1. Which of the following explains features of a traditional stateful firewall?

A. Access control is done by application awareness and visibility.

B. Access control is done by the five-tuple (source and destination IP addresses, source and destination ports, and protocol).

C. Application inspection is not supported.

D. Traditional stateful firewalls support advanced malware protection.

2. Which of the following describes a traditional IPS?

A. A network security appliance or software technology that resides in stateful firewalls

B. A network security appliance or software technology that supports advanced malware protection

C. A network security appliance or software technology that inspects network traffic to detect and prevent security threats and exploits

D. A virtual appliance that can be deployed with the Cisco Adaptive Security Manager (ASM)

3. Stateful and traditional firewalls can analyse packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet?

A. Session headers

B. NetFlow flow information

C. Source and destination ports and source and destination IP addresses

D. Protocol information

4. Amplification attacks are so called because:

A. Attackers deliver traffic to the victim by reflecting it off a third party so that the origin of the attack is concealed from the victim.

B. Attackers can amplify their message across the globe by using these attacks.

C. The traffic sent by the attacker is substantially greater than the traffic received by the victim.

D. The traffic received by the victim is substantially greater than the traffic sent by the attacker.

1. B. ACLs are the heart of a traditional stateful firewall, and they are based on source and destination IP addresses, source and destination ports, and protocol information.

2. C. A traditional IPS is a network security appliance or software technology that inspects network traffic to detect and prevent security threats and exploits.

3. C and D. ACLs inspect and apply policies based on source and destination IP addresses as well as source and destination ports and protocol information.

4. D. For example, in DNS amplification attack, the size of the response packet is always larger than the query packet, because a query response includes both the original query and the answer.