

THEME A: CONCEPTS · A2.4

Network security — Mark scheme

34 marks · covers A2.4.1–A2.4.4

How to mark. Each creditworthy point is on its own line and ends with a semicolon (;). A line beginning with ... is an *expansion* of the line above it, so the pair is worth the marks shown. A slash (/) separates acceptable alternative wordings. Words in (brackets) are not needed for the mark. Mark positively: credit what the student has got right rather than penalising what is missing, and accept any valid alternative not listed here. Do not award more than the maximum for a part. Where a later part uses a wrong answer from an earlier part correctly, award follow-through marks (FT). HL marks parts that assess higher level only content.

Q	ANSWER	MARKS
1(a) A2.4.1	Award [2] max Award [1] per point up to [2] max. The firewall inspects each packet of incoming and outgoing traffic as it crosses the network boundary; It compares the packet against a set of rules, for example the source and destination address, the port or the protocol; Traffic matching an allow rule is passed on and traffic matching a block rule is discarded; Rules may be built from whitelists of permitted sources and blacklists of blocked ones;	2
1(b) A2.4.1	Award [4] max This is a discuss question (AO3), so both strengths and limitations are required. Award [1] per point up to [4] max, but award a maximum of [3] if only one side is given. Credit a supported conclusion. Strengths It blocks unsolicited inbound connections, so attackers cannot reach internal services directly from the internet; It restricts outbound traffic to approved ports and destinations, which limits what malware inside can send out; It logs traffic, so unusual activity can be detected and investigated; It gives one central point at which the company's security policy is enforced; Limitations It only inspects traffic that crosses the boundary, so it cannot stop an attack spreading between machines already inside; It cannot see inside encrypted traffic unless it is configured to decrypt it, so malicious content can pass through; It does not stop an authorised user being tricked, for example by a phishing email, since that traffic is permitted; Staff working from cafes and airports are outside the firewall entirely, so their laptops are unprotected by it; It is only as good as its rules, and a misconfiguration can leave a port exposed; Conclusion (credit a supported judgement, for example) The firewall is a necessary boundary defence but not sufficient on its own; it must be combined with VPNs for remote staff, endpoint protection and staff training;	4
2(a) A2.4.1	Award [2] max	2

Q	ANSWER	MARKS
	Award up to [1] per difference, [2] max. A whitelist permits only the sources on the list and blocks everything else, whereas a blacklist blocks the sources on the list and permits everything else; A whitelist is more secure because anything unknown is denied by default, whereas a blacklist cannot block a threat that is not yet known; A whitelist is more restrictive and needs more maintenance, whereas a blacklist is easier to run but leaves gaps;	
2(b) A2.4.1	Award [2] max Award [1] for the point and [1] for the expansion. NAT hides the private addresses of the internal machines behind a single public address; ...(so) an attacker on the internet cannot see or address an individual internal device directly; Inbound traffic has no NAT table entry unless an internal device started the exchange; ...(so) unsolicited incoming connections are dropped, acting as a basic filter;	2
3(a) A2.4.4	Award [3] max Award [1] per point up to [3] max. The contrast must be clear. Symmetric cryptography uses the same single key to encrypt and to decrypt, whereas asymmetric uses a matched pair of different keys; In symmetric cryptography the key must be shared with the other party in advance, which is the difficult part to do securely, whereas in asymmetric only the public key is shared; Symmetric encryption is much faster and better suited to large volumes of data, whereas asymmetric is slower; In practice the two are combined: asymmetric cryptography is used to exchange a symmetric key, which then encrypts the data;	3
3(b) A2.4.4	Award [3] max Award [1] per point up to [3] max. The receiving office generates a key pair and publishes its public key, keeping its private key secret; The sending office encrypts the file using the receiving office's public key; Data encrypted with that public key can only be decrypted with the matching private key; ...(so) even if the file is intercepted in transit it cannot be read; The receiving office decrypts it with its private key, which never leaves that office;	3
4(a) A2.4.4	Award [3] max Award [1] per point up to [3] max. The certificate contains the website's public key together with details of the site it belongs to; It is issued and digitally signed by a trusted certificate authority; The browser checks that signature to confirm the certificate is genuine and has not expired or been revoked; ...(so) the employee can be confident the site really is the company's, and not an impostor; The public key in the certificate is then used to agree a session key for encrypting the rest of the traffic;	3
4(b) A2.4.4	Award [2] max Award [1] for the point and [1] for the expansion. The security of the whole system depends on the private keys staying secret;	2

Q	ANSWER	MARKS
	...(so if) a private key is exposed, an attacker can decrypt intercepted traffic or impersonate the company; Keys must be generated, stored, rotated and revoked in a controlled way; ...(so that) a lost or compromised key can be replaced without the company losing access to its own data;	
HL 5(a) A2.4.2	Award [3] max Award [1] per point up to [3] max. Many compromised machines, often a botnet, send requests to the retailer's servers at the same time; The volume of traffic exhausts the server's bandwidth, connections or processing capacity; Genuine customers cannot reach the site, or it becomes too slow to use; The retailer loses sales for as long as the attack continues, and its reputation suffers; Because the traffic comes from many different addresses, it is hard to block by simply banning one source;	3
HL 5(b) A2.4.2	Award [2] max Award [1] per point up to [2] max. The attacker types SQL code into the search box instead of an ordinary search term; If the input is passed straight into a database query, that code is executed as part of the query; ...(so) the attacker can read, change or delete data they should not be able to reach, such as customer records;	2
HL 5(c) A2.4.2	Award [2] max Award [1] for the point and [1] for the expansion. A zero-day exploit attacks a vulnerability that the software vendor does not yet know about; ...(so) no patch exists and the retailer has had zero days to fix it, leaving normal patching useless as a defence;	2
HL 6(a) A2.4.3	Award [3] max Award [1] per point up to [3] max. MFA requires more than one form of evidence before access is granted, typically something the user knows plus something they have; A password alone is therefore not enough to log in; ...(so) an attacker who guesses, phishes or buys a weak password still cannot get in without the second factor; The second factor, such as a code from an app or a hardware token, changes and is tied to a device the attacker does not hold; It also alerts the genuine user, because they receive a prompt they did not ask for;	3
HL 6(b) A2.4.3	Award [2] max Award [1] per point up to [2] max. Input validation checks what the user has typed before it is used, rejecting anything that does not match the expected format; Filtering or whitelisting allows only permitted characters, so SQL keywords and symbols cannot be smuggled through; ...(so) the input is treated as data to search for rather than as code to run;	2
	Award [1] max	1

Q	ANSWER	MARKS
HL 6(c) A2.4.3	Any one, [1] max. Many attacks target people rather than systems, so staff need to recognise phishing attempts; Technical controls cannot stop an authorised user being tricked into handing over credentials; Staff need to know the procedures for reporting a suspected incident quickly;	

Total for this paper: 34 marks