6.3 IPSec

Internet Protocol Security (IPSec) is a technology used to create virtual private networks. IPSec is used in addition to the IP protocol that adds security and privacy to TCP/IP communication. IPSec is incorporated with Microsoft operating systems as well as many other operating systems.

For example, the security settings in the Internet Connection Firewall that ships with Windows XP and later versions enables users to turn on IPSec for transmissions. IPSec is a set of protocols developed by the IETF (Internet Engineering Task Force; www.ietf.org) to support secure exchange of packets. IPSec has been deployed widely to implement VPNs.

IPSec has two encryption modes: transport and tunnel. The transport mode works by encrypting the data in each packet but leaves the header unencrypted. This means that the source and destination addresses, as well as other header information, are not encrypted. The tunnel mode encrypts both the header and the data.

This is more secure than transport mode but it may slow down the process. On the receiving end, an IPSec-compliant device decrypts each packet. For IPSec to work, the sending and receiving devices must share a key, an indication that IPSec is a single-key encryption technology. IPSec also offers two other protocols besides the two modes that have already been described:

- **Authentication Header (AH):** The AH protocol provides a mechanism for authentication only. AH provides data integrity, data origin authentication, and an optional replay protection service. Data integrity is ensured by using a message digest that is generated by an algorithm such as HMAC-MD5 or HMAC-SHA. Data origin authentication is ensured by using a shared secret key to create the message digest.

- **Encapsulating Security Payload (ESP):** The ESP protocol provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection). ESP can be used with confidentiality only, authentication only, or both confidentiality and authentication.

Either protocol can be used alone to protect an IP packet, or both protocols can be applied together to the same IP packet.

IPSec can also work in two modes. Those modes are transport mode and tunnel mode. Transport mode is the mode where IPSec encrypts the data. However, the packet header is not encrypted. Tunnelling mode, on the other hand, does encrypt the header as well as the packet data.

There are other protocols involved in making IPSec work. IKE, or Internet Key Exchange, is used in setting up security associations in IPSec. A security association is formed by the two endpoints of the VPN tunnel. This takes place once it is decided how they are going to be encrypted and authenticated. For example, will they use AES for encrypting packets, what protocol will be used for key exchange, and what protocol will be used for authentication?

All of these issues are negotiated between the two endpoints, and the decisions are stored in a security association (SA). This is accomplished via the IKE protocol. Internet Key Exchange (IKE and IKEv2) is used to set up an SA by handling negotiation of protocols and algorithms and to generate the encryption and authentication keys to be used.

The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange. Once the IKE protocol sets up the SA, it signals that it is time to actually perform the authentication and key exchange.

The first exchange between VPN endpoints establishes the basic security policy; the initiator proposes the encryption and authentication algorithms it is willing to use. The responder chooses the appropriate proposal and sends it to the initiator. The next exchange passes Diffie-Hellman public keys and other data.

Those Diffie-Hellman public keys will be used to encrypt the data being sent between the two endpoints. The third exchange authenticates the ISAKMP session. This process is called main mode. Once the IKE SA is established, IPSec negotiation (Quick Mode) begins.

Quick Mode IPSec negotiation, or Quick Mode, is similar to an Aggressive Mode IKE negotiation, except negotiation must be protected within an IKE SA. Quick Mode negotiates the SA for the data encryption and manages the key exchange for that IPSec SA.

In other words, Quick Mode uses the Diffie-Hellman keys exchanged in main mode, to continue exchanging symmetric keys that will be used for actual encryption in the VPN.

Aggressive Mode squeezes the IKE SA negotiation into three packets, including all data required for the SA passed by the initiator. The responder sends the proposal, key material, and ID, and authenticates the session in the next packet. The initiator replies by authenticating the session. Negotiation is quicker, and the initiator and responder ID pass in the clear. (are given the green light)