

Firewall Rule Order and Least-Privilege Verification

Recommended time: 50-70 minutes | Focus: First-match policy, rule shadowing, narrow corrections, negative testing

Learning Objectives

1. Normalize a firewall flow by source, destination, protocol, port, and direction.
2. Identify first-match rule shadowing.
3. Propose a narrow correction that preserves the security requirement.
4. Verify both required access and required denial.

Teacher design rule: Require a prediction before configuration and an explanation after verification. A working fix without supported reasoning is still useful formative-assessment evidence.

Requirement

App clients 10.10.40.0/24 may reach API 10.50.20.10 on TCP/8443. Other 10.10.0.0/16 to 10.50.0.0/16 access should remain denied.

Policy Artifact

Rule 10: DENY 10.10.0.0/16 → 10.50.0.0/16 ANY. Rule 20: ALLOW 10.10.40.0/24 → 10.50.20.10 TCP/8443.

Observed Log

src=10.10.40.25 | dst=10.50.20.10 | proto=tcp | dport=8443 | action=deny | rule=10

Student Questions

Why does rule 20 not help? Which exact fields match rule 10? What narrow change preserves the broad segmentation policy? What negative test proves the correction is not overly broad?

Expected Reasoning

On a first-match ordered policy, rule 10 matches before rule 20 is evaluated. A narrow required allow can be placed before the broad deny when that matches the intended policy model.

Positive and Negative Tests

Positive: 10.10.40.25 → 10.50.20.10 TCP/8443 succeeds.

Negative: TCP/22 to the same server remains denied, or an unauthorized source subnet remains denied.

Misconception to Expose

Incorrect fix: "Delete the deny rule."

Why weak: that abandons the segmentation requirement instead of implementing the narrow authorized exception.

Exit Ticket

Explain the chain: observation → matched rule → shadowing mechanism → narrow correction → positive verification → negative verification.

Quick Assessment Rubric

Criterion	Strong Evidence
Prediction	States the expected network behavior or artifact before the change.
Interpretation	Explains what the evidence proves and what remains unresolved.
Decision	Changes only what the evidence supports.
Verification	Repeats the original test and includes a control or negative test when appropriate.

Independent resource notice: AP Networking Exam Prep is independent and is not affiliated with, sponsored by, or endorsed by College Board. AP and Advanced Placement are trademarks of College Board.