MODULE G SECURITY · G7

Firewalls and anti-malware: mark scheme

21 marks · OCR J277 spec 1.4.2

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative answers; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. **...** at the start of a bullet means it builds on the bullet before. **NE** = not enough. Spec points covered (J277 1.4.2): anti-malware software and firewalls as prevention methods, including what each may limit/prevent and how it limits the attack (threats from 1.4.1). Penetration testing, user access levels, passwords, encryption and physical security (also 1.4.2) are tested in other Module G worksheets, not here.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.2	Checks data in and out of a network against rules: Firewall Compares files with a database of known malware: Anti-malware software Moves an infected file into quarantine: Anti-malware software Can block traffic from a particular IP address: Firewall	**4**	1 mark per correct row. 2+ ticks in a row = 0 for that row.
2(a) J277 1.4.2	Monitors / examines (all) traffic / data (packets) coming into (and going out of) the network Checks the traffic against a set of rules / criteria (set by the company) Blocks / rejects traffic that breaks the rules // that comes from an unknown / untrusted / blocked source Only allows traffic that meets the rules / that is from a trusted source // that the network asked for Sits between the network and the internet // acts as a barrier, so a hacker's connection from the internet does not reach the computers / server Can log / alert staff to blocked attempts to get in	**3**	Max 3. "Stops hackers" alone = NE (must say how). "Blocks viruses" alone = NE here. Do not accept answers that describe scanning files on the computer (that is anti-malware). Credit any other valid answer.
2(b) J277 1.4.2	Block traffic from (a list of) particular / suspicious IP addresses Only allow traffic from (a list of) trusted IP addresses / devices // whitelist Block access to particular websites / web addresses Block particular ports // only allow traffic on certain ports Block particular programs / types of traffic from using the network // e.g. block file-sharing traffic Block incoming connections that the network did not request Block traffic at certain times // e.g. outside office hours	**2**	1 mark each to max 2. Mark first two answers only. Two answers that are the same rule reworded = 1 mark. "Block hackers" / "block bad traffic" = NE. Credit any other valid rule.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.2 (threats from 1.4.1)	**Form of attack (1 mark):** Malware // named type of malware e.g. virus, worm, spyware, ransomware Denial of service (DoS / DDoS) **How (max 2), e.g.:** *Malware:* blocks downloads / traffic from known malicious / blocked websites or IP addresses ... stops malware already on a computer connecting to / sending data out to the attacker ... blocks unrequested incoming connections that malware (e.g. a worm) uses to spread *DoS:* identifies traffic from the attacking IP address(es) ... and blocks / drops it before it reaches the server ... can limit / block an unusually large number of requests (from one source) // so the server is not overwhelmed / stays available	**3**	1 mark for a valid attack, then up to 2 for how the firewall limits that attack. No marks for "how" if the attack is invalid. Do **not** accept data interception (a firewall does not stop data being intercepted while it travels across the internet). Do not accept "unauthorised access / hacking" (excluded by the question). Credit any other valid attack with a valid "how", e.g. brute-force: blocks repeated login attempts from the same IP address.
4(a) J277 1.4.2	Scans files / programs / downloads / email attachments / memory (for malware) Compares them with a database / list / signatures of known malware Checks files as they are opened / downloaded // real-time scanning // runs scheduled scans Removes / deletes the malware // quarantines the infected file (so it cannot run / spread) Alerts / warns the user that malware has been found Can detect suspicious behaviour of a program (that may be new malware) Can stop malware being installed / downloaded // blocks it before it runs	**3**	Max 3. "Gets rid of viruses" alone = 1 mark (removes malware) only. "Stops hackers" = NE. Do not accept answers that describe checking network traffic against rules (that is a firewall). Credit any other valid answer.
4(b) J277 1.4.2	New malware is being created all the time ... the update adds the new malware to the database / definitions / signatures ... otherwise (new) malware not in the database would not be detected / could infect the computer Updates can also fix weaknesses / bugs in the anti-malware software itself	**2**	Max 2. "To keep it up to date" / "to make it work better" = NE. Credit any other valid answer.

QUESTION	ANSWER	MARKS	GUIDANCE
5(a) J277 1.4.2	**Why the firewall will not stop it (max 2):** A firewall (only) monitors / filters network traffic // data passing between the network and the internet The memory stick is connected directly to the computer // the malware does not travel across the network / through the firewall A firewall does not scan / check files stored on a device **How anti-malware limits it (max 2):** Scans the files on the memory stick (when it is plugged in / when a file is opened) Compares the files with its database of known malware Quarantines / deletes the infected file // stops it running ... before it can infect / damage the computer // spread to other computers on the network Warns the worker that the file contains malware	**4**	Max 4. Max 2 for each half: an answer that covers only one half scores max 2. "The firewall doesn't work offline" = NE. Do not credit the claim that anti-malware stops the memory stick being plugged in. Credit any other valid answer.

Total: 21 marks