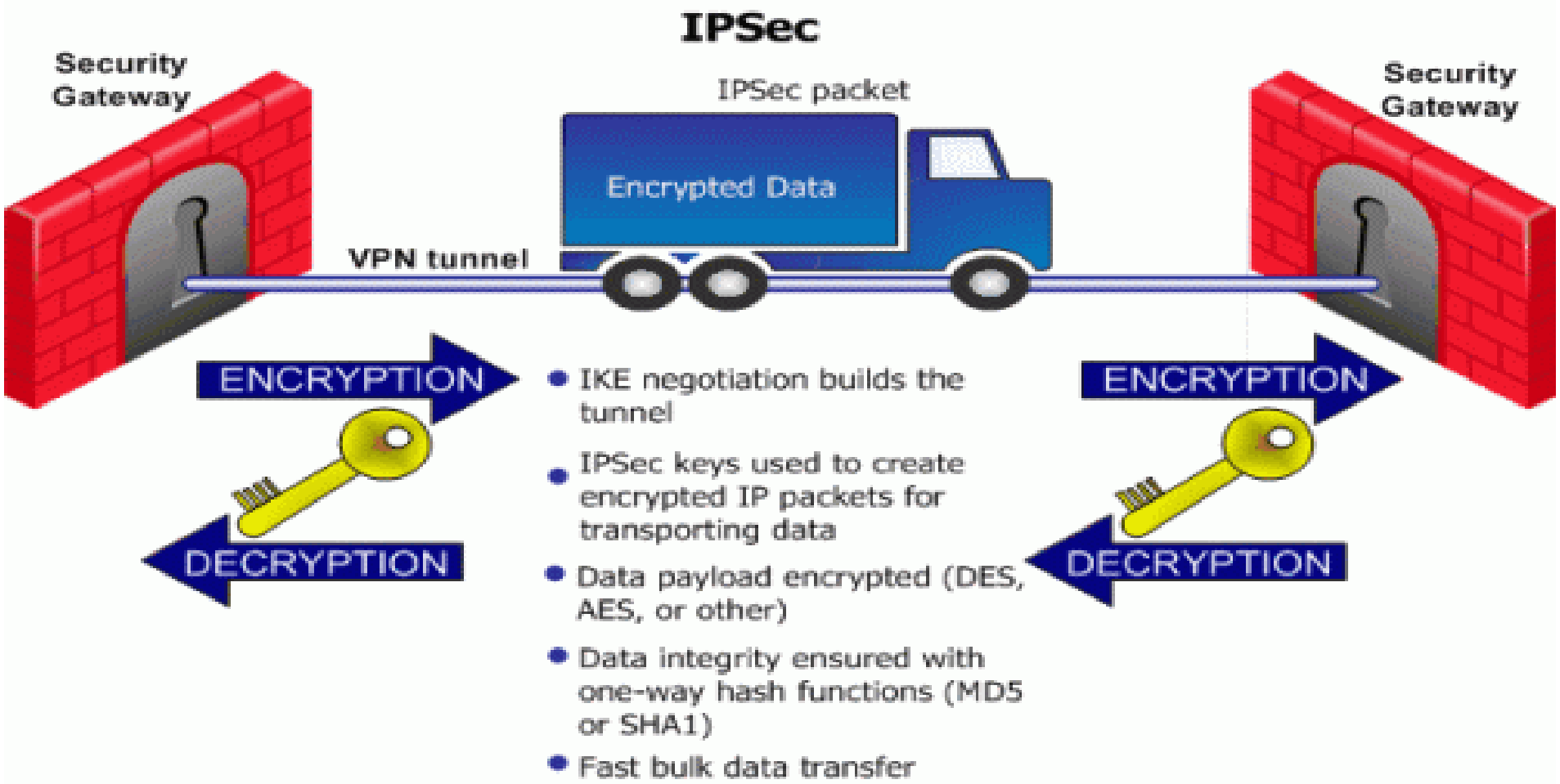
IPSec
Internet Protocol Security



Why IPSec??

- IP protocol was designed in the late 70s to early 80s
  - ➢ Part of DARPA Internet Project
  - ➢ Very small network
    - All hosts are known!
    - So are the users!
    - Therefore, security was not an issue

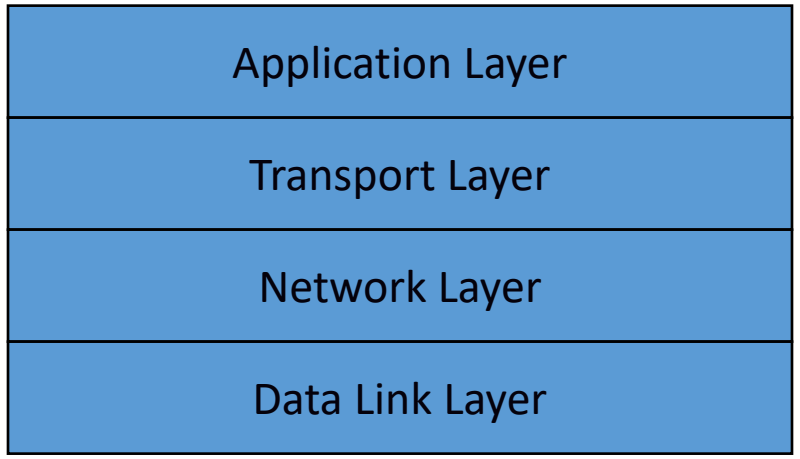
source spoofing
replay packets
no data integrity or confidentiality

- DOS attacks
- Replay attacks
- Spying
- and more…

Fundamental Issue:

Networks are not (and will never be) fully secure!!!!

Security at Different Layers



PGP, Kerberos, SSH, etc.

Transport Layer Security (TLS)

IP Security

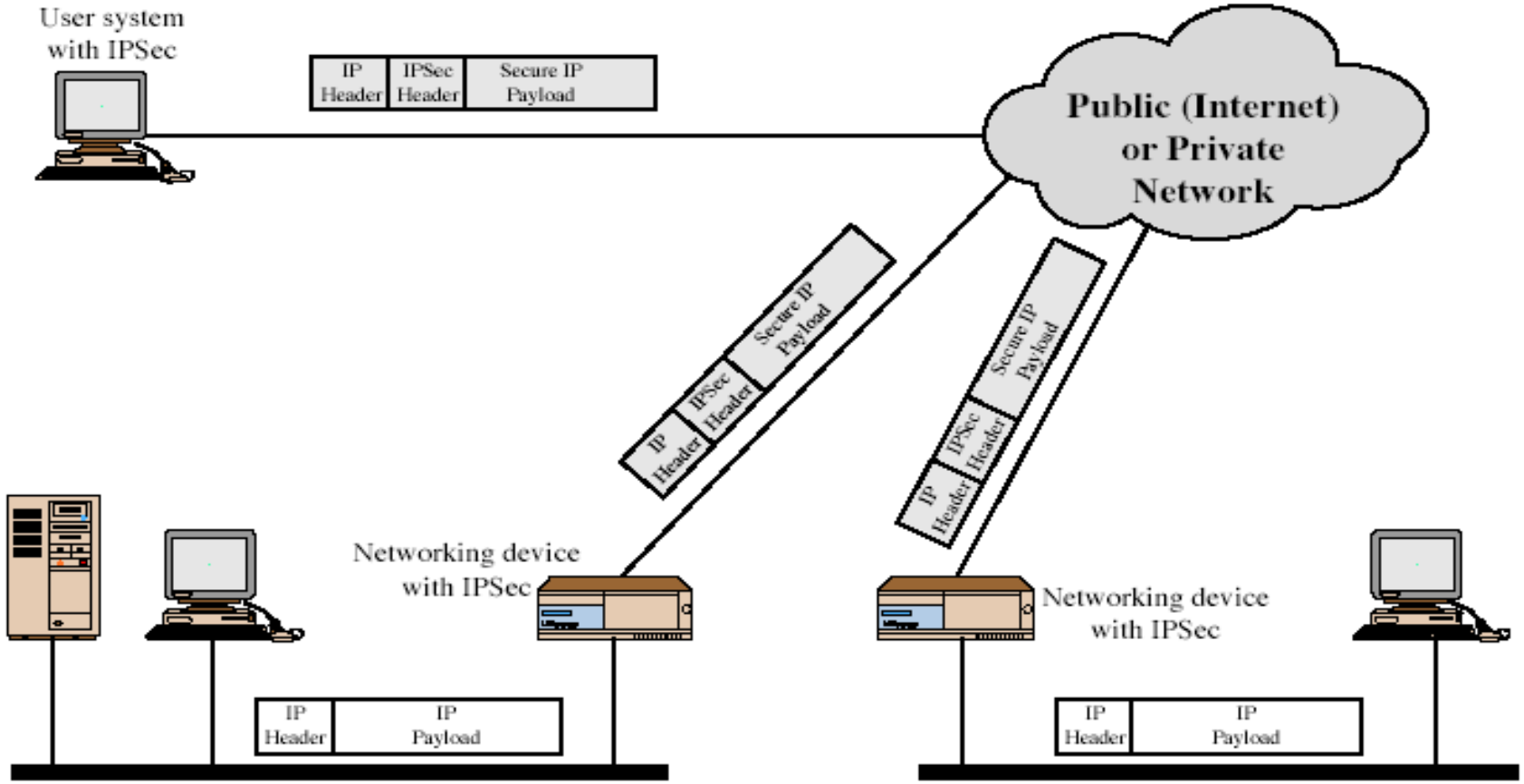
Hardware encryption

- Internet Protocol security (IPSec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services.
- IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection.

Applications of IPSec

- ☺ Secure Branch Office Connectivity over the Internet
- ☺ Secure Remote access over the internet
- ☺ Establishing extranet and intranet connectivity with partners
- ☺ Enhancing electronic commerce security

- The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate *all* traffic at the IP level.
- Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.



- An organization maintains LANs at dispersed locations. Nonsecure 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

Benefits of IPSec

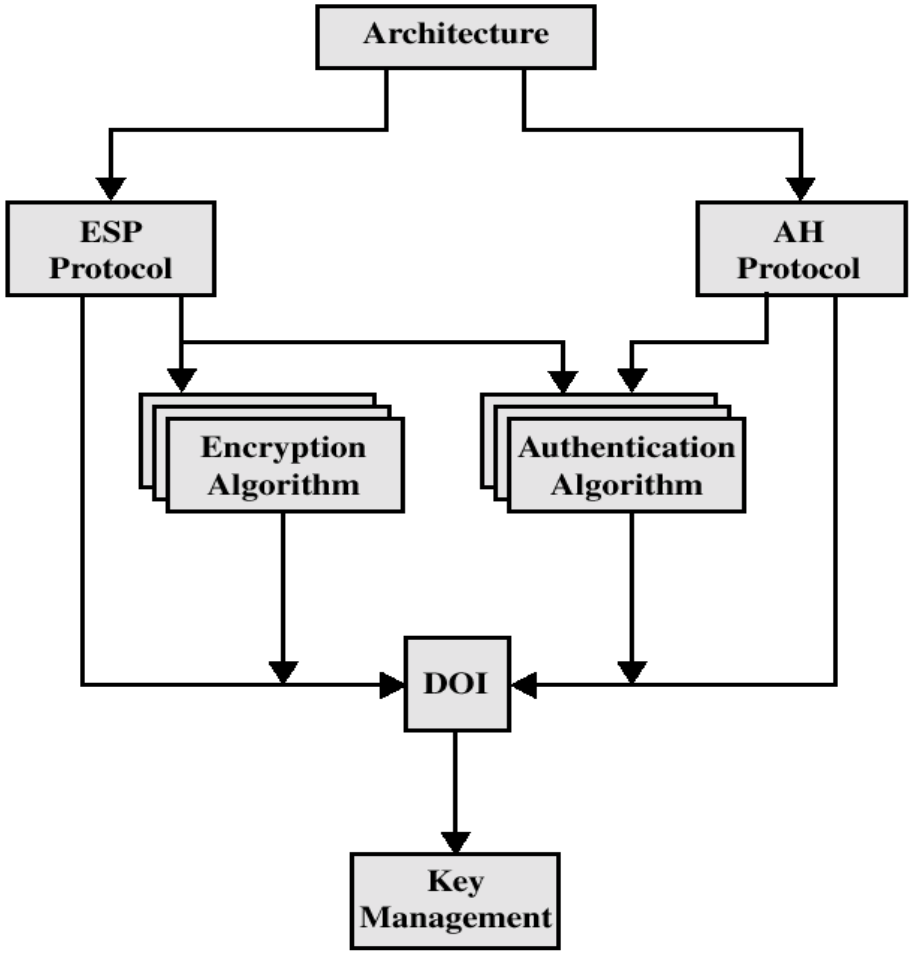
- Implemented in a firewall/router provides strong security to all traffic crossing the perimeter
- IPSec in a firewall/router is resistant to bypass
- Is below transport layer, hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users
- Plays a vital role in routing architecture
  - ✓ Ensures a router advertisement comes from an authorized router.
  - ✓Ensures a neighbour advertisement comes from an authorized router.
  - ✓A redirect message comes from the router to which the initial IP packet was sent
  - ✓A routing update is not forged

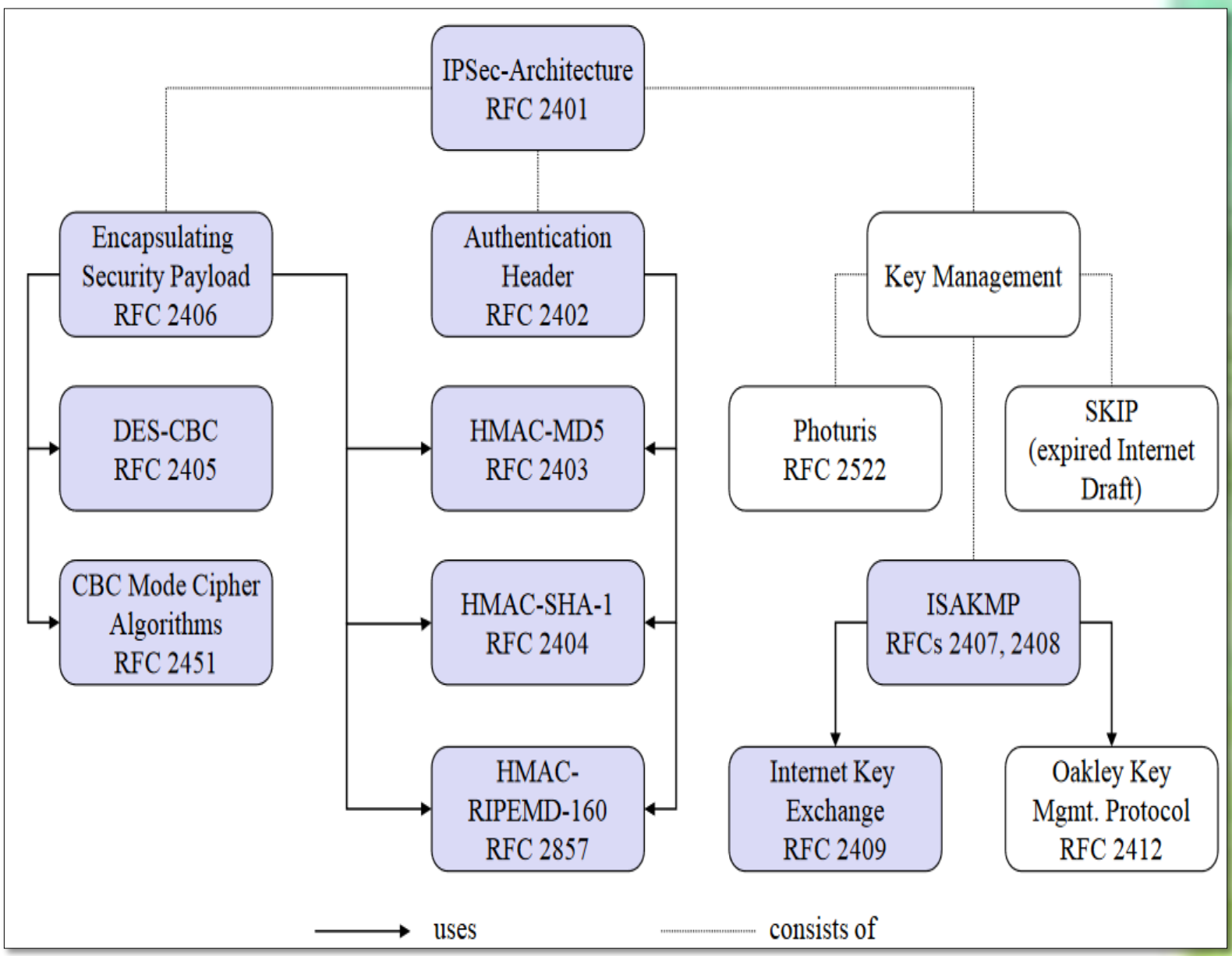
IPSec Documents

- The IPSec specification has become quite complex. The IPSec specification consists of numerous documents. The most important of these, issued in November of 1998, are
  - RFC 2401: An overview of a security architecture
  - RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
  - RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
  - RFC 2408: Specification of key management capabilities
- In addition to these four RFCs, a number of additional drafts have been published by the IP Security Protocol Working Group set up by the IETF. The documents are divided into seven groups.
  - **Architecture, Encapsulating Security Payload (ESP), Authentication Header (AH), Encryption Algorithm, Authentication Algorithm, Key Management & DOI**
- Support for these features is mandatory for IPv6 and optional for IPv4.

- ***Architecture:*** Covers the general concepts, security requirements, definitions, and mechanisms defining IPSec technology. Current specification is RFC 4301.
- ***Authentication Header (AH):*** Covers the packet format and general issues related to the use of AH for packet authentication. Current specification is RFC 4302.
- ***Encapsulating Security Payload (ESP):*** Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication. Current specification is RFC 4303.
- ***Encryption Algorithm:*** A set of documents that describe how various encryption algorithms are used for ESP.
- ***Authentication Algorithm:*** A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.
- ***Key Management:*** Documents that describe key management schemes. The main specification is RFC 4306, Internet Key Exchange (IKEv2) protocol.
- ***Domain of Interpretation (DOI):*** Contains values needed for the other documents to relate to each other. Other RFC's dealing with security policy and Management information base (MIB) content.

IPSec Document Overview





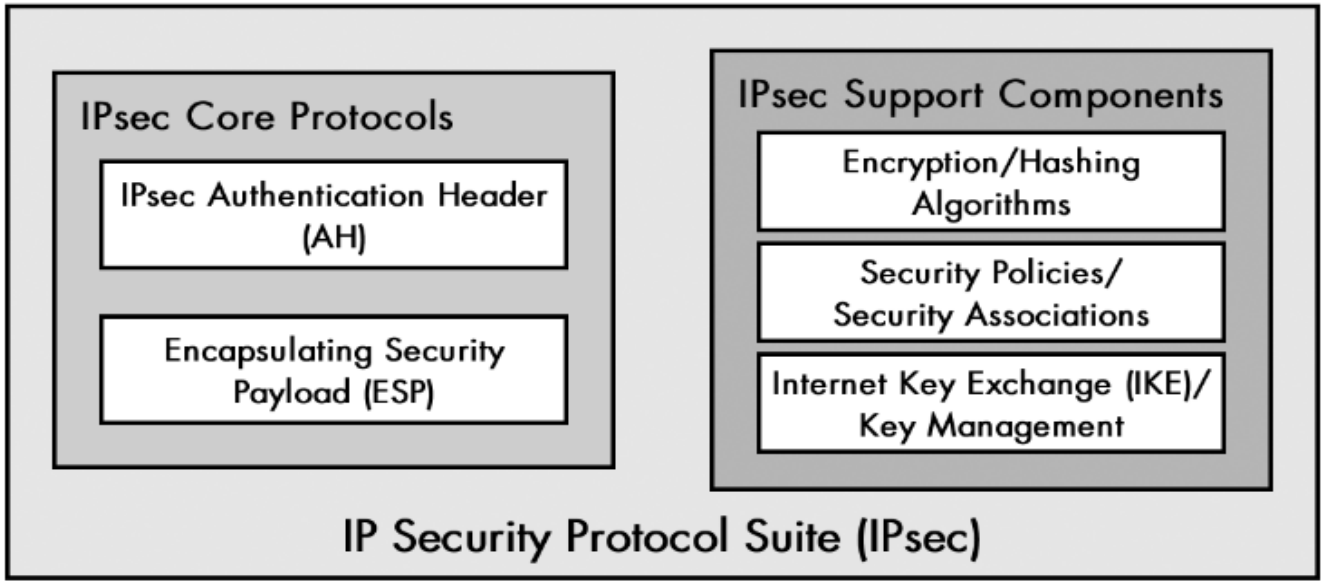
IPSec Services

- **Connectionless Integrity:-** Data integrity service is provided by IPSec via AH which prevents the data from being altered during transmission.
- **Data Origin Authentication**:- This IPSec service prevents the occurrence of replay attacks, address spoofing etc., which can be fatal
- **Access Control**:- The cryptographic keys are distributed and the traffic flow is controlled in both AH and ESP protocols, which is done to accomplish access control over the data transmission.
- **Confidentiality**:- Confidentiality on the data packet is obtained by using an encryption technique in which all the data packets are transformed into ciphertext packets which are unreadable and difficult to understand.
- **Limited Traffic Flow Confidentiality**:- This facility or service provided by IPSec ensures that the confidentiality is maintained on the number of packets transferred or received. This can be done using padding in ESP.
- **Replay packets Rejection**:- The duplicate or replay packets are identified and discarded using the sequence number field in both AH and ESP.

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

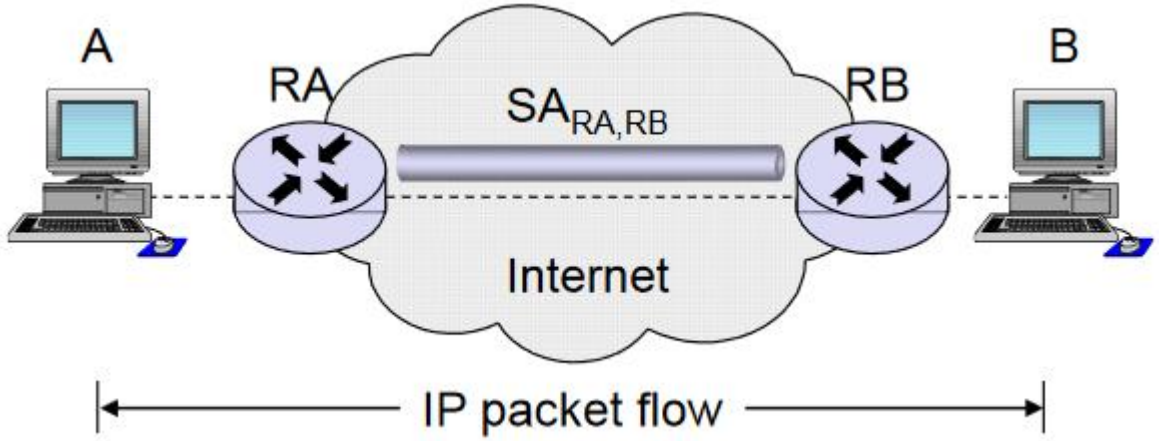
IPSec Protocols

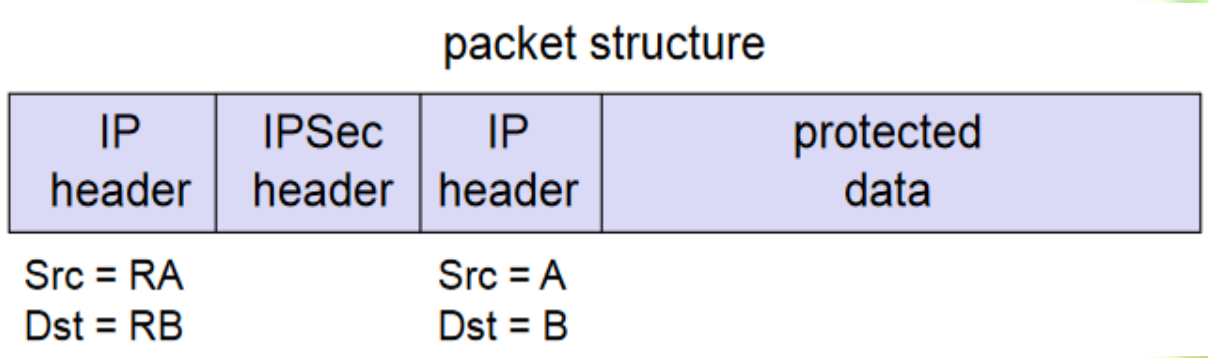
- The protocols used to provide security are the Authentication Header (AH) and Encapsulating Security Payload (ESP)
- Each protocol can be used in one of two modes
  - Transport mode – used to protect upper layer payloads of an IP packet (tcp, udp)
  - Tunnel mode – used to protect an entire IP packet including its payload (VPN)
- Transport mode is used as an SA between two hosts.
- Tunnel mode is used as an SA between two gateways or a host and gateway

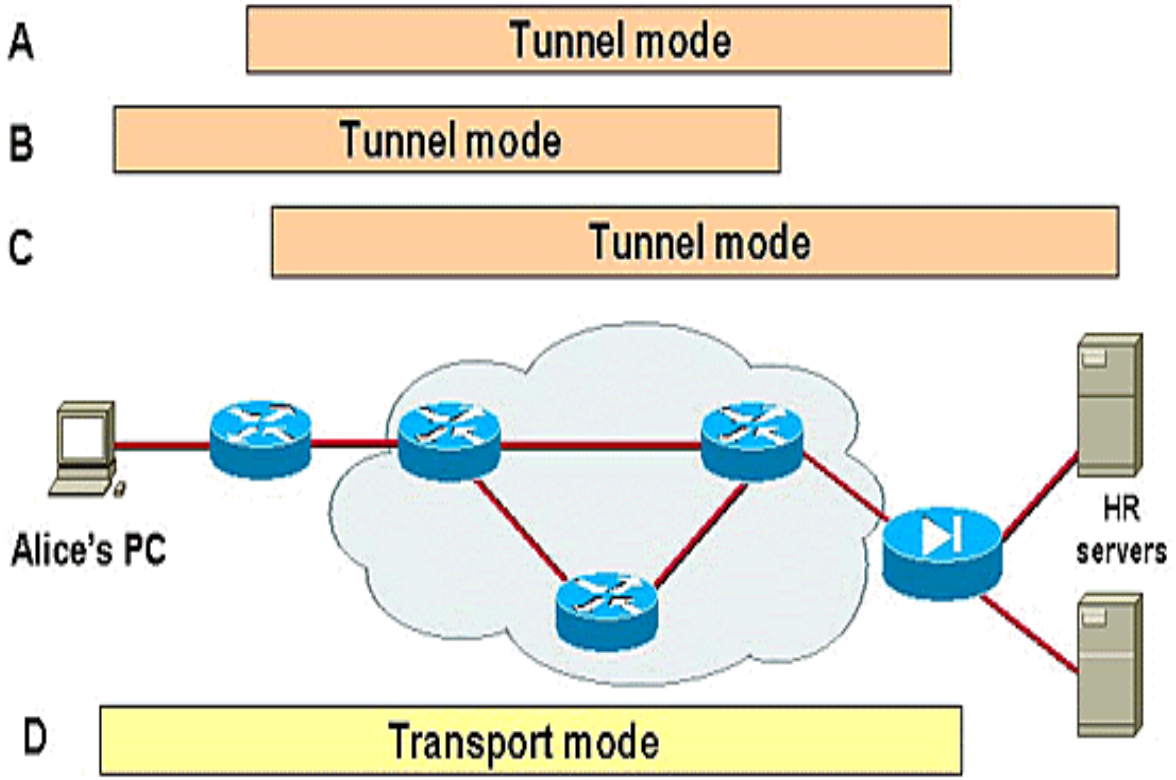


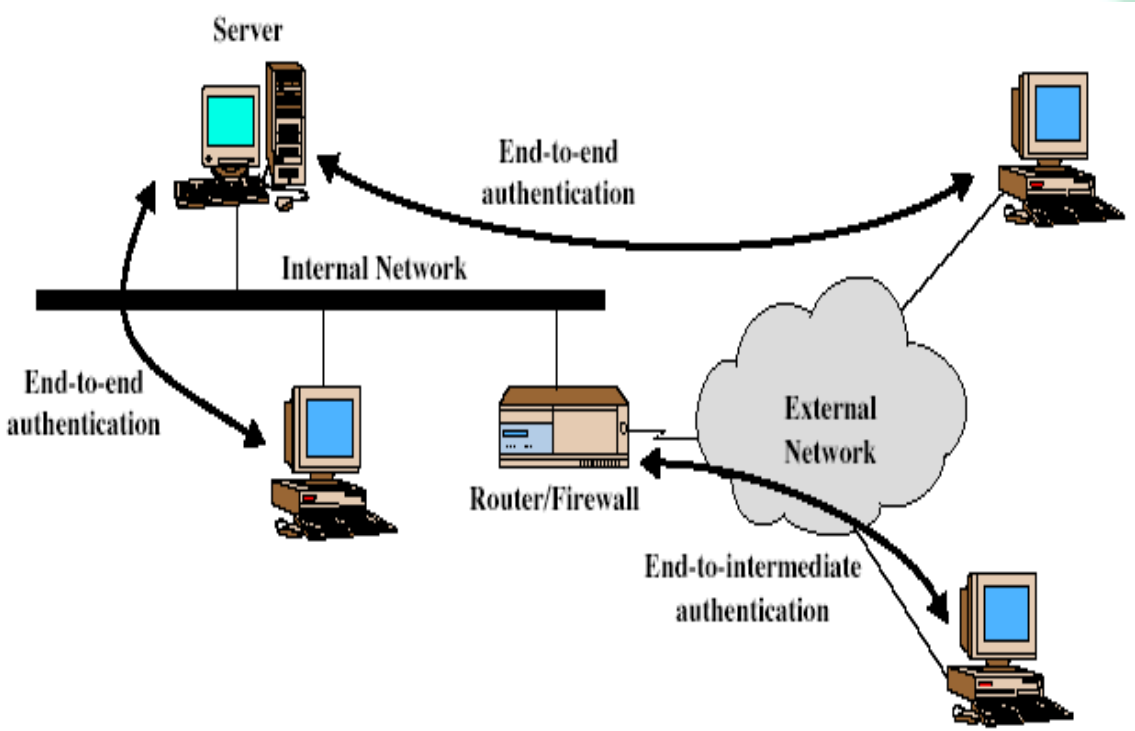
IPSec Protocol Modes

- **Transport mode** can only be used between end-points of a communication.
- **Tunnel mode** can be used with arbitrary peers.
- Transport mode is used when the “cryptographic endpoints” are also the “communication endpoints” of the secured IP packets
  - *Cryptographic endpoints: the entities that generate or process an IPSec header*
  - *Communication endpoints: source and destination of an IP packet*
- Tunnel mode is used when at least one “cryptographic endpoint” is not a “communication endpoint” of the secured IP packets.
  - This allows for gateways securing IP traffic on behalf of other entities





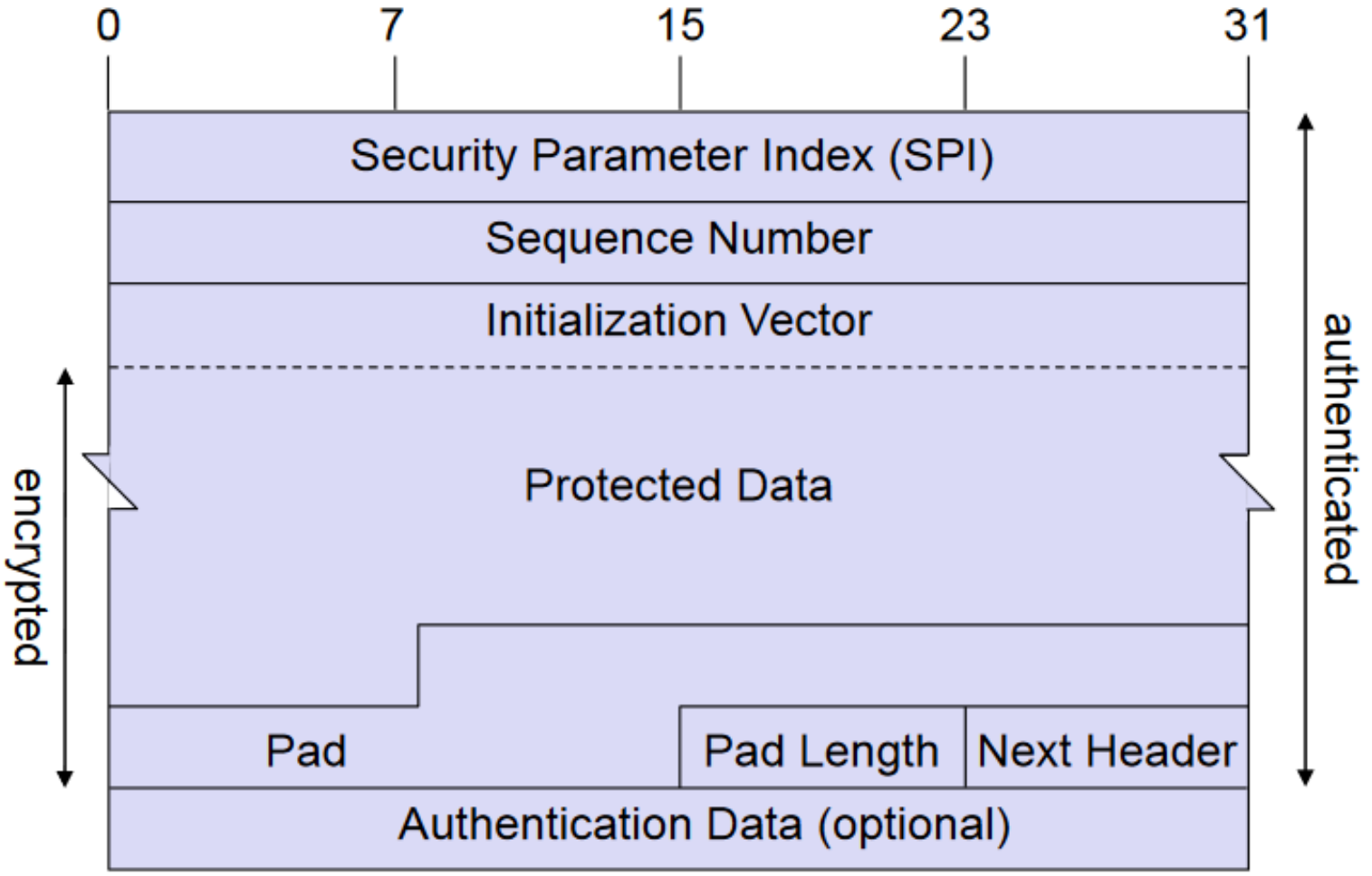




- Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
- Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

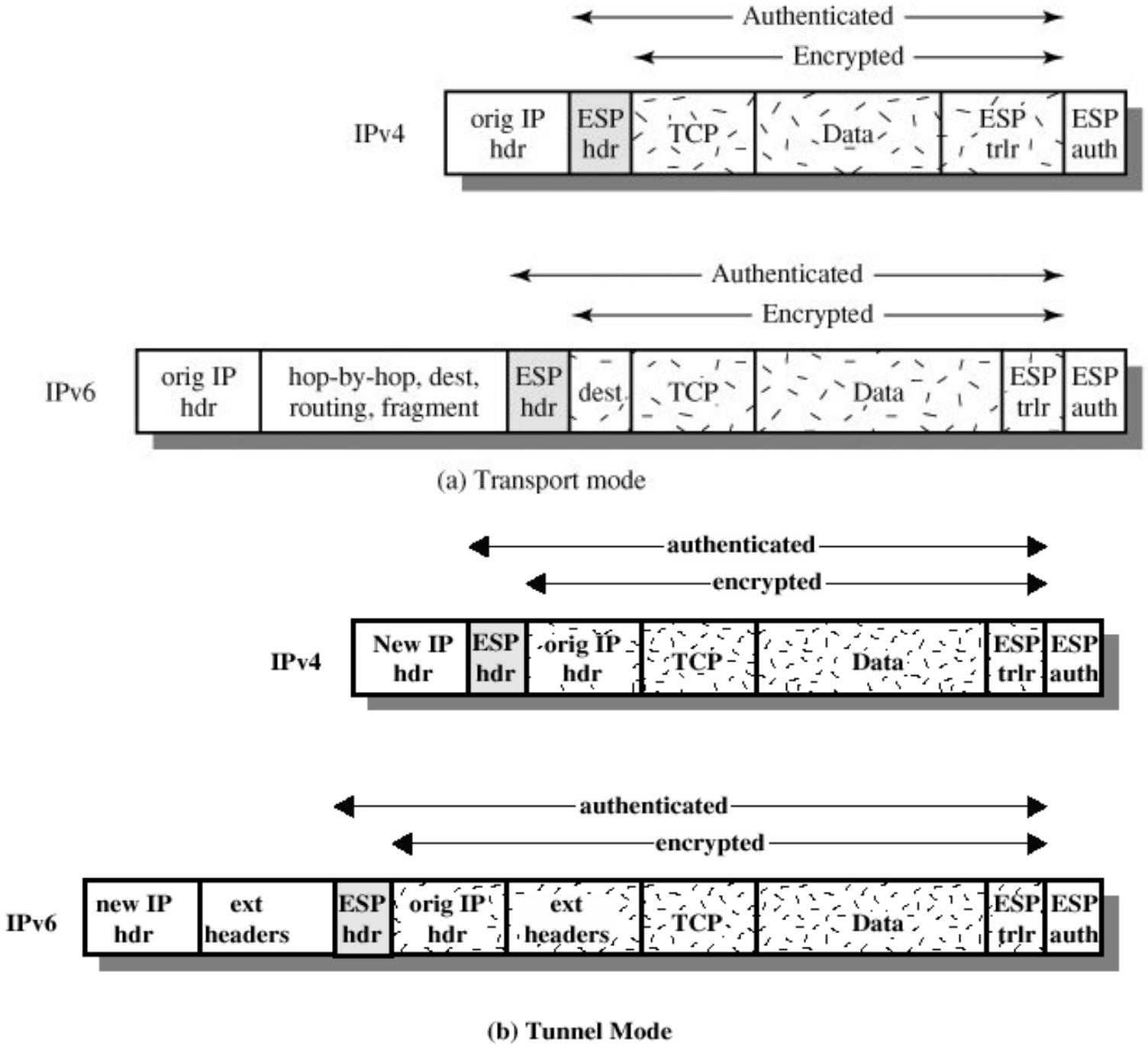
Encapsulating Security Payload (ESP) Protocol

- The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service.

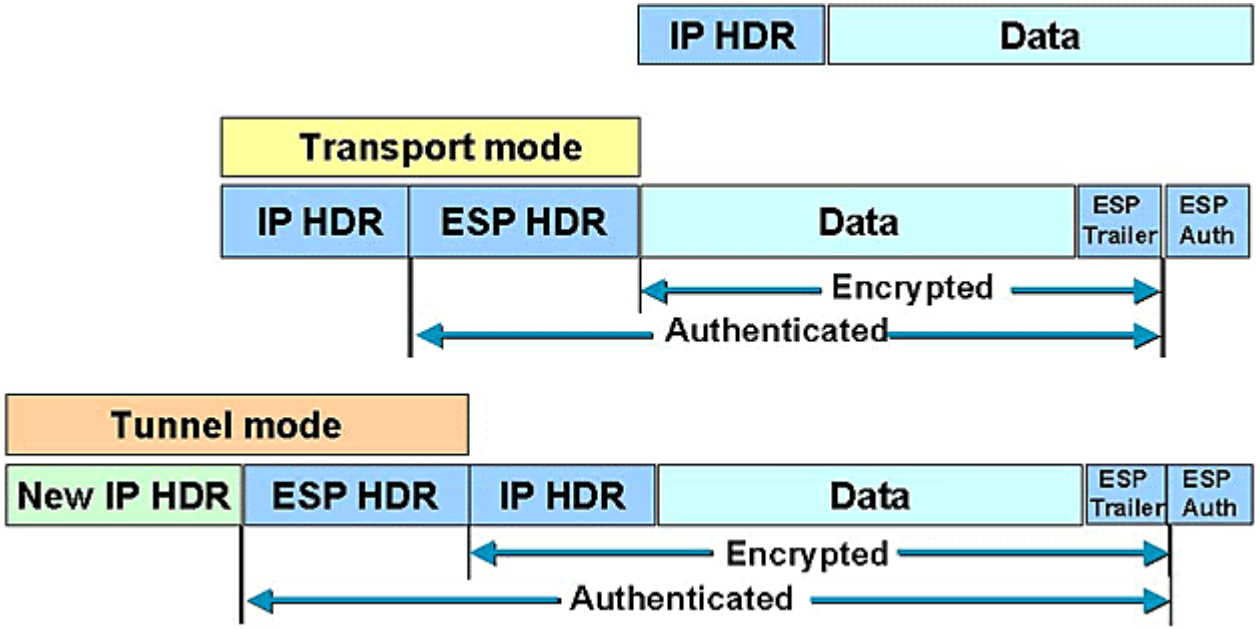


- The ESP header immediately follows an IP header or an AH header.
- The next-header field of the preceding header indicates “50” for ESP

- **Security Parameters Index** (32 bits): Identifies a security association.
- **Sequence Number** (32 bits): A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0-255 bytes):** This field is used to make the length of the plaintext to be a multiple of some desired number of bytes. It is also added to provide confidentiality.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
- **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.



- Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP.
- The entire transport-level segment plus the ESP trailer are encrypted.
- Authentication covers all of the ciphertext plus the ESP header
- In case of tunnel mode ESP, ESP header and the ESP trailer are attached before and after the IP packet respectively, then the complete IP packet which includes IP header, Transport header and data field along with the ESP trailer is encrypted.
- Tunnel mode ESP is used to protect against the traffic flow analysis.



- The above figure shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP doesn't authenticate the IP header itself.
- When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.
- When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.