Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/22/2022 9:08:18 pm • Time spent: 02:51

Score: 100% Passing Score: 80%

Question 1: ✓ Correct

Which of the following terms describes a network device that is exposed to attacks and has been hardened against those attacks?

○ Circuit proxy

○ Kernel proxy

➡ ● Bastion or sacrificial host

○ Multi-homed

EXPLANATION

A bastion or sacrificial host is one that is unprotected by a firewall. The term bastion host is used to describe any device fortified against attack (such as a firewall). A sacrificial host might be a device intentionally exposed to attack, such as a honeypot.

Circuit proxy and kernel proxy are types of firewall devices.

Multi-homed describes a device with multiple network interface cards.

REFERENCES

5.2.4 DMZ Facts

q_dmz_bastion_secp7.question.fex

▼ **Question 2:** ✓ Correct

Of the following security zones, which one can serve as a buffer network between a private secured network and the untrusted internet?

○ Padded cell

○ Intranet

➡ ● DMZ

○ Extranet

EXPLANATION

A DMZ, or demilitarized zone, is a network placed between a private secured network and the untrusted internet to grant external users access to internally controlled services. The DMZ serves as a buffer network.

An intranet is a private network that happens to employ internet information services. An extranet is a division of a private network that is accessible to a limited number of users, such as business partners, suppliers, and certain customers. A padded cell is an intrusion detection countermeasure used to delay intruders sufficiently to record meaningful information about them for discovery and prosecution.

REFERENCES

5.2.4 DMZ Facts

q_dmz_dmz_01_secp7.question.fex

Question 3: ✓ Correct

Which of the following is the MOST likely to happen if the firewall managing traffic into the DMZ fails?

○ All devices in the DMZ and LAN will be compromised.

○ Nothing will happen - all devices will stay protected.

➡ ● Only the servers in the DMZ are compromised, but the LAN will stay protected.

○ The LAN is compromised, but the DMZ stays protected.

EXPLANATION

If the firewall managing traffic into the DMZ fails, only the servers in the DMZ are subject to compromise. The LAN is protected by default.

None of the other options are correct in this scenario.

REFERENCES

3.1.1 Physical Security

3.1.2 Physical Security Facts

3.1.3 Implement Physical Security

3.2.4 Physical Network Protection Facts

5.2.4 DMZ Facts

q_dmz_dmz_02_secp7.question.fex

▼ Question 4: ✓ Correct

You have a company network that is connected to the internet. You want all users to have internet access, but you need to protect your private network and users. You also need to make a web server publicly available to internet users.

Which solution should you use?

- ○ Use firewalls to create a DMZ. Place the web server and the private network inside the DMZ.
- ○ Use a single firewall. Put the web server in front of the firewall and the private network behind the firewall.
- ○ Use a single firewall. Put the web server and the private network behind the firewall.
- ➡ ● Use firewalls to create a DMZ. Place the web server inside the DMZ and the private network behind the DMZ.

EXPLANATION

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. A common configuration uses two firewalls, one connected to the public network and one connected to the private network. Publicly-accessible resources (servers) are placed inside the screened subnet. Examples of publicly-accessible resources include web, FTP, or email servers. Private resources that are not accessible from the internet are placed behind the DMZ (behind the inner firewall).

Placing the web server inside the private network would mean opening ports in the firewall leading to the private network, which could expose other devices to attack. Placing the web server outside of the firewall would leave it unprotected.

REFERENCES

5.2.4 DMZ Facts

q_dmz_firewall_secp7.question.fex

Question 5: ✓ Correct

How many network interfaces does a dual-homed gateway typically have?

- ➡ ● 3
- ○ 1
- ○ 2
- ○ 4

EXPLANATION

A dual-homed gateway is a firewall device that typically has three network interfaces: one connected to the internet, one connected to the public subnet, and one connected to the private network.

REFERENCES

5.2.4 DMZ Facts

q_dmz_homed_secp7.question.fex

Question 6: ✓ Correct

What needs to be configured on a firewall to allow traffic directed to the public resource in the DMZ?

○ FTP

○ Subnet

➡ ● Packet filters

○ VPN

EXPLANATION

Packet filters on the firewall allow traffic directed to the public resources inside the DMZ. Packet filters also prevent unauthorized traffic from reaching the private network.

A subnet is used to segment a network.

A VPN provides a secure outside connection to an internal network's resources. A VPN does not need to be configured on the firewall to allow traffic to the public resource in the DMZ.

FTP is a protocol used to transfer files. This does not need to be configured on the firewall to allow traffic to the public resource in the DMZ.

REFERENCES

- 3.1.1 Physical Security
- 3.1.2 Physical Security Facts
- 3.1.3 Implement Physical Security
- 3.2.4 Physical Network Protection Facts
- 5.2.4 DMZ Facts

q_dmz_packets_secp7.question.fex

Question 7: ✓ 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 inside the DMZ.
- ➡ ☑ Put the database server on the private network.
- □ Put the database server inside the DMZ.
- □ Put the web server on the private network.

EXPLANATION

Publicly accessible resources (servers) are placed inside the DMZ. Examples of publicly accessible resources include web, FTP, or 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

5.2.4 DMZ Facts

q_dmz_private_secp7.question.fex

▼ 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 to encrypt data sent between two hosts using the internet.
- ➡ ● You want to protect a public web server from attack.
- ○ You want internet users to see a single IP address when accessing your company network.

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. All publicly-accessible hosts are inside the DMZ. 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

5.2.4 DMZ Facts

q_dmz_public_secp7.question.fex

Question 9: ✓ Correct

Which of the following is another name for a firewall that performs router functions?

➡ ● Screening router

○ Dual-homed gateway

○ Screened-host gateway

○ Screened subnet

EXPLANATION

A firewall performing router functions is considered a screening router. A screening router is the router that is most external to your network and closest to the internet. It uses access control lists (ACLs) to filter packets as a form of security.

A dual-homed gateway is a firewall device that typically has three network interfaces: one connected to the internet, one connected to the public subnet, and one connected to the private network.

A screened-host gateway resides within the DMZ, requiring users to authenticate in order to access resources within the DMZ or the intranet.

A screened subnet uses two firewalls. The external firewall is connected to the internet and allows access to public resources. The internal firewall connects the screened subnet to the private network.

REFERENCES

5.2.4 DMZ Facts

q_dmz_screen_secp7.question.fex

▼ Question 10: ✓ Correct

Which of the following is the BEST solution to allow access to private resources from the internet?

➡ ● VPN

○ Subnet

○ Packet filters

○ FTP

EXPLANATION

A VPN provides a secure outside connection to an internal network's resources. A VPN server can be placed inside the DMZ. Internet users can be required to authenticate to the VPN server and then allowed communications from the VPN server to the private network. Only communications coming through the VPN server are allowed through the inner firewall.

Packet filters on the firewall allow traffic directed to a public resource inside the DMZ. Packet filters also prevent unauthorized traffic from reaching the private network. Packet filters won't allow access to private resources from the internet.

A subnet is used to segment a network.

File Transfer Protocol (FTP) is a protocol used to transfer files. This does not allow access to private resources from the internet.

REFERENCES

☰ 5.2.4 DMZ Facts

q_dmz_vpn_secp7.question.fex