

Internet Protocol Security

by *Simon Salomon*

In today's world information has become of much concern. Whether it be business transactions, letters, business secrets, or any other kind of sensitive information it has all become stored digitally somewhere on a storage device. This raises a big concern among the owners of that information because of the risk of it being intercepted by users who have no authority to access that information. Before the internet people did not need to worry about information being stolen through wired cables because we used physical means of sending that information. Either through the U.S.P.S or other more reliable sources, we were more concerned on whether the information would get to its destination on time than on its integrity because if someone were to open the envelope or cut the box open it would be evident. We were not concerned much with the authentication of the information because we had a signature which would prove who was the author of that information. In today's world things have totally shifted. We have made some serious changes because of the way the Internet works. Today the basic three components of information secure delivery have become confidentiality, integrity, and availability. This is where IPsec Virtual Private Networks (VPNs) play an important role.

IPsec VPNs to many people usually means encryption and because the IP protocol lacks intrinsic security we need a way to secure the transmission of data between two endpoints. This is where IPsec can prove to be effective. IPsec is a security protocol that was designed to provide authentication and encryption over the internet. If you break down IPsec to its most critical elements there is really only three main technologies. The three main elements of IPsec are Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP). These three protocols are used to provide security when exchanging information from eavesdroppers or from outsiders trying to tamper with the information. Another goal of IPsec Suite is to provide a standard for secure interoperability between multiple vendors so that all the products of each vendor will work correctly together without any problems. IPsec-based security starts with the forming of a security association (SA) between two parties.

A security association (SA) is an agreement between two parties or entities that will say how they will support secure communication between each other. The great thing about IPsec is that it not only supports multiple protocols, but that it also allows for various encryption algorithms and different hash types. In order for a secure

communication to be established between two entities the encryption method and the hash type must be negotiated. Without this prior negotiation we might have one end using a different encryption algorithm than the entity on the other side of the communication channel. This would result in a break down of the communication because the data would not be decrypted correctly. Therefore, all the details must be decided before the information is sent across the medium.

Once the SA has been agreed upon it is placed in a security association database (SAD). This is necessary because each connection might be using different rules and different encryption algorithms. Remember IPsec supports multiple encryption algorithms, so we must keep track of which connection is using which encryption algorithm and hash types. For example, look at the figure below.

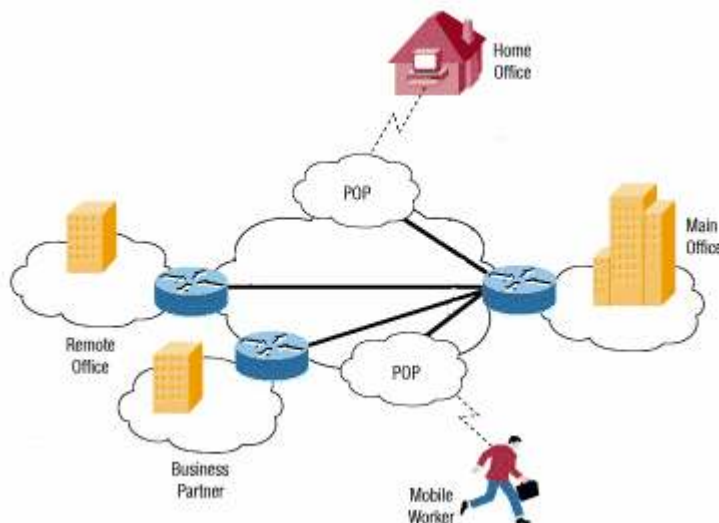
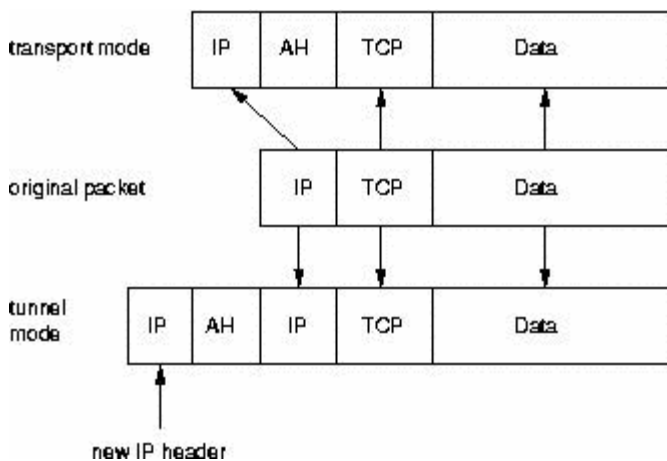


Image courtesy Cisco Systems, Inc.

In this image you can see that there is a mobile worker who can connect to the VPN and a home office which can connect to the VPN. In this scenario let us assume that the mobile worker is host 1 and that the home office is host 2. Host 1 might only support DES and not any other encryption algorithm. Hence, when negotiation ends the encryption selected would be DES encryption. However, host 2 might not support DES. Host 2 might support only AES, therefore there must be a way to keep track of these multiple connections using various encryption algorithms and that is where the SAD comes into play.

There are two main modes which IPSec uses in order to operate. The first mode is transport mode and the second is tunnel mode. Transport mode is used when an SA is made between two hosts that usually reside in the same network. It's usually referred to as host-to-host. In this case only the packet's payload is encrypted. This mode can also be used when you don't care whether the IP addresses of the communicating parties are made public or not. Also, transport mode lacks the ability to participate in gateway-to-gateway communications.

Tunnel mode is used when an SA is made between two IPSec gateways. This is usually what is used in VPNs because in tunnel mode not only is the payload encrypted but the entire original packet. This hides the IP addresses of the source and destination of the IP packet. Another advantage of tunnel mode is that it can occur not only with gateway-to-gateway, but also between host-to-host and host-to-gateway.



The above image shows the difference between tunnel mode and transport mode. As you can see in transport mode the original IP packet is used whereas in the tunnel mode a new IP header is planted on the packet.

The protocol that is the authenticator and negotiator of IPSec is the Internet key exchange (IKE) protocol. It is what verifies whether your system has the right to start an encrypted communication with the device in question. It then negotiates which encryption algorithm will be used during the connection. There are two phases in the IKE transaction that support the creation of an SA between two parties. They are referred to as phase 1 and phase 2.

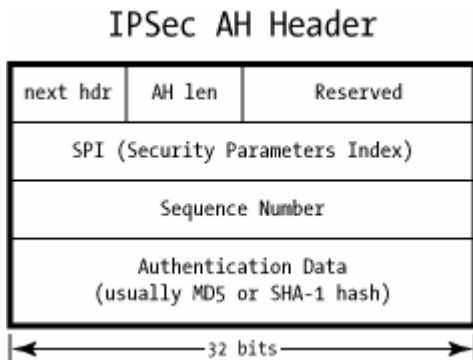
Phase 1 begins when an initiator wants to begin a session with a VPN gateway device. In this phase two things occur. One is the authentication of the remote client and the other is to exchange public key information that will be used for the next phase. Various ways exist that can be used to verify authentication. Some of which are pre-shared keys which is a key that has been pre-configured between the communicating devices. This is a very simple way of authentication however it does have many drawbacks because if the key is broken you must reconfigure all the devices that used that key. The second method of authentication that can be used is digital signatures also called digital certificates. In this case a Certificate Authority (CA) remotely manages and administers each certificate. The CA is the center piece of the Public Key Infrastructure (PKI) encryption method. In this concept the PKI is publicly available to anyone who wants it. They are typically available in certificates.

Phase 2 of the IKE transaction deals with the negotiation of the parameters of IPsec SAs. Once Phase 2 is complete IPsec SA is formed and the VPN connection is made. During the Phase 2 exchanges all the packets are encrypted using whatever protocols were negotiated during Phase 1 and any other protection that might be used are hashes that confirm the origin of the packets.

The IPsec Security Protocols that are used in IPsec are the Authentication Header (AH) and the Encapsulating Security Payload (ESP). When creating an IPsec-based VPN you can choose to use either AH or ESP. You also can use both of them at the same time depending on the needs of the users. Although you are able to use either one the most popular security protocol that is being used is ESP.

Authentication Header (AH) protocol is IP protocol 51. It provides authentication and integrity, but it does not offer confidentiality for the packet's payload. That means that anyone will be able to see the payload. This is a security limit that AH has and may not be suitable for most secure communications. However, if your concern is confidentiality then AH can be used. AH guarantees that the information it contains came from the person who claimed to have sent it. A good characteristic of AH is that because it does not use complex encryption algorithms it has a smaller size payload than ESP. This means that AH packets have a smaller processing burden on the device that is sending the packet. There is no need to keep adding headers that take time to encrypt and decrypt. When integrity and IP address authentication isn't important and performance is, then AH would make a good solution.

The following diagram shows an AH packet header.

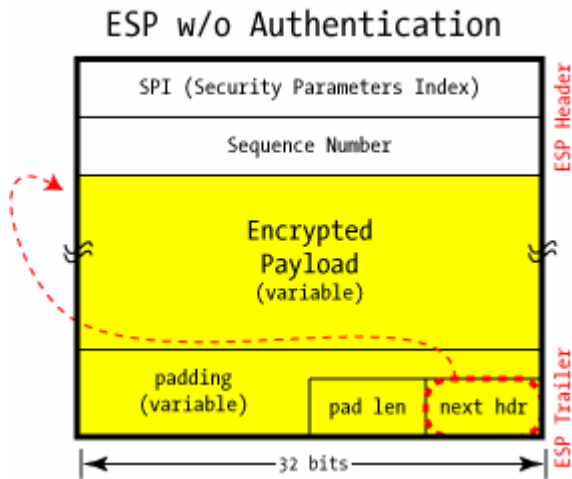


- The next header field identifies the protocol type of the next packet header after the AH packet header.
- The AH length field states the length of the AH header information.
- Reserved field is for future extensions of the AH protocol.
- The SPI field shows to which SA the packet belongs to.
- The sequence number field is an incrementing value that prevents against replay attacks.
- The authentication data contains the information for authenticating the packet.

The Encapsulating Security Payload (ESP) is the second security protocol that IPSec offers. ESP is IP protocol 50. Unlike AH, ESP offers confidentiality. Depending on the mode used, transport or tunnel, ESP works differently. When ESP is in transport mode it adds its own header to the IP header and then encrypts the payload. It may also contain a trailer which provides confirmation on the packets integrity and authentication.

In tunnel mode ESP actually encapsulates the whole packet. It will encrypt the whole original packet and add a new IP header and a new ESP header to the packet. A trailer will then be added for authentication purposes if the ESP authentication service is used. Unlike AH, ESP will work with NAT given it is used in tunnel mode. This is because of the way the whole packet is encapsulated and encrypting it does not invalidate the NAT's integrity check.

The following diagram shows an ESP packet header.



- The SPI is the security parameters index.
- The sequence number is used to prevent replay attacks.
- The next field is the encrypted payload.
- The next field uses padding which is optional.
- The next header field shows the protocol number for the information inside the ESP packet.

The IPsec protocol is used as a means of secure encryption. Although there are two protocols that are available in the IPsec suite only ESP is usually used. This is because ESP offers message authentication, integrity, and confidentiality. Whereas AH only offers message authentication and integrity but no confidentiality. One of the great features of IPsec is that it can be used with many other applications not just VPNs. This makes IPsec a very good security solution. For those users who are using IPv6 IPsec is compatible with IPv4 as well as IPv6. This ensures that IPsec will be around in the future as the Internet continues to grow and become popular.

Bibliography

Wikipedia, "IPsec",
http://en.wikipedia.org/wiki/IP_Security.

Answers.com, "IPsec"
<http://www.answers.com/IPsec>.

Jeff Tyson, "How Virtual Private Networks Work",
<http://computer.howstuffworks.com/vpn.htm>.

Forouzan, Behrouz, 2006, *TCP/IP Protocol Suite*, McGraw-Hill, New York, NY, pp 682-683, 736, 749-750, 754-760.

Convery, Sean, 2004, *Network Security Architectures*, Cisco Press, Indianapolis, IN, pp 353-381.

Stephen, Northcutt, Lenny Zelster, Scott Winters, Karen Kent, Ronald Ritchey, 2005, *Inside Network Perimeter Security*, Sams Publishing, Indianapolis, IN, pp 170-182.