IP Security (IPSEC)

collection of protocols.
To provide security to data in transit.

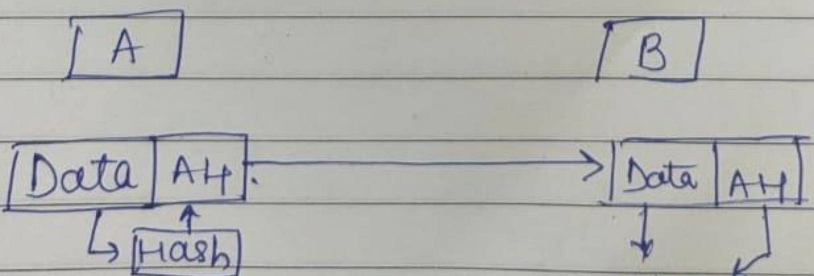
It ensures the data confidentiality integrity & authenticity of data transmitted over different type of network.

In IPSEC, there are three important components -

→ Key exchange
→ MODES
→ Protocol

Security Protocols.

1. Authentication Header (AH)



The data is hashed and hash value is attached.

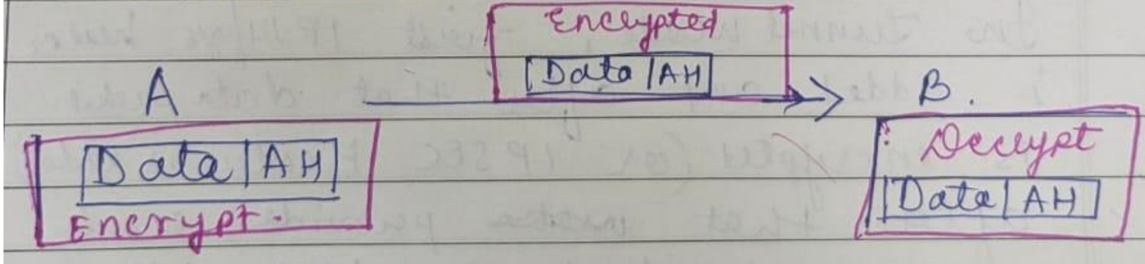
Ensures Integrity not security.

at the receiver's end hash value is compared with the generated hash value of received data.

2. Encapsulating Security Payload (ESP) Protocol.

Ensures: Confidentiality, integrity & authentication.

It is appended in previous protocol (AH). In AH, the data and its hashed value are sent to receiver to ensure integrity (data is not modified). Here, ~~Data+AH~~ we encrypt the data and Hash value combo. to ensure confidentiality and authentication.



IPSEC Modes

When data packet is coming from transport layer to network layer a IP SEC header and trailer is appended at network layer to data packet.

The data packet coming from transport layer is with TCP or UDP it doesn't matter we just append IPSEC header and trailer like for example we keep it in a IPSEC envelope and IPSEC envelope is then inserted in IPV4 or IPV6 is envelope; which is task of Layer.
This is done in Transport Mode-

In Tunnel mode, first IPV4/V6 header is added and after that data packet is encrypted (or IPSEC Header is added) after that ~~make~~ provide route new IPV4/V6 header is added. This provides more security.

WORKING OF IPSEC

Step 1:

Host Recognition - The host will check if the packet is to be transmitted or not acc. to Security policies. To ensure it is properly encrypted.

Step 2:

IKE Phase 1: In this step, host devices (Sender & receiver) will authenticate each other to establish a secure channel.

There are 2 modes.

1. Main mode - better security.
2. Aggressive mode - faster.

Step 3:

IKE Phase 2: The hosts decide the type of cryptographic algo. to apply over the session. and share the secret keys.

Step 4:

IPSEC Transmission

Data is transmitted under the

inspection of Security Associations (SA).

Step 5

IPSEC Termination:

After the completion of data exchange or session timeout, the IPsec tunnel is terminated & the security key is discarded by the hosts.

Internet Key Exchange (IKE)

Protocol is used to set up a Security association (SA) in IPsec.
There are two protocols implemented in IKE :-

Oakley.
SKEME

IKE is a hybrid protocols implements above two protocols within an internet security association & key mangement ~~ISAKA~~ (ISAKMP), protocol.
ISAKMP is used for establishing security associations and securing connections between hosts.
There are two phases in IKE as explained in step 2 & step 3 of IPSec working.