13.7.2 VPN Facts

A virtual private network (VPN) is a type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. A VPN is used primarily to support secure communications over an untrusted network.

- VPNs work by using a tunneling protocol that encrypts packet contents and wraps them in an unencrypted packet.
- Tunnel endpoints are devices that can encrypt and decrypt packets. When you create a VPN, you establish a security association between the two tunnel endpoints. The endpoints create a secure virtual communication channel. Only the destination tunnel endpoint can unwrap packets and decrypt the packet contents.
- Routers use the unencrypted packet headers to deliver the packet to the destination device. Intermediate routers along the path cannot read the encrypted packet contents.
- A VPN can be used over a local area network, across a WAN connection, over the internet, and even over a dial-up connection.
- VPNs can be implemented in the following ways:
  - With a *host-to-host* VPN, two hosts establish a secure channel and communicate directly. With this configuration, both devices must be capable of creating the VPN connection.
  - With a *site-to-site* VPN, routers on the edge of each site establish a VPN with the router at the other location. Data from hosts within the site are encrypted before being sent to the other site. With this configuration, individual hosts are unaware of the VPN.
  - 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 in a *client-to-site* configuration. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

Common VPN Tunneling Protocols

The following table describes the most common VPN tunneling protocols.

Protocol	Description
Point-to-Point Tunneling Protocol (PPTP)	PPTP was developed by Microsoft as one of the first VPN protocols. PPTP: - Uses standard authentication protocols such as CHAP and PAP. - Supports TCP/IP only. - Encapsulates other LAN protocols and carries the data securely over an IP network. - Uses MPPE for data encryption. - Is supported by most operating systems and servers. - Uses TCP port 1723.
Layer 2 Tunneling Protocol (L2TP)	L2TP is an open standard for secure multi-protocol routing. L2TP: - Supports multiple protocols (not just IP). - Uses IPsec for encryption. - Is not supported by older operating systems. - Uses TCP port 1701 and UDP port 500.

Internet Protocol Security (IPsec)	IPsec provides authentication and encryption, and it can be used in conjunction with L2TP or by itself as a VPN solution. IPsec includes the following three protocols for authentication, data encryption, and connection negotiation:
	- Authentication Header (AH), which enables authentication with IPsec.
	  - AH provides a message integrity check with the keyed-hash message authentication code (HMAC). With HMAC, a symmetric key is embedded into a message before the message is hashed. When the message is received, the recipient's symmetric key is added back into the message before the message is hashed. If the hash values match, message integrity is proven.
	  - AH uses SHA-1 (secure hashing algorithm 1) or MD5 (message digest v5) for integrity validation.
	  - AH by itself does not provide data encryption.
	- Encapsulating security payload (ESP), which provides data encryption.
	- Internet Key Exchange (IKE), which negotiates the connection. As two end points secure an IPsec network, they have to negotiate what is called a security association (SA). An inbound and outbound SA is necessary for each connection with a remote endpoint. IKE uses the Diffie-Hellman key exchange to generate symmetric keys used for the encryption of the negotiation of the SA.
	
	IPsec can be used to secure the following types of communications:
	- Host-to-host communications within a LAN.
	- VPN communications through the internet, either by itself or in conjunction with the L2TP VPN protocol.
	- Any traffic supported by the IP protocol, including web, email, Telnet, file transfer, SNMP traffic, and countless others.
	
	IPsec uses either digital certificates or pre-shared keys.

	In most cases, IPsec cannot be used used with NAT. This is because when NAT modifies the source or destination address of a packet, it affects the hash value of the AH and causes a checksum failure.
Generic Routing Encapsulation (GRE)	GRE is a tunneling protocol that was developed by Cisco. GRE can be used to route any Layer 3 protocol across an IP network. GRE: ▪ Creates a tunnel between two routers. ▪ Encapsulates packets by adding a GRE header and a new IP header to the original packet. ▪ Does not offer any type of encryption. ▪ Can be paired with other protocols, such as IPsec or PPTP, to create a secure VPN connection.
Secure Sockets Layer (SSL)	The SSL protocol has long been used to secure traffic generated by IP protocols such as HTTP, FTP, and email. SSL can also be used as a VPN solution, typically in a remote access scenario. SSL: ▪ 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. Implementations that use SSL for VPN tunneling include Microsoft's SSTP and Cisco's SSL VPN.
Transport Layer Protocol (TLS)	TLS ensures that messages being transmitted on the internet are private and tamper proof. TLS is a new version of SSL and is used to increase security by encrypting data using public key cryptography. TLS is implemented through two protocols: ▪ TLS record can provide connection security with encryption (with DES for example). ▪ TLS handshake provides mutual authentication and choice of encryption method.
Datagram Transport Layer Security (DTLS)	DTLS is a communication protocol similar to SSL and TLS. DTLS: ▪ Focuses on datagram-based applications. ▪ Allows applications to communicate preventing eavesdropping and tampering. ▪ Is based on the TLS protocol and provides similar security guarantees.
Dynamic Multipoint Virtual Private Network (DMVPN)	DMVPN allows more than one connection through a VPN. ▪ Its infrastructure consists of a hub with multiple spokes that connect to reach the company site. ▪ The spokes also have the ability to communicate with one another via a dynamic IPsec VPN tunnel.

You should be aware that ports must be open in firewalls to allow VPN protocols. For this reason, using SSL for the VPN often works through firewalls when other solutions do not. Additionally, some NAT solutions do not work well with VPN connections.