9.10.7 IPsec Facts

IP security (IPsec) provides secure data transmission over unprotected TCP/IP networks, such as the internet. IPsec operates on OSI Layer 3, the network layer. It provides mutual authentication, integrity, nonrepudiation, and confidentiality.

IPsec includes two protocols:

Protocol	Function
Authentication Header (AH)	AH provides authenticity, non-repudiation, and integrity. AH: ▪ Does not provide confidentiality because the data in the packet is not encrypted. ▪ Provides protection against replay and man-in the-middle attacks. ▪ Uses a keyed hash based on all the bytes in the packet for the authentication information. ▪ Authenticates packets by digitally signing them. ▪ Uses IP Protocol 51.
Encapsulating Security Payload (ESP)	ESP provides all the security of AH plus confidentiality. ESP: ▪ Is the most commonly used IPsec protocol. ▪ Provides data encryption. ▪ Uses IP Protocol 50.

Whether you use AH or ESP, there are two modes of operation that can be implemented with IPsec:

- Transport mode, which encrypts only the payload (data).
- Tunnel mode, which encrypts the entire packet. Both the data inside the packet and the IP headers are encrypted. The entire packet is encapsulated in a new packet.

A *Security Association* (SA) is the establishment of shared security information between two network entities to support secure communications. An SA may include algorithm selection, cryptographic keys, and/or digital certificates. A security association can be established manually or automatically through a protocol called internet key exchange (IKE). IKE helps to establish automatic security association (SAs). IKE:

- Helps the two endpoints set up a secure tunnel by providing a secure exchange of shared keys before a full IPsec transmission begins.
- Uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived.
- Uses mutual authentication that is provided by either pre-shared keys on both endpoints or certificates issued by a CA.
- Can be implemented to automate the selection of the best security association for each connection.
- Uses UDP port 500.

Be aware of the following:

- IPsec is included in Windows Firewall with Advanced Security and is named Connection Security Rules.
- Network Address Translation (NAT) can cause communication errors with an IPsec VPN tunnel because it makes changes to the IP headers, such as changing source and destination IP addresses and ports. NAT-Traversal (NAT-T) is a new method designed to allow IPsec to function properly through a NAT device.
- IPsec tunnels are established in two phases, main mode and quick mode.

IPsec is most commonly used with L2TP VPNs.