CyberBruhArmy Follow
Apr 8, 2020 · 5 min read · Listen

Save

IPSEC VPN In Details

IPsec (Internet Protocol Security) is a framework that helps us to protect IP traffic on the network layer. Why? because the IP protocol itself doesn’t have any security features at all. IPsec can protect our traffic with the following features:

Confidentiality : by encrypting our data, nobody except the sender and receiver will be able to read our data.

Integrity : we want to make sure that nobody changes the data in our packets. By calculating a hash value , the sender and receiver will be able to check if changes have been made to the packet.

Authentication : the sender and receiver will authenticate each other to make sure that we are really talking with the device we intend to.

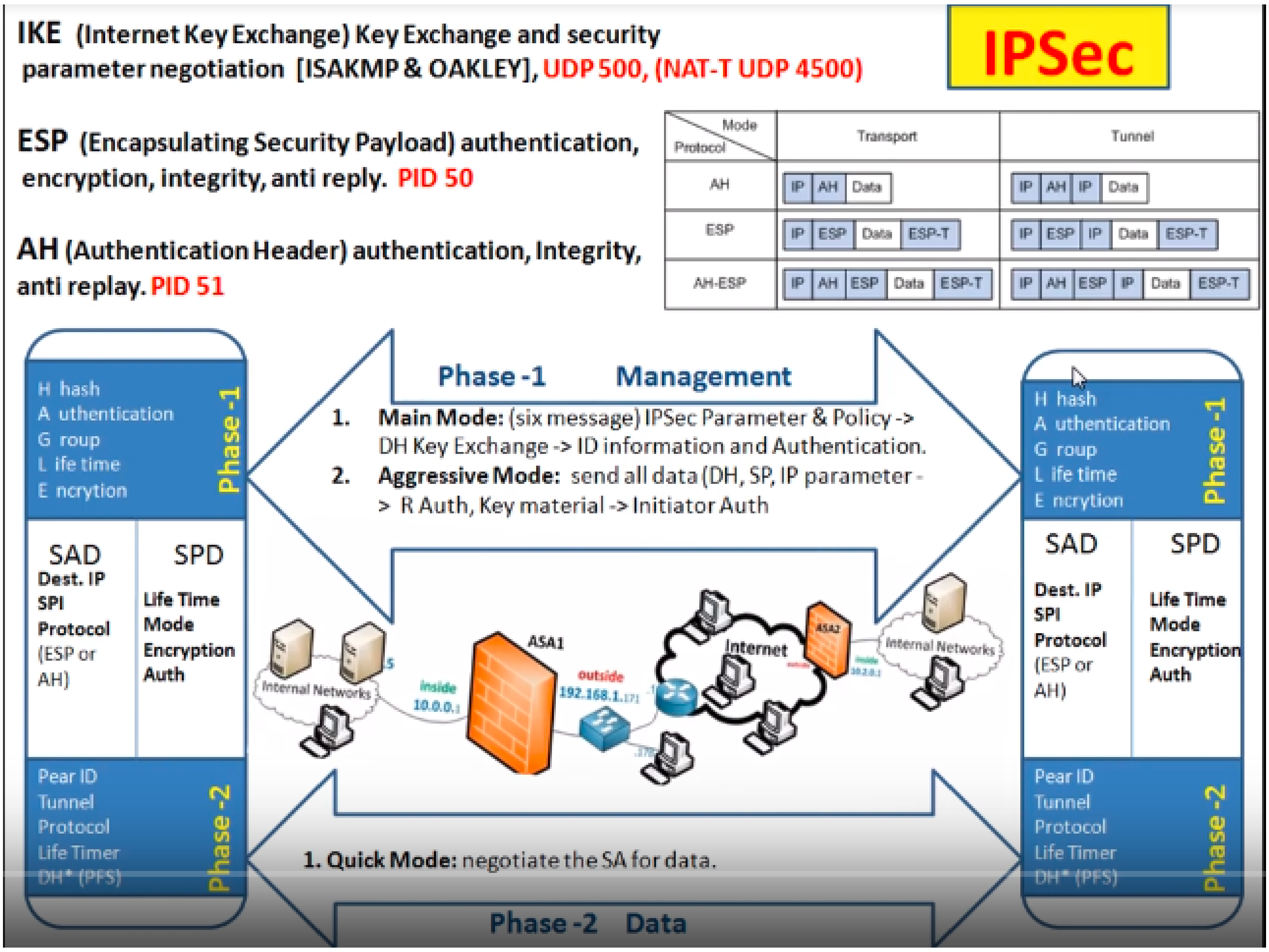
Anti-replay : even if a packet is encrypted and authenticated, an attacker could try to capture these packets and send them again. By using sequence numbers, IPsec will not transmit any duplicate packets

To establish an IPsec tunnel, we use a protocol called IKE (Internet Key Exchange) and parameter negotiation (ISAKMP & OAKLEY) UDP-500 (NAT-T UDP 4500)

ESP (Encapsulating Security Payload)- Provide Encryption, Authentication, Integrity, anti-replay PID- 50

AH (Authentication Header) — Provide only Authentication, Integrity, anti-replay PID-51

AH and ESP both offer authentication and integrity but only ESP supports encryption



IPSec

IKE (Internet Key Exchange) Key Exchange and security parameter negotiation [ISAKMP & OAKLEY], UDP 500, (NAT-T UDP 4500)

ESP (Encapsulating Security Payload) authentication, encryption, integrity, anti reply. PID 50

AH (Authentication Header) authentication, Integrity, anti replay. PID 51

Mode / Protocol	Transport	Tunnel
AH	IP | AH | Data	IP | AH | IP | Data
ESP	IP | ESP | Data | ESP-T	IP | ESP | IP | Data | ESP-T
AH-ESP	IP | AH | ESP | Data | ESP-T	IP | AH | ESP | IP | Data | ESP-T

Phase -1 Management

1. **Main Mode:** (six message) IPSec Parameter & Policy -> DH Key Exchange -> ID information and Authentication.
2. **Aggressive Mode:** send all data (DH, SP, IP parameter -> R Auth, Key material -> Initiator Auth

Phase -1

H hash
A uthentication
G roup
L ife time
E ncrytion

SAD
Dest. IP
SPI
Protocol
(ESP or AH)

SPD
Life Time
Mode
Encryption
Auth

Phase -2

Pear ID
Tunnel
Protocol
Life Timer
DH* (PFS)

1. **Quick Mode:** negotiate the SA for data.

Phase -2 Data

IPSEC has two phases (IKE Phase-1 Management Traffic & IKE Phase-2 Data Traffic)

Step 1: Negotiation

(Hashing : MD5 or SHA, Authentication : pre-shared key or digital certificates, DH (Diffe Hellman) group: key exchange process, Lifetime : how long does the IKE phase 1 tunnel stand up?, Encryption : DES, 3DES or AES

Step 2: DH Key Exchange

Once the negotiation has succeeded, the two peers will know what policy to use. They will now use the DH group that they negotiated to exchange keying material. The end result will be that both peers will have a shared key.

Step 3: Authentication

The last step is that the two peers will authenticate each other using the authentication both peers can send and receive on this tunnel.

The three steps above can be completed using two different modes: Main mode & Aggressive mode

There are two tunnel modes in IPSEC VPN

1> Tunnel Mode

IPsec VPNs that work in tunnel mode encrypt an entire outgoing packet , wrapping the old packet in a new, secure one with a new packet header and ESP trailer.

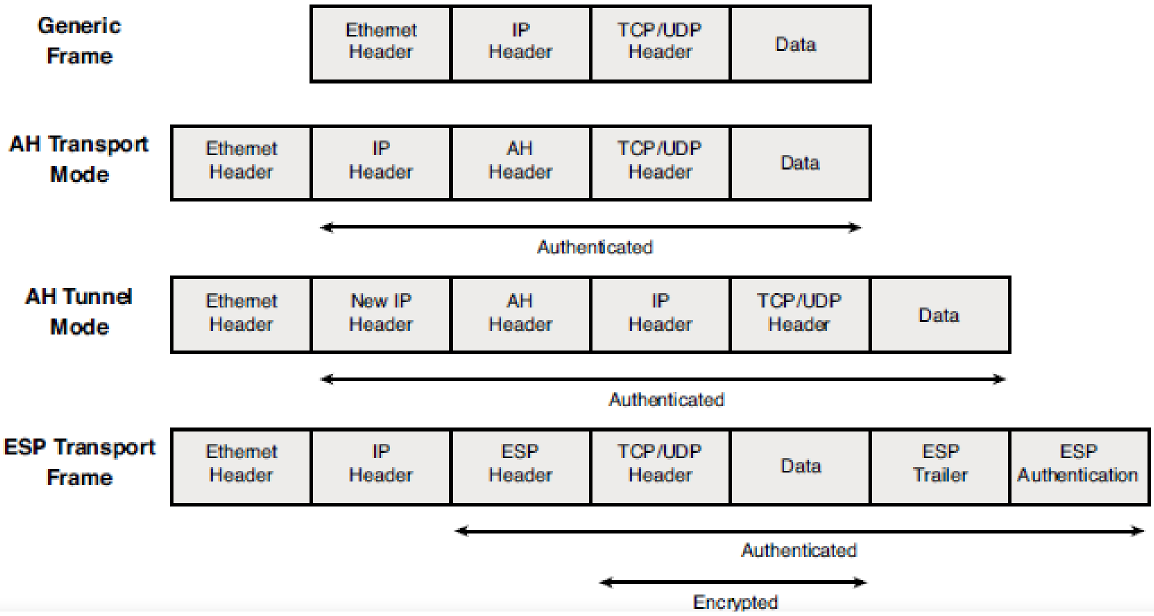
They also authenticate the receiving site using an authentication header in the packet.

Tunnel mode IPsec VPN is typically implemented on a secure gateway, such as on a firewall or router port, which acts as a proxy for the two communicating sites.

2>Transparent Mode

Transport mode on the other hand only encrypts the IP payload and ESP trailer being sent between two sites.

Usually meant for use in end-to-end communication between sites, transport mode doesn't alter the IP header of the outgoing packet.



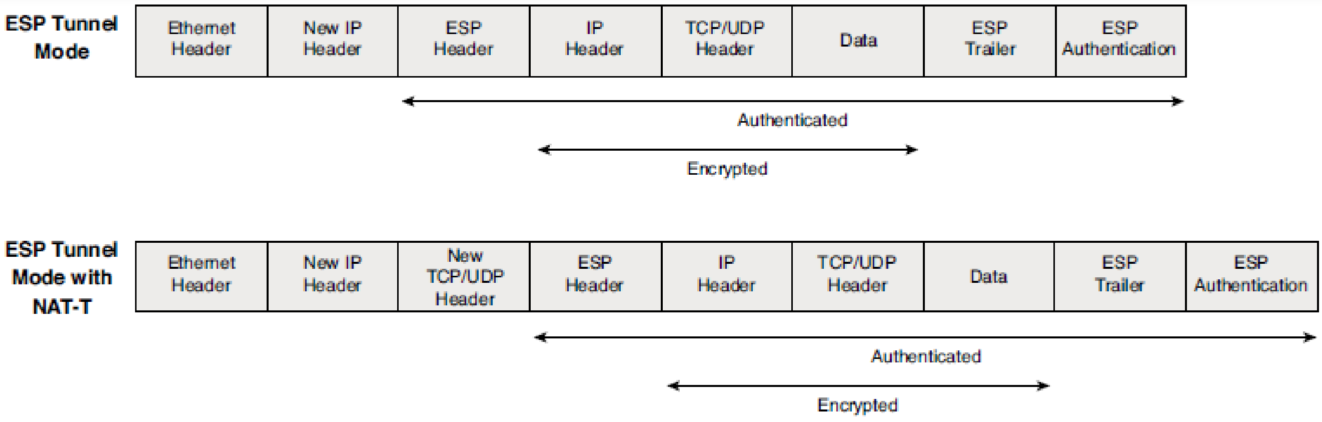


Figure 1-6 *ESP and ESP with NAT-T Frame Format*

How IPSec Works

IPSec involves many component technologies and encryption methods. Yet IPSec's operation can be broken down into five main steps. The five steps are summarized as follows:

Interesting traffic initiates the IPSec process -Traffic is deemed interesting when the IPSec security policy configured in the IPSec peers starts the IKE process.

Negotiates IPSec Security Parameters, IPSec Transforms Sets

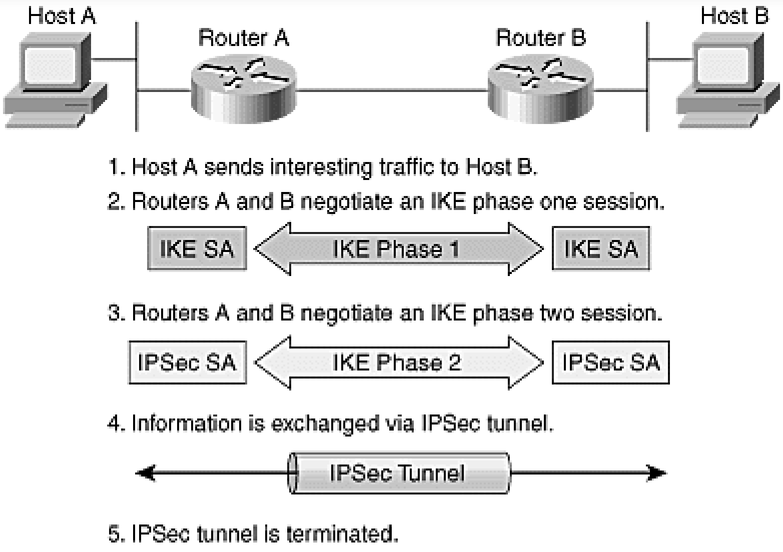
Establishes IPSec SAs security association

Periodically renegotiates IPSec SAs to ensure security

Optimally, performs an additional DH exchange

Data transfer -Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

IPSec tunnel termination -IPSec SAs terminate through deletion or by timing out.

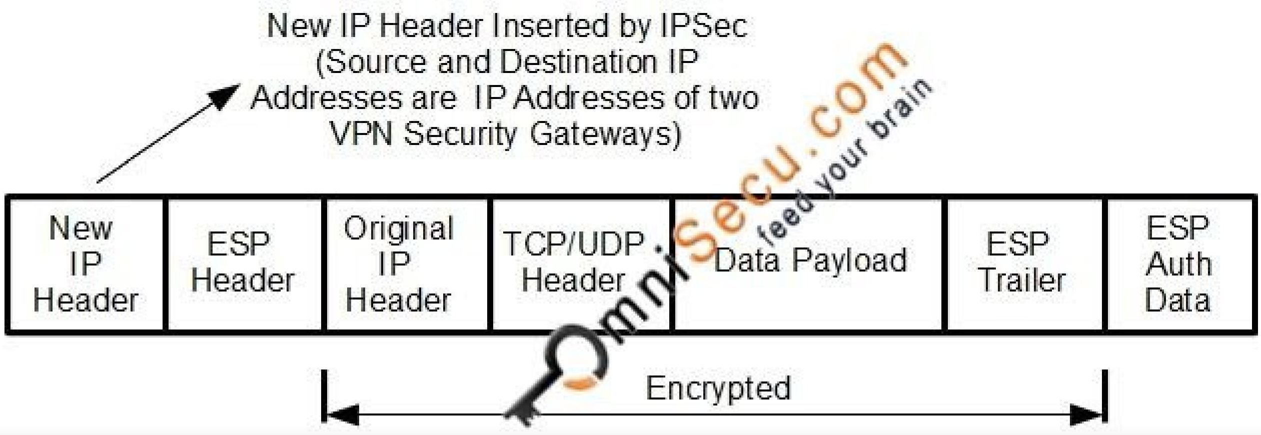

Host A
Router A
Router B
Host B
1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE phase one session.
IKE SA
IKE Phase 1
IKE SA
3. Routers A and B negotiate an IKE phase two session.
IPSec SA
IKE Phase 2
IPSec SA
4. Information is exchanged via IPSec tunnel.
IPSec Tunnel
5. IPSec tunnel is terminated.

The keys negotiated for IKE and IPsec/CHILD SAs should only be used for a limited amount of time and to protect a limited amount of data. This means that each SA should expire after a specific lifetime. To avoid interruptions a replacement SA may be negotiated before that happens, which is called “rekeying”.

http://www.omnisecu.com/tcpip/what-is-nat-traversal-in-ipsec.php

IPSec does not work if we have a NAT Device between two IPSec peers, performing Port Address Translation. It is not possible for the IPSec ESP packets to traverse (Travel across or pass over) across a NAT Device performing PAT.

When IPSec is used to secure IPv4 traffic, original TCP/UDP Port Numbers are kept encrypted and encapsulated using ESP. Following image shows how IPSec encapsulates IPv4 datagram.



Difference between Policy Based VPN and Route Based VPN

Route Based VPN:

A route-based VPN creates a virtual IPSec interface, and whatever traffic hits that interface is encrypted and decrypted according to the phase 1 and phase 2 IPSec settings.

Route based VPN is more flexible, more powerful and recommended over policy based. However, a policy-based VPN is usually simpler to create.

If your requirement is to create redundant VPN connections and your firewall is in route\NAT mode (99% of the time it is) then use a route-based VPN.

A static route is also required for a route-based VPN,

so, anything destined to the remote network must go through the virtual IPSec interface which was created when specifying this within the Phase 1 settings.

Policy Based VPN:

In policy-based VPN the tunnel is specified within the policy itself with an action of "IPSec".

Also, for policy-based VPN only one policy is required.

A route-based VPN is created with two policies, one for inbound and another for outbound with a normal "Accept" action