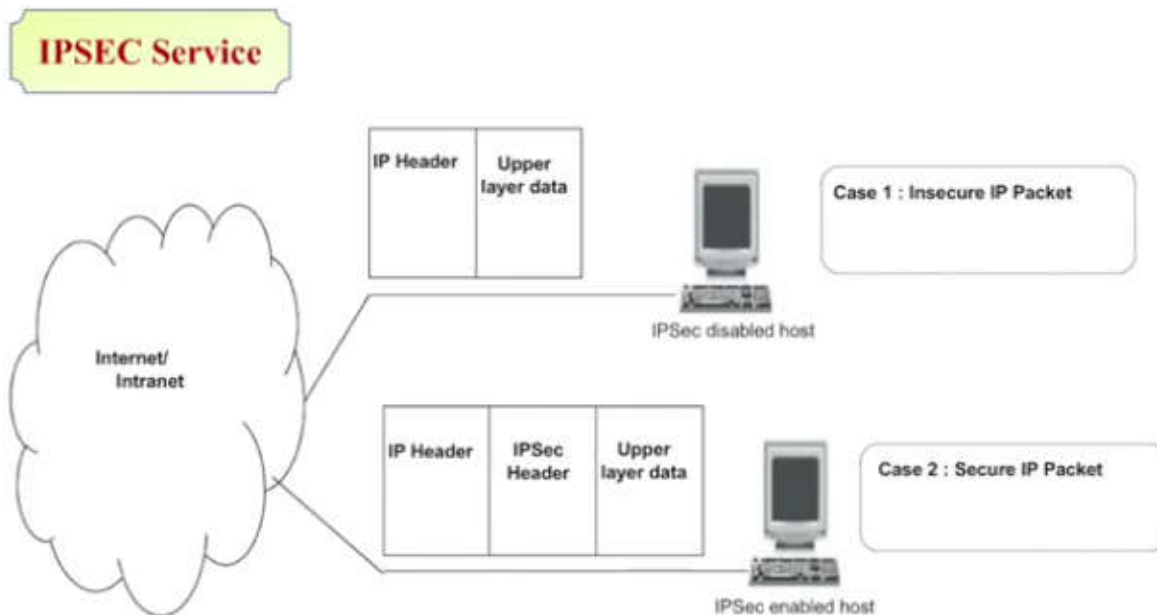


The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.



Uses of IP Security –

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted.

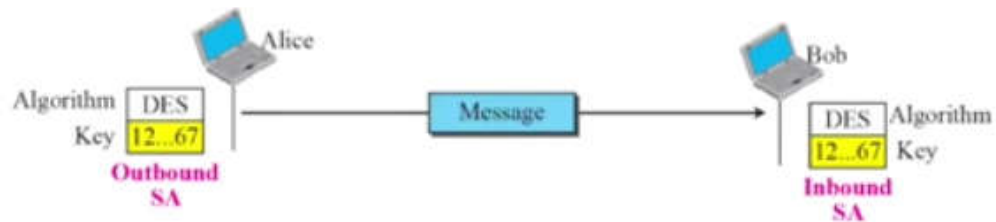
Idea of Security Association

- Security Association is a very important aspect of IPSec. IPSec requires a logical relationship, called a Security Association (SA), between two host

Idea of Security Association

- A Security Association is a contract between two parties; it creates a secure channel between them
- Let us assume that Alice needs to unidirectionally communicate with Bob. If Alice and Bob are interested only in the confidentiality aspect of security, they can create a shared secret key between themselves.
- We can say that there are two Security Associations (SAs) between Alice and Bob; one outbound SA and one inbound SA
- Each of them stores the value of the key in a variable and the name of the encryption/ decryption algorithm in another. Alice uses the algorithm and the key to encrypt a message to Bob; Bob uses the algorithm and the key when he needs to decrypt the message received from Alice

Simple SA

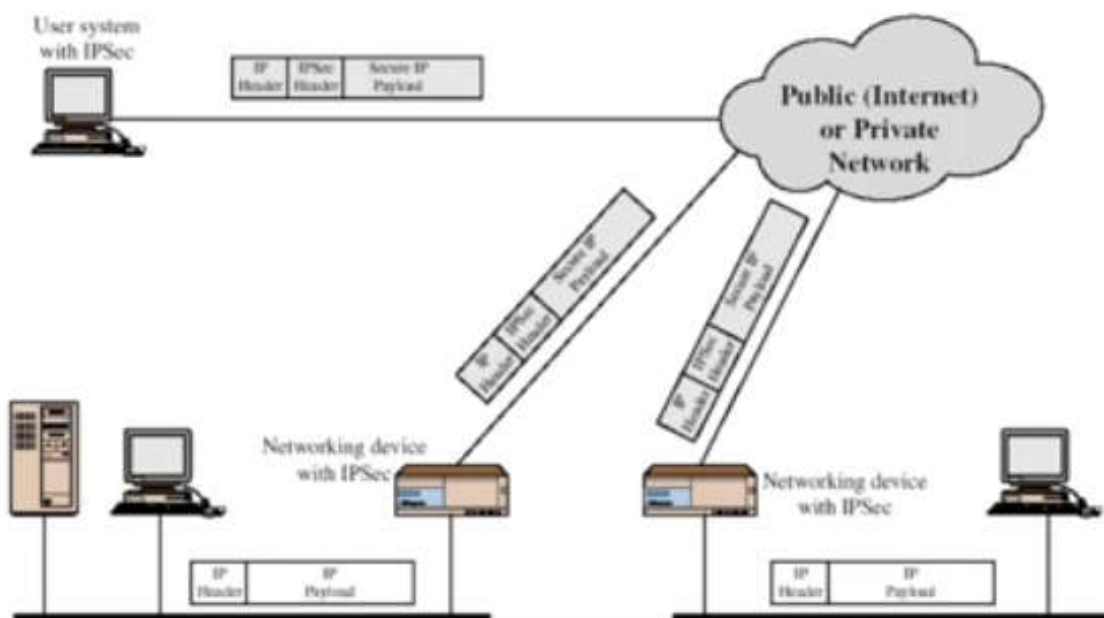


Security Association

- One of the most important concepts in IPSec is called a Security Association (SA). Defined in RFC 1825
- SAs are the combination of a given Security Parameter Index (SPI) and Destination Address
- SAs are one way. A minimum of two SAs are required for a single IPSec connection

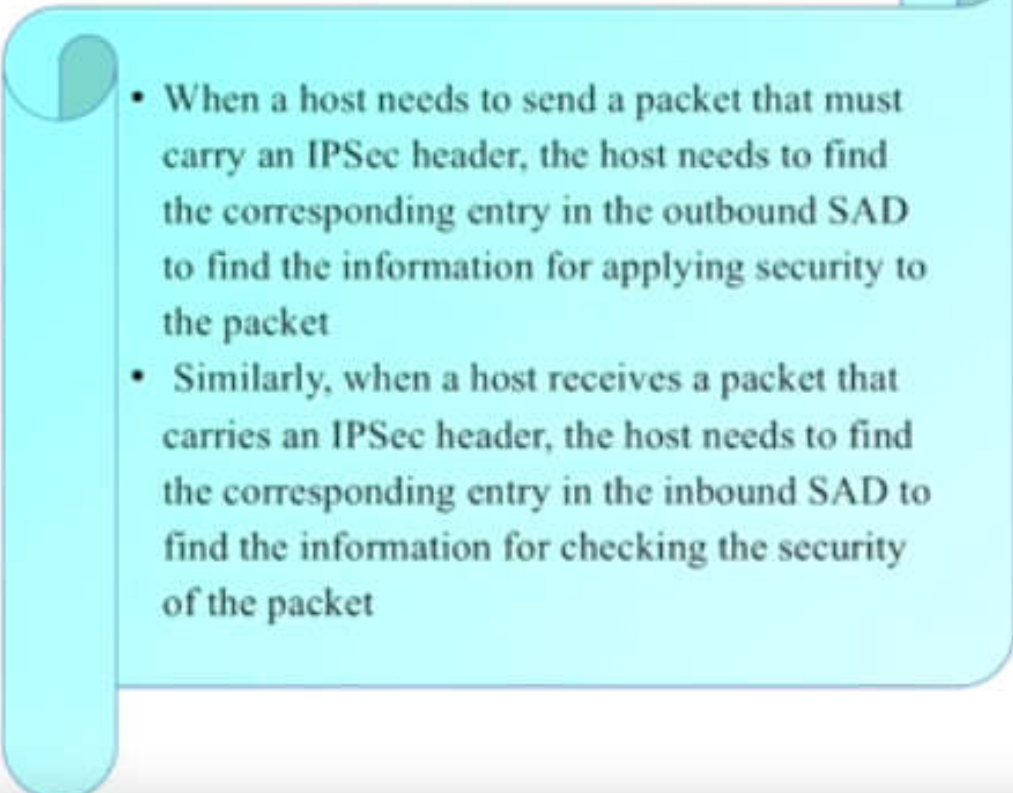
- SAs contain parameters including:
 - Authentication algorithm and algorithm mode
 - Encryption algorithm and algorithm mode
 - Key(s) used with the authentication/encryption algorithm(s)
 - Lifetime of the key
 - Lifetime of the SA
 - Source Address(es) of the SA
 - Sensitivity level (ie Secret or Unclassified)

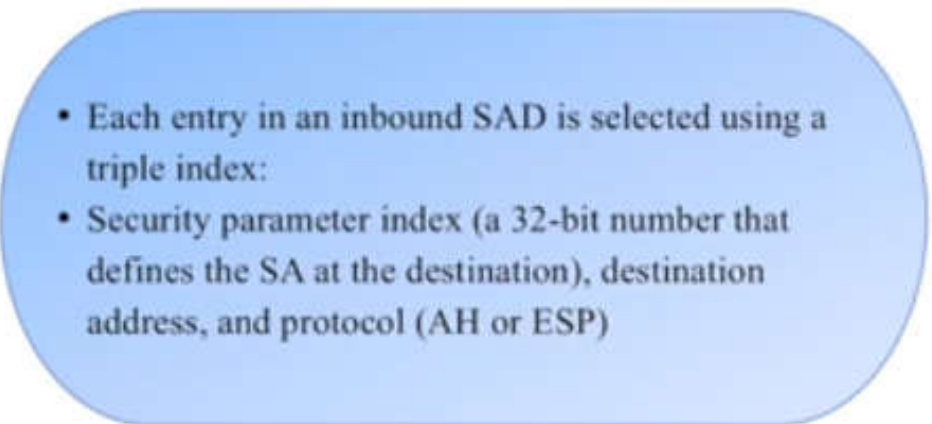
IP security scenario



Security Association Database (SAD)

- A Security Association can be very complex. This is particularly true if Alice wants to send messages to many people and Bob needs to receive messages from many people
- In addition, each site needs to have both inbound and outbound SAs to allow bidirectional communication.
- In other words, we need a set of SAs that can be collected into a database. This database is called the Security Association Database (SAD)
- The database can be thought of as a two-dimensional table with each row defining a single SA
- Normally, there are two SADs, one inbound and one outbound

- 
- When a host needs to send a packet that must carry an IPSec header, the host needs to find the corresponding entry in the outbound SAD to find the information for applying security to the packet
 - Similarly, when a host receives a packet that carries an IPSec header, the host needs to find the corresponding entry in the inbound SAD to find the information for checking the security of the packet

- 
- Each entry in an inbound SAD is selected using a triple index:
 - Security parameter index (a 32-bit number that defines the SA at the destination), destination address, and protocol (AH or ESP)

Index	SN	OF	ARW	AH/ESP	LT	Mode	MTU
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							

Security Association Database

Legend:

SPI: Security Parameter Index

DA: Destination Address

AH/ESP: Information for either one

P: Protocol

Mode: IPSec Mode Flag

SN: Sequence Number

OF: Overflow Flag

ARW: Anti-Replay Window

LT: Lifetime

MTU: Path MTU

- Security Policy
- Another important aspect of IPSec is the Security Policy (SP), which defines the type of security applied to a packet when it is to be sent or when it has arrived
- Before using the SAD, a host must determine the predefined policy for the packet

- Security Policy Database
- Each host that is using the IPSec protocol needs to keep a Security Policy Database (SPD)
- Again, there is a need for an inbound SPD and an outbound SPD
- Each entry in the SPD can be accessed using a six tuple index: source address, destination address, name, protocol, source port, and destination port, as shown in Figure

SPD

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	

Legend:

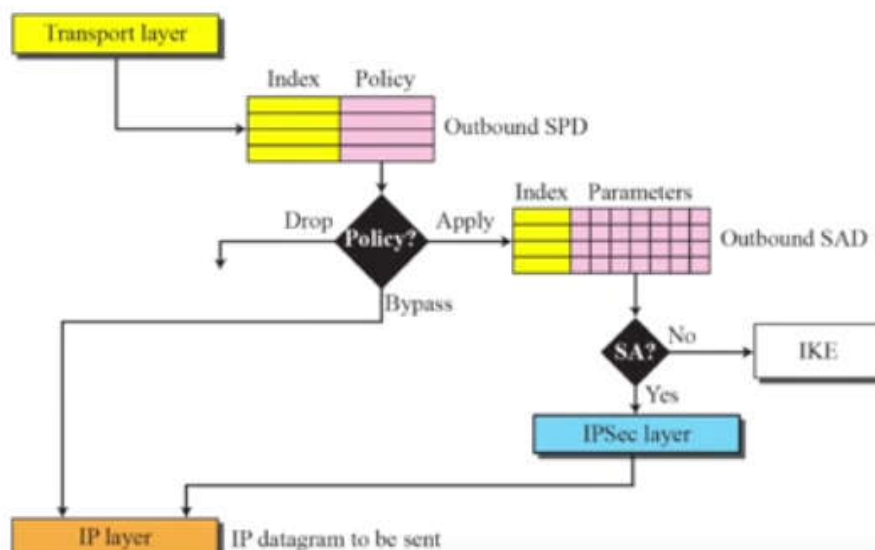
SA: Source Address
DA: Destination Address
P: Protocol

SPort: Source Port
DPort: Destination Port

Outbound SPD

- When a packet is to be sent out, the outbound SPD is consulted
- Figure 30.11 shows the processing of a packet by a sender
- The input to the outbound SPD is the ~~six~~ tuple index; the output is one of the three following cases: drop (packet cannot be sent), bypass (bypassing security header), and apply (apply the security according to the SAD; if no SAD, create one)

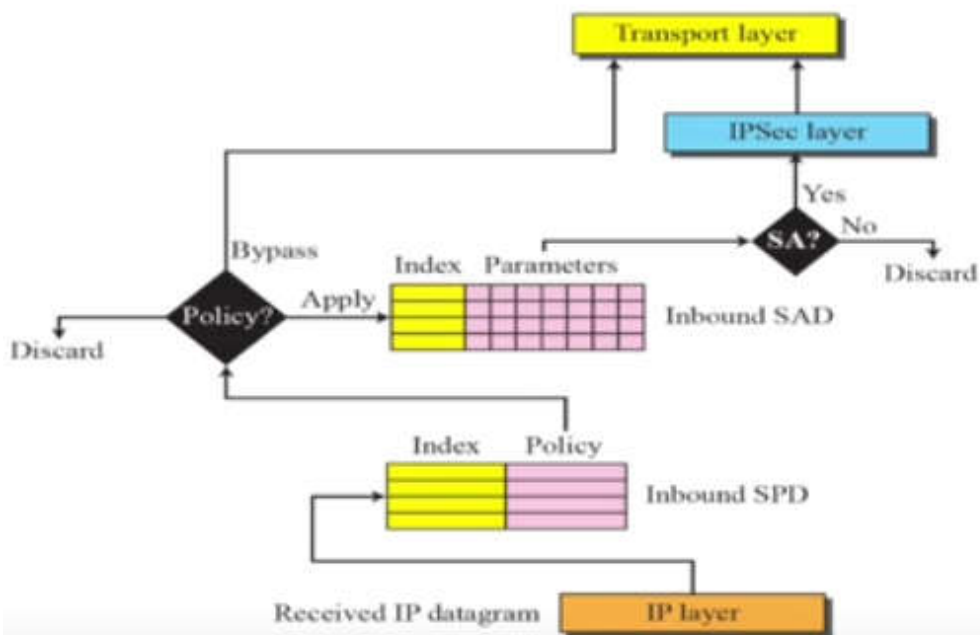
Outbound processing



Inbound SPD

- When a packet arrives, the inbound SPD is consulted. Each entry in the inbound SPD is also accessed using the same ~~six~~ tuple index
- Figure shows the processing of a packet by a receiver
- The input to the inbound SPD is the ~~six~~ tuple index; the output is one of the three following cases: discard (drop the packet), bypass (bypass the security and deliver the packet to the transport layer), and apply (apply the policy using the SAD)

Inbound processing



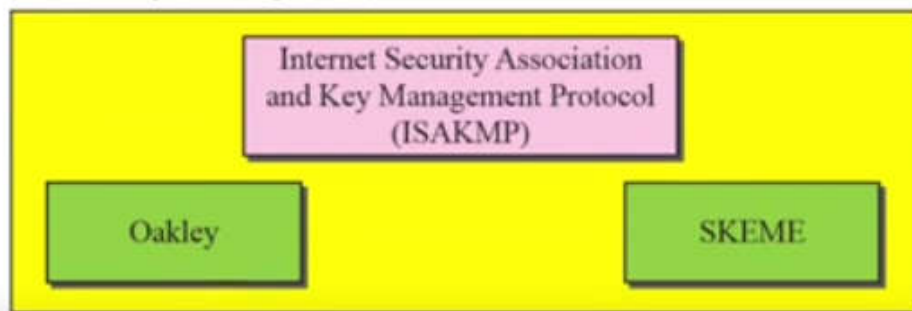
Internet Key Exchange (IKE)

- The Internet Key Exchange (IKE) is a protocol designed to create both inbound and outbound Security Associations
- As we discussed in the previous section, when a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic

IKE components

- IKE is a complex protocol based on three other protocols: Oakley, SKEME, and ISAKMP

Internet Key Exchange (IKE)



IP sec Application

- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
 - Secure branch office connectivity over the Internet
 - Secure remote access over the Internet
 - Establishing extranet and intranet connectivity with partners
 - Enhancing electronic commerce security

- **Access Control**
- IPSec provides access control indirectly using a Security Association Database (SAD). When a packet arrives at a destination, and there is no Security Association already established for this packet, the packet is discarded
- **Message Integrity**
- Message integrity is preserved in both AH and ESP. A digest of data is created and sent by the sender to be checked by the receiver
- **Entity Authentication**
- The Security Association and the keyed-hash digest of the data sent by the sender authenticate the sender of the data in both AH and ESP

- **Confidentiality**
- The encryption of the message in ESP provides confidentiality. AH, however, does not provide confidentiality. If confidentiality is needed, one should use ESP instead of AH

- **Replay Attack Protection**
- In both protocols, the replay attack is prevented by using sequence numbers and a sliding receiver window
- Each IPSec header contains a unique sequence number when the Security Association is established. The number starts from 0 and increases until the value reaches $2^{32} - 1$
- When the sequence number reaches the maximum, it is reset to 0 and, at the same time, the old Security Association is deleted and a new one is established.
- To prevent processing duplicate packets, IPSec mandates the use of a fixed-size window at the receiver. The size of the window is determined by the receiver with a default value of 64

Why not use IPSec?

- Processor overhead to encrypt and verify each packet can be great
- Added complexity in network design

Components of IP Security –

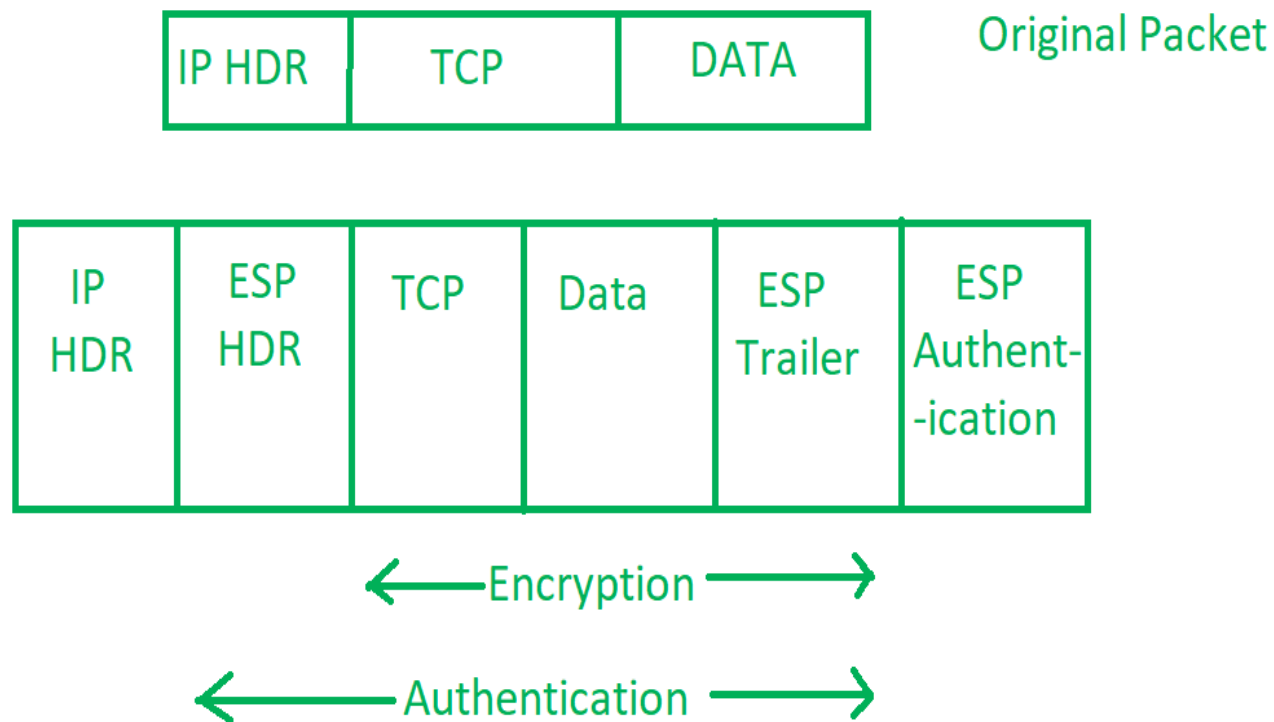
It has the following components:

1. **Encapsulating Security Payload (ESP)** –
It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH)** –
It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.



3. **Internet Key Exchange (IKE)** –
It is a network security protocol designed to **dynamically exchange encryption keys** and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides **message content protection** and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security –

1. The **host checks if the packet should be transmitted using IPsec or not**. These packet traffic triggers the **security policy** for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 **hosts(using IPsec) authenticate themselves** to each other to **start a secure channel**. It has 2 **modes**. The **Main mode** which provides the **greater security** and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts **negotiate the type of cryptographic algorithms** to use on the session and agreeing on **secret keying material** to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the **communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts**.

IPsec Tunnel vs. Transport Mode

In order to authenticate data packets and guarantee their integrity, IPsec includes two protocols. These are the AH (Authentication Header) protocol and the ESP (Encapsulating Security

Payload) protocol. Both protocols, in turn, support two encapsulation modes—tunnel mode and transport mode. Let's break down their core differences.

Tunnel Mode

In tunnel mode, the entire original IP packet is encapsulated to become the payload of a new IP packet. Additionally, a new IP header is added on top of the original IP packet. Since a new packet is created using the original information, tunnel mode is useful for protecting traffic between different networks. An additional advantage of this mode is that it makes it very easy to establish a "tunnel" between two secure IPsec gateways.

These IPsec gateways in turn can connect two different networks securely. Using secure IPsec proxies like the ones shown in the diagram below can be very useful for connecting two distant branches using an encrypted connection.

The process used by IPsec to encapsulate the original IP header differs depending on whether AH tunnel mode or ESP tunnel mode is used:

1. The original packet is encapsulated in a new IP packet (both its IP header and its payload).
2. In the case of AH tunnel mode, an AH header and a new IP header are added. For ESP tunnel mode, an ESP header, a new IP header, an ESP trailer, and an ESP authentication trailer are added.
3. When AH tunnel mode is used, the entire packet is signed for integrity and authentication. But when ESP tunnel mode is used, the encapsulated packet between the ESP header and the ESP trailer is signed for integrity and authentication. The new packet can also be encrypted for greater security.

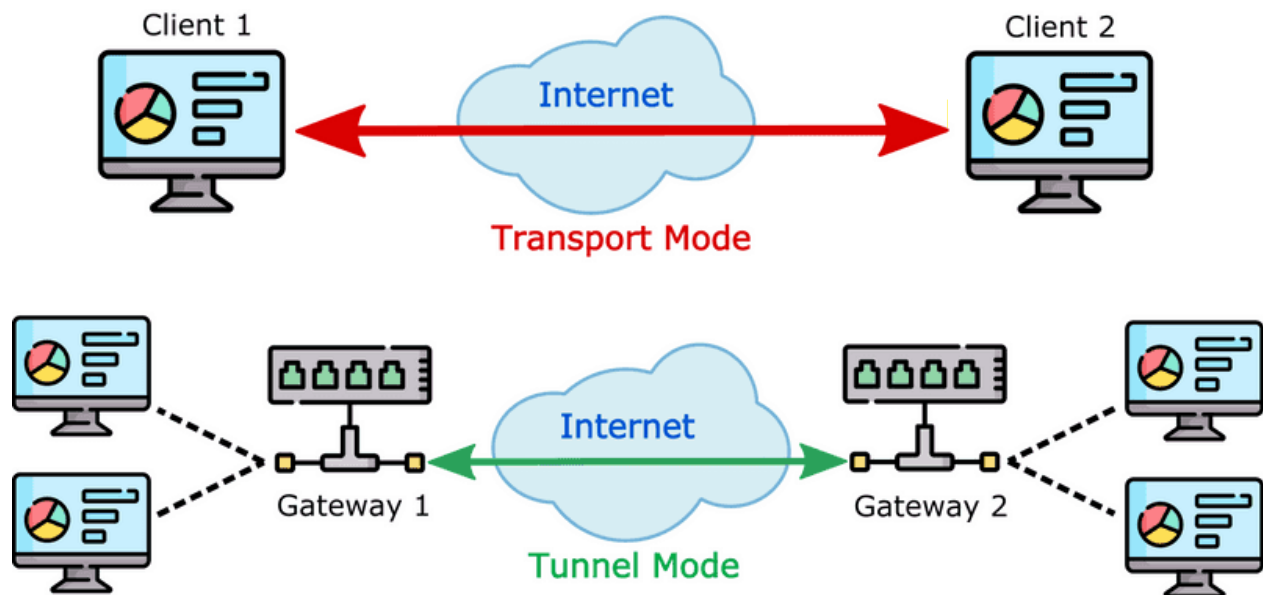
Transport Mode

The main difference in transport mode is that it retains the original IP header. In other words, payload data transmitted within the original IP packet is protected, but not the IP header. In transport mode, encrypted traffic is sent directly between two hosts that previously established a secure IPsec tunnel.

Since a new IP header isn't created, the process used by transport mode is less complex than tunnel mode:

1. Depending on the protocol used, a new AH or ESP header is created and inserted just after the original IP header.
2. For the ESP protocol, both an ESP trailer and an ESP authentication trailer are created and added after the original package.
3. When using AH transport mode, the entire packet is signed for integrity and authentication. For ESP transport mode, the original packet payload is signed by authentication (that is, not including its IP header) and encrypted if required.

IPSec Modes



A diagram showing IPSec encapsulation modes

When to Use IPSec Tunnel Mode

Tunnel mode is most commonly used for configurations that need a secure connection between two different networks, separated by an intermediate untrusted network (like the Internet).

Typical tunnel mode use cases are gateway-to-gateway, server-to-gateway, and server-to-server. Here's a list of various reasons why tunnel mode works best for these use cases:

- Tunnel mode protects internal routing information by encrypting the original packet's IP header by creating a new IP header on top of it. This allows tunnel mode to protect against traffic analysis, since attackers can only determine the tunnel endpoints.
- Tunnel mode is mandatory when one of the peers is a security gateway applying IPSec on behalf of another host. In other words, it's more compatible with existing gateways than transport mode.
- Tunnel mode makes it easier to traverse NATs.
- Both VPN clients and VPN gateways can use IPSec tunnel mode.

Despite its advantages, tunnel mode has a greater overhead and smaller MTU than transport mode.

When to Use IPSec Transport Mode

Transport mode is commonly used when fast and secure end-to-end communications are required, such as client-server communications (workstation-to-gateway and host-to-host scenarios). Reasons to use transport mode include:

- Transport mode provides end-to-end security (authentication, integrity, and anti-replay protection).
- Transport mode has a larger MTU than tunnel mode.
- Transport mode has a lower overhead than tunnel mode.

Transport mode is not without its flaws. It has poor compatibility with security gateways, as well as greater difficulty in implementing traversal NATs. For this reason, transport mode can't be used in protected gateway-to-gateway configurations.

Setting Each Mode Up

To successfully set up each mode, it's essential to know how IPsec negotiates packet security using the IKE (Internet Key Exchange) protocol.

During the IPsec tunnel set up, the peers establish security associations (SA), defining which parameters will be used to secure the traffic between them. The process of negotiating such parameters happens in two phases:

IKE Phase 1: This phase creates a secure tunnel to protect the negotiation messages peers will exchange in the second phase.

IKE Phase 2: During this phase, the SA parameters of a second IPsec tunnel are negotiated. While the first tunnel is used to protect SA negotiations, this tunnel protects the data.

Once the secure tunnel (IKE Phase 2) has been established, IPsec protects the traffic sent between the two tunnel endpoints. It does this by applying the security parameters defined by the SAs during tunnel configuration. The encapsulation mode is part of these parameters.

For clarification, IPsec only uses the IKE protocol to build secure tunnels between the two devices and set up SA parameters. Authentication and encryption are handled by the AH and ESP protocols, respectively.

Regardless of whether you use tunnel mode or transport mode, the encapsulation mode used by the AH and ESP protocols must be set up during IKE Phase 2—before the actual data transmission.