5.7.6 VPN Facts

A Virtual Private Network (VPN) is a remote access connection that uses encryption to securely send data over an untrusted network. By using a VPN, you can take advantage of an existing internet connection to securely communicate between devices.

- A VPN provides an alternative to:
  - WAN connections
  - Connections that use telephone lines and a remote access server
- VPNs work by using a *tunneling* protocol that encrypts packet contents and encapsulates those packets.
  - The encapsulated packets are routed through the internet using the information in the packet header.
  - When the packet reaches the destination device, the outer wrapping encapsulating the packets and the encryption is removed.
  - Only the destination device is allowed to remove the wrapping and restore the packet to its original form.
- The following are two styles of VPN Tunnels commonly used:
  - Full tunnel, which routes all of a user's network traffic through the VPN tunnel. This can sometimes send traffic that is not necessary over the tunnel.
  - Split tunnel, which 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.
- VPNs can be implemented in the following ways:
  - 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 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 remote access VPN uses a server (called a VPN concentrator) configured to accept VPN connections from individual hosts.
    - The VPN concentrator is located on the edge of a network.
    - The VPN concentrator establishes multiple connections with multiple hosts.
    - The individual hosts must be able to establish a VPN connection.
    - The hosts can access resources on the VPN server or the private network using the VPN connection.
  - An *always-on* VPN employs the concept that a user is always on VPN, whether physically within the LAN or remotely. There is no turning it on or off. All traffic is basically fully tunneled.
- 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. These endpoints create a secure virtual communication channel. Only the destination tunnel endpoint can unwrap packets and decrypt the packet contents.
- Routers use the decrypted packet headers to deliver the packet to the destination device. Intermediate routers along the path cannot read the encrypted packet contents.

When implementing a VPN, be sure to:

- Select a protocol that is supported by all devices that need to encrypt and encapsulate packets.
- Open the appropriate ports to allow VPN traffic through the firewall.

VPNs can also be used to help secure connections made over open wireless networks. Many establishments, such as airports, hotels, and restaurants, provide unsecured public Wi-Fi access. Because encryption is not used to secure the wireless connection, many users are hesitant to use these networks. In most cases, this hesitancy is warranted; however, 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. Avoid using PPTP with MS-CHAPv2, as this configuration is no longer secure.

If you are using a VPN over an open wireless network and need to access a secure website, be sure your browser's HTTPS requests 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 insecure open wireless network instead of through the secure VPN tunnel.