

Exam Report: 13.7.6 Practice Questions

Date: 12/2/2019 11:41:30 am
Time Spent: 7:18

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 92%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

A group of salesmen in your organization would like to access your private network through the internet while they are traveling. You want to control access to the private network through a single server.

Which solution should you implement?

☐ IPS

☐ RADIUS

☐ DMZ

☐ IDS

➡ ☒ VPN concentrator

Explanation

With a remote access VPN, a server on the edge of a network (called a VPN concentrator) is configured to accept VPN connections from individual hosts. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

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 RADIUS server is used to centralize authentication, authorization, and accounting for multiple remote access servers. However, clients still connect to individual remote access servers.

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 13.7.
[netpro18v5_all_questions_en.exm NP09_6-1 #MCS5]

▼ Question 2: Correct

A salesperson in your organization spends most of her time traveling between customer sites. After a customer visit, she must complete various managerial tasks, such as updating your organization's order database.

Because she rarely comes back to your home office, she usually accesses the network from her notebook computer using Wi-Fi access provided by hotels, restaurants, and airports.

Many of these locations provide unencrypted public Wi-Fi access, and you are concerned that sensitive data could be exposed. To remedy this situation, you decide to configure her notebook

to use a VPN when accessing the home network over an open wireless connection. Which key steps should you take when implementing this configuration? (Select two.)

- ☐ Configure the VPN connection to use PPTP.
- ➔ ☒ Configure the browser to send HTTPS requests through the VPN connection.
- ➔ ☒ Configure the VPN connection to use IPsec.
- ☐ Configure the browser to send HTTPS requests directly to the Wi-Fi network **without** going through the VPN connection.
- ☐ Configure the VPN connection to use MS-CHAPv2.

Explanation

It is generally considered acceptable to use a VPN connection to securely transfer data over an open Wi-Fi network. As long as strong tunneling ciphers and protocols are used, the VPN provides sufficient encryption to secure the connection, even though the wireless network itself is not encrypted. It is recommended that you use IPsec or SSL to secure the VPN, as these protocols are relatively secure. You should also configure the browser's HTTPS requests go through the VPN connection. To conserve VPN bandwidth and to improve latency, many VPN solutions automatically reroute web browsing traffic through the client's default network connection instead of through the VPN tunnel. This behavior would result in HTTP/HTTPS traffic being transmitted over the unsecure open wireless network instead of through the secure VPN tunnel.

Avoid using PPTP with MS-CHAPv2 in a VPN over open wireless configuration, as these protocols are no longer considered secure.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm RT-SP-6.9-1]

▼ Question 3: Correct

A VPN is used primarily for which purpose?

- ☐ Support the distribution of public web documents.
- ☐ Allow remote systems to save on long-distance charges.
- ➔ ☒ Support secured communications over an untrusted network.
- ☐ Allow the use of network-attached printers.

Explanation

A VPN (virtual private network) is used primarily to support secured communications over an untrusted network. A VPN can be used over a local area network, across a WAN connection, over the internet, and even between a client and a server over a dial-up connection through the internet. All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm NP05_2-16 #7]

▼ Question 4: Correct

You want to use a protocol that can encapsulate other LAN protocols and carry the data securely over an IP network. Which of the following protocols is suitable for this task?

- ☐ NetBEUI
- ☐

☐ SLIP
☐ PPP

➡ ☒ PPTP

Explanation

PPTP is used with VPNs, which allow you to send data securely over a public network.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm NP05_2-16 #40]

▼ Question 5: Correct

Which of the following protocols can your portable computer use to connect to your company's network via a virtual tunnel through the internet? (Select two.)

➡ ☒ PPTP

➡ ☒ L2TP

☐ PPPoE

☐ VNC

☐ ICA

Explanation

PPTP (point-to-point tunneling protocol) or L2TP (layer two tunneling protocol) are two VPN (virtual private networking) protocols that let you access your company's network through a public network such as the internet.

PPPoE is used for connecting to the internet through an Ethernet connection to include authentication and accounting. VNC and ICA are remote desktop protocols used for remote administration or remote access.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm NP05_2-17 #32]

▼ Question 6: Correct

IPsec is implemented through two separate protocols. What are these protocols called? (Select two.)

➡ ☒ AH

☐ EPS

➡ ☒ ESP

☐ L2TP

☐ SSL

Explanation

IPsec is implemented through two separate protocols, IP Authentication Header and IPsec Encapsulating Security Payload. IPsec AH provides authentication and non-repudiation services to verify that the sender is genuine and the data has not been modified in transit. IPsec ESP provides data encryption services for the data within the packet.

IPsec SSL and IPsec EPS are not protocols associated with IPsec.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm NP05_2-17 #49]

▼ Question 7: Incorrect

Which of the following network layer protocols provides authentication and encryption services for IP-based network traffic?

- ☐ TCP
- ☐ L2TP
- ☒ ~~SSL~~

➡ ☐ IPsec

Explanation

IPsec is a security implementation that provides security for all other TCP/IP based protocols that operate above the network layer. IPsec provides authentication through a protocol called IPsec authentication header (AH) and encryption services through a protocol called IPsec encapsulating security payloads (ESP)

The transmission control protocol (TCP) is a transport layer connection-oriented protocol that provides data transmission services. It is not a secure protocol and relies on other measures, such as IPsec, to provide security. The Secure Sockets Layer (SSL) is an application layer protocol that is designed to secure network traffic from certain other protocols, such as hypertext transfer protocol (HTTP) and post office protocol version 3 (POP3). It does not provide security for protocols lower in the TCP/IP protocol stack, such as TCP and UDP. The Layer 2 tunneling protocol (L2TP) is a protocol used to encapsulate point-to-point protocol (PPP) traffic.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm NP05_2-17 #66]

▼ Question 8: Correct

Which of the following statements about SSL VPN are true? (Select two.)

- ➡ ☒ Encrypts the entire communication session.
- ☐ Encapsulates packets by adding a GRE header.
- ☐ Uses pre-shared keys for authentication.
- ☐ Uses UDP port 500.
- ➡ ☒ Uses port 443.
- ☐ Provides message integrity using HMAC.

Explanation

SSL VPN uses the SSL protocol to secure communications. SSL VPN:

- Authenticates the server to the client using public key cryptography and digital certificates.
- Encrypts the entire communication session.
- Uses port 443, which is already open on most firewalls.

Pre-shared keys are used by IPsec to provide authentication with other protocols. IPsec also uses HMAC to provide message integrity checks. GRE headers are used exclusively by the GRE tunneling protocol. UDP port 500 is used by the Layer 2 tunneling protocol (L2TP).

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm *NP15_REMOTE_ACCESS_SECURITY_01]

▼ Question 9: Correct

Which of the following can route Layer 3 protocols across an IP network?

- ☐ PTPP
- ☐ IPsec
- ☐ SSL

➡ ☒ GRE

Explanation

Generic routing encapsulation (GRE) is a tunneling protocol that creates a tunnel between two routers. It does this by adding a GRE header and a new IP header to the original packet.

IPsec, PTPP, and SSL are all authentication protocols that are used to secure communications.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm *NP15_REMOTE_ACCESS_SECURITY_02]

▼ Question 10: Correct

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the website. The two hashes match. What do you know about the file?

- ☐ You can prove the source of the file.
- ☐ No one has read the file contents as it was downloaded.
- ➡ ☒ Your copy is the same as the copy posted on the website.
- ☐ You will be the only one able to open the downloaded file.

Explanation

A hash is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. The sender and the receiver use the same hashing algorithm on the original data. If the hashes match, then the data can be assumed to be unmodified.

Hashes do not ensure confidentiality (in other words, hashes are not used to encrypt data). Non-repudiation proves the source of a file and is accomplished using digital signatures.

References

LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm SP08_5-2 2]

▼ Question 11: Correct

Which of the following networking devices or services prevents the use of IPsec in most cases?

- ➡ ☒ NAT
- ☐ Router
- ☐ Switch
- ☐ Firewall

Explanation

IPsec cannot typically be used when static IP addresses are not used by both communication partners. NAT proxy performs network address translation on all communications. For this reason, the IP address seen for a system outside of the proxied network is not the real IP address of that system. This prevents the use of IPsec.

IPsec can be deployed without problems with the presence of firewalls, routers, and switches. However, in the case of firewalls, special access ports will need to be configured to allow IPsec traffic to pass.

References


LabSim for Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm SP02_2-1 [134]]

▼ Question 12: Correct

A group of salesmen in your organization would like to access your private network through the internet while they are traveling. You want to control access to the private network through a single server.

Which solution should you implement?

- ☐ IPS
-  ☒ VPN concentrator
- ☐ DMZ
- ☐ IDS
- ☐ RADIUS

Explanation

If you are using a remote access VPN, a server on the edge of a network (called a VPN concentrator) is configured to accept VPN connections from individual hosts. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

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 RADIUS server is used to centralize authentication, authorization, and accounting for multiple remote access servers. However, clients still connect to individual remote access servers.

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 Network Pro, Section 13.7.

[netpro18v5_all_questions_en.exm NP09_6-1 MCS5]