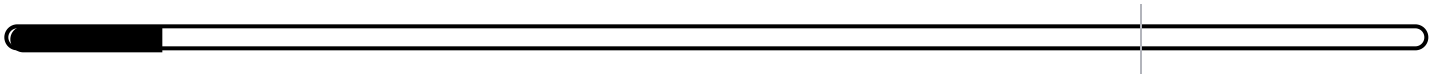
Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 7:49:10 pm • Time spent: 00:14

Score: 10%

Passing Score: 80%



Question 1: ✕ Incorrect

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
- [x] Configure the browser to send HTTPS requests through the VPN connection
- [ ] 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 IPsec
- [x] ~~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 to go through the VPN connection. To conserve VPN bandwidth and 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 though 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

5.5.6 VPN Facts

q_vpn_config_secp7.question.fex

Question 2: ✕ Incorrect

A group of salesmen would like to remotely 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~~
- IDS
- DMZ
- 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 it does not take action to stop or prevent an 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

5.5.6 VPN Facts

q_vpn_remote_secp7.question.fex

Question 3: ✕ Incorrect

A VPN is primarily used for which of the following purposes?

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

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 internet connection. All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

REFERENCES

5.5.6 VPN Facts

q_vpn_secure_secp7.question.fex

Question 4: ✔ Correct

Which VPN implementation uses routers on the edge of each site?

- Always-on VPN
- Remote access VPN
- Site-to-site VPN
- Host-to-host VPN

EXPLANATION

A site-to-site VPN uses routers on the edge of each site. The routers are configured for a VPN connection and encrypt and decrypt the packets being passed between the sites. With this configuration, individual hosts are unaware of the VPN.

A host-to-host VPN allows an individual host connected to the internet to establish a VPN connection to another host on the internet. Both devices must be configured for a VPN connection and have the software to encrypt and encapsulate the packets.

A remote access VPN uses a server (called a VPN concentrator) configured to accept VPN connections from individual hosts.

An always-on VPN employs the concept that a user is always on the VPN, whether physically within the LAN or remotely. There is no turning it on or off. All traffic is basically fully tunneled.

REFERENCES

5.5.6 VPN Facts

q_vpn_site_secp7.question.fex

Question 5: ✕ Incorrect

Which VPN tunnel style routes only certain types of traffic?

- Site-to-site
- Split
- Full
- Host-to-host

EXPLANATION

A VPN split tunnel routes only certain types of traffic, usually determined by destination IP address, through the VPN tunnel. All other traffic is passed through the normal internet connection.

A full VPN tunnel routes all of a user's network traffic through the VPN tunnel. This can sometimes send traffic that is not necessary.

A site-to-site VPN is a VPN implementation that uses routers on the edge of each site.

A host-to-host VPN implementation allows an individual host connected to the internet to establish a VPN connection to another host on the internet.

REFERENCES

5.5.6 VPN Facts

q_vpn_split_secp7.question.fex

Question 6: ✕ Incorrect

Which IPSec subprotocol provides data encryption?

- SSL
- AH
- ESP
- AES

EXPLANATION

Encapsulating Security Payload (ESP) Protocol provides data encryption for IPSec traffic.

Authentication Header (AH) provides message integrity through authentication, verifying that data is received unaltered from the trusted destination. AH provides no privacy and is often combined with ESP to achieve integrity and confidentiality.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_esp_01_secp7.question.fex

Question 7: ✕ Incorrect

In addition to Authentication Header (AH), IPsec is comprised of what other service?

- Advanced Encryption Standard (AES)
- ➡ Encapsulating Security Payload (ESP)
- Extended Authentication Protocol (EAP)
- Encryption File System (EFS)

EXPLANATION

IPsec is comprised of two services. One service is named Authentication Header (AH), and the other named Encapsulating Security Payload (ESP). AH is used primarily for authenticating the two communication partners of an IPsec link. ESP is used primarily to encrypt and secure the data transferred between IPsec partners. IPSec employs ISAKMP for encryption key management.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_esp_02_secp7.question.fex

Question 8: ✕ Incorrect

Which statement BEST describes IPsec when used in tunnel mode?

- IPsec in tunnel mode may not be used for WAN traffic
- Packets are routed using the original headers, and only the payload is encrypted
- ➡ The entire data packet, including headers, is encapsulated
- The identities of the communicating parties are not protected

EXPLANATION

When using IPsec in tunnel mode, the entire data packet, including original headers, is encapsulated. New encrypted packets are created with headers indicating only the endpoint addresses. Tunneling protects the identities of the communicating parties and original packet contents. Tunneling is frequently used to secure traffic traveling across insecure public channels, such as the internet. IPsec in tunnel mode is the most common configuration for gateway-to-gateway communications.

In transport mode, routing is performed using the original headers; only the packet's payload is encrypted. Transport mode is primarily used in direct host-to-host communication outside of a dedicated IPsec gateway/firewall configuration.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_ipsec_secp7.question.fex

Question 9: ✕ Incorrect

Which VPN protocol typically employs IPsec as its data encryption mechanism?

- PPP
- L2TP
- PPTP
- L2F

EXPLANATION

L2TP (Layer 2 Tunneling Protocol) is the VPN protocol that typically employs IPsec as its data encryption mechanism. L2TP is the recommended VPN protocol to use on dial-up VPN connections.

PPTP and PPP only support CHAP and PAP for data encryption. L2F offers no data encryption.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_l2tp_secp7.question.fex

Question 10: ✕ Incorrect

Which of the following VPN protocols is no longer considered secure?

- PPTP
- IPsec
- SSL
- TLS

EXPLANATION

Point-to-Point Tunneling Protocol (PPTP) was one of the first VPN protocols and was developed by Microsoft. It is no longer considered secure and is essentially obsolete.

Internet Protocol Security (IPsec) provides authentication and encryption, and it can be used in conjunction with L2TP or by itself as a VPN solution. IPSec is still considered very secure.

The Secure Sockets Layer (SSL) Protocol has long been used to secure traffic generated by other IP protocols, such as HTTP, FTP, and email. SSL can also be used as a VPN solution, typically in a remote access scenario.

Transport Layer Security (TLS) Protocol works in a similar way to SSL, even though they are not interoperable.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_pptp_secp7.question.fex