

THEME A: CONCEPTS · A2.4

Network security

Original practice questions · 34 marks · about 50 minutes · covers A2.4.1–A2.4.4

Instructions. Answer all questions. The maximum mark for this paper is [34 marks]. The marks available are shown in brackets. Parts badged **HL** assess higher level only content; standard level students may leave these out.

1**Total: 6 marks**

A company installs a firewall between its internal network and the internet. Staff also work from cafes and airports using company laptops.

- (a) Outline how a firewall uses rules to decide which traffic to allow. [2]

- (b) **Discuss** how effective this firewall will be at protecting the company's data. [4]

2**Total: 4 marks**

The company's firewall is configured using lists of permitted and blocked sources.

- (a) Distinguish between a whitelist and a blacklist. [2]

- (b) Explain how network address translation (NAT) contributes to the security of the internal network. [2]

3

Total: 6 marks

Two offices of the same company exchange confidential design files over the internet.

- (a) Distinguish between symmetric and asymmetric cryptography. [3]

- (b) Describe how a public key and a private key are used so that only the receiving office can read a file that is sent. [3]

4

Total: 5 marks

An employee's browser connects to the company's website and shows a padlock in the address bar.

- (a) Describe the role of a digital certificate in establishing this secure connection. [3]

- (b) Outline why key management is important to the company. [2]

An online retailer runs a website with a customer login page and a product search box.

- (a) **HL** Describe how a distributed denial of service (DDoS) attack would affect the retailer. **[3]**

- (b) **HL** Describe how an SQL injection attack against the search box works. **[2]**

- (c) **HL** Outline what is meant by a zero-day exploit. **[2]**

The retailer reviews the countermeasures protecting its systems.

- (a) **HL** Describe how multifactor authentication (MFA) reduces the risk from weak passwords. **[3]**

- (b) **HL** Outline how input validation defends the search box against attack. **[2]**

- (c) **HL** State **one** reason why regular staff training forms part of network security. **[1]**

END OF QUESTIONS