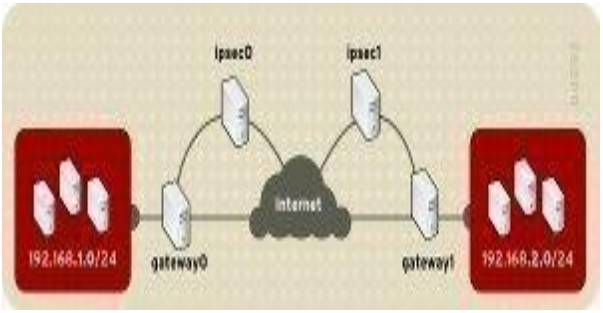
IPsec

IPSec (IP Security) is a suite of protocols which was designed by Internet Engineering Task Force (IETF) to protect data by signing and encrypting data before it is transmitted over public networks. The IETF Request for Comments (RFCs) 2401-2409 defines the IPSec protocols with regard to security protocols, security associations and key management, and authentication and encryptionalgorithms. IPSec is a framework of open standards for encrypting TCP/IP traffic within networking environments. IPSec works by encrypting the information contained in IP datagrams through encapsulating. This in turn provides network level data integrity, data confidentiality, data origin authentication, and replay protection. Online financial institutions and private servers most commonly use IPsec in order to protect customers' financial information and identity. However, any software system can also use IPsec in order to create a secure connection between two or more devices.

IPsec is described in RFC 3193: Securing L2TP using IPsec.
The primary features of IPSec are:



- Authentication; protects the private network and the private data it contains. IPSec secures private data from man-in-the-middle attacks, from attackers attempting to access the network, and from an attacker changing the contents of data packets.
- Encryption; conceals the actual content of data packets so that it cannot be interpreted by unauthorized parties.

IPSec can be used to provide packet filtering capabilities. It can also authenticate traffic between two hosts and encrypt traffic passed between the hosts. IPSec can be used to create a virtual private network (VPN). IPSec can also be used to enable communication between remote offices and remote access clients over the Internet.

IPSec operates at the network layer to provide end-to-end encryption. This basically means that data is encrypted at the source computer sending the data. All intermediate systems handle the encrypted portion of the packets as payload. Intermediate systems such as routers merely forward the packet to its end

destination. Intermediate systems do not decrypt the encrypted data. The encrypted data is only decrypted when it reaches the destination.

IPSec interfaces with the TCP/UDP transport layer and the Internet layer, and is applied transparently to applications. IPSec is transparent to users as well. This basically means that IPSec can provide security for most of the protocols within the TCP/IP protocol suite. When it comes to applications, all applications that use TCP/IP can enjoy the security features of IPSec. You do not have to configure security for each specific TCP/IP based application. By using rules and filters, IPSec can receive network traffic and select the required security protocols, determine which algorithms to use, and can apply cryptographic keys required by any of the services.

The security features and capabilities of IPSec can be used to secure the private network and private confidential data from the following

- Denial-of-service (Dos) attacks
- Data pilfering.
- Data corruption.
- Theft of user credentials

The security functions and features provided by IPSec are summarized below:

- Authentication; a digital signature is used to verify the identity of the sender of the information. IPSec can use Kerberos, a preshared key, or digital certificates for authentication.
- Data integrity; a hash algorithm is used to ensure that data is not tampered with. A checksum called a hash message authentication code (HMAC) is calculated for the data of the packet. When a packet is modified while in transit, the calculated HMAC changes. This change will be detected by the receiving computer.
- Data privacy; encryption algorithms are utilized to ensure that data being transmitted is undecipherable.
- Anti-replay; prevents an attacker from resending packets in an attempt to gain access to the privatenetwork.
- Nonrepudiation; public key digital signatures are used to prove message origin.
- Dynamic rekeying; keys can be created during data sending to protect segments of the communication with different keys.

- Key generation; the Diffie-Hellman key agreement algorithm is used to enable two computers to exchange a shared encryption key.
- IP Packet filtering; the packet filtering capability of IPSec can be used to filter and block specific types of traffic, based on either of the following elements or on a combination of them:
  - IP addresses
  - Protocols
  - Ports

How IPsec Works

An IPsec enabled server or host contacts the client computer for a list of ciphers and algorithms that both devices support. Once a cipher has been chosen, the client encrypts any data that it sends by using that specific algorithm so that only the server can decrypt the data by using the agreed upon public key. The IPsec enabled server will then re-encrypt any data that is sent back to the client in the same manner. The two devices will communicate in this way until the session has closed.

A security association (SA) has to first be established between two computers before data can be securely passed between the computers. A Security Association (SA) is a relationship between devices that define how they use security services and settings. The SA provides the information necessary for two computers to communicate securely. Internet Security Association and Key Management Protocol (ISAKMP) and the IKE protocol are the mechanism that enables two computers to establish security associations. When an SA is established between two computers, the computers negotiate on which security settings to utilize to secure data. A security key is exchanged and used to enable the computers to communicate securely.

The security association (SA) contains the following:

- The policy agreement which dictates which algorithms and key lengths the two computers will use to secure data.
- The security keys used to secure data communication.
- The security parameters index (SPI).

With IPSec, two separate SAs are established for each direction of data communication:

- One SA secures inbound traffic.

- One SA secures outbound traffic.

In addition to the above, there is a unique SA for each IPSec security protocol. There are therefore basically two types of SAs:

- ISAKMP SA: When traffic flow is two directional and IPSec needs to establish a connection between computers, an ISAKMP SA is established. The ISAKMP SA defines and handles security parameters between the two computers. The two computers agree on a number of elements to establish the ISAKMP SA:
  - Determine which connections should be authenticated.
  - Determine the encryption algorithm to use.
  - Determine the algorithm to verify message integrity.

  After the above elements have been negotiated between the two computers, the computers use the Oakley protocol to agree on the ISAKMP master key. This is the shared master key which will be used with the above elements to enable secure data communication.

  After a secured communication channel is established between the two computers, the computers start to negotiate the following elements:

  - Determine whether the Authentication Header (AH) IPSec protocol should be used for the connection.
  - Determine the authentication protocol which should be used with the AH protocol for the connection.
  - Determine whether the Encapsulating Security Payload (ESP) IPSec protocol should be used for the connection.
  - Determine the encryption algorithm which should be used with the ESP protocol for the connection.
- IPSec SA: IPSec SAs pertain to the IPSec tunnel and IP packet, and define security parameters to use during a connection. The IPSec SA is derived from the above four elements just negotiated between the two computers.

To secure and protect data, IPSec uses cryptography to provide the following capabilities:

- Authentication: Authentication deals with verifying the identity of the computer sending the data, or the identity of the computer receiving the data. The methods which IPSec can use to authenticate the sender or receiver of data are:
  - Digital certificates: Provides the most secure means of authenticating identities. Certificate authorities(CAs) such as Netscape, Entrust, VeriSign,

and Microsoft provide certificates which can be used for authentication purposes.
    - Kerberos authentication: A downside of using the Kerberos v5 authentication protocol is that the identity of the computer remains unencrypted up to the point that the whole payload is encrypted at authentication.
    - Pre-shared keys; should be used when none of the former authentication methods can be used.

  Anti-replay ensures that the authentication data cannot be interpreted as it is sent over the network. In addition to authentication, IPSec can provide nonrepudiation. With nonrepudiation, the sender of the data cannot at a later stage deny actually sending the data.

- Data integrity: Data integrity deals with ensuring that the data received at the recipient has not been tampered with. A hashing algorithm is used to ensure that the data is not modified as it is passed over the network. The hashing algorithms which can be used by IPSec are:
    - Message Digest (MD5); a one-way hash that results in a 128-bit hash which is used for integrity checking.
    - Secure Hash Algorithm 1 (SHA1); a 160-bit secret key to generate a 160-bit message digest which provides more security than MD5.
- Data confidentiality: IPSec ensures data confidentiality by applying encryption algorithms to data before it is sent over the network. If the data is intercepted, encryption ensures that the intruder cannot interpret the data. To ensure data confidentiality, IPSec can use either of the following encryption algorithms:
    - Data Encryption Standard (DES); the default encryption algorithm used in Windows Server 2003 which uses 56-bit encryption.
    - Triple DEC (3DES); data is encrypted with one key, decrypted with another key, and encrypted again with a different key.
    - 40-bit DES; the least secure encryption algorithm.

Understanding IPSec Terminology

This section of the Article lists the commonly used IPSec terminology and concepts:

- *Authentication Header (AH)*: This is one of the main security protocols used by IPSec. AH provides data authentication and integrity, and can therefore be used

on its own when data integrity and authentication are relevant factors and confidentiality is not. This is because AH does not provide for encryption, and therefore cannot provide data confidentiality. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the main security protocols used in IPSec. These security protocols and can be used separately, or together.

- *Encapsulating Security Payload (ESP)*: This is one of the main security protocols used by IPSec. ESP ensures data confidentiality through encryption, data integrity, data authentication, and other features that support optional anti-replay services. To ensure data confidentiality, a number of symmetric encryption algorithms are used.
- *Certificate Authorities (CAs)*: This is an entity that generates and validates digital certificates. The CA adds its own signature to the public key of the client. CAs issue and revoke digital certificates.
- *Diffie-Hellman groups*: Diffie-Hellman Key Agreement enables two computers to create a shared private key that authenticates data and encrypts an IP datagram. The different Diffie-Hellman groups are listed here:
  - Group 1; provides 768-bit key strength
  - Group 2; provides 1024-bit key strength
  - Group 3; provides 2048-bit key strength
- *Internet Key Exchange (IKE)*: The IKE protocol is used by computers to create a security association (SA) and to exchange information to generate Diffie-Hellman keys. IKE manages and exchanges cryptographic keys so that computers can have a common set of security settings. Negotiation occurs on which authentication method, and encryption algorithm and hashing algorithm the computers will use.
- *IPSec Driver*: The IPSec driver performs a number of operations to enable secure network communication, including the following:
  - Creates IPSec packets
  - Generates checksums.
  - Initiates the IKE communication
  - Adds the AH and ESP headers
  - Encrypts data before it is transmitted.
  - Calculates hashes and checksums for incoming packets.
- *IPSec Policies*: IPSec policies define when and how data should be secured, and defines which security methods to use for securing data. IPSec policies contain a number of elements:

    - Actions.
    - Rules
    - Filter lists
    - Filter actions.
- *IPSec Policy Agent*: This is a service running on a computer running Windows Server 2003 that accesses IPSec policy information. The IPSec Policy Agent accesses the IPSec policy information in either the Windows registry or in Active Directory.
- *Oakley key determination protocol*: The Diffie-Hellman algorithm is used for two authenticated entities to negotiate and be in agreement on a secret key.
- *Security Association (SA)*: A SA is a relationship between devices that define how they use security services and settings.
- *Triple Data Encryption (3DES)*: This is a strong encryption algorithm used on client machines running Windows, and on Windows Server 2003 computers. 3DES uses 56-bit keys for encryption.

Understanding the IPSec Modes

IPSec can operate in one of the following modes:

- *Tunnel mode*: IPSec tunnel mode can be used to provide security for WAN and VPN connections that use the Internet as the connection medium. In tunnel mode, IPSec encrypts the IP header and the IP payload. With tunneling, the data contained in a packet is encapsulated inside an additional packet. The new packet is then sent over the network.
  Tunnel mode is typically used for the following configurations:
    - Server to server
    - Server to gateway
    - Gateway to gateway

  The process of communication that occurs when tunnel mode is defined as the IPSec mode is detailed below:
    - Data is transmitted using unprotected IP datagrams from a computer on the private network.
    - When the packets arrive at the router, the router encapsulates the packet using IPSec security protocols.

    - The router then forwards the packet to the router at the other end of the connection.
    - This router checks the integrity of the packet.
    - The packet is decrypted.
    - The data of the packet is then added to unprotected IP datagrams and sent to the destination computer on the private network.
- *Transport Mode*: This is the default mode of operation used by IPSec in which only the IP payload is encrypted through the AH protocol or ESP protocol. Transport mode is used for end-to-end communication security between two computers on the network.

Many networks which are not able to support Tunnel Mode are able to successfully support Transport mode.

Understanding the IPSec Protocols

The main IPSec security protocols are the Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols. There are other IPSec protocols such as ISAKMP, IKE, and Oakley that use the Diffie-Hellman algorithm.

Authentication Header (AH) Protocol

The AH protocol provides the following security services to secure data:

- Authentication
- Anti-replay
- Data integrity

The AH protocol ensures that data is not modified as it moves over the network. It also ensures that the data originated from the sender.

The AH protocol does not though provide data confidentiality because it does not encrypt the data contained in the IP packets. This basically means, that if the AH protocol is used by itself; intruders that are able to capture data would be able to read the data. They would not though be able to change the data. The AH protocol can be used in combination with the ESP protocol if you need to ensure data confidentiality as well.

The communication process which occurs when the AH protocol is used is shown here:

1. One computer transmits data to another computer.

2. The IP header, AH header, and the data itself is signed to ensure data integrity.
3. The AH header is inserted between the IP header and IP payload to provide authentication and integrity.

The fields within a AH header, together with the role performed by each field is listed here:

- *Next Header*; used to specify the type of IP payload through the IP protocol ID that exists after this AH header.
- *Length*; indicates the length of the AH header.
- *Security Parameters Index (SPI)*; indicates the correct security association for the communication through a combination of the following:
  - IPSec security protocol.
  - Destination IP address
- *Sequence Number*; used to provide IPSec anti-replay protection for the communication. The sequence number commences at 1, and is incremented by 1 in each ensuing packet. Packets that have the same sequence number and security association are discarded.
- *Authentication Data*; holds the integrity check value (ICV) calculated by the sending computer to provide data integrity and authentication. The receiving computer calculates the ICV over the IP header, AH header, and IP payload, and then compares the two ICV values.

Encapsulating Security Payload (ESP) protocol

The ESP protocol provides the following security services to secure data:

- Authentication
- Anti-replay
- Data integrity
- Data confidentiality

The primary difference between the AH protocol and the ESP protocol is that the ESP protocol provides all the security services provided by the AH protocol, together with data confidentiality through encryption. ESP can be used on its own, and it can be used together with the AH protocol. In transport mode, the ESP protocol only signs and

protects the IP payload. The IP header is not protected. If the ESP protocol is used together with the AH protocol, then the entire packet is signed.

ESP inserts an ESP header and ESP trailer, which basically encloses the payload of the IP datagram. All data after the ESP header to the point of the ESP trailer, and the actual ESP trailer is encrypted.

The fields within an ESP header, together with the role performed by each field are listed here:

- *Security Parameters Index (SPI)*; indicates the correct security association for the communication through a combination of the following:
  - IPSec security protocol.
  - Destination IP address
- *Sequence Number*; used to provide IPSec anti-replay protection for the communication. The sequence number commences at 1, and is incremented by 1 in each ensuing packet. Packets that have the same sequence number and security association are discarded.

The fields within an ESP trailer, together with the role performed by each field are listed here:

- *Padding*; required by the encryption algorithm to ensure that byte boundaries are present.
- *Padding Length*; indicates the length (bytes) of the padding which was used in the Padding field.
- *Next Header*; used to specify the type of IP payload through the IP protocol ID.
- *Authentication Data*; holds the integrity check value (ICV) calculated by the sending computer to provide data integrity and authentication. The receiving computer calculates the ICV over the IP header, AH header, and IP payload, and then compares the two ICV values.

IPsec and ISAKMP

IPsec relies on ISAKMP (Internet Security Association and Key Management Protocol) for key exchange.

FreeS/WAN IPsec

FreeS/WAN is an implementation of IPsec and IKE for Linux.

The primary objective of the FreeS/WAN project is to help make IPsec widespread by providing source code which is freely available, runs on a range of machines

including ubiquitous cheap PCs, and is not subject to US or other nations' export restrictions.

Understanding IPSec Security Filters, Security Methods, and Security Policies

Security filters basically match security protocols to a specific network address. IPSec filters can be used to filter out unauthorized traffic. The filter contains the following information:

- Source and destination IP address
- Protocol used
- Source and destination ports

Each IP address contains a network ID portion and a host ID portion. Through security filters, you can filter traffic according to the following:

- Traffic allowed to pass through
- Traffic to secure
- Traffic to block

Security filters can be grouped into a filter list. There is no limit to the number of filters which can be included in a filter list. IPSec policies uses IP filters to ascertain whether an IP security rule should be used in a packet.

You can use a security method to specify the manner in which an IPSec policy should deal with traffic matching an IP filter. Security methods are also referred to as filter actions. The filter actions result in either of the following events:

- Drops traffic
- Allows Traffic
- Negotiates security.

To apply security in your network, IPSec policies are used. The IPSec policies define when and how data should be secured. The IPSec policies also determine which security methods to use when securing data at the different levels in your network. You can configure IPSec policies so that different types of traffic are affected by each individual policy.

IPSec policies can be applied at the following levels within a network:

- Active Directory domain

- Active Directory site
- Active Directory organizational unit
- Computers
- Applications

The different components of an IPSec policy are listed here:

- *IP filter*; informs the IPSec driver on the type of inbound traffic and outbound traffic which should be secured.
- *IP filter list*; used to group multiple IP filters into a single list in order to isolate a specific set of network traffic.
- *Filter action*; used to define how the IPSec driver should secure traffic.
- *Security method*; refers to security types and algorithms used for the key exchange process and for authentication.
- *Connection type*: identifies the type of connection which the IPSec policy impacts.
- *Tunnel setting*; the tunnel endpoint's IP address/DNS name.
- *Rule*; a grouping of the following components to secure a specific subset of traffic in a particular manner:
  - IP filter
  - Filter action.
  - Security method
  - Connection type
  - Tunnel setting.

Source: http://www.tech-faq.com/ipsec.html