AP CYBERSECURITY • EXERCISE SHEET

3.4 Protecting Networks: Firewalls

Name: _____ Class: _____ Date: _____ **Total: 43 marks**

KEY WORDS access control list 访问控制列表 • stateful 有状态 • stateless 无状态 • network firewalls 网络防火墙 • firewall 防火墙

Objective

Build the skills to answer exam questions on **network firewalls** 网络防火墙: the three types, the **access control list** 访问控制列表, firewall placement, and writing rules that do what you intend.

You must be able to:

- describe a stateless, a stateful and a next-generation firewall, and choose between them
- explain how an ACL is evaluated, and what an ACL rule specifies
- determine where firewalls should be placed in a network
- write firewall rules and order them correctly

1 Worked examples

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

The three firewall types

A firewall allows or denies network traffic in or out of a network. It is **software**, which may be hosted on a standalone device or run alongside other functions.

Type	What it inspects	Consequence
Stateless	information in **packet headers** - IP addresses, ports, protocols	fast and simple; judges each packet on its own, with no memory of what came before
Stateful (dynamic packet filtering)	tracks the **state of connections** passing through it	can allow a reply that belongs to a connection the network itself started, and deny an identical packet that does not
Next-generation (NGFW)	everything above, plus advanced features such as intrusion prevention	most capable, most expensive, most demanding to run

The distinction that earns marks: a **stateless** firewall cannot tell a legitimate reply from an unsolicited packet that merely looks like one, because it has no record of the outbound request. A **stateful** firewall can, because it remembers the connection.

The access control list

Administrators create a set of rules - the **ACL** - which the firewall uses to permit or deny **inbound and outbound** traffic.

A typical rule specifies:

- the **direction** - inbound or outbound
- the **criterion** to filter by - IP address, logical port, service, or application
- the **action** - allow or deny

Rules are checked in order, and the first rule that matches is executed. Nothing after it is consulted for that traffic.

Worked example. The requirement: allow the public to reach the web server on port 443, allow the administrators' subnet to reach it on port 22, and deny everything else inbound.

```
1  ALLOW  inbound  any          -> 203.0.113.10 : 443
2  ALLOW  inbound  10.0.5.0/24  -> 203.0.113.10 : 22
3  DENY   inbound  any          -> any
```

Move rule 3 to the top and the server becomes unreachable, including for the administrators - the rules are unchanged, only their order, and the network is now broken. **Whenever a question asks you to write or check an ACL, check the order before checking the rules.**

Where firewalls go

Three placement rules, and each answers a different question:

1. **Every segment** of a network should have a firewall controlling the flow of data in and out of that segment.
2. Segments may have **different security needs**, so each firewall's level of security can be set **independently** - a records segment can be far stricter than a guest segment.
3. **Every point of ingress and egress** between the internal network and the public internet should have a firewall.

The mistake to avoid is thinking of one firewall at the perimeter. A single boundary firewall does nothing about traffic that is already inside - and lateral movement is exactly the phase segment firewalls exist to stop.

2 Practice

2.1 State what a firewall does and what it physically is. [2]

2.2 Describe the difference between a stateless and a stateful firewall. [3]

2.3 State **one** advantage of a next-generation firewall and **one** disadvantage. [2]

2.4 State the **three** things a typical ACL rule specifies. [3]

2.5 Explain how a firewall decides which rule to apply when two rules could both match. [2]

2.6 These rules are checked in order:

```
1  DENY   inbound  any         -> port 443
2  ALLOW  inbound  any         -> port 443
```

(a) State what happens to inbound traffic on port 443. [1]

(b) Explain why. [1]

2.7 State the **three** placement rules for firewalls in a network. [3]

2.8 Explain why a single firewall at the internet boundary is not sufficient. [2]

2.9 Write an ACL, in the correct order, that allows inbound web traffic on port 80 to the server at 198.51.100.5, allows the subnet 172.16.2.0/24 to reach that server on port 3306, and denies all other inbound traffic. [3]

3 Exam-style questions

3.1 A firewall that filters using only information in packet headers is [1]

- **A** stateful
- **B** stateless
- **C** next-generation
- **D** host-based

3.2 Which firewall can distinguish a reply belonging to a connection the network started from an unsolicited packet? [1]

- **A** stateless
- **B** stateful
- **C** neither
- **D** both equally

3.3 In an ACL, changing the order of the rules [1]

- **A** has no effect, since all rules are applied
- **B** can change which traffic is allowed or denied
- **C** only matters for outbound rules
- **D** is prevented by the firewall software

3.4 Firewalls should be placed [1]

- **A** only at the boundary with the public internet
- **B** on each network segment and at each point of ingress and egress
- **C** only on segments containing sensitive data
- **D** only on devices, not on the network

3.5 A manufacturing company has one firewall, at the point where its network meets the internet. Behind it, a single flat network carries office computers, a customer database server at 10.0.1.20, and the machinery control system at 10.0.9.5, which must never be reachable from the internet and is only operated from the engineering subnet 10.0.4.0/24. An adversary phishes an office employee, and from that office computer reaches both the database and the control system.

(a) Explain why the boundary firewall did not prevent the adversary reaching the control system. [3]

(b) Recommend a firewall placement for this network and justify it against the three placement rules. [4]

(c) Write an ACL for the control-system segment that permits only what the scenario requires, in a correct order. [4]

(d) The IT lead proposes a stateless firewall for the control segment on cost grounds. Evaluate this choice for this specific segment. [3]

(e) A colleague adds `DENY inbound any -> any` as the **first** rule of the office segment's ACL "to be safe". Explain what happens and how to fix it. [3]

Solutions

2.1 it allows or denies network traffic into or out of a network; it is software, which can be hosted on a standalone device or run alongside other functions.

2.2 a **stateless** firewall filters on information in packet headers - IP addresses, ports, protocols - judging each packet independently; a **stateful** firewall tracks the state of the connections passing through it, so it can permit a packet that belongs to a connection already established and deny an identical packet that does not.

2.3 advantage: it has the capabilities of both stateless and stateful firewalls plus advanced features such as intrusion prevention. Disadvantage: it costs more, and requires more resources and expertise to run.

2.4 the direction of traffic - inbound or outbound; the criterion to filter by - IP address, logical port, service or application; whether to allow or deny.

2.5 rules are checked **in order**, and the first rule whose criteria match is the one executed for that traffic - nothing after it is consulted.

2.6 (a) it is denied. (b) rule 1 matches first, and the first matching rule executes, so rule 2 is never reached.

2.7 each segment of a network should have a firewall controlling data in and out of that segment; each firewall's security level can be set independently, according to that segment's needs; every point of ingress and egress between the internal network and the public internet should have a firewall.

2.8 a boundary firewall only inspects traffic crossing the boundary; once an adversary is inside - through phishing, a rogue access point, or a compromised device - all their traffic stays internal, so nothing filters their lateral movement between systems.

2.9:

```
1  ALLOW  inbound  any            -> 198.51.100.5 : 80
2  ALLOW  inbound  172.16.2.0/24  -> 198.51.100.5 : 3306
3  DENY   inbound  any            -> any
```

3.1 B.

3.2 B. Only a stateful firewall keeps the record of the connection.

3.3 B. Rules execute on first match, so order determines the outcome.

3.4 B.

3.5 (a) the boundary firewall filters only traffic crossing between the internal network and the internet. The adversary's entry was a phished employee, so the malicious traffic **originated inside** the network and never crossed that boundary; with a single flat network there was no firewall between the office computers and either the database or the control system, so nothing filtered the lateral movement.

(b) segment the network and put a firewall on each segment - office, database, engineering, control, because each segment should have a firewall controlling data in and out of it. Set each one's security level independently, so the control segment is far stricter than the

office segment. Keep a firewall at every point of ingress and egress with the internet, including any second connection such as a supplier link or remote-support line.

(c):

```
1  ALLOW  inbound  10.0.4.0/24 -> 10.0.9.5
2  DENY   inbound  any         -> 10.0.9.5
3  DENY   outbound 10.0.9.5    -> any
```

Rule 3 is worth including: the control system has no reason to initiate outbound traffic, and blocking it stops a compromised controller calling out.

(d) A stateless firewall filters on headers alone and cannot tell a genuine reply from a crafted packet that imitates one. For a segment that "must never be reachable from the internet" and controls machinery - where a compromise is a safety issue, not only a data one - that is the wrong economy; the criticality criterion justifies at least a stateful firewall here, whatever is used on the office segment.

(e) every packet matches rule 1 first, and the first matching rule executes, so all inbound traffic to the office segment is denied and nothing after it is ever consulted - the office is cut off entirely. The fix is to move the broad deny to the **end**, below the specific allows, which is the standard shape: specific rules first, general deny last.