Module Practice and Quiz

8.4.1

What did I learn in this module?

A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network. A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network. Benefits of VPNs are cost savings, security, scalability, and compatibility. VPNs are commonly deployed in one of the following configurations: site-to-site or remote-access. VPNs can be managed and deployed as enterprise VPNs and service provider VPNs.

Remote-access VPNs let remote and mobile users securely connect to the enterprise by creating an encrypted tunnel. Remote access VPNs can be created using either IPsec or SSL. When a client negotiates an SSL VPN connection with the VPN gateway, it actually connects using TLS. SSL uses the public key infrastructure and digital certificates to authenticate peers. Site-to-site VPNs are used to connect networks across an untrusted network such as the internet. In a site-to-site VPN, end hosts send and receive normal unencrypted TCP/IP traffic through a VPN terminating device. The VPN terminating device is typically called a VPN gateway. A VPN gateway could be a router or a firewall. GRE is a non-secure site-to-site VPN tunneling protocol. DMVPN is a Cisco software solution for easily building multiple, dynamic, scalable VPNs. Like DMVPNs, IPsec VTI simplifies the configuration process required to support multiple sites and remote access. IPsec VTI configurations are applied to a virtual interface instead of static mapping the IPsec sessions to a physical interface. IPsec VTI can send and receive both IP unicast and multicast encrypted traffic. MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider. There are two types of MPLS VPN solutions supported by service providers, Layer 3 MPLS VPN and Layer 2 MPLS VPN.

IPsec protects and authenticates IP packets between source and destination. IPsec can protect traffic from Layer 4 through Layer 7. Using the IPsec framework, IPsec provides confidentiality, integrity, origin authentication, and Diffie-Hellman. Choosing the IPsec protocol encapsulation is the first building block of the framework. IPsec encapsulates packets using AH or ESP. The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm. The HMAC is an algorithm that guarantees the integrity of the message using a hash value. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. A PSK value is entered into each peer manually. The PSK is combined with other information to form the authentication key. RSA authentication uses digital certificates to authenticate the peers. The local device derives a hash and encrypts it with its private key. The encrypted hash is attached to the message and is forwarded to the remote end and acts like a signature. DH provides a way for two peers to establish a shared secret key that only they know, even though they are communicating over an insecure channel.

8.4.2

Module Quiz - VPN and IPsec Concepts

1. Which two statements describe a remote access VPN? (Choose two.)

- [x] It may require VPN client software on hosts.
- [ ] It requires static configuration of the VPN tunnel.
- [x] It is used to connect individual hosts securely to a company network over the Internet.
- [ ] It requires hosts to send TCP/IP traffic through a VPN gateway.
- [ ] It connects entire networks to each other.

2. The use of 3DES within the IPsec framework is an example of which of the five IPsec building blocks?

- ( ) nonrepudiation
- ( ) integrity
- ( ) authentication
- (•) confidentiality
- ( ) Diffie-Hellman

3. Which type of VPN may require the Cisco VPN Client software?

- ( ) SSL VPN
- (•) remote access VPN
- ( ) site-to-site VPN
- ( ) MPLS VPN

4. Which technique is necessary to ensure a private transfer of data using a VPN?

- ( ) authorization
- ( ) virtualization
- ( ) scalability
- (•) encryption

5. What are the two fundamental Dynamic Multipoint VPN tunnel types? (Choose two.)

- [x] hub-to-spoke
- [x] spoke-to-spoke
- [ ] server-to-client
- [ ] site-to-site
- [ ] client-to-site

6. What are two reasons a company would use a VPN? (Choose two.)

- [ ] to test network connections to remote users
- [ ] to eliminate the need of having a gateway
- [x] to connect remote users to the network
- [ ] to increase bandwidth to the network
- [x] to allow suppliers to access the network

7. True or False?
All VPNs securely transmit clear text across the Internet.

- (•) false
- ( ) true

8. Which solution allows workers to telecommute effectively and securely?

- ( ) dial-up connection
- ( ) DSL connection
- (•) remote-access VPN
- ( ) site-to-site VPN

9. Which VPN type is a service provider managed VPN?

- (•) Layer 3 MPLS VPN
- ( ) GRE over IPsec VPN
- ( ) remote access VPN
- ( ) site-to-site VPN

10. Which IPsec framework protocol provides data integrity and data authentication, but does not provide data confidentiality?

- (•) AH
- ( ) ESP
- ( ) DH
- ( ) IP protocol 50

11. What algorithm is used to provide data integrity of a message through the use of a calculated hash value?

- ( ) AES
- ( ) DH
- (•) HMAC
- ( ) RSA

12. Which statement describes the effect of key length in deterring an attacker from hacking through an encryption key?

- (•) The longer the key, the more key possibilities exist.
- ( ) The length of a key will not vary between encryption algorithms.
- ( ) The shorter the key, the harder it is to break.
- ( ) The length of a key does not affect the degree of security.

13. What is a type of VPN that is generally transparent to the end user?

- ( ) private
- (•) site-to-site
- ( ) remote access
- ( ) public

Check

Show Me

Reset