1. IP Security (IPSec)

- The IP Security (IPSec) is an Internet Engineering Task Force (IETF) standard
- IP security is a security N/w protocol suite that authentication and encryption of secure encrypted communication b/w two computers over internet
- IP security can protect data b/w a pair of host and pair of security gateway b/w security gateway and host

Uses of IP security

- 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 N/w data by setting up circuit using IPSec tunneling in which all data is being sent b/w the two endpoints is encrypted, as with a VPN connection.

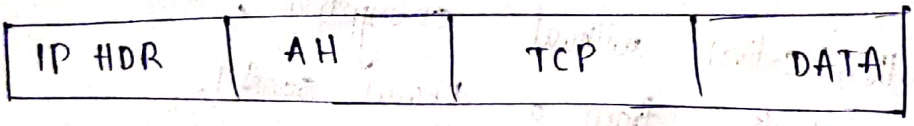
Components of IP Security

1. Encapsulating Security payload (ESP)

* it provides data integrity, encryption, authentication and anti replay, it also provides authentication for payload.

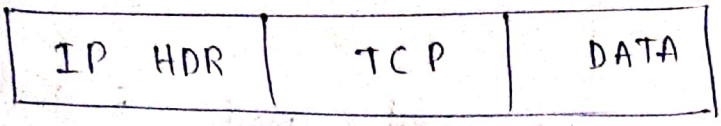
2. Authentication Header (AH)

* it also provides data integrity, authentication and anti replay and it does not encryption.
* the anti replay protection, protects against unauthorized transmission of packets.
* it does not protect data's confidentiality.

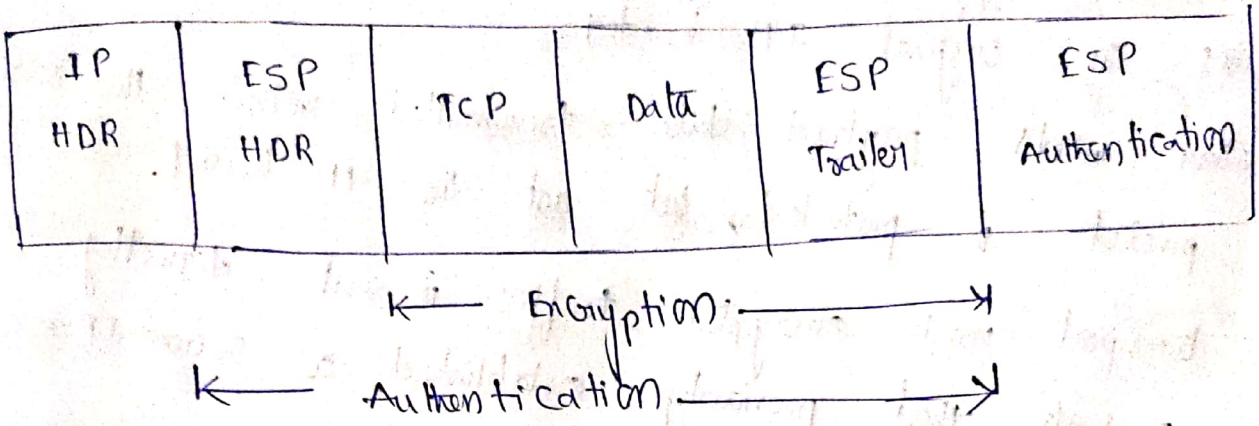


3. Internet Key Exchange (IKE)

* it is a n/w security protocol designed to dynamically exchange encryption keys and find a way over security association (SA) b/w two devices.
* the Security Association (SA) establishes shared security attributes b/w 2 network entities to support secure communication.



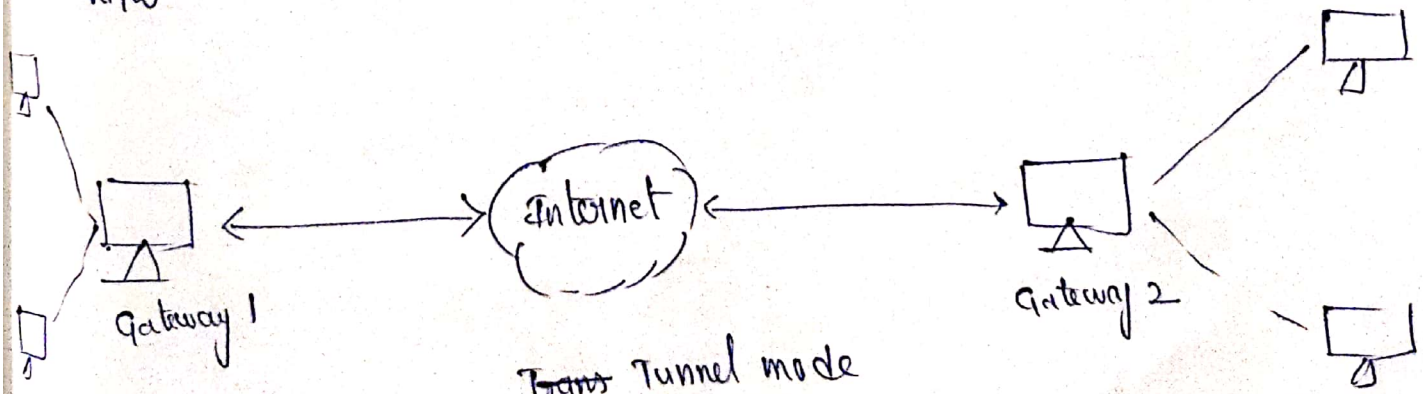
original packet



Modes of IPSec

1. 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.
- tunnel mode is useful for protecting traffic b/w different N/w



Trans Tunnel mode

2. 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 b/w 2 hosts that previously established a secure IPsec tunnel.