Chapter 6 - Key Topics

Description	Element	Page	Summary
Clientless & client-based SSL VPNs	List	214	Point-to-Point Tunneling Protocol (PPTP) Layer 2 Forwarding (L2F) Protocol Layer 2 Tunneling Protocol (L2TP) Generic Routing Encapsulation (GRE) Multiprotocol Label Switching (MPLS) Internet Protocol Security (IPsec) Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
Remote-access VPNs & site-to-site VPNs	List	215	**Site-to-site VPNs** - Enable organizations to establish VPN tunnels between two or more network infrastructure devices in different sites so they can communicate over a share medium such as the internet. Examples, IPsec, GRE, & MPLS VPNs as site-to-site VPN protocols. **Remote-access VPNs** - Enable users to work from remote locations such as homes, hotels, & other premises as if they were connected to their corporate network.
The phases of IPsec	List	217	**Internet Key Exchange v1 (IKv1)** attributes exchanged - Encryption algorithms, Hashing algorithms, Diffie-Hellman groups, Authentication method, Vendor-specific attributes. **Encryption Algorithms in IPsec** - Data Encryption Standard (DES) - 64 bits, Triple DES (3DES) - 168 bits, Advanced Encryption Standard (AES) - 128 bits, AES 192 - 192 bits, AES 256 - 256 bits
Hashing Algorithms used in VPNs	List	217	Secure Message Algorithm (SHA), Message Digest Algorithm 5 (MD5)

Description	Element	Page	Summary
NAT-traversal (NAT-T)	Tip	220	Related to IPsec protocols Authentication Header (AH) and Encapsulating Security Payload (ESP). With NAT-T, VPN peers dynamically discover whether an address translation device exists between them. If NAT/PAT device is discovered they use UDP port 4500 to encapsulate data packets allowing NAT/PAT device to forward and translate packets.
IPsec Attributes	Table 6-2	220	**Encryption** - None, DES, 3DES, AES128, AES192, AES256 (AES recommended with higher key length) **Hashing** - MD5, SHA, null (SHA is recommended) **Identity information** - Network, protocol, port number **Lifetime** - 120-2,147,483,647 seconds, 10-2,147,483,647 kilobytes **Mode** - Tunnel or transport **Perfect Forward Secrecy (PFS) groups** - None, 1, 2, or 5
IKEv1 & IKEv2	List	223	**IKEv1 Exchange** - Phase 1 has two possible exchanges: main mode & aggressive mode. There is a single exchange of a message pair for IKEv2 IKE_SA. **IKEv1 Authentication** - Does not allow the use of Extensible Authentication Protocol (EAP), EAP allows IKEv2 to provide a solution for a remote-access VPN. **IKEv2 Exchange Efficiency** - Has a simple exchange of two message pairs for the CHILD_SA. IKEv1 has at least three message pairs for Phase 2. IKEv2 is designed to be more efficient than IKEv1 since fewer packets are exchanged. IKEv2 supports the use of next-generation encryption protocols and anti-DoS capabilities.
SSL VPN Technologies	List	226	Reverse proxy technology, Port-forwarding technology & smart tunnels, SSL VPN tunnel client (AnyConnect Secure Mobility Client), & Integrated terminal services.