Exercise walk-through

Protecting Networks: Firewalls ▪ 3.4

eXercise

You must be able to

- explain how an ACL is checked (in order, first match wins)
- predict which traffic an ordered rule set allows or denies
- distinguish stateless from stateful firewalls

Method — First match wins

A firewall checks its ACL top-to-bottom and applies the first rule that matches the packet. A Deny placed above an Allow for the same traffic blocks it - even though the Allow exists lower down.

Method — Order changes the result

Rule 1 ALLOW TCP 22; Rule 2 DENY TCP 22 → SSH is allowed. Swap them → SSH is denied. The same rules give opposite results just by changing order.

Practice 2.1 ▪ 1 mark

In a firewall ACL, which rule is applied to a matching packet?

Solution 2.1

Method: First match wins

Worked steps

the first rule that matches **B1**.

Practice 2.2 ▪ 2 marks

Explain why the ORDER of firewall rules matters.

Solution 2.2

Method: Order changes the result

Worked steps

rules are checked top-down and the first match wins B1, so reordering can change whether traffic is allowed or denied B1.

Practice 2.3 ▪ 1 mark

A firewall has: Rule 1 DENY TCP 443 from 192.168.*; Rule 7 ALLOW TCP 443 from ALL (lower down). A user on 192.168.45.37 cannot reach port 443.
(a) Explain why the user is blocked.
(b) State one change that would let them through.

Solution 2.3

Method: First match wins

Worked steps

(a) Rule 1 denies their range and is checked before Rule 7 B1. (b) move the ALLOW rule above the DENY rule B1.

Exam-style 3.1 ▪ 1 mark

A firewall that tracks the state of each connection is

A stateless

B stateful

C wireless

D physical

Solution 3.1

A stateless

B stateful ✓

C wireless

D physical

Worked steps

B. stateful firewalls track connections.

Exam-style 3.2 ▪ 1 mark

A DENY rule placed above a matching ALLOW rule will

A be ignored

B block the traffic

C allow the traffic

D crash the firewall

Solution 3.2

Method: First match wins

A be ignored

B block the traffic ✓

C allow the traffic

D crash the firewall

Worked steps

B. first match wins, so the DENY fires first.

Exam-style 3.3 ▪ 2 marks

An administrator needs to allow SSH (port 22) but deny everything else inbound.
(a) Write the two rules in the correct order.

Solution 3.3

Method: Order changes the result

Worked steps

(a) Rule 1: ALLOW inbound TCP 22 from ALL B1; Rule 2: DENY inbound ALL from ALL B1. The allow must come first.