Exam Report: 8.3.9 Practice Questions

Date: 10/16/2019 1:22:39 pm
Time Spent: 14:44

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 93%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Match the firewall type on the right with the OSI layer at which it operates.

Each OSI Layer may be used once, more than once, or not at all.

Packet filtering firewall	Circuit-level proxy	Application-level gateway	Routed firewall	Transparent firewall
OSI Layer 3	OSI Layer 5	OSI Layer 7	OSI Layer 3	OSI Layer 2

Explanation

Each firewall type operate at a specific layer of the OSI model.

- Packet filtering firewalls operate at Layer 3.
- Circuit-level proxies operate at Layer 5.
- Application-level gateways operate at Layer 7.
- Routed firewalls operate at Layer 3.
- Transparent firewalls operate at Layer 2.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm *NP15_FIREWALLS_03]

Question 2: Correct

Your company has a connection to the internet that allows users to access the internet. You also have a web server and an email server that you want to make available to internet users. You want to create a DMZ for these two servers.

Which type of device should you use to create the DMZ?

- IPS
- Host-based firewall
- IDS
- Network-based firewall
- VPN concentrator

Explanation

A demilitarized zone (DMZ) is a buffer network, or subnet, that sits between the private network and an untrusted network, such as the internet. To create a DMZ, use two network-based firewall devices, one connected to the public network, and one connected to the private network.

A host-based firewall inspects traffic received by a host. Use a host-based firewall to protect

your network from attacks when there is no network-based firewall, such as when you connect to the internet from a public location.

A VPN concentrator is a device that is used to establish remote access VPN connections. An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A passive IDS monitors, logs, and detects security breaches, but takes no action to stop or prevent attacks. An active IDS (also called an intrusion protection system, or IPS) performs the functions of an IDS, but can also react when security breaches occur.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP09_6-1 #MCS6]

Question 3: Correct

You have used firewalls to create a demilitarized zone. You have a web server that needs to be accessible to internet users. The web server must communicate with a database server for retrieving product, customer, and order information.

How should you place devices on the network to best protect the servers? (Select two.)

- [ ] Put the web server on the private network.
- [x] Put the web server inside the DMZ.
- [x] Put the database server on the private network.
- [ ] Put the database server inside the DMZ.

Explanation

Publicly accessible resources (servers) are placed inside the DMZ. Examples of publicly accessible resources include web, FTP, and email servers. Devices that should not be accessible to public users are placed on the private network. If you have a public server that communicates with another server, such as a database server, and that server should not have direct contact with public hosts, place the server on the private network and allow only traffic from the public server to cross the inner firewall.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP09_6-2 #MCM3]

Question 4: 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?

- (•) IP address
- ( ) Session ID
- ( ) Username and password
- ( ) MAC address

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 and is used by switches and wireless access points to control access. The session ID is used by a circuit-level gateway, and usernames and passwords are used by Application layer firewalls.

References

LabSim for Network Pro, Section 8.3.

[netpro18v5_all_questions_en.exm NP09 6-3 MCS3]

Question 5: 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.)

- [x] Destination address of a packet
- [x] Source address of a packet
- [ ] Acknowledgement number
- [ ] Checksum
- [x] Port number
- [ ] Digital signature
- [ ] Sequence number

Explanation

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

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP09_6-2 NP05_3-5 #49]

Question 6: Correct

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

- (•) An access list filters traffic based on the IP header information such as source or destination IP address, protocol, or socket numbers.
- ( ) An access list filters traffic based on the frame header such as source or destination MAC address.
- ( ) An access list looks for patterns of traffic between multiple packets and takes action to stop detected attacks.
- ( ) An access list identifies traffic that must use authentication or encryption.

Explanation

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

Port security is configured on switches and filters 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 defensive action when a suspicious pattern of traffic is detected.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm C802_701-4-5 MULTIPLE CHOICE [275]]

Question 7: Incorrect

Which of the following is likely to be located in a DMZ?

- ( ) Backup server
- (•) ~~User workstations~~

- Domain controller
- FTP server

Explanation

An FTP server is the most likely component from this list to be located in a DMZ (demilitarized zone) or a buffer subnet. A DMZ should only contain servers that are to be accessed by external visitors. Often it is assumed that any server placed in the DMZ will be compromised. Therefore, no mission critical or sensitive systems are located in a DMZ.

A domain controller may appear in a DMZ when the DMZ is an entire isolated domain, but this practice is not common. User workstations are never located in a DMZ. Unless specifically deployed for just the DMZ, backup servers are never located in a DMZ.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm SSCP-3 SP [809]]

Question 8: Correct

In which of the following situations would you most likely implement a demilitarized zone (DMZ)?

- You want to detect and respond to attacks in real time.
- You want internet users to see a single IP address when accessing your company network.
- You want to protect a public web server from attack.
- You want to encrypt data sent between two hosts using the internet.

Explanation

Use a demilitarized zone (DMZ) to protect public hosts on the internet, such as a web server, from attack. The DMZ uses an outer firewall that prevents internet attacks. Inside the DMZ are all publicly accessible hosts. A second firewall protects the private network from the internet.

Use a virtual private network (VPN) to encrypt data between two hosts on the internet. Use Network address translation (NAT) to hide internal IP addresses from the internet. Use an intrusion prevention system (IPS) to detect and respond to threats in real time.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm C802_601-603 MULTIPLE CHOICE [197]]

Question 9: Correct

Match the firewall type on the left with its associated characteristics on the right. Each firewall type may be used once, more than once, or not at all.

Operates at Layer 2.
- Virtual firewall

Operates at Layer 3.
- Routed firewall

Counts as a hop in the path between hosts.
- Routed firewall

Does not count as a hop in the path between hosts.
- Virtual firewall

Each interface connects to a different network.

Routed firewall

Each interface connects to the same network segment.

Virtual firewall

Explanation

In a routed firewall, the firewall is also a Layer 3 router. In fact, many hardware routers include firewall functionality. Transmitting data through this type of firewall counts as a router hop. A routed firewall usually supports multiple interfaces, each connected to a different network segment.

A transparent firewall (also called a virtual firewall) works differently. It operates at Layer 2, and it is not seen as a router hop by connected devices. Both the internal and external interfaces on a transparent firewall connect to the same network segment. Because it is not a router, you can easily introduce a transparent firewall into an existing network.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm RT NP15_3.5-2]

Question 10: Correct

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

- Close all 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.
- Open all ports; close ports that expose common network attacks.
- Close all ports; open only ports required by applications inside the DMZ.

Explanation

When designing a firewall, the recommended practice is to close all ports and then only open the ports that allow the traffic that you want 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 will open depend on the services provided inside the DMZ.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm SSCP 3 382]

Question 11: Correct

After blocking a number of ports to secure your server, you are unable to send email. To allow email service, which of the following needs to be done?

- Open port 25 to allow SMTP service.
- Open port 25 to allow SNMP service.
- Open port 110 to allow SMTP service.
- Open port 80 to allow SNMP service.
- Open port 80 to allow SMTP service.
- Open port 110 to allow POP3 service.

Explanation

The simple mail transfer protocol (SMTP) uses TCP port 25 and is responsible for sending email. If port 25 is blocked, users will not be able to send email, but they could receive email using port 110 and the POP3 protocol.

SNMP is used to monitor network traffic. POP3 uses port 110 and is used to retrieve email from a mail server.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP05_2-10 #299]

Question 12: Correct

You administer a web server on your network. The computer has multiple IP addresses. They are 192.168.23.8 to 192.168.23.17. The name of the computer is www.westsim.com. You configured the website as follows:

- IP address: 192.168.23.8
- HTTP Port: 1030
- SSL Port: 443

Users complain that they can't connect to the website when they type www.westsim.com. What is the most likely source of the problem?

- SSL is blocking internet traffic.
- ➡ The HTTP port should be changed to 80.
- Clients are configured to look for the wrong IP address.
- FTP is not configured on the server.

Explanation

The default HTTP port for the web is 80. You can change the default port; however, port 80 is the default port used by web browsers to make a connection to a web server. If you change the default port, the users must specify the correct port number, or they won't be able to connect to the server.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP05_2-12 #15]

Question 13: Correct

You want to maintain tight security on your internal network, so you restrict access to the network through certain port numbers. If you want to allow users to continue to use DNS, which port should you enable?

- 21
- ➡ 53
- 42
- 443
- 80

Explanation

The DNS service uses port 53.

References

LabSim for Network Pro, Section 8.3.

[netpro18v5_all_questions_en.exm NP05_2-12 #32]

Question 14: Correct

In the output of the **netstat** command, you notice that a remote system has made a connection to your Windows Server 2016 system using TCP/IP port 21.

Which of the following actions is the remote system most likely performing?

- Downloading a file
- Performing a name resolution request
- Downloading email
- Downloading a web page

Explanation

TCP/IP port 21 is assigned to the file transfer protocol (FTP). A system connected on this port is most likely downloading a file from an FTP server application hosted on the system.

Downloading email can be achieved via 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. Web pages are downloaded using the hypertext transfer protocol (HTTP) on TCP/IP port 80. Name resolution requests use the domain name service (DNS) protocol on TCP/IP port 53.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP05_2-12 #66]

Question 15: Correct

You want to allow users to download files from a server running the TCP/IP protocol. You want to require user authentication to gain access to specific directories on the server.

Which TCP/IP protocol should you implement to provide this capability?

- TCP
- HTML
- HTTP
- TFTP
- FTP
- IP

Explanation

You should implement the file transfer protocol (FTP). It enables file transfers and supports user authentication. The trivial file transfer protocol (TFTP) enables file transfer, but does not support user authentication.

References

LabSim for Network Pro, Section 8.3.
[netpro18v5_all_questions_en.exm NP05_2-10 #68]