IPSec (IP Security), What Makes it Work.

Roger W. Younglove, CISSP

Sr. Network Security Consultant, NetworkCare Security Services, Lucent Technologies

Businesses are giving a lot of attention to VPNs today because they allow replacement of traditional dial-up or leased lines with IP connections to more economically link branch offices and remote workers to corporate network resources. More importantly, by delivering cost-effective, secure communications services, VPNs enable businesses to engage with their partners, suppliers, and customers in ways never before possible.

VPNs require establishment of a tunnel (a technique for sending data packets securely over the Internet or other public network) into the corporate network and encryption of the data passing between end users and the corporate servers.

Two tunneling protocols are widely used today: *L2TP*, a network Layer 2 (Data Link Layer of the OSI model) protocol typically utilized by the SPs (Service Providers) to provide remote dialup VPN access for customers; and *IPSec*, a Layer 3 (Network Layer) protocol designed to allow data packets to be encrypted and encapsulated for secure transfer across an IP network. IPSec is typically used in enterprise networks, which is our area of interest in this article.

In a previous article we looked at some of the reasons for the popularity of VPNs, examined the technologies that make them work, and viewed IPSec from a high level. In this article we will give telecom managers, network planners and engineers a more detailed look at how IPSec works.

Evolution of IPSec

IPSec (RFC 2401), with additional RFCs 2402/2412 to codify the essential components, has become the de facto industry standard for an IP based VPN infrastructure. Widespread implementation is likely because of the requirements of higher levels of security required in Internet communications.

Following the successful pattern of other Internet services, IPSec developed organically over time. From the swIPe Experimental Protocol written in March, 1993, IPSec was defined as a mandatory protocol for IPv6 in July, 1994. RFCs 1825-29 were written in August, 1995, then superseded by the present RFCs in November, 1998.

Protocols For Security

IPSec as shown above is composed of a number of different pieces that together provide a set of security services. Those services include: access control, connectionless integrity, data origin authentication, protection against replays, confidentiality (encryption), and a limited traffic flow confidentiality.

These services are provided by two traffic security protocols—the Authentication Header (AH) and the Encapsulating Security Payload (ESP)—plus the use of cryptographic key management procedures and protocols. We just encountered two more acronyms—AH and ESP. Let's examine where they fit in IPSec.

Authentication Header (AH)

AH is protocol 51 and is the authentication mechanism used to ensure that the endpoint one thinks they are communicating with is truly correct. AH is algorithm independent, which means that AH will operate with the algorithm of choice, depending on the level of security required.

Currently the algorithm options are HMAC (Hashed Message Authentication Code) MD5 (Message Digest 5) or HMAC SHA1(Secure Hash Algorithm 1 - 96, FIPS-180-1). Optionally AH will, if selected, provide protection against replays (man-in-the-middle attacks) as long as the receiver checks the sequence numbers. AH authenticates all of the packet including the upper protocol data, with the exception of the destination address. AH can be used alone, when only authentication is required, or in combination with ESP when a higher level of security is required.

Encapsulating Security Payload (ESP)

ESP is protocol 50 and normally is used to provide encryption and limited traffic flow confidentiality. ESP is also designed to be algorithm independent and the options are: DES (64 bit, commonly called 56bit), 3DES, RC5, Blowfish, Idea, Cast and others are being added. Because DES and 3 DES are mandatory, we will delve into them.

DES, its common name, in ESP actually is DES-CBC (Data Encryption Standard-Cipher Black Chaining) with explicit IV (initialization vector) of 64 bits preceding the encrypted payload. Including the IV in each datagram ensures that decryption of each received datagram can be performed, even if some are dropped or reordered. It is common practice to use random data for the first IV and then the last 8 octets of encrypted data from the previous encryption for the next IV. This process has the advantage of

limiting the leakage of information from the random number generator.

DES is described in FIPS-46-2, FIPS-74 and FIPS-81. 3DES is actually the application of encrypting with DES, decrypting with DES and encrypting the same data with DES a second time. If a stronger form of encryption is required than DES or 3DES then one must review the individual vendor products offered.

It is true that 56 bit DES has been broken in less than 23 hours, but, as we'll see later, with the proper implementation DES can meet rigid security standards.

We've now looked at the two main requirements for an IPSec VPN, authentication and encryption, but how does it work?

Setting Up An IPSec Tunnel

Two databases are required to ensure proper operation of an IPSec client or gateway in the handling of both inbound and outbound IP traffic: a Security Policy Database (SPD), and a Security Association Database (SAD).

Security Policy Database (SPD). The SPD is constructed with the policies that specify what services are to be offered, i.e., what addresses have IPSec applied at what standard of security, and what addresses are passed through without IPSec.

Security Association Database (SAD). The SAD contains parameters associated with each Security Association (SA) that has been determined with the SPD. A Security Association is a "connection" that affords security services to the traffic it carries. Three things found in the Ethernet packet comprise the SA: a Security Parameter Index (SPI), a Destination IP Address, and a security protocol identifier.

Prior to the issuance of the first IPSec communication, all of this SPD and SAD information is entered into the IPSec endpoint (client or gateway). Currently all of this information must be entered into both ends of the IPSec VPN. However, as the implementation of IPSec evolves, the desire is to enter the SPD only.

Now that the information required to set up an IPSec tunnel is in place, what happens next?

Negotiating Authentication of the Endpoints

A client initiates a data transmission that will be transmitted by IPSec to a server.

The client (IP address 175.37.25.15) sends a packet to the server (192.37.58.25). That packet is directed to IPSec gateway1 (IP address 175.37.25.2) that has been instructed by the SPD that the server (192.37.58.25) can be found behind IPSec gateway2 (192.37.58.2). These two gateways start negotiations with a pre-shared key or digital certificates (PKI) using IKE (Internet Key Exchange).

IKE is a hybrid protocol, combining parts of Oakley (describes a series of key exchanges called "modes") and parts of SKEME (a forerunner protocol to IPSec) with ISAKMP [Internet Security Association & Key Management Protocol (a framework for authentication)]. IKE is used to negotiate and derive keying material for security associations in a secure and authenticated manner.

Within the IKE framework, three modes of negotiation can be used:

- **Main Mode**
  uses an exchange of six (6) different messages between the two IPSec endpoints to complete negotiation of authentication of the endpoints and keying material. This negotiation, if required, will provide Perfect Forward Secrecy (PFS), which means that, after the first two messages are exchanged, subsequent communication is protected.

- **Aggressive Mode**
  authenticates the endpoints with only three messages, but it does not provide PFS. Moreover, SA negotiation is limited with Aggressive Mode.

- **Quick Mode**
  is used after the tunnel is established to regenerate fresh key material for encryption purposes—it does not authenticate the endpoints. The new key data is used to encrypt subsequent communications data, which is why we indicated earlier that 56 bit DES is often strong enough. Here is what happens: Main Mode negotiation takes place with PFS hiding the negotiation of the first encryption hash and setting the tunnel. Once that's established, Quick Mode can be run as often as desired. Because this negotiation all occurs in a tunnel, as long as Quick Mode is run every 30 minutes, if someone breaks the tunnel and acquires the encrypted data stream, a maximum of 30 minutes of data may be compromised.

After negotiations are completed, communication between the client (IP address 175.37.25.15) and the server (IP address 192.37.58.25) takes place encrypted, with whatever encryption algorithm desired, in an authenticated tunnel. When the communication is complete, the tunnel is torn down.

Depending on the type of endpoints involved, IPSec operates in one of two methods: transport and tunnel. If the implementation is between two clients, the method is *transport*, which means the clients hold the SAs and perform the mode negotiation and form tunnels between themselves. Whereas, if one or both endpoints are gateways, then *tunnel* mode is used, meaning that the communication comes to, and leaves from, the gateways unencrypted.

Only the gateways have a tunnel and encrypted data between them. The only time a gateway would operate in transport mode is if a client was communicating with it for network management.

Secure Communications Into The Future

IPSec was developed by a group of individuals that make up the IETF IPSec workgroup to provide the telecommunications world with a secure method to communicate. As authorization and encryption algorithms become stronger, so does IPSec. It is important to remember that IPSec is only as strong as the algorithms chosen by individuals for its implementation—it all boils down to human choices. However, in my opinion, IPSec will take us well into the 21 century.