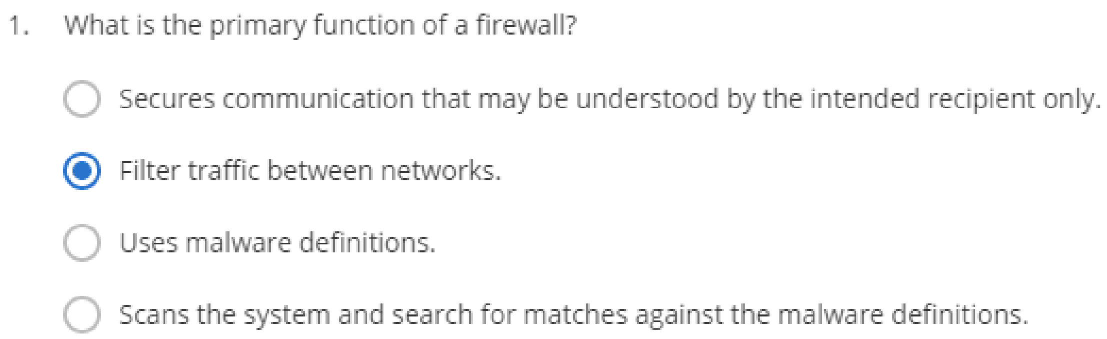
Quiz - Key security tools



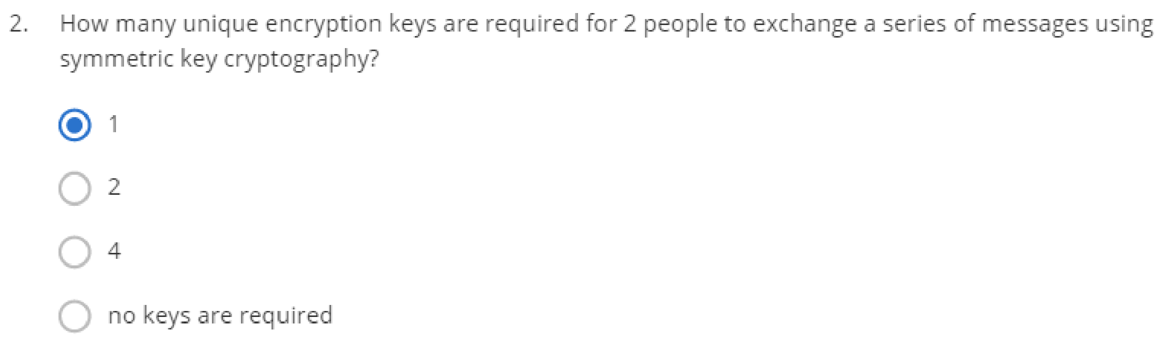
1. What is the primary function of a firewall?

○ Secures communication that may be understood by the intended recipient only.

● Filter traffic between networks.

○ Uses malware definitions.

○ Scans the system and search for matches against the malware definitions.



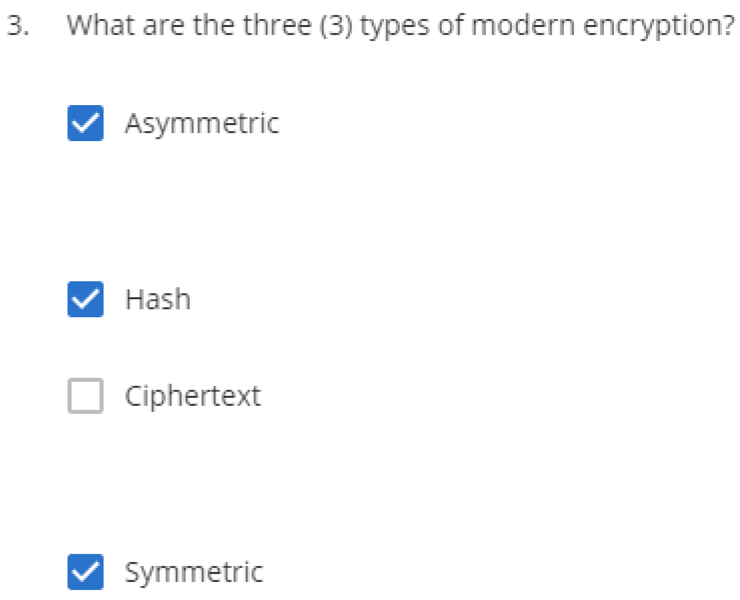
2. How many unique encryption keys are required for 2 people to exchange a series of messages using symmetric key cryptography?

● 1

○ 2

○ 4

○ no keys are required



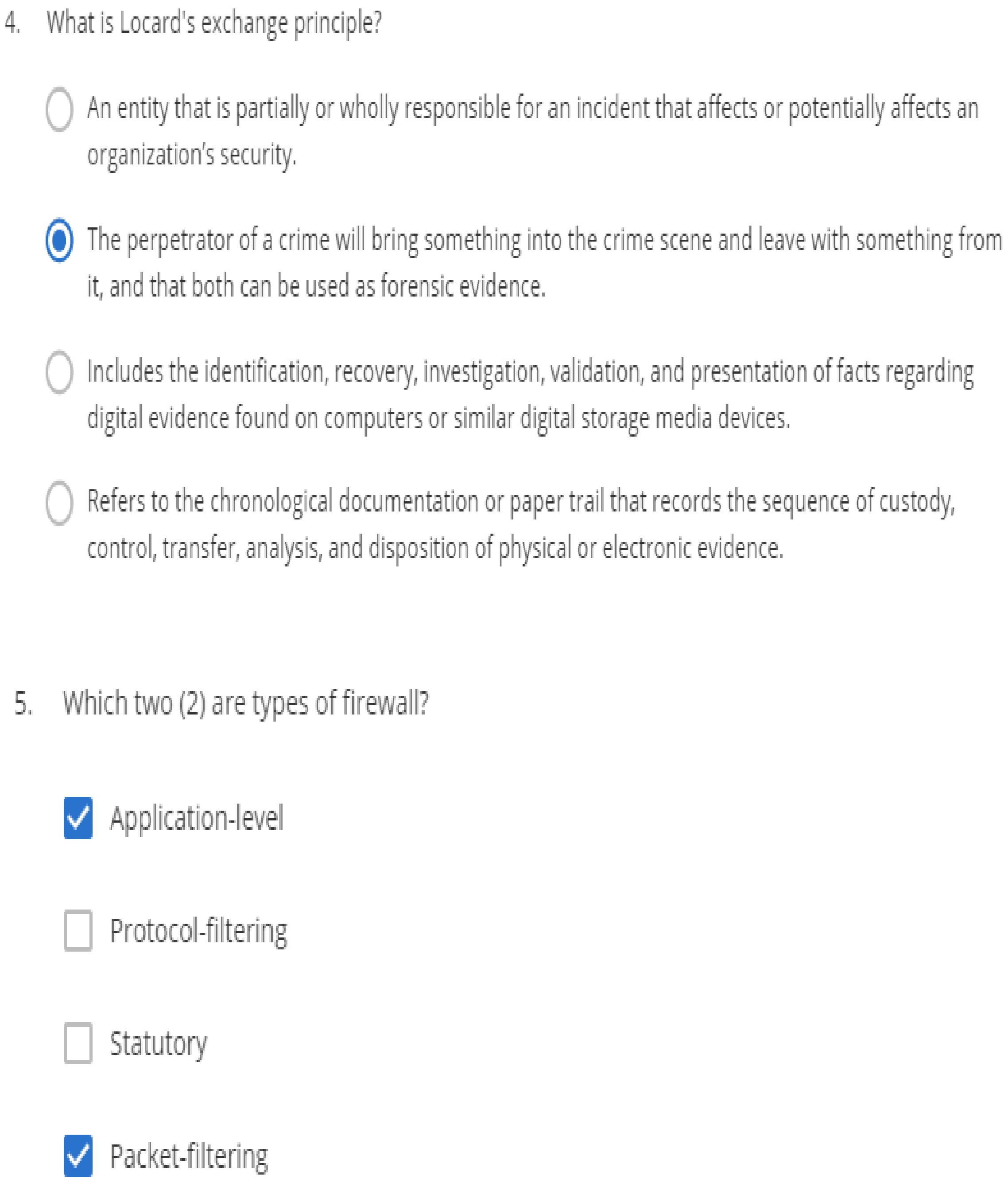
3. What are the three (3) types of modern encryption?

☑ Asymmetric

☑ Hash

□ Ciphertext

☑ Symmetric



4. What is Locard's exchange principle?

○ An entity that is partially or wholly responsible for an incident that affects or potentially affects an organization's security.

● The perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.

○ Includes the identification, recovery, investigation, validation, and presentation of facts regarding digital evidence found on computers or similar digital storage media devices.

○ Refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

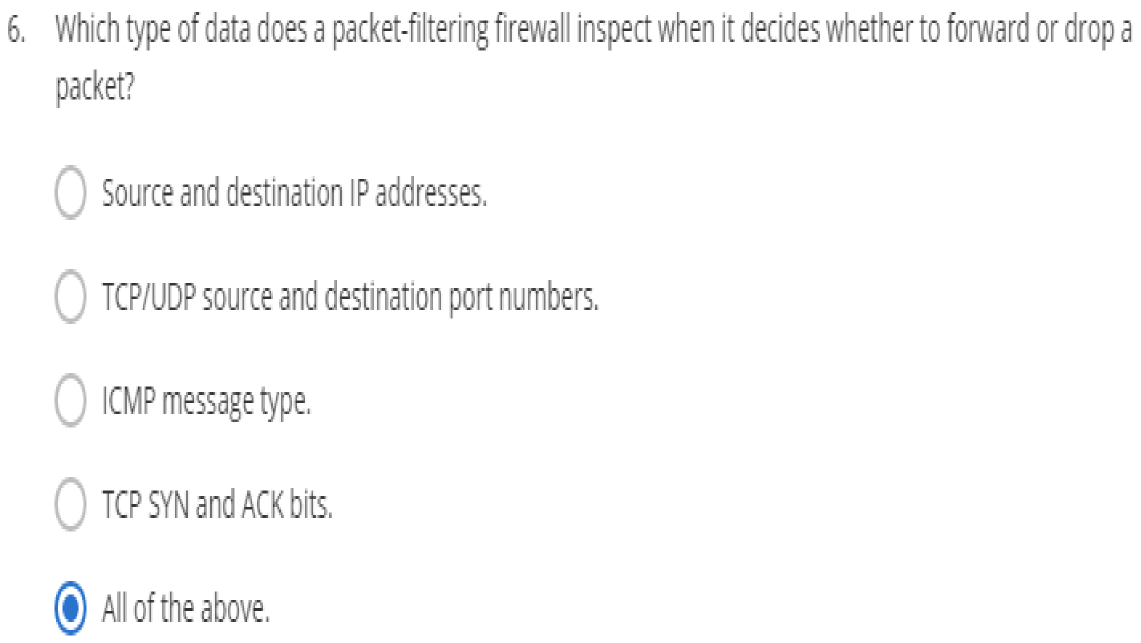
5. Which two (2) are types of firewall?

☑ Application-level

□ Protocol-filtering

□ Statutory

☑ Packet-filtering



6. Which type of data does a packet-filtering firewall inspect when it decides whether to forward or drop a packet?

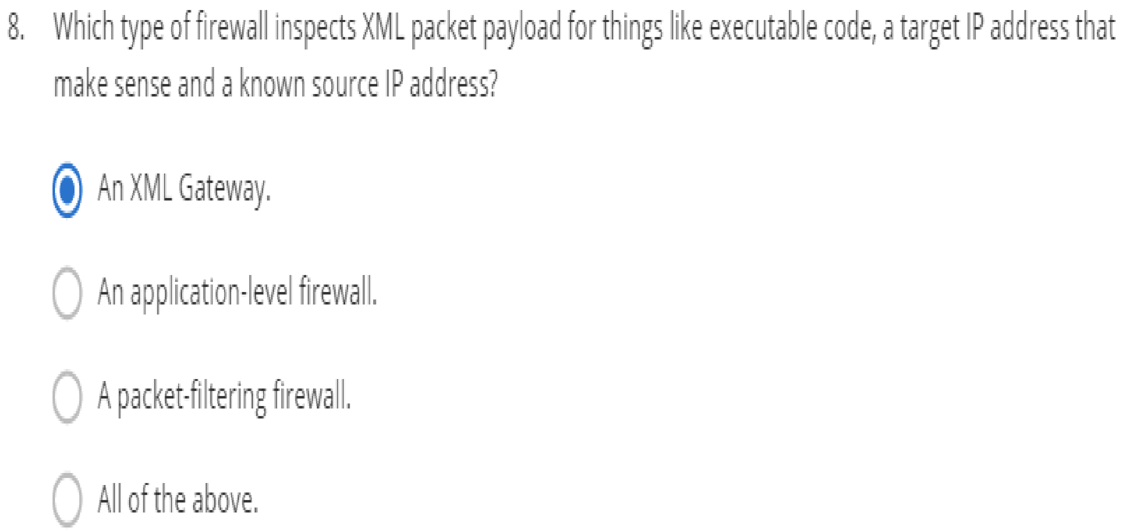
○ Source and destination IP addresses.

○ TCP/UDP source and destination port numbers.

○ ICMP message type.

○ TCP SYN and ACK bits.

● All of the above.



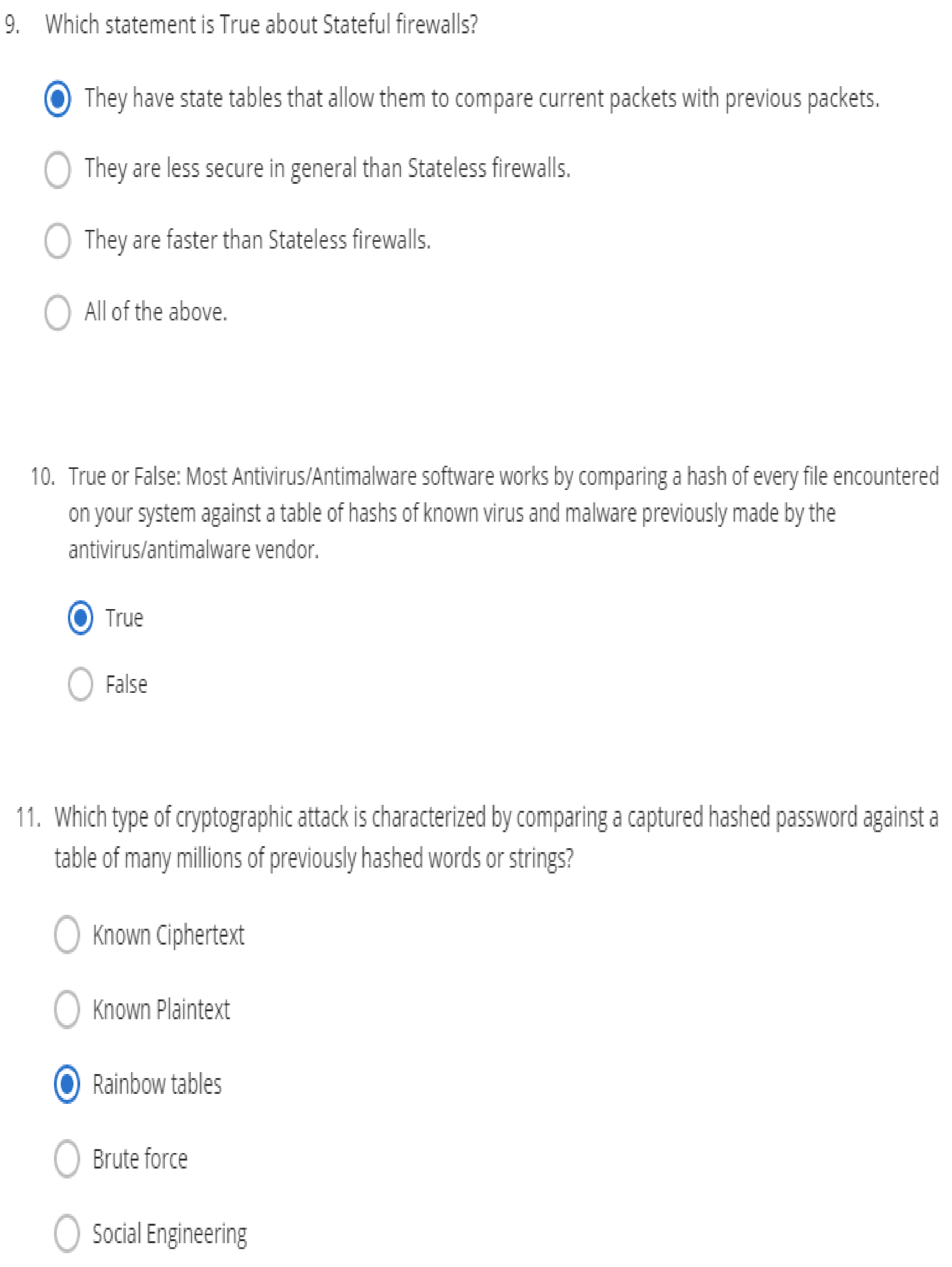
8. Which type of firewall inspects XML packet payload for things like executable code, a target IP address that make sense and a known source IP address?

● An XML Gateway.

○ An application-level firewall.

○ A packet-filtering firewall.

○ All of the above.



9. Which statement is True about Stateful firewalls?

● They have state tables that allow them to compare current packets with previous packets.

○ They are less secure in general than Stateless firewalls.

○ They are faster than Stateless firewalls.

○ All of the above.

10. True or False: Most Antivirus/Antimalware software works by comparing a hash of every file encountered on your system against a table of hashs of known virus and malware previously made by the antivirus/antimalware vendor.

● True

○ False

11. Which type of cryptographic attack is characterized by comparing a captured hashed password against a table of many millions of previously hashed words or strings?

○ Known Ciphertext

○ Known Plaintext

● Rainbow tables

○ Brute force

○ Social Engineering