# Protecting networks

4.2.1b · Networks · revision notes

The three methods of protecting a network on the specification: access control, physical security and firewalls. Expect 'State', 'Explain how…' and 'Explain why…' questions, tables of firewall rules to interpret, and 6-mark 'Discuss' questions about protecting an organisation's network.

### Key facts

- Access control: only authorised users, and only the data they need
- Two-factor authentication: two different kinds of proof, e.g. something you know + something you have
- Physical security: locks, key cards, biometric locks, CCTV, guards, alarms
- Firewall rules can use IP addresses, port numbers and protocols; the first matching rule decides
- Authentication: proving who you are (password, biometrics, two-factor authentication)
- Access levels: no access, read-only, read and write
- Firewall: checks packets against rules and blocks unauthorised traffic in and out
- Use all three methods together

## Notes

### Access control

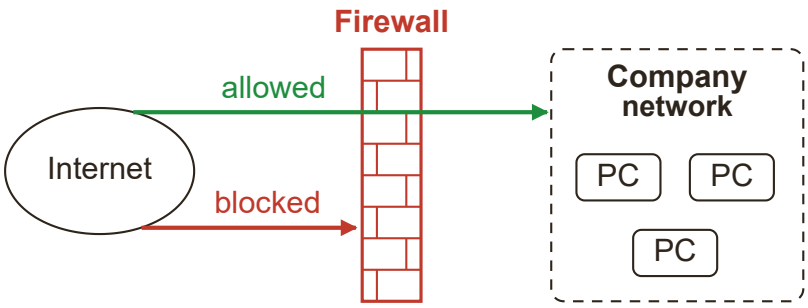
- **Access control** makes sure that only authorised people can use the network, and that each user can only reach the data and programs they need.
- **Authentication** checks who a user is: a username and password, biometrics (e.g. a fingerprint) or **two-factor authentication** (two different kinds of proof, e.g. a password plus a code sent to a phone).
- **Access levels** (permissions) control what each user can do, e.g. no access, read-only, or read and write. A student cannot open staff files; a receptionist cannot change medical records.
- Good practice: strong password rules, locking an account after several wrong attempts, locking screens automatically and removing accounts as soon as people leave.

### Physical security

- **Physical security** stops unauthorised people reaching the hardware: locked server rooms, key cards or keypads, biometric locks, CCTV, alarms, security guards and signing in visitors.
- It matters because an intruder could steal a server or laptop, plug a device into the network behind the firewall, insert a USB stick containing malware, or damage equipment.

## Firewalls

- A **firewall** is hardware or software that sits between a network and the internet (or protects a single computer).
- It examines each packet entering or leaving and compares it with a set of **rules**, e.g. about which IP addresses, port numbers or protocols are allowed.
- Packets that break the rules are blocked; the rest are let through. Blocked attempts can be logged for the network manager to investigate.




Each packet is checked against the rules.

The firewall lets through packets that the rules allow and blocks the rest.

- The rules are usually checked in order and the first rule that matches decides, so the order of the rules matters.
- A firewall cannot stop everything: it does not stop attacks from inside the network, or harmful content carried in traffic that it allows, such as a phishing email. Grade 7+ only

## Using the methods together

- No single method is enough. Access control stops unauthorised logins, physical security protects the hardware and firewalls block unwanted traffic, so organisations use all three together.

## How to answer each type of question

**State a purpose or give examples** 1 to 2 marks Grade 4

1. Give short, specific answers, e.g. 'a locked server room' rather than 'security'.
2. For physical security, give things you could see or touch, not software.

**Example.** (a) State the purpose of a firewall. (1)
(b) Give **two** physical security measures that could protect a company's server room. (2)

**Model answer.**

(a) To monitor the traffic entering and leaving a network and block any that its rules do not allow (1)
(b) Any two from: a locked door (1); key-card or keypad entry (1); a biometric lock, e.g. a fingerprint scanner (1); CCTV (1); a security guard (1); an alarm (1).

### Explain how a firewall protects a network

3 to 4 marks **Grade 6**

1. Say where it sits: between the network and the internet.
2. Say what it does: examines each packet entering or leaving.
3. Say how it decides: compares each packet with rules, e.g. about IP addresses or port numbers.
4. Say the result: packets that break the rules are blocked.

**Example.** Explain how a firewall protects a company's network. (4)

---

**Model answer.** The firewall sits between the company's network and the internet (1). It examines every packet entering or leaving the network (1) and compares it with a set of rules, e.g. about which IP addresses or port numbers are allowed (1). Packets that break the rules are blocked, so unauthorised access attempts from outside are stopped (1).

### Explain how access control protects a network in context

4 marks **Grade 6**

1. Choose two different methods: individual logins, access levels, two-factor authentication or account lockout.
2. For each, explain what it prevents in this scenario.

**Example.** Explain **two** ways that access control can protect the patient records on a doctors' surgery network. (4)

---

**Model answer.** Every member of staff must log in with their own username and a strong password (1), so only authorised staff can use the network and each person's actions can be traced (1). Staff are given access levels based on their job (1), so, for example, receptionists can see appointments but cannot open or change medical records (1).

**Interpret firewall rules**

2 to 3 marks **Grade 7**

1. Take each packet in turn and check the rules from the top.
2. The first rule that matches decides; ignore the rules below it.
3. Give the decision (allow or block) and the number of the rule that decides it.

**Example.** A firewall checks these rules in order, starting with rule 1. The first rule that matches a packet decides what happens to it.

| Rule | Direction | From IP address | Port | Action |
|---|---|---|---|---|
| 1 | Incoming | 203.0.113.9 | Any | Block |
| 2 | Incoming | Any | 443 (HTTPS) to the web server | Allow |
| 3 | Incoming | Any | Any | Block |

State whether each packet is allowed or blocked.
(i) An HTTPS request on port 443 to the web server from 198.51.100.20 (1)
(ii) An HTTPS request on port 443 to the web server from 203.0.113.9 (1)
(iii) A request on port 21 (FTP) to the web server from 198.51.100.20 (1)

---

**Model answer.**

(i) Allowed, by rule 2 (1)
(ii) Blocked, by rule 1, which is checked before rule 2 (1)
(iii) Blocked, by rule 3 (1)

**6-mark: Discuss how to protect a network** 6 marks (levels-based) **Grade 8**

1. Cover all three methods: access control, physical security and firewalls.
2. Develop each point: say what the measure stops, in the context of the scenario.
3. Weigh them up: explain how each method covers gaps in the others, and any drawbacks.
4. Finish with a conclusion.

**Example.** A small accountancy firm keeps its clients' financial records on a server in its office. Discuss how the firm could protect its network from unauthorised access. (6)

**Model answer.** Marked by levels: the top band covers all three methods with developed points linked to the firm and weighs them up. Points could include: each employee has their own username and strong password, with no shared accounts, so actions can be traced; access levels mean staff can only open the records they need for their work; two-factor authentication means a stolen password alone is not enough, which matters for staff working from home; accounts are locked after repeated wrong passwords and removed when staff leave; the server is kept in a locked room with key-card entry and CCTV, so it cannot be stolen or tampered with; a firewall between the office network and the internet blocks unauthorised incoming connections. Evaluation: each method covers gaps in the others (a firewall does not stop someone walking in, and a lock does not stop an online attack), so the firm should use all three, while keeping them easy enough for staff to use.

## Don’t lose marks

- Saying a firewall removes viruses. That is anti-malware software; a firewall filters network traffic.
- Describing two-factor authentication as 'two passwords'. The two factors must be different types of proof.
- Giving something that is not physical, such as passwords, as an example of physical security.
- Ignoring the order of firewall rules: a packet may match several rules, but only the first match counts.
- Writing 'use passwords' without explaining how that protects the network, e.g. only authorised users can log in.

## More tips

### Memory tricks

- The three protections are A, F, P: access control, firewalls, physical security.
- A firewall is like a security guard on the door, checking every packet against a list of who is allowed in and out.
- Two-factor means two different types of proof: something you know, something you have, something you are. Two passwords is not two-factor.
- Firewall rules: read from the top; the first match wins.

### Exam technique

- Use the three terms from the specification: access control, physical security and firewalls.
- Each 'Explain' point needs the method and what it stops, in the context of the question.
- In 6-mark answers, cover all three methods and say why they are needed together.
- In firewall rule questions, give the number of the rule that decides each case to show your reasoning.

## What each grade needs

What you need to be able to do, from the first marks up to the top grade.

**Grade 3** — **State the purpose of a firewall**
A firewall blocks unauthorised traffic entering or leaving a network.

**Grade 4** — **Give examples of physical security**
Locked server rooms, key cards, biometric locks, CCTV and security guards.

**Grade 5** — **Explain how access control protects a network**
Usernames, passwords and access levels mean only authorised users can reach only the data they need.

**Grade 5** — **Define two-factor authentication**
Proving your identity in two different ways, e.g. a password plus a code sent to your phone.

**Grade 6** — **Explain how a firewall works**
It checks each packet against rules (e.g. IP addresses and port numbers) and blocks packets that break them.

**Grade 7** — **Interpret a table of firewall rules**
Apply the rules in order to decide whether each packet is allowed or blocked.

**Grade 8** — **Evaluate a combination of protection methods**
Explain why no single method is enough and how the three methods cover each other's gaps.

Free notes, Full packs, practice papers and mock exams at chhetriacademy.com. Written for this site; not taken from past papers. Stuck? 1-to-1 tutoring with a free 30-minute trial lesson.