Solutions

Each answer shows the steps, then the **result**.

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