Which type of firewall only performs its security inspection during the establishment of the session between a host and server?

Circuit-level gateway

Application-level gateway

NAT filtering

Packet filtering

Answer: A

Explanation: A circuit-level gateway firewall operates at the session layer of the OSI model and only conducts its security inspection during the initial establishment of the TCP or UDP connection between the devices. After the connection is made, the packets can flow back and forth between the two devices without any further inspection.

You are working as a security administrator for a medium-sized company. Your boss has requested that a proxy server be installed so that Facebook can be blocked during working hours. Which type of proxy should you choose to meet this requirement?

Caching proxy

IP proxy

Content filter

Web security gateway

Answer: c

Explanation: An Internet content filter is a type of proxy server that can be used to log, monitor, and block certain websites from being accessed by your organization’s users. All devices will request the website from the content filter proxy, and if it is allowed to be accessed, the content filter will forward the request for the website on your workstation’s behalf.

You want to inspect all the traffic being sent into the network from outside of the LAN. You can only afford to purchase and install a single device to accomplish this. If you find malicious activity though, you want to be able to block it from entering the network based upon signatures you will create. Which device/software should you install?

NIDS

NIPS

HIDS

HIPS

Answer: B

Explanation: The Network Intrusion Prevention System can be installed at the perimeter of the network and monitor all traffic entering and leaving the network. If a signature on the NIPS matches the traffic entering or leaving the network, the NIPS can take action to block that traffic. A NIDS could detect the malicious traffic, but would be unable to act. HIDS and HIPS are host-based IDS and IPS, and therefore, could only protect one host on the network, not the entire network.