A2 NETWORKS · A2.4

Network security

The **threats** networks face and the layered **defences** against them, from **firewalls** to **encryption** and digital certificates.

01 Firewalls & NAT

Firewall	Filters traffic against rules.
Basic	Filters by IP address and port.
Next-gen	Inspects packet content (layer 7).
Limits	Misconfig and phishing bypass it.
NAT	Hides internal private IP addresses.

02 Common threats

Malware	Viruses, worms, trojans, ransomware.
Phishing	Social engineering for credentials.
MitM	Intercepts traffic between two parties.
DoS/ DDoS	Floods a service so it's unavailable.
SQL inject	Malicious input run as a DB query.
Weak pwd	Guessed, brute-forced, or breached.

03 Countermeasures · defence in depth

Firewall	Filters traffic and blocks unauthorised packets by IP, port, or content.	FILTER
Antivirus + patching	Detects and removes malware; regular updates close known vulnerabilities.	DETECT
Passwords + MFA	Strong, unique passwords plus a second factor so a stolen password is not enough.	VERIFY
Encryption	WPA2/WPA3 for Wi-Fi and HTTPS in transit keep intercepted data unreadable.	HIDE
Backups + training	Backups recover data after an attack; training helps staff spot phishing.	RECOVER

04 Encryption

Symmetric

One shared secret key for both steps. Fast, but sharing the key securely is the hard part.

Asymmetric

Public key encrypts, private key decrypts. Slower; no shared secret. Used by HTTPS/TLS.

05 Certificates & HTTPS

Certificate	Proves a public key is the real site's.
CA	The trusted authority that issues it.
HTTPS	Encrypted and identity-verified.
Padlock	Shows a valid certificate.
Handshake	Asymmetric agrees a symmetric key.

06 Know the difference

Symmetric vs asymmetric	One shared key versus a public/private key pair.	KEYS
DoS vs DDoS	Flooding from one source versus from many machines (a botnet).	ATTACK
Virus vs worm	A virus needs a host file and user action; a worm self-spreads across a network.	MALWARE
Public vs private key	The public key encrypts and is shared; the private key decrypts and is kept secret.	PAIR

FINAL PASS BEFORE THE EXAM

Rapid exam tips

Eight things that lose marks in Paper 1 if you slip on them. Skim before you walk in.

01

A **firewall** is not a full defence: misconfig and phishing get around it.

02

Symmetric = one shared key; **asymmetric** = a public/private pair.

03

The **private key** decrypts what the **public key** encrypted, not the reverse.

04

DDoS is distributed across many machines; **DoS** is from one source.

05

A **worm** self-spreads; a **virus** needs a host file and a user to run it.

06

HTTPS encrypts data in transit and verifies identity. It is not total safety.

07

A **digital certificate** proves a public key belongs to the real site (the padlock).

08

Defence in depth: layer firewall, antivirus, patching, MFA, encryption, backups, training.