Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 7:23:09 pm • Time spent: 07:57

Score: 70% Passing Score: 80%

Question 1: ✓ Correct

Which of the following describes how access control lists can be used to improve network security?

○ An access control list filters traffic based on the frame header, such as source or destination MAC address.

○ An access control list identifies traffic that must use authentication or encryption.

➡ ● An access control list filters traffic based on the IP header information, such as source or destination IP address, protocol, or socket number.

○ An access control list looks for patterns of traffic between multiple packets and takes action to stop detected attacks.

EXPLANATION

An access control list filters traffic based on the IP header information, such as source or destination IP address, protocol, or socket number. Access control lists are configured on routers, and they operate on Layer 3 information.

Port security is configured on switches, which filter traffic based on the MAC address in the frame. An intrusion detection system (IDS) or intrusion prevention system (IPS) examines patterns detected across multiple packets. An IPS can take action when a suspicious pattern of traffic is detected.

REFERENCES

- 4.3.3 File Permission Facts
- 5.3.2 Firewall Facts
- 5.13.3 Router Security Facts
- 6.3.3 Authorization Facts

q_firewall_acl_02_secp7.question.fex

Question 2: ✕ Incorrect

Which of the following are features of an application-level gateway? (Select two.)

➡ □ Reassembles entire messages

➡ ☑ Stops each packet at the firewall for inspection

□ Verifies that packets are properly sequenced

☑ ~~Allows only valid packets within approved sessions~~

□ Uses access control lists

EXPLANATION

Application-level gateways:

- Operate up to OSL Layer 7 (Application layer)
- Stop each packet at the firewall for inspection (no IP forwarding)
- Inspect encrypted packets, such as an SSL inspection
- Examine the entire content that is sent (not just individual packets)
- Understand or interface with the application-layer protocol
- Can filter based on user, group, and data (such as URLs within an HTTP request)
- Is the slowest form of firewall protection because entire messages are reassembled at the Application layer

Allowing only valid packets within approved sessions and verifying that packets are properly sequenced are features of a stateful firewall.

Using access control lists is a feature of a packet-filtering firewall.

REFERENCES

5.3.2 Firewall Facts

q_firewall_application_02_secp7.question.fex

Question 3: ✕ Incorrect

You want to install a firewall that can reject packets that are not part of an active session. Which type of firewall should you use?

- ● ~~Application-level gateway~~
- ○ VPN concentrator
- ➡ ○ Circuit-level gateway
- ○ Packet-filtering firewall

EXPLANATION

A circuit-level proxy or gateway makes decisions about which traffic to allow based on virtual circuits or sessions. A circuit-level gateway:

- Operates at OSI Layer 5 (Session layer).
- Keeps a table of known connections and sessions. Packets directed to known sessions are accepted.
- Verifies that packets are properly sequenced.
- Ensures that the TCP three-way handshake process occurs only when appropriate.
- Does not filter packets. Rather, it allows or denies sessions.

A packet-filtering firewall makes decisions about which network traffic to allow by examining information in the IP packet header, such as source and destination addresses, ports, and service protocols. An Application-level gateway is a firewall that is capable of filtering based on information contained within the data portion of a packet (such as URLs within an HTTP request). A VPN concentrator is a device that is used to establish remote access VPN connections.

REFERENCES

5.3.2 Firewall Facts

q_firewall_circuit_01_secp7.question.fex

Question 4: ✕ Incorrect

Jessica needs to set up a firewall to protect her internal network from the internet. Which of the following would be the BEST type of firewall for her to use?

➡ ○ Hardware

● ~~Stateful~~

○ Tunneling

○ Software

EXPLANATION

Hardware firewalls are physical devices that are usually placed at the junction or gateway between two networks, generally a private network and a public network like the internet. Hardware firewalls can be a standalone product or can also be built into devices like broadband routers.

Software firewalls are generally used to protect individual hosts.

Tunneling is when an attacker wraps a malicious command in an HTTP, ICMP, or ACK tunneling packet that bypasses the firewall and reaches an internal system.

Stateful firewalls, also referred to as stateful multilayer firewalls, determine the legitimacy of traffic based on the state of the connection from which the traffic originated.

REFERENCES

5.3.2 Firewall Facts

q_firewall_hardware_secp7.question.fex

Question 5: ✓ Correct

You have been given a laptop to use for work. You connect the laptop to your company network, use it from home, and use it while traveling.

You want to protect the laptop from internet-based attacks. Which solution should you use?

○ Network-based firewall

○ VPN concentrator

○ Proxy server

➡ ● Host-based firewall

EXPLANATION

A host-based firewall inspects traffic received by a host. Use a host-based firewall to protect against attacks when there is no network-based firewall, such as when you connect to the internet from a public location.

A network-based firewall inspects traffic as it flows between networks. For example, you can install a network-based firewall on the edge of your private network that connects to the internet to protect against attacks from internet hosts.

A VPN concentrator is a device connected to the edge of a private network that is used for remote access VPN connections. Remote clients establish a VPN connection to the VPN concentrator and are granted access to the private network.

A proxy server is an Application-level firewall that acts as an intermediary between a secure private network and the public. Access to the public network from the private network goes through the proxy server.

REFERENCES

5.3.2 Firewall Facts

q_firewall_host_secp7.question.fex

Question 6: ✓ Correct

You have just installed a packet-filtering firewall on your network. Which options are you able to set on your firewall? (Select all that apply.)

- ☑ ~~Sequence number~~
- □ Checksum
- ➡ ☑ Destination address of a packet
- ➡ ☑ Port number
- ➡ ☑ Source address of a packet
- □ Acknowledgement number
- □ Digital signature

EXPLANATION

A packet-filtering firewall makes decisions about which network traffic to allow by examining information in the IP packet header, such as source and destination addresses, ports, and service protocols.

REFERENCES

5.3.2 Firewall Facts

q_firewall_packet_02_secp7.question.fex

Question 7: ✓ Correct

When designing a firewall, what is the recommended approach for opening and closing ports?

- ○ Open all ports; close ports that show improper traffic or attacks in progress.
- ○ Close all ports; open ports 20, 21, 53, 80, and 443.
- ○ Close all ports.
- ➡ ● Close all ports; open only ports required by applications inside the DMZ.
- ○ Open all ports; close ports that expose common network attacks.

EXPLANATION

When designing a firewall, the recommended practice is to close all ports and then only open those ports that allow the traffic that you want to allow inside the DMZ or the private network. Ports 20, 21, 53, 80, and 443 are common ports that are opened, but the exact ports you open depends on the services provided inside the DMZ.

REFERENCES

5.3.2 Firewall Facts

q_firewall_ports_secp7.question.fex

Question 8: ✓ Correct

You connect your computer to a wireless network available at the local library. You find that you can access all of the websites you want on the internet except for two.

What might be causing the problem?

➡ ◉ A proxy server is blocking access to the websites.

○ The router has not been configured to perform port forwarding.

○ A firewall is blocking ports 80 and 443.

○ Port triggering is redirecting traffic to the wrong IP address.

EXPLANATION

A proxy server can be configured to block internet access based on website or URL. Many schools and public networks use proxy servers to prevent access to websites with objectionable content.

Ports 80 and 443 are used by HTTP to retrieve all web content. If a firewall were blocking these ports, access would be denied to all websites. Port forwarding directs incoming connections to a host on the private network. Port triggering dynamically opens firewall ports based on applications that initiate contact from the private network.

REFERENCES

5.3.2 Firewall Facts

q_firewall_proxy_01_secp7.question.fex

Question 9: ✓ Correct

Which of the following best describes a stateful inspection?

○ Designed to sit between a host and a web server and communicate with the server on behalf of the host.

○ Allows all internal traffic to share a single public IP address when connecting to an outside entity.

○ Offers secure connectivity between many entities and uses encryption to provide an effective defense against sniffing.

➡ ● Determines the legitimacy of traffic based on the state of the connection from which the traffic originated.

EXPLANATION

Stateful firewalls, also referred to as stateful multilayer firewalls, determine the legitimacy of traffic based on the state of the connection from which the traffic originated. The stateful firewall maintains a state table that tracks the ongoing record of active connections.

A virtual private network (VPN) is a network that provides secure access to a private network through a public network or the internet. Virtual private networks offer secure connectivity between many entities, both internally and remotely. Their use of encryption provides an effective defense against sniffing.

Network Address Translation (NAT) separates IP addresses into two sets. This technology allows all internal traffic to share a single public IP address when connecting to an outside entity.

A firewall can be implemented on circuit-level gateways or Application-level gateways. Both of these firewall designs sit between a host and a web server and communicate with the server on behalf of the host. They can also be used to cache frequently accessed websites for faster web page loading.

REFERENCES

5.3.2 Firewall Facts

q_firewall_stateful_02_secp7.question.fex

Question 10: ✓ Correct

Which of the following are characteristics of a packet-filtering firewall? (Select two.)

- □ Filters based on URL
- □ Filters based on sessions
- ➡ ☑ Stateless
- ➡ ☑ Filters IP address and port
- □ Stateful

EXPLANATION

A packet-filtering firewall makes decisions about which network traffic to allow by examining information in the IP packet header, such as source and destination addresses, ports, and service protocols. A packet-filtering firewall is considered a stateless firewall because it examines each packet and uses rules to accept or reject each packet without considering whether the packet is part of a valid and active session.

A circuit-level proxy or gateway makes decisions about which traffic to allow based on virtual circuits or sessions. A circuit-level proxy is considered a stateful firewall because it keeps track of the state of a session. Application-level gateways filter on Application layer data, which might include data such as URLs within an HTTP request.

REFERENCES

5.3.2 Firewall Facts

q_firewall_stateless_secp7.question.fex

Copyright © 2022 TestOut Corporation All rights reserved.