15.11.4 Practice Questions

Candidate: Ethan Bonavida (suborange)

Date: 12/9/2022 12:40:54 am • **Time Spent:** 00:22

Score: 100%

Passing Score: 80%

▼ **Question 1:** ✓ Correct

Which of the following provides security for datagram-based applications by allowing them a communication method designed to prevent eavesdropping, tampering, and message forgery?

○ IPSec

➡ ● DTLS

○ NAT

○ Transport mode

Explanation

DTLS is based on the TLS protocol and provides security for datagram-based applications by allowing them to a communication method designed to prevent eavesdropping, tampering, and message forgery.

NAT provides network address translation.

Internet Protocol Security (IPSec), is an extension to the IP protocol that, like SSL, also secures sessions between computers by validating and encrypting the packets of data that are sent across a network.

Transport mode is an IPSec mode that encapsulates and encrypts IP packets through a VPN tunnel.

References

15.11.1 VPN Access and Authentication

15.11.2 Configuring VPN Access and Authentication

15.11.3 VPN Access and Authentication Facts

q_vpn_lp5_dtls.question.fex

▼ Question 2: ✓ Correct

Carlos, a system administrator, needs to set up a VPN tunnel from a branch office to the main office. Data security is a high priority.

Which of the following will allow the IP packets to be encrypted and encapsulated in a new IP header that is sent through the VPN tunnel?

○ VNC

○ DTLS

➡ ● IPSec

○ NAT

Explanation

Internet Protocol Security (IPsec) is an extension to the IP protocol that, like SSL, also secures sessions between computers by validating and encrypting the packets of data that are sent across a network.

VNC allows you to connect to and control a remote computer. It can transmit the keyboard and mouse events from the remote server back to the client computer.

DTLS is based on the TLS protocol and provides security for datagram-based applications by allowing them a communication method designed to prevent eavesdropping, tampering, and message forgery.

NAT provides network address translation.

References

15.11.1 VPN Access and Authentication

15.11.2 Configuring VPN Access and Authentication

15.11.3 VPN Access and Authentication Facts

q_vpn_lp5_ipsec.question.fex

Question 3: ✓ Correct

Which of the following is a key difference between VPN tunnel and transport modes?

➡ ● With transport mode, only the payload of the IP packet is encrypted, and the original IP headers are left intact.

○ Transport mode only provides unencrypted data because the connection is secure.

○ Only tunnel mode is provided by IPSec.

○ Tunnel mode provides lower overhead.

Explanation

With transport mode, only the payload of the IP packet is encrypted, and the original IP headers are left intact. With tunnel mode, the entire original IP packet is protected by IPSec, meaning that IPSec wraps and encrypts the original packet and then adds a new IP header, which is then sent on to the other side of the VPN tunnel.

Both tunnel and transport are IPSec modes.

Transport mode provides lower overhead because it only encrypts the payload of the IP packet.

Transport mode encrypts the payload of the IP packet.

References

15.11.1 VPN Access and Authentication

15.11.2 Configuring VPN Access and Authentication

15.11.3 VPN Access and Authentication Facts

q_vpn_lp5_modes.question.fex

▼ Question 4: ✓ Correct

Which of the following virtual private networks (VPNs) utilizes digital certificates to ensure that only the intended recipients can view and use the data sent?

○ DTLS

➡ ● SSL/TLS

○ IPSec Transport

○ IPSec Tunnel

Explanation

An SSL VPN is a type of virtual private network that uses the SSL protocol or the Transport Layer Security (TLS) protocol to provide secure remote-access VPN capability.

Secure Sockets Layer (SSL) and the more commonly used Transport Layer Security (TLS) are the standard technology used for keeping an internet connection secure. They encrypt the data sent between systems and use digital certificates to ensure that only the intended recipients can view and use the data sent.

References

▷ **15.11.1 VPN Access and Authentication**

15.11.2 Configuring VPN Access and Authentication

☰ **15.11.3 VPN Access and Authentication Facts**

q_vpn_lp5_ssl.question.fex

Question 5: ✓ Correct

Maria, a user, is working remotely from a hotel while traveling for business. Maria needs to access some sales resources on the company's network.

Which of the following would allow Maria to securely access the resources she needs?

○ Telnet

➡ ● VPN

○ IP Header

○ NAT

Explanation

VPN will allow a secure connection from a remote location to the company's network.

Telnet is not secure and should not be used to access company resources.

NAT provides network address translation.

An IP header is part of an IP packet.

References

▷ **15.11.1 VPN Access and Authentication**

15.11.2 Configuring VPN Access and Authentication

☰ **15.11.3 VPN Access and Authentication Facts**

q_vpn_lp5_vpn.question.fex