Aula 23 — Segurança Básica de Redes Locais

UC01 • Planejar e executar a instalação de redes locais | Aula 23 de 27 | 3h30 | Turma TR5 | Prof. Msc Arlindo Batista Xavier Filho

Objetivos de aprendizagem

- Reconhecer o papel do firewall de host e das regras de controle de acesso em redes locais.
- Relacionar endereços de origem e destino, protocolo TCP/UDP e porta de serviço a uma decisão de acesso.
- Diferenciar conectividade IP, permissão de firewall, autenticação SMB e autorização de arquivos.
- Construir uma matriz de política mínima e validar cenários permitido/bloqueado em simulação isolada.
- Registrar testes, risco, alteração autorizada, reteste e plano de reversão.

1. Situação-problema: a rede funciona, mas o acesso está excessivo

A Escola Horizonte concluiu os serviços DHCP/DNS da Aula 22. Um técnico descobriu que a rede de visitantes pode tentar conectar-se ao servidor de arquivos, algo que o projeto não previa. A solução não é desativar a rede ou o firewall: é definir uma política de acesso clara, aplicar no ponto correto e demonstrar que o serviço continua disponível aos usuários autorizados.

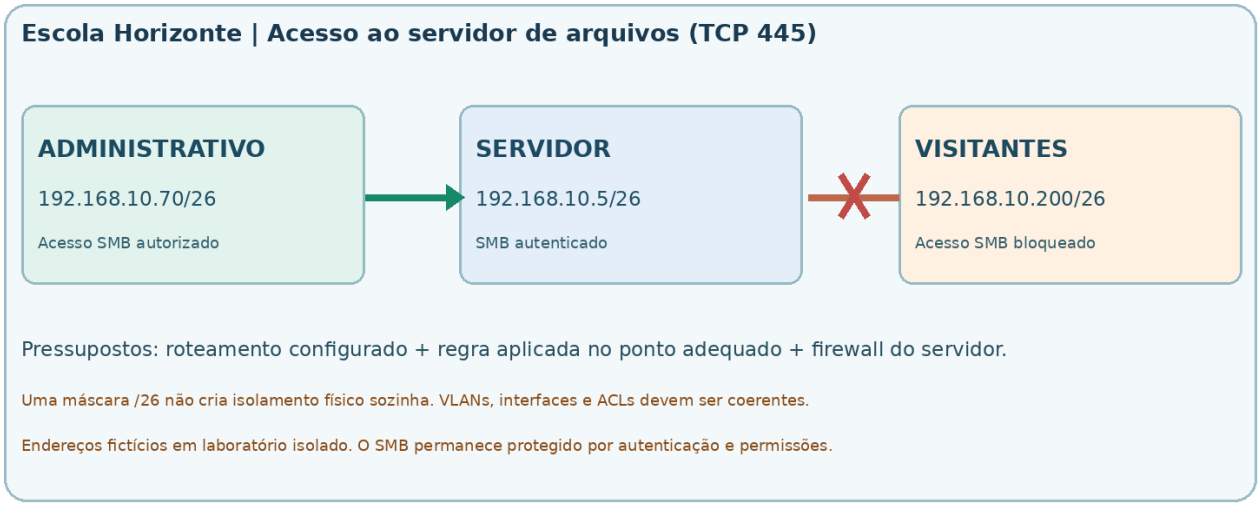


Figura 23.1 — Três papéis na política: origem autorizada, servidor protegido e origem que deve ser bloqueada.

2. Conceitos fundamentais

Termo	Interpretação técnica
Superfície de exposição	Serviços, portas e interfaces que podem receber conexões.
Firewall de host	Filtra tráfego de entrada/saída no próprio Windows ou Linux.
ACL em roteador	Filtra tráfego roteado conforme origem, destino, protocolo e porta.
Segmentação	Combina endereçamento e mecanismos reais de isolamento (VLANs, interfaces e ACLs).
Menor privilégio	Permitir somente as origens e os serviços necessários.
Defesa em profundidade	Firewall não substitui autenticação, permissões e atualização do sistema.

A sub-rede /26 é uma divisão de endereços IP: não fornece, por si só, isolamento de camada 2. Se visitantes e setores compartilham a mesma rede física sem mecanismos de separação, uma simples mudança de

máscara não os protege. Também é necessário distinguir a política de entrada (inbound) da política de saída (outbound).

3. Leitura segura de regras — sem alterar o computador

Windows / PowerShell (consultas)

```
Get-NetFirewallProfile | Select-Object Name, Enabled, DefaultInboundAction
Get-NetFirewallRule -PolicyStore ActiveStore |
  Select-Object -First 12 DisplayName, Enabled, Direction, Action
Get-NetTCPConnection -State Listen -ErrorAction SilentlyContinue |
  Select-Object -First 12 LocalAddress, LocalPort, State
Test-NetConnection -ComputerName 192.168.10.5 -Port 445
```

Atenção: Get-NetFirewallRule exibe as regras; endereços e portas associados estão em filtros separados. Um “TcpTestSucceeded: False” indica que o teste de conexão não se completou, mas exige investigação adicional para determinar se a causa foi firewall, serviço parado ou falta de conectividade.

Debian (consultas de observação)

```
ip -br address
ip route
ss -lnt
sudo nft list ruleset       # somente na VM isolada autorizada
```

O nftables é o framework de filtragem padrão do Debian. O comando de listagem pode exigir privilégio de administrador e pode retornar conjuntos vazios se o host não estiver filtrando tráfego por regras nftables. Nesta aula, não altere o firewall da estação institucional.

4. Política mínima da Escola Horizonte

Origem	Destino / serviço	Decisão
Administração: 192.168.10.64/26	Servidor 192.168.10.5 TCP 445	Permitir, com autenticação
Visitantes: 192.168.10.192/26	Servidor 192.168.10.5 TCP 445	Bloquear
Demais origens	Servidor 192.168.10.5 TCP 445	Bloquear, salvo exceção aprovada
Clientes autorizados	DHCP/DNS necessários	Manter funcional conforme projeto

A política exemplifica regras de filtragem para o tráfego TCP 445. Ela não libera automaticamente acesso a pastas: as permissões de compartilhamento e de sistema de arquivos continuam exigidas. Regras de ACL de roteador só afetam tráfego que passa por esse roteador; acessos locais no mesmo segmento precisam de firewall no host ou outra medida de isolamento.

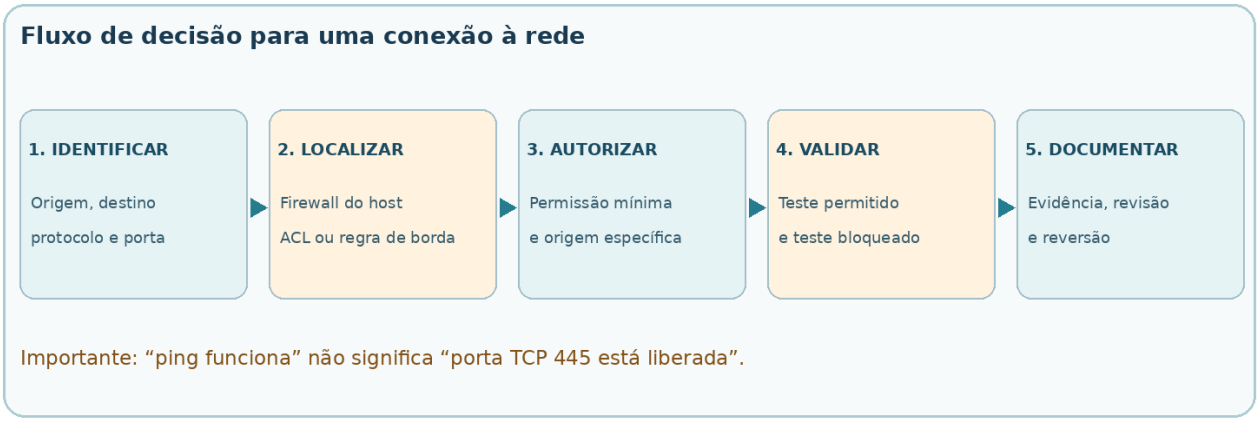


Figura 23.2 — Fluxo de validação técnica: registrar, aplicar em simulação, testar e documentar.

5. Oficina prática — três estações, uma política

1. No Packet Tracer, desenhe as três redes do projeto: servidor (192.168.10.0/26), administração (192.168.10.64/26) e visitantes (192.168.10.192/26). Inclua interfaces/gateways e roteamento coerentes.
2. Documente os endereços de três equipamentos representativos: servidor .5, cliente administrativo .70 e visitante .200. Não pressuponha que o Packet Tracer modele um serviço SMB real em todas as versões.
3. Preencha uma matriz de controle de acesso contendo origem, destino, protocolo, porta, decisão, justificativa e evidência a coletar.
4. Simule uma ACL no roteador ou compare saídas esperadas em cartões de cenário. Para TCP 445: administração → servidor permitida; visitantes → servidor bloqueada; outras origens → servidor bloqueadas.
5. Execute testes equivalentes que a plataforma suporte; quando TCP 445 não puder ser simulado, valide a ordem e a lógica da ACL e registre que a aplicação SMB não foi testada.
6. Compare os resultados de ping e dos testes de portas. Explique por que ICMP e TCP 445 podem receber tratamentos distintos.
7. Produza relatório: situação inicial, política proposta, resultados previstos/obtidos, pendências e plano para desfazer alterações simuladas.

6. Casos de diagnóstico

Situação	Pergunta orientadora
Visitante alcança o IP, mas não abre pasta	O bloqueio pode ser específico à porta?
Administrativo não abre SMB	Há rota, serviço, regra e credenciais válidas?
Regra de permissão existe e acesso falha	Existe outra regra prioritária ou filtro aplicado?
Visitante está na mesma VLAN do servidor	Uma ACL só no roteador interceptará esse tráfego?

7. Entrega no Teams

- Arquivo de simulação ou diagrama da topologia, com três redes identificadas.
- Matriz de política com ao menos quatro regras justificadas.
- Registro de dois testes: um permitido e um bloqueado (ou declaração de limites da simulação).
- Ficha de laboratório preenchida e recomendação final de segurança.

Referências e aprofundamento

MICROSOFT. Get-NetFirewallRule (NetSecurity). Disponível em: https://learn.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallrule. Acesso em: 31 out. 2026.

MICROSOFT. Gerenciar o Firewall do Windows com a linha de comando. Disponível em: https://learn.microsoft.com/pt-br/windows/security/operating-system-security/network-security/windows-firewall/configure-with-command-line. Acesso em: 31 out. 2026.

MICROSOFT. Secure SMB Traffic in Windows Server. Disponível em: https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-secure-traffic. Acesso em: 31 out. 2026.

DEBIAN. nftables (Debian Wiki). Disponível em: https://wiki.debian.org/nftables. Acesso em: 31 out. 2026.

CISCO. Access Lists: configuração e conceito. Disponível em: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html. Acesso em: 31 out. 2026.