

8.3.2 Protection of Data

Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- Characteristics and methods of protecting data: user ID and password, two-factor authentication, biometrics, digital certificate, secure socket layer (SSL), encryption and firewall

Method	Purpose and how it works	Points to know
User ID and password	The user ID identifies the user and the password proves it is them, so only authorised users can get into the system.	Strong passwords, changed regularly; accounts lock after several wrong attempts; user IDs can have different access levels
Two-factor authentication	Needs two different proofs of identity: something you know (password), something you have (phone or token) or something you are (fingerprint).	A stolen password alone is not enough; e.g. a code is sent to a phone, or an app shows a one-time code
Biometrics	Uses a unique body feature, such as a fingerprint, face, iris or voice, to prove who the user is. The data is stored as a template and compared with the scan.	Cannot be forgotten or easily shared; hard to forge. Biometric data is sensitive, must be protected, and cannot be changed if stolen
Digital certificate	An electronic document, issued by a trusted certificate authority, that proves the identity of a website or person and holds their public key.	Contains: owner's name, public key, serial number, expiry date, the issuer's name and the issuer's digital signature
Secure socket layer (SSL)	A protocol that creates an encrypted link between the server and the client computer. The browser checks the server's certificate, then they agree on keys and all data is encrypted.	Shown by https and a padlock in the address bar; protects logins and payments from being read
Encryption	Scrambles data (plain text) into unreadable cipher text using an algorithm and a key. Only someone with the right key can read it.	Used for hard disks, email, cloud storage and HTTPS websites; protects data if it is stolen or intercepted, but does not stop it being stolen
Firewall	Hardware or software between a computer or network and the internet. It checks incoming and outgoing traffic against rules and blocks anything that is not allowed.	Protects against hackers and some malware; can block certain websites; does not remove viruses that are already inside

Figure 34: A firewall filters traffic between the internet and a network

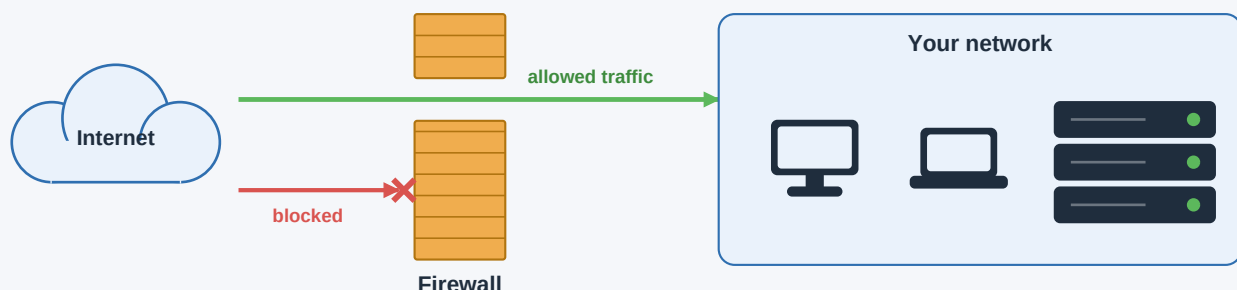


Figure 35: A secure link with SSL, a digital certificate and encryption

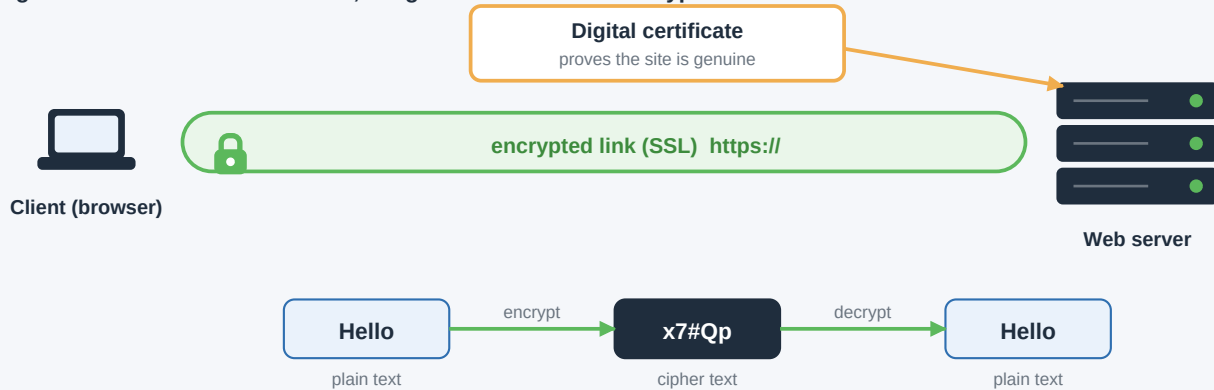
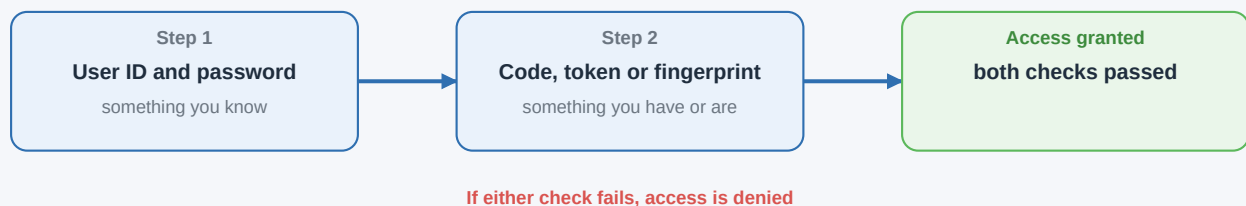


Figure 36: Two-factor authentication



Using several methods together

No single method protects data completely, so they are used in layers. For example, a bank uses a firewall to keep hackers out, SSL and encryption to protect data as it travels, and a user ID, password and two-factor authentication to confirm who the customer is.

EXAM TIP

Describe **what each method does**, not just its name. Be exact: a firewall **filters traffic**, encryption makes data **unreadable**, SSL makes an **encrypted link** and a digital certificate **proves identity**.

Key terms

Term	Meaning
Authentication	Checking that a user is who they claim to be.
Two-factor authentication	Using two different proofs of identity.
Biometrics	Identification using unique body features.
Digital certificate	An electronic document that proves identity.
SSL	Secure socket layer; an encrypted link between a server and a client.
Encryption	Scrambling data so it cannot be read without a key.
Cipher text	Data after it has been encrypted.
Firewall	Filters traffic between a network and the internet.
Certificate authority	A trusted body that issues digital certificates.

Practice questions

Answer each question in full sentences. Command words used: State (give a short answer), Describe (say what it is like), Explain (give reasons), Analyse (break it down and examine it), Suggest (apply your knowledge to a situation), Compare and contrast (similarities and differences), Evaluate (weigh up and reach a judgement).

No.	Question	Marks
1	State the purpose of a firewall.	[2]
2	Describe how SSL creates a secure link between a web server and a browser.	[3]
3	Explain how two-factor authentication improves the security of an online account.	[3]
4	Compare and contrast encryption with the use of a firewall.	[4]
5	Evaluate the use of biometrics to protect data.	[5]

Total: 17 marks