no portal desta aula.