AP CYBERSECURITY • EXERCISE SHEET

3.4 Protecting Networks: Firewalls

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

Objective

Build the skills to answer exam questions on **firewalls** 防火墙 and **access control lists (ACLs)** 访问控制列表.

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

1 Worked examples

Study these first. Each one shows the method for a task used later.

> ■ **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.
>
> ■ **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.

2 Practice

2.1 In a firewall ACL, which rule is applied to a matching packet? [1]

2.2 Explain why the ORDER of firewall rules matters. [2]

2.3 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. [1]

(b) State one change that would let them through. [1]

3 Exam-style questions

3.1 A firewall that tracks the state of each connection is [1]

- **A** stateless
- **B** stateful
- **C** wireless
- **D** physical

3.2 A DENY rule placed above a matching ALLOW rule will [1]

- **A** be ignored
- **B** block the traffic
- **C** allow the traffic
- **D** crash the firewall

3.3 An administrator needs to allow SSH (port 22) but deny everything else inbound.

(a) Write the two rules in the correct order. [2]

4 Go further

- work through the **3.4 Protecting Networks: Firewalls** lesson on the **Learn** page;
- read the **Securing Networks** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 the first rule that matches.

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

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

3.1 B. stateful firewalls track connections.

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

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