Exam Report: 8.1.9 Practice Questions

Date: 10/16/2019 1:00:50 pm
Time Spent: 11:22

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 87%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Which of the following is a firewall function?

➡ ● Packet filtering

○ Protocol conversion

○ Encrypting

○ FTP hosting

○ Frame filtering

Explanation

Firewalls often filter packets by checking each packet against a set of administrator-defined criteria. If the packet is not accepted, it is simply dropped.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP05 3-5 23]

Question 2: Incorrect

You would like to control internet access based on users, time of day, and websites visited. How can you do this?

○ Configure a packet filtering firewall. Add rules to allow or deny internet access.

○ Configure the Local Security Policy of each system to add internet restrictions.

○ Enable Windows Firewall on each system. Add or remove exceptions to control access.

● ~~Configure internet zones using Internet Options.~~

➡ ○ Install a proxy server. Allow internet access only through the proxy server.

Explanation

Use a proxy server to control internet access based on users, time of day, and websites visited. You configure these rules on the proxy server, and all internet access requests are routed through the proxy server.

Use a packet filtering firewall, such as Windows Firewall, to allow or deny individual packets based on characteristics such as source or destination address and port number. Configure internet zones to identify trusted or restricted websites and control the types of actions that can be performed when visiting those sites.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm APTECH_5-2 MULTIPLE CHOICE [100]]

▼ Question 3: Correct

Which of the following are true of a circuit proxy filter firewall? (Select two.)

- □ Operates at the Network and Transport layers.
- ➡ ☑ Operates at the Session layer.
- □ Examines the entire message contents.
- ➡ ☑ Verifies sequencing of session packets.
- □ Operates at the Application layer.
- □ Operates at ring 0 of the operating system.

Explanation

A circuit proxy filter firewall operates at the Session layer. It verifies the sequencing of session packets, breaks the connections, and acts as a proxy between the server and the client.

An Application layer firewall operates at the Application layer, examines the entire message, and can act as a proxy to clients. A stateful inspection firewall operates at the Network and Transport layers. It filters on both IP addresses and port numbers. A kernel proxy filtering firewall operates at the operating system ring 0.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP15_FIREWALL_FACTS_01]

▼ Question 4: Correct

Which of the following are true about reverse proxy? (Select two.)

- □ Clients always know they are using reverse proxy.
- □ Handles requests from inside a private network out to the internet.
- ➡ ☑ Can perform load balancing, authentication, and caching.
- ➡ ☑ Handles requests from the internet to a server in a private network.
- □ Sits between a client computer and the internet.

Explanation

A reverse proxy server handles requests from the internet to a server located inside a private network. Reverse proxies can perform load balancing, authentication, and caching.

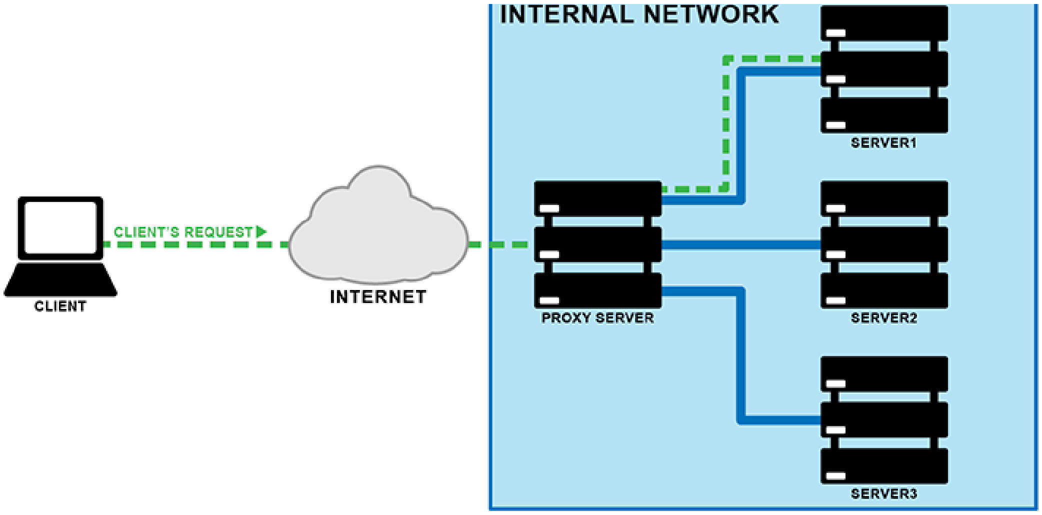
Reverse proxies often work transparently, meaning clients don't know they are connected to a reverse proxy.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm *NP15_FIREWALLS_01]

▼ Question 5: Correct

This question includes an image to help you answer the question. Close



Based on the diagram, which type of proxy server is handling the client's request?

○ Forward proxy server

➡ ◉ Reverse proxy server

○ Circuit-level proxy server

○ Open proxy server

Explanation

A reverse proxy server handles requests from the internet to an internal network. Instead of requests for a server going directly to the server, they first go to the reverse proxy server.

A forward proxy server handles requests from an internal network out to the internet. An open proxy server is accessible to any user on the internet and is used to forward requests to and from anywhere on the internet. A circuit-level proxy server is typically used as a stateful firewall to allow or deny sessions.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm *NP15_FIREWALLS_02]

▼ **Question 6:** Correct

You have a router that is configured as a firewall. The router is a Layer 3 device only.

Which of the following does the router use for identifying allowed or denied packets?

○ MAC address

➡ ◉ IP address

○ Username and password

○ Session ID

Explanation

A router acting as a firewall at Layer 3 is capable of making forwarding decisions based on the IP address.

The MAC address is associated with OSI model layer 2. Switches and wireless access points use MAC addresses to control access. The session ID is used by a circuit-level gateway, and username and password are used by Application layer firewalls.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP09_6-3 #MCS3]

Question 7: Incorrect

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?

● ~~Proxy server~~

○ VPN concentrator

➡ ○ Host-based firewall

○ Network-based firewall

Explanation

A host-based firewall inspects traffic received by a host. Use a host-based firewall to protect your computer from 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 your data from 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 layer 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

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP09_6-1 #MCS2]

Question 8: Correct

Which of the following are characteristics of a circuit-level gateway? (Select two.)

□ Stateless

➡ ☑ Filters by session

□ Filters by URL

➡ ☑ Stateful

□ Filters IP addresses, but not ports

Explanation

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.

Packet filtering firewalls are stateless and filter by on IP address and port number. Application-level gateways filter by the application layer data, which might include data such as URLs within an HTTP request.

References

LabSim for Network Pro, Section 8.1.

[netpro18v5_all_questions_en.exm NP09_6-2 #MCM1]

▼ **Question 9:** Correct

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

What might be causing the problem?

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

○ A firewall is blocking ports 80 and 443.

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

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

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

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm AP09PA_3-1 D7]

▼ **Question 10:** Correct

You have just installed a packet filtering firewall on your network.

Which options will you be able to set on your firewall? (Select all that apply.)

➡ ☑ Destination address of a packet

☐ Sequence number

☐ Checksum

☐ Acknowledgement number

➡ ☑ Port number

➡ ☑ Source address of a packet

☐ Digital signature

Explanation

Firewalls allow you to filter by IP address and port number.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP05_3-5 #49]

▼ **Question 11:** Correct

Haley configures a website using Windows Server 2016 default values.

What are the HTTP port and SSL port settings?

○ 160 for HTTP; 440 for SSL

○ 443 for HTTP; 80 for SSL

➡ ● 80 for HTTP; 443 for SSL

○ 440 for HTTP; 160 for SSL

Explanation

The default TCP port setting for HTTP is 80. You can change that setting to another TCP setting that is not in use, but users will have to know they must request the non-default setting, or they will be unable to connect. The SSL port number is 443 and is only used with secure socket layers for encryption.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP05_2-12 #7]

▼ Question 12: Correct

You have recently installed a new Windows Server 2016 system. To ensure the accuracy of the system time, you have loaded an application that synchronizes the hardware clock on the server with an external time source on the internet. Now, you must configure the firewall on your network to allow time synchronization traffic through.

Which of the following ports are you most likely to open on the firewall?

○ 80

➡ ● 123

○ 119

○ 110

Explanation

TCP/IP port 123 is assigned to the network time protocol (NTP). NTP is used to communicate time synchronization information between systems on a network.

The hypertext transfer protocol (HTTP) uses TCP/IP port 80. HTTP is the protocol used to send requests to a web server and retrieve web pages from a web server. TCP/IP port 119 is used by the network news transfer protocol (NNTP). NNTP is used to access and retrieve messages from newsgroups. TCP/IP port 110 is used by the post office protocol version 3 (POP3). POP3 is used to download email from mail servers.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP05_2-12 #58]

▼ Question 13: Correct

You are configuring a firewall to allow access to a server hosted on the demilitarized zone of your network. You open TCP/IP ports 80, 25, 110, and 143.

Assuming that no other ports on the firewall need to be configured to provide access, which applications are most likely to be hosted on the server?

➡ ● Web server and email server

○ Web server, DNS server, and email server

○ Email server, Newsgroup server, and DNS server

○ Web server, DNS server, and DHCP server

Explanation

TCP/IP port 80 is associated with accessing web pages from a web server using the hypertext transfer protocol (HTTP). Email can be accessed using a number of protocols, including the simple mail transfer protocol (SMTP), the post office protocol version 3 (POP3) and the internet message access protocol version 4 (IMAP4). SMTP uses TCP/IP port 25, while POP3 uses TCP/IP port 110, and IMAP4 uses TCP/IP port 143.

Domain name service (DNS) traffic uses TCP/IP port 53. Newsgroup servers are accessed using the network news transfer (NNTP) protocol on TCP/IP port 119. Dynamic host configuration protocol (DHCP) traffic uses the BOOTP protocol on TCP/IP ports 67 and 68.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm NP05_2-12 #74]

▼ Question 14: Correct

You are monitoring network traffic on your network, and you see traffic between two network hosts on port 2427.

Which kind of network traffic uses this port?

➡ ● The MGCP protocol is generating traffic, which VoIP uses to send voice data over a network.

○ Someone is remotely accessing another system using the SSH protocol.

○ A workstation is using the DHCP protocol to request an IP address from a DHCP server.

○ A ping of death attack on a network host is in progress.

Explanation

Someone on the network is using voice over IP (VoIP) to make a telephone call. Some VoIP implementations use the media gateway control protocol (MGCP) to set up, maintain, tear down, and redirect calls. MGCP uses port 2427.

The DHCP protocol is used to automatically assign IP addresses to network hosts and utilizes IP ports 67 and 68. A ping of death attack utilizes an oversized ICMP echo request packet to crash a target system. The SSH protocol is used to remotely access another network host and uses port 22.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm RT NP15_5.9-2]

▼ Question 15: Correct

You are monitoring network traffic on your network, and you see traffic between two network hosts on port 1720.

What is the source of this network traffic?

○ A man-in-the-middle attack is in progress.

○ Someone is downloading files from a server using the FTP protocol.

○ A workstation is using the DNS protocol to send a name resolution request to a DNS server.

➡ ● Someone is using voice over IP (VoIP) to make a telephone call.

Explanation

Someone on the network is using voice over IP (VoIP) to make a telephone call. Some VoIP implementations use the H.323 protocol to set up, maintain, tear down, and redirect calls. H.323 uses port 1720.

The DNS protocol sends name resolution requests to a DNS server on port 53. In a man-in-the-middle attack, a legitimate communication session between two network hosts is intercepted and possibly modified by an attacker. The FTP protocol uses ports 20 and 21 to transfer files between two network hosts.

References

LabSim for Network Pro, Section 8.1.
[netpro18v5_all_questions_en.exm RT NP15_5.9-3]