IPsec (Internet Protocol Security)

What is IPsec (Internet Protocol Security)?

IPsec (Internet Protocol Security) is a suite of protocols and algorithms for securing data transmitted over the internet or any public network. The Internet Engineering Task Force, or IETF, developed the IPsec protocols in the mid-1990s to provide security at the IP layer through authentication and encryption of IP network packets.

IPsec originally defined two protocols for securing IP packets: **Authentication Header (AH) and Encapsulating Security Payload (ESP).** The former provides data integrity and anti-replay services, and the latter encrypts and authenticates data.

The IPsec suite also includes **Internet Key Exchange (IKE)**, which is used to generate shared security keys to establish a **security association (SA)**. SAs are needed for the encryption and decryption processes to negotiate a security level between two entities. A special router or firewall that sits between two networks usually handles the SA negotiation process.

Applications of IPsec

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

- **Secure branch office connectivity over the Internet:** A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

- **Secure remote access over the Internet:** An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

- **Establishing extranet and intranet connectivity with partners:** IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

- **Enhancing electronic commerce security:** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the net work administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

Figure 1 is a typical scenario of IPsec usage. An organization maintains LANs at dispersed locations. Non secure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world.

The IPsec networking device will typically encrypt and compress all traffic going into the WAN and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPsec protocols to provide security

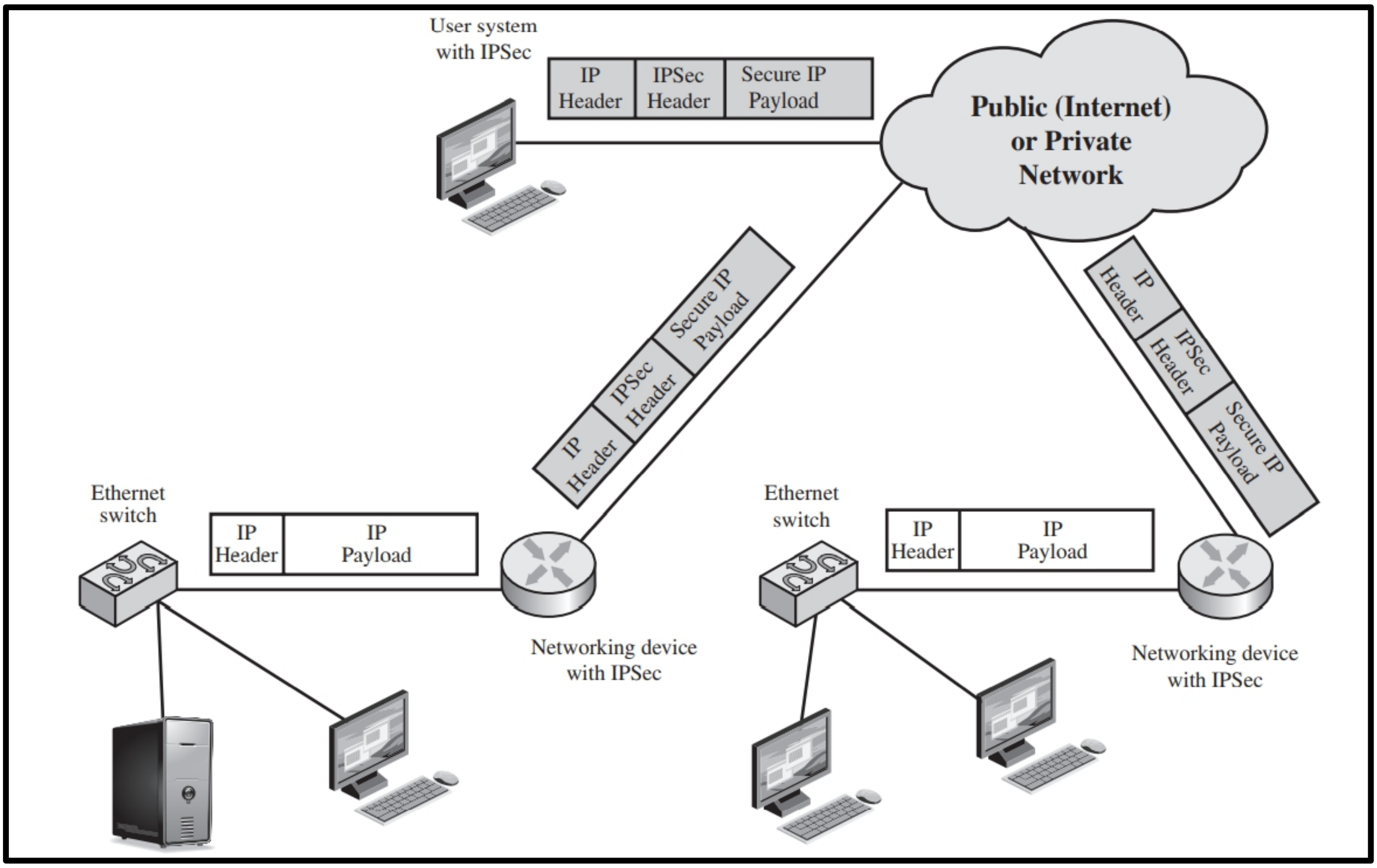
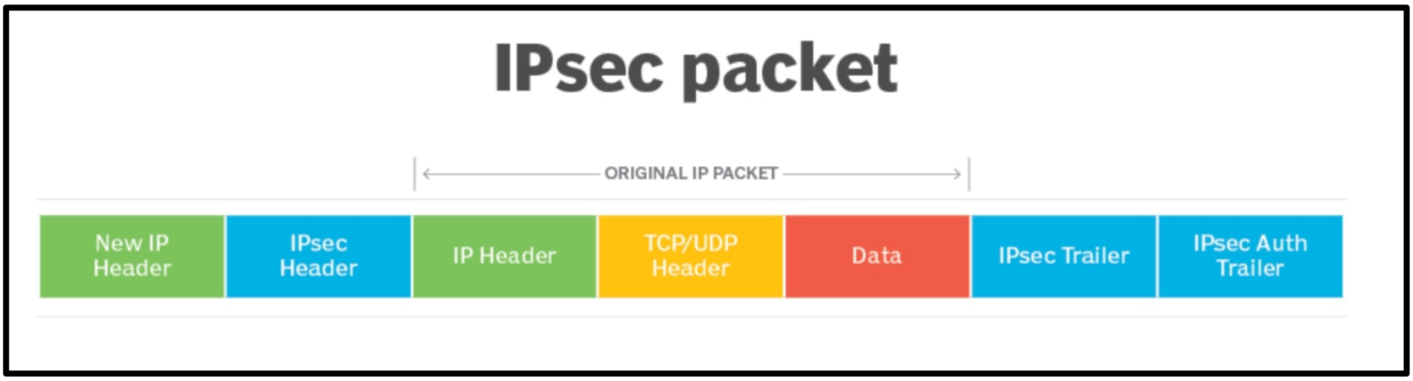


Figure 1: An IP Security Scenario

IPsec protocols

IPsec authenticates and encrypts data packets sent over both IPv4- and IPv6-based networks. IPsec protocol headers are found in the IP header of a packet and define how the data in a packet is handled, including its routing and delivery across a network. IPsec adds several components to the IP header, including security information and one or more cryptographic algorithms.



The following are key IPsec protocols:

- **IP Authentication Header (AH).** It provides data integrity and transport protection services. AH was designed to be inserted into an IP packet to add authentication data and protect the contents from modification.
- **IP ESP.** ESP provides authentication, integrity and confidentiality through encryption of IP packets.
- **IKE.** IKE is a protocol that enables two systems or devices to establish a secure communication channel over an untrusted network. The protocol uses a series of key exchanges to create a secure tunnel between a client and a server through which they can send encrypted traffic. The security of the tunnel is based on the Diffie-Hellman key exchange.
- **Internet Security Association and Key Management Protocol (ISAKMP).** It is a framework for key establishment, authentication and negotiation of an SA for a secure exchange of packets at the IP layer. In other words, ISAKMP defines the security parameters for how two systems, or hosts, communicate with each other. Each SA defines a connection in one direction, from one host to another. The SA includes all attributes of the connection, including the cryptographic algorithm, the IPsec mode, the encryption key and any other parameters related to data transmission over the connection.

How does IPsec work?

There are five key steps involved with how IPsec works. They are as follows:

1. **Host recognition.** The IPsec process begins when a host system recognizes that a packet needs protection and should be transmitted using IPsec policies. Such packets are considered "interesting traffic" for IPsec purposes, and they trigger the security policies. For outgoing packets, this means the appropriate encryption and authentication are applied. When an incoming packet is determined to be interesting, the host system verifies that it has been properly encrypted and authenticated.
2. **Negotiation, or IKE Phase 1.** In the second step, **the hosts use IPsec to negotiate the set of policies they will use for a secured circuit.** They also authenticate themselves to each other and set up a secure channel between them that is used to negotiate the way the IPsec circuit will encrypt or authenticate data sent across it. This negotiation process occurs using either main mode or aggressive mode.

   With **main mode**, the host initiating the session sends proposals indicating its preferred encryption and authentication algorithms. The negotiation continues until both hosts agree and set up an IKE SA that defines the IPsec circuit they will use. **This method is more secure than aggressive mode because it creates a secure tunnel for exchanging data.**

   In **aggressive mode**, the initiating host does not allow for negotiation and specifies the IKE SA to be used. The responding host's acceptance authenticates the session. With this method, the hosts can set up an IPsec circuit faster.

3. **IPsec circuit, or IKE Phase 2.** Step **three sets up an IPsec circuit over the secure channel established in IKE Phase 1.** The IPsec hosts negotiate the algorithms that will be used during the data transmission. The hosts also agree upon and exchange the encryption and decryption keys they plan to use for traffic to and from the protected network. **The hosts also exchange cryptographic nonces, which are random numbers used to authenticate sessions.**

4. **IPsec transmission.** In the fourth step, the hosts exchange the actual data across the secure tunnel they've established. **The IPsec SAs set up earlier are used to encrypt and decrypt the packets.**

5. **IPsec termination.** **Finally, the IPsec tunnel is terminated. Usually, this happens after a previously specified number of bytes have passed through the IPsec tunnel or the session times out.** When either of those events happens, the hosts communicate, and termination occurs. After termination, the hosts dispose of the private keys used during data transmission.

What are the IPsec modes?

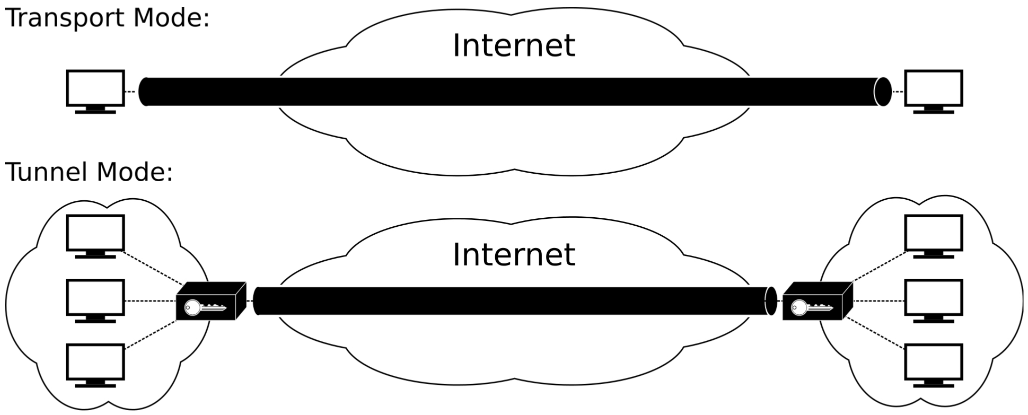
There are 2 modes in IPSec Security:

Transport mode:

- The transport mode encrypts only the payload ; so the IP header of the original packet is not encrypted.
- The IPsec Transport mode is implemented for client-to-site VPN scenarios.
- The transport mode is usually used when another tunneling protocol is used to first encapsulate the IP data packet, then IPsec is used to protect the packets.
- In transport mode, the IP addresses in the outer header are used to determine the IPsec policy that will be applied to the packet.

Tunnel mode:

- Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by a another set of IP headers.
- It is widely implemented in site-to-site VPN scenarios.
- In tunnel mode, two IP headers are sent. The inner IP packet determines the IPsec policy that protects its contents.


Transport Mode:
Internet
Tunnel Mode:
Internet