Exam Report: 5.5.5 Practice Questions

Date: 1/20/2020 8:21:57 pm
Time Spent: 13:25

Candidate: Garsteck, Matthew
Login: mGarsteck

## Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

## Individual Responses

**Question 1:** 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?

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

### Explanation

A *demilitarized zone* (DMZ), or *screened subnet*, 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 one network-based firewall 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 against 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 the attack. 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 Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_01]

**Question 2:** Correct

Which of the following is a firewall function?

- Packet filtering
- Frame filtering
- FTP hosting
- Encrypting
-

Protocol conversion

## 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 Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_02]

**Question 3:** Incorrect

You manage a small network at work. Users use workstations connected to your network. No portable computers are allowed.

As part of your security plan, you would like to implement scanning of e-mails for all users. You want to scan the e-mails and prevent any e-mails with malicious attachments from being received by users.

Your solution should minimize administration, allowing you to centrally manage the scan settings.

Which solution should you use?

- SMTP
- Network based firewall
- DMZ
- ~~Host based firewall~~

## Explanation

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 and scans all incoming e-mail. Scanning e-mail as it arrives at your e-mail server allows you to centralize management and stop malicious e-mails before they arrive at client computers.

A *demilitarized zone* (DMZ), also called a *screened subnet*, is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the Internet). SMTP is an e-mail protocol used by e-mail servers for sending mail.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_03]

**Question 4:** Correct

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

- [ ] Stateless
- [x] Filters based on sessions
- [ ] Filters IP address and port
- [x] Stateful
- [ ] Filters based on URL

## 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 based on IP address and port number. Application level gateways filter on the application layer data, which might include data such as URLs within an HTTP request.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_04]

**Question 5:** Correct

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

- [x] Stateless
- [x] Filters IP address and port
- [ ] Filters based on sessions
- [ ] Filters based on URL
- [ ] 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 the application layer data, which might include data such as URLs within an HTTP request.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_05]

**Question 6:** 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?

- [ ] Circuit-level
- [x] ~~Packet filtering~~
- [ ] VPN concentrator
- [ ] Application level

## 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

LabSim for Security Pro, Section 5.5.

[All Questions SecPro2017_v6.exm FIREWALLS_06]

**Question 7:** Correct

You provide internet access for a local school. You want to control Internet access based on user, and prevent access to specific URLs.

Which type of firewall should you install?

- IPS
- Circuit-level
- Application level
- Packet filtering

## Explanation

An application-level gateway is a firewall that is capable of filtering based on information contained within the data portion of a packet. An application level gateway can filter based on user, group, and data such as URLs within an HTTP request. One example of an application level gateway is a *proxy* server. Proxies can be configured to restrict access by user or by specific Web sites.

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 *circuit-level proxy* or *gateway* makes decisions about which traffic to allow based on virtual circuits or sessions. An intrusion prevention system (IPS) looks for network attacks and takes appropriate actions to stop or reduce the effects of those attacks.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_07]

**Question 8:** Correct

Which of the following is the best device to deploy to protect your private network from a public untrusted network?

- Firewall
- Gateway
- Router
- Hub

## Explanation

A firewall is the best device to deploy to protect your private network from a public untrusted network. Firewalls are used to control traffic entering and leaving your trusted network environment. Firewalls can manage traffic based on source or destination IP address, port number, service protocol, application or service type, user account, and even traffic content.

Routers offer some packet-based access control, but not as extensive as that of a full fledged firewall. Hubs and gateways are not sufficient for managing the interface between a trusted and an untrusted network.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_08]

**Question 9:** 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?

- ~~Network based firewall~~
- Host based firewall
- VPN concentrator
- Proxy server

## 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 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 Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_09]

**Question 10:** Correct

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

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

## 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 also act as a proxy to clients.
A stateless inspection firewall operates at the Network (layer 3) and Transport layers (layer 4) and filters on both IP addresses and port numbers.
A kernel proxy filtering firewall operates at the operating system ring 0.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_12]

**Question 11:** Incorrect

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

- Enable Windows Firewall on each system. Add or remove exceptions to control access.
- ~~Configure the Local Security Policy of each system to add Internet restrictions.~~

- Configure Internet zones using the Internet Options.
- Install a proxy server. Allow Internet access only through the proxy server.
- Configure a packet-filtering firewall. Add rules to allow or deny Internet access.

## 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 to control the types of actions that can be performed when going to those sites.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_14]

**Question 12:** Correct

Which of the following does a router acting as a firewall use to control which packets are forwarded or dropped?

- VNC
- ACL
- RDP
- PPP
- IPsec

## Explanation

When you configure a router as a firewall, you configure the access control list (ACL) with statements that identify traffic characteristics, such as the direction of traffic (inbound or outbound), the source or destination IP address, and the port number. ACL statements include an action to either allow or deny the traffic specified by the ACL statement.

IPsec is a protocol for encrypting packets. RDP and VNC are remote desktop protocols used for remotely accessing a computer's desktop. PPP is a protocol for establishing a remote access connection over a dial-up link.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_15]

**Question 13:** Incorrect

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

- An access list looks for patterns of traffic between multiple packets and takes action to stop detected attacks.
- An access list filters traffic based on the frame header such as source or destination MAC address.
- 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 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 action when a suspicious pattern of traffic is detected.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_17]

**Question 14:** Correct

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

- ○ Open all ports; close ports that expose common network attacks.
- ○ Close all ports.
- ○ Close all ports; open ports 20, 21, 53, 80, and 443.
- ○ Open all ports; close ports that show improper traffic or attacks in progress.
- ➡ ◉ 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 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 will open depend on the services provided inside the DMZ.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_18]

**Question 15:** Correct

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

- ☐ Uses access control lists.
- ☐ Verifies that packets are properly sequenced.
- ➡ ☑ Stops each packet at the firewall and inspects it.
- ➡ ☑ The entire messages are reassembled.
- ☐ Allow only valid packets within approved sessions.

## Explanation

Application-level gateways:

- Operate up to OSL Layer 7 (Application layer)
- Stops each packet at the firewall and inspects it, so there is no IP forwarding
- Inspects encrypted packets, such as in SSL inspection
- Examines the entire content (not just individual packets)
- Understands or interfaces 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 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.

Uses access control lists is a feature of a Packet Filtering firewall.

## References

LabSim for Security Pro, Section 5.5.
[All Questions SecPro2017_v6.exm FIREWALLS_19||/]