Aula 09 | Projeto Final de WLAN Segura

Implantação simulada, aceitação técnica, documentação e devolutiva formativa

IDENTIFICAÇÃO	INFORMAÇÕES
Unidade curricular	UC09 — Planejar e implementar a segurança em redes sem fio
Turma / encontro	TSC03 · Aula 09 de 09 · 4 horas (240 min)
Professor	Msc Arlindo Batista Xavier Filho
Documento	Material do aluno — disponibilizar no Teams e portal

1. Desafio profissional: entrega do Centro Horizonte

A direção do Centro Horizonte solicitou o aceite técnico da WLAN implantada ao longo das Aulas 01 a 08. A equipe deverá consolidar topologia, segurança da rede sem fio, segmentação corporativa/visitantes, testes de conectividade e relatório de implantação. Não basta mostrar um cliente conectado: o projeto deve demonstrar o que funciona, o que é bloqueado e quais riscos não foram validados em ambiente real.

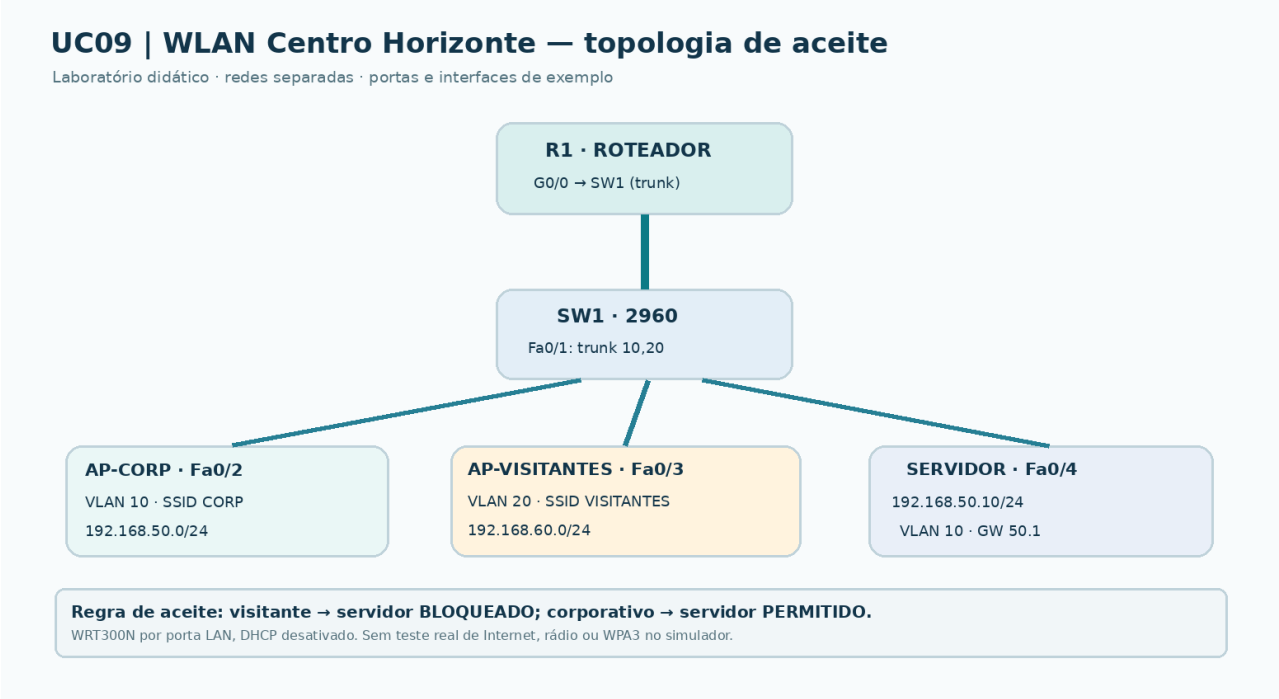
2. O que você deverá demonstrar

- I1: plano de configuração de segurança, requisitos, decisões e documentação.
- I2: interligação coerente entre a rede cabeada e as WLANs, com justificativa de cobertura.
- I3: configuração do access point, cliente, SSID, IP, autenticação e conectividade.
- I4: diagnóstico, correção e validação com evidências reproduzíveis.

3. Roteiro das 4 horas

MOMENTO	TEMPO	ATIVIDADE
Acolhimento e contrato de aceite	20 min	Retomar requisitos e definir responsabilidades.
Planejamento e critérios	40 min	Revisar desenho, topologia, matriz de acesso e checklist.
Oficina final Packet Tracer	90 min	Consolidar .pkt, configurar e fazer testes T01–T08.
Desafio / apresentação e auditoria cruzada	70 min	Trocar pareceres, retestar, apresentar e corrigir pendências.
Feedback e autoavaliação	20 min	Refletir sobre indicadores, registrar evolução e encaminhamentos.

4. Topologia e plano de endereçamento



ELEMENTO	CONFIGURAÇÃO DE REFERÊNCIA
R1 / G0/0.10	VLAN 10 · 192.168.50.1/24 · DHCP CORP
R1 / G0/0.20	VLAN 20 · 192.168.60.1/24 · DHCP VISITANTES
SW1 / Fa0/1	Trunk 802.1Q com VLANs 10 e 20 para R1
SW1 / Fa0/2 e Fa0/3	AP corporativo (VLAN 10) e AP visitante (VLAN 20)
SW1 / Fa0/4	Servidor 192.168.50.10/24 (gateway 50.1) na VLAN 10
WRT300N em modo AP simplificado	Conectar pela LAN, DHCP desativado, SSIDs distintos, WPA2-Personal/AES quando disponível

Não presumir suporte a múltiplos SSIDs/VLANs no WRT300N. Use dois equipamentos sem fio simulados em portas access separadas. Não declarar proteção WPA3, PMF, 802.1X/RADIUS ou levantamento de radiofrequência como comprovados por esta configuração.

5. Oficina final: implementação e verificação

1. Abra e duplique o arquivo .pkt da Aula 08: nomeie TSC03_UC09_A09_EquipeXX.pkt.
2. Confirme que as portas LAN dos APs estão em Fa0/2 e Fa0/3; DHCP dos APs está desativado.
3. Confirme subinterfaces dot1Q, gateways e os pools do R1; evite IPs duplicados.
4. Faça a política de visitantes: negar 192.168.60.0/24 → 192.168.50.0/24, permitindo o restante conforme cenário.
5. Execute e documente a matriz T01–T08. Guarde evidências visuais ou saídas de comandos com interpretação.
6. Faça uma auditoria cruzada: outro grupo tenta reproduzir dois testes e identifica uma melhoria.

6. Comandos de conferência (modelo)

```
SW1# show vlan brief
SW1# show interfaces trunk
R1# show ip interface brief
R1# show ip dhcp binding
R1# show ip access-lists
R1# show ip interface gigabitEthernet0/0.20
```

Nos clientes: Desktop → IP Configuration / PC Wireless / Command Prompt; use ipconfig e ping. Ajuste nomes de portas e comandos ao equipamento escolhido. Um ping bloqueado, isoladamente, não comprova a aplicação correta da ACL: combine com um teste positivo de referência e a inspeção da configuração.

7. Matriz de aceite da WLAN (preencha evidências)

ID	TESTE / ALVO	RESULTADO ESPERADO
T01	Cliente corporativo	Permitido / válido
T02	Cliente visitante	Permitido / válido
T03	Cliente corporativo → servidor	Permitido
T04	Cliente visitante → GW próprio	Permitido
T05	Cliente visitante → servidor	Bloqueado pela ACL
T06	Configuração e segmentos	Conforme projeto
T07	DHCP separado	Conforme projeto
T08	Segurança WLAN	Conforme projeto

Baixe a matriz CSV no portal e preencha status (conforme, não conforme ou não verificado), resultado observado e evidência. T08 usa autenticação simulada didática, sem registrar senhas em relatórios.

8. Entrega no Teams

- Arquivo .pkt desenvolvido e aberto com sucesso na versão utilizada do simulador.
- Relatório técnico PDF/DOCX/TXT: objetivo, escopo, topologia, IPs, SSIDs, medidas de segurança, resultados da matriz e pendências.
- Ao menos quatro evidências comentadas: duas de funcionamento, uma de bloqueio e uma de configuração ou correção.
- Plano de validação em ambiente físico: pesquisa de cobertura, SNR, interferências, disponibilidade e testes de segurança que o simulador não oferece.
- Parecer final: APROVADO COM RESSALVAS, NECESSITA CORREÇÃO ou VALIDADO NO LABORATÓRIO, sem confundir teste didático com homologação real.

9. Autoavaliação e encerramento

- Qual indicador foi demonstrado com maior autonomia? Qual ainda requer apoio?
- Sua evidência seria suficiente para outra equipe reproduzir o teste?
- Quais controles dependem de equipamentos reais e autorização da organização?
- Que conhecimento das aulas 01–08 foi indispensável para concluir a solução?

Fontes e referências

[1] SENAC SÃO PAULO. Plano de Curso nº 316 — Técnico em Segurança Cibernética (2023). UC09, 36 h. Documento institucional utilizado no projeto TSC03.

[2] SENAC SÃO PAULO. Plano de Orientação para a Oferta (PO), PC 316, seção UC09. Documento institucional utilizado no projeto TSC03.

[3] NIST. Guidelines for Securing Wireless Local Area Networks (WLANs), SP 800-153, 2012. https://csrc.nist.gov/pubs/sp/800/153/final Acesso em: 1 nov. 2026.

[4] CISCO. Packet Tracer — WRT300N GUI. https://tutorials.ptnetacad.net/help/default/GUI_wrt300n.htm Acesso em: 1 nov. 2026.

[5] CISCO. Fundamentals of VLANs — Router on a Stick. https://learningnetwork.cisco.com/s/article/fundamentals-of-vlan-s-router-on-a-stick Acesso em: 1 nov. 2026.