IP Security

- **IP security** (IPSec) is an

Internet Engineering Task Force (IETF) standard suite of protocols between communication points across the **IP** network

- provides data authentication, integrity, and confidentiality
- IPsec protects one or more paths between:

- pair of hosts
- pair of security gateways
- or a security gateway and a host

TCP

- Responsible for providing connection – oriented services.
- Guaranties delivery of packets.
- Packet identification is based on sequence numbers.
- During the connection; source & destination exchange the initial sequence numbers. (ISN)
- However, If packet is not in a sequence, but in the range of specified window, is accepted.

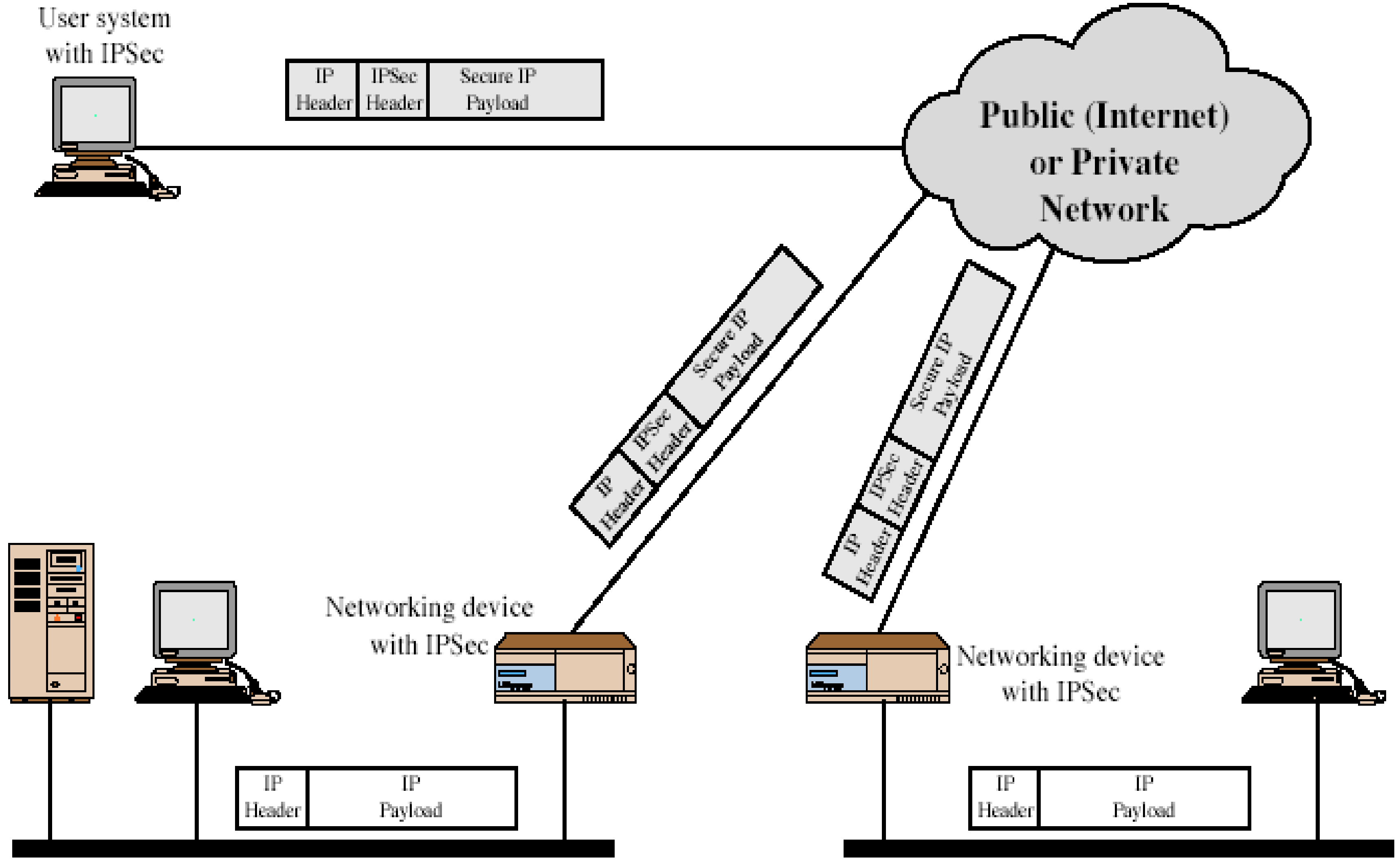
IP

- Connectionless protocol.
- Can not ensure delivery of packets.
- IP is mainly responsible for routing the packets over the n/w.
- The packets might take different routes to reach the destination in different sequence.
- A large IP packet can be broken down causing fragmentation.

IP Security

- have considered some application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Benefits of IPSec

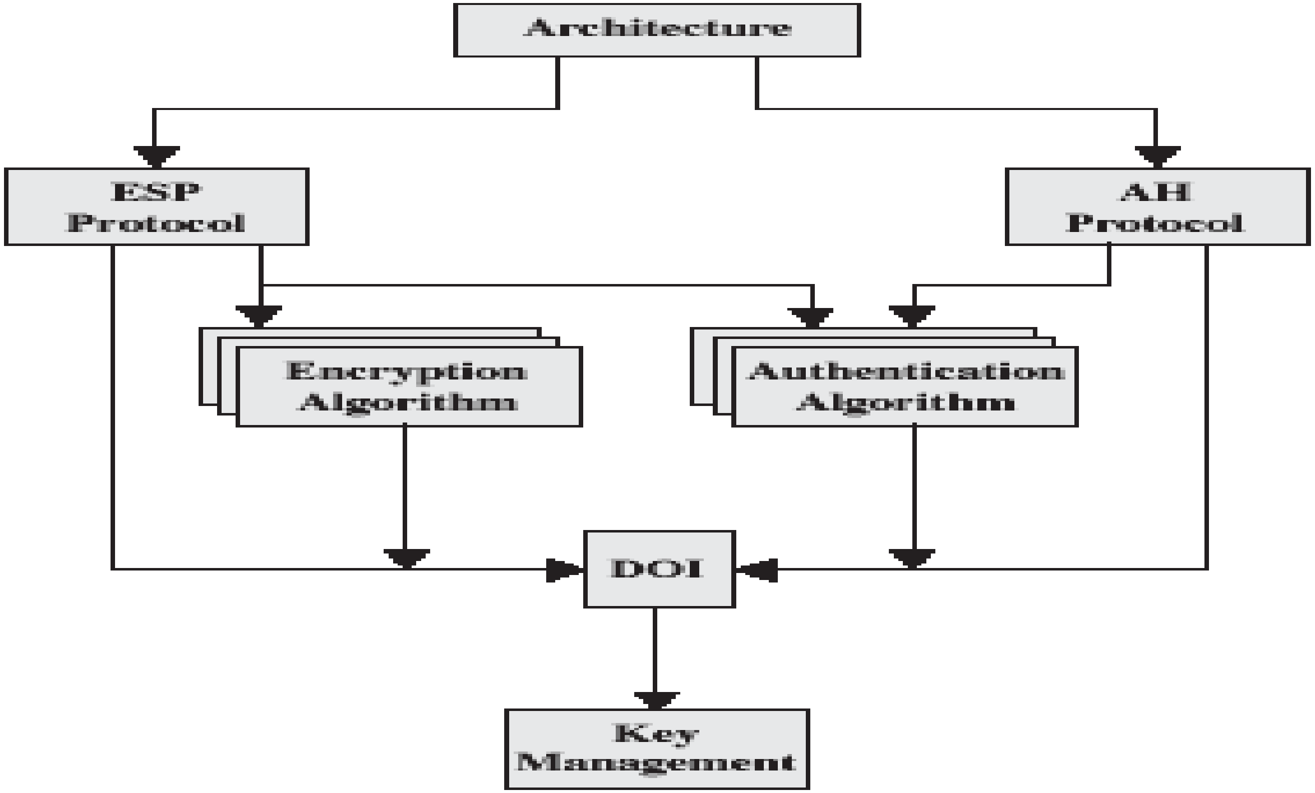
- in a firewall/router provides strong security to all traffic crossing the perimeter
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users if desired

IP Security Architecture

- specification is quite complex
- defined in numerous RFC’s.
  - 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

IP Security Architecture

- In addition to these four RFCs, a number of additional drafts have been published by the IP Security Protocol Working Group.
- The documents are divided into seven groups



IPSec Document Overview

IP Security Architecture

- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPSec technology.
- **Encapsulating Security Payload (ESP):** Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.
- **Authentication Header (AH):** Covers the packet format and general issues related to the use of AH for packet authentication.
- **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 auth. algorithms are used for AH and for the authentication option of ESP.
- **Key Management:** Documents that describe key management schemes.
- **Domain of Interpretation (DOI):** Contains values needed for the other documents to relate to each other.

Q) What does IP MAC mean?

The physical address -- which is also called a media access control, or MAC, address -- identifies a device to other devices on the same local network.

The internet address -- or IP address -- identifies the device globally.

A network packet needs both addresses to get to its destination.

Q) Is MAC Same as IP address?

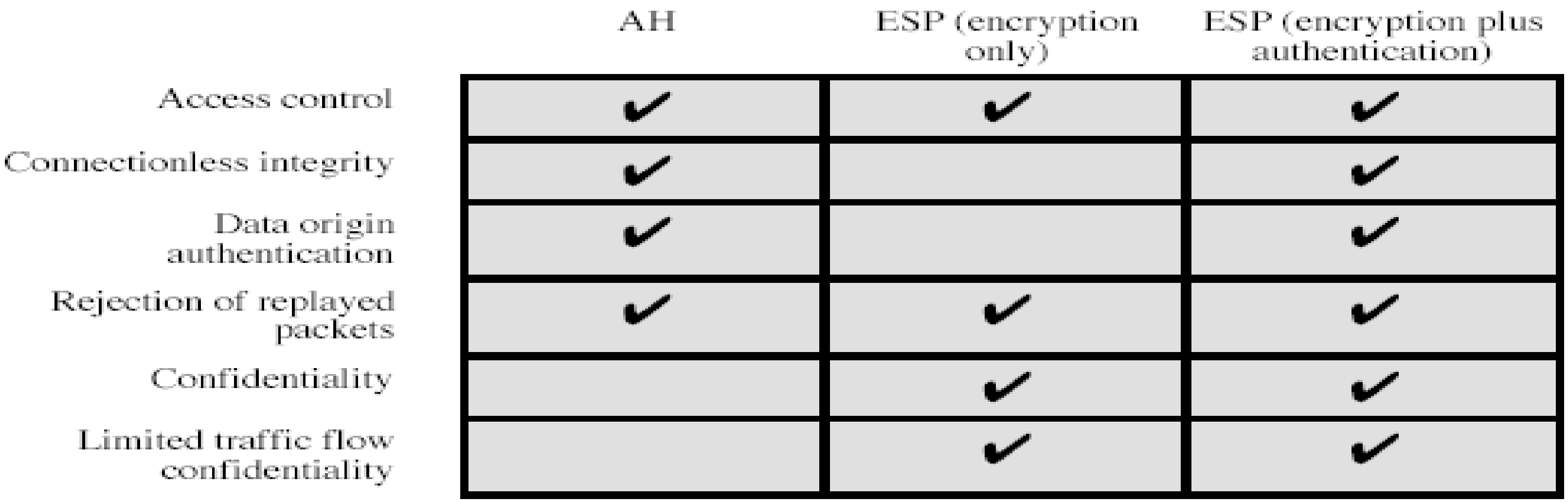
MAC address is a unique identifier that is assigned to a Network Interface Controller/ Card.

An IP address is an address that helps you to identify a network connection.

IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Table: IPSec Services



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

Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - sequence no, AH & ESP info, lifetime etc
- have a database of Security Associations

Transport and Tunnel Modes

- AH and ESP support two modes of use: transport and tunnel mode.
- **Transport Mode:**
  - ➢ Transport mode provides protection primarily for upper-layer protocols. Examples include a TCP or UDP segment or an ICMP packet, all of which operate directly above IP in a host protocol stack.
  - ➢ Transport mode is used for end-to end communication between two hosts (e.g. a client and a server, or two workstations).
  - ➢ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
  - ➢AH in transport mode authenticates the IP payload and selected portions of the IP header.

Transport and Tunnel Modes

Tunnel Mode:

- Tunnel mode provides protection to the entire IP packet.

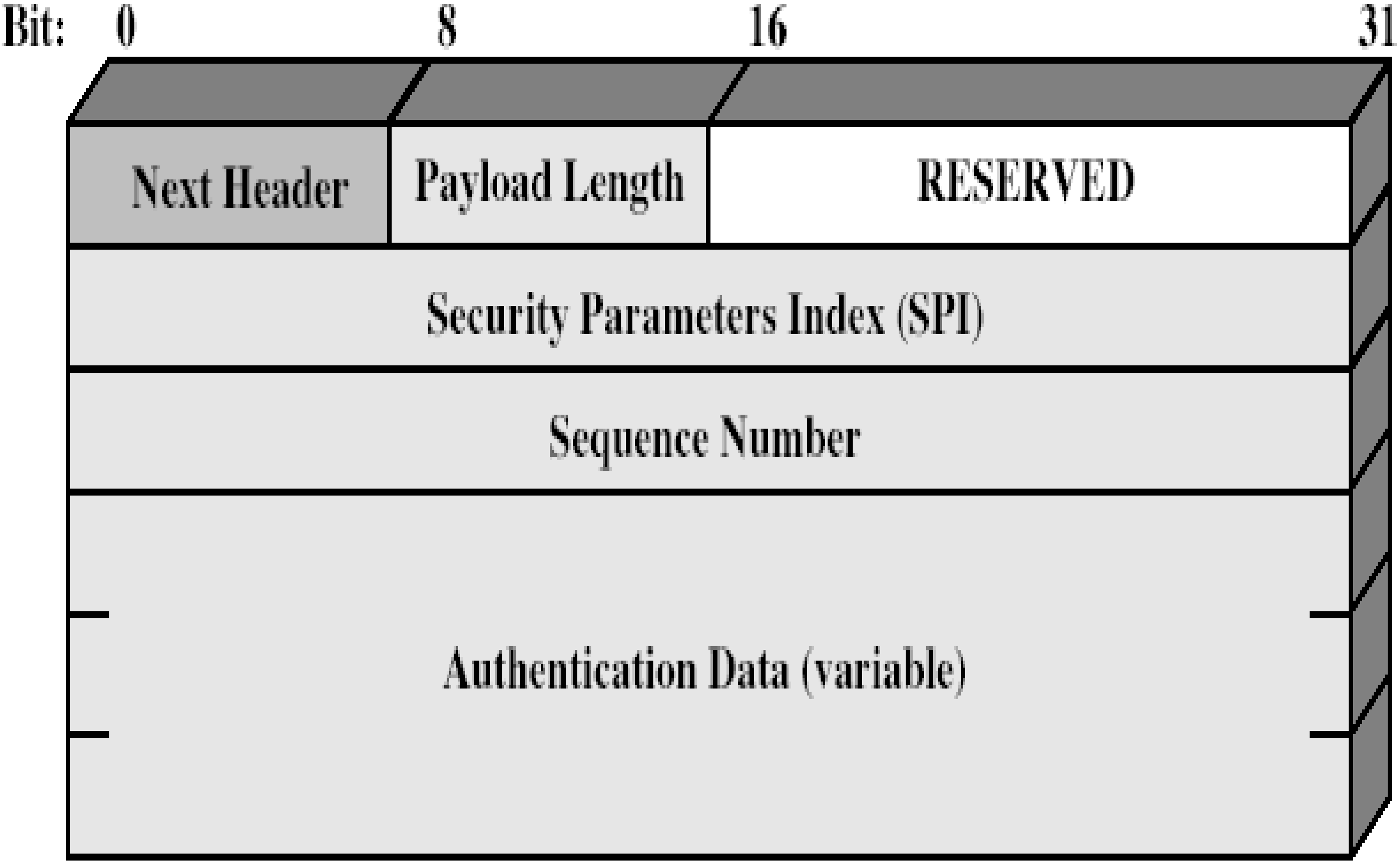
- The entire original, or inner, packet travels through a "tunnel" from one point of an IP network to another; no routers along the way are able to examine the inner IP header.

- Tunnel mode is used when one or both ends of an SA is a security gateway, such as a firewall or router that implements IPSec.

Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/application
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

Authentication Header



Bit: 0 8 16 31

Next Header

Payload Length

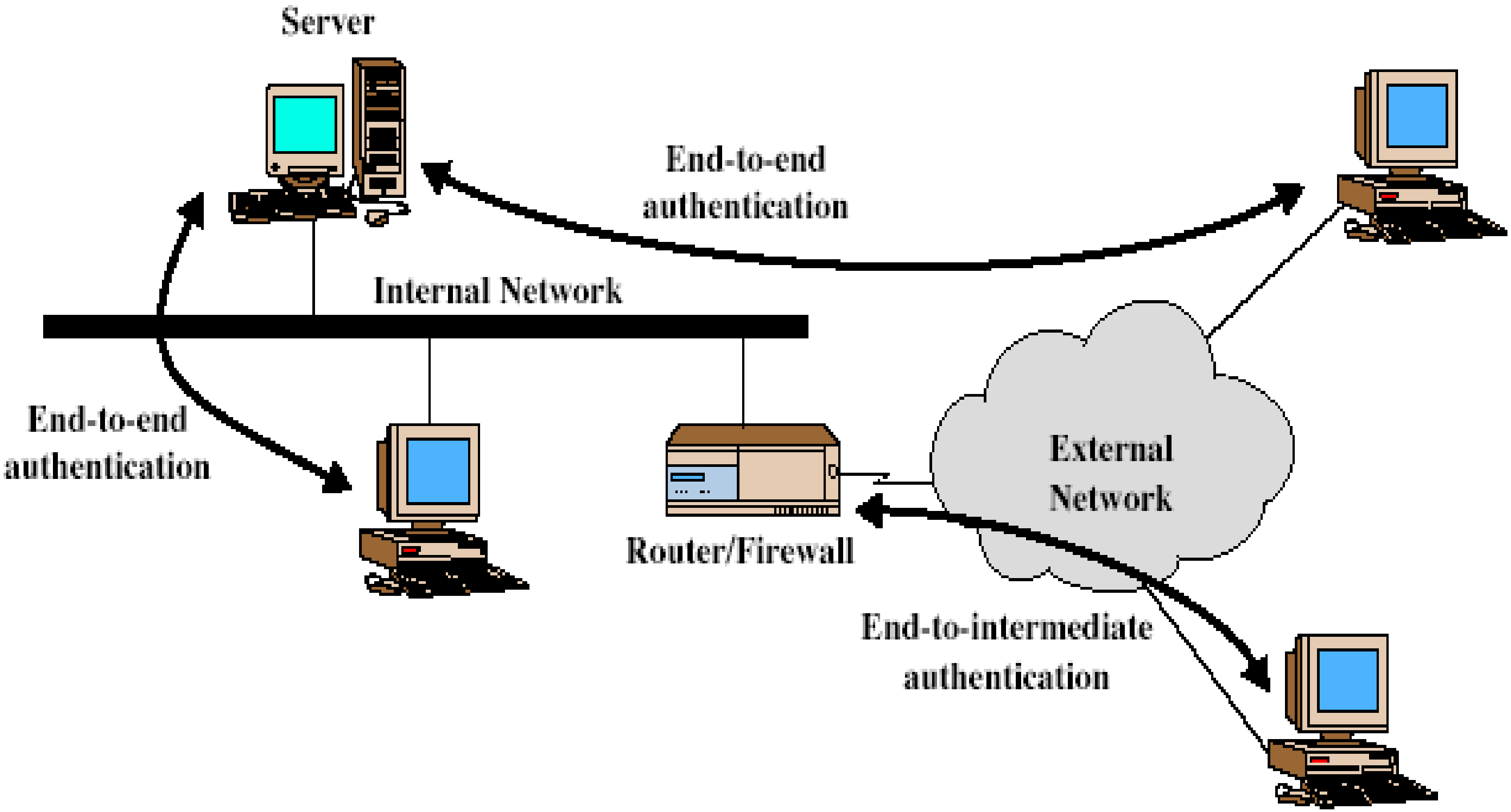
RESERVED

Security Parameters Index (SPI)

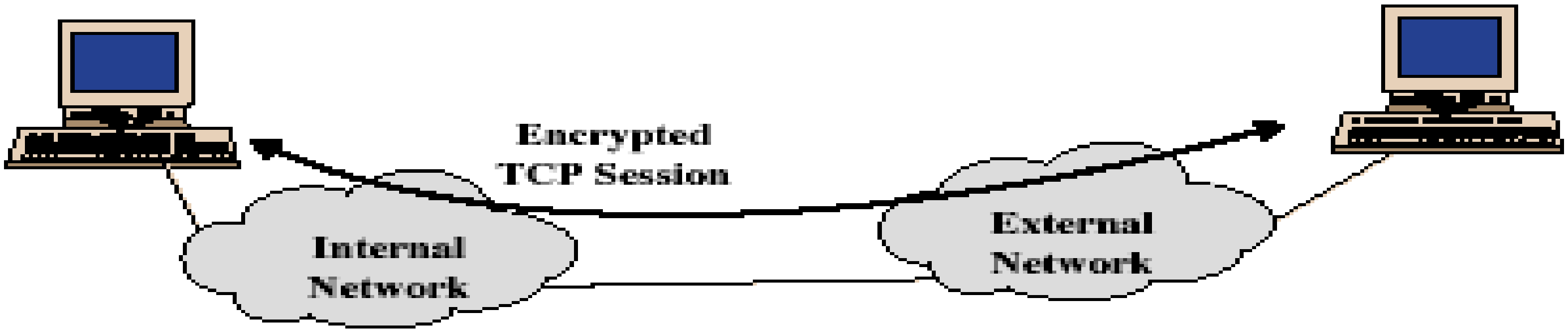
Sequence Number

Authentication Data (variable)

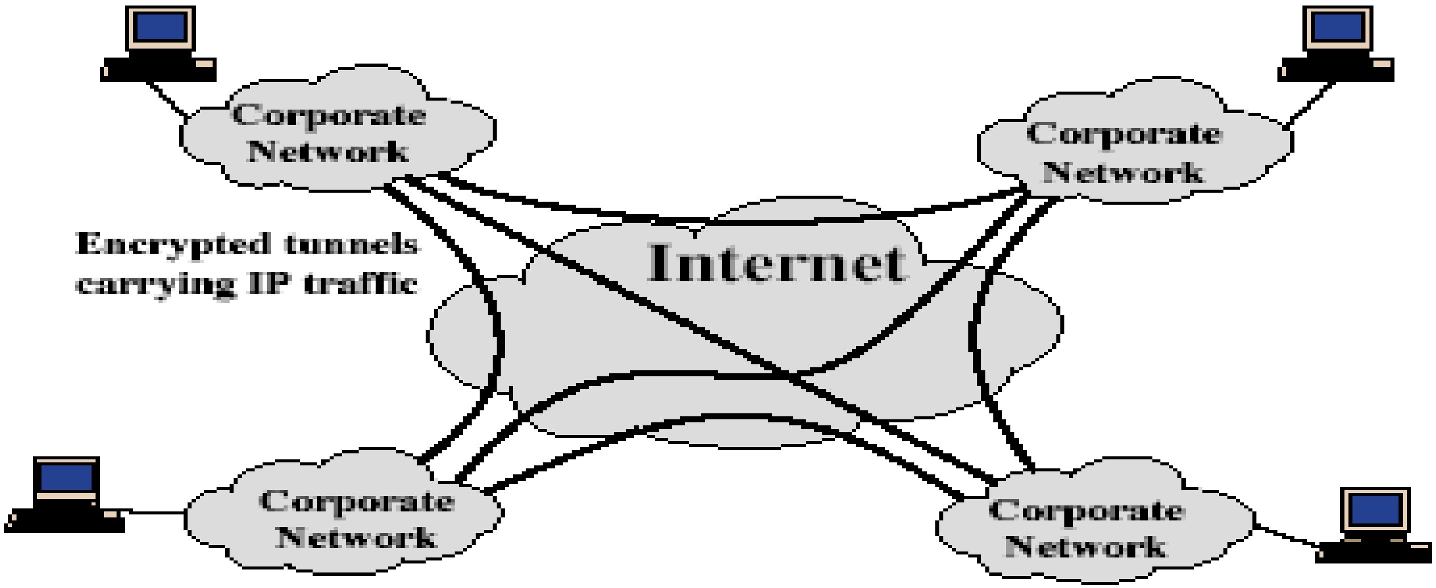
Transport & Tunnel Modes


Server
End-to-end authentication
Internal Network
End-to-end authentication
External Network
Router/Firewall
End-to-intermediate authentication

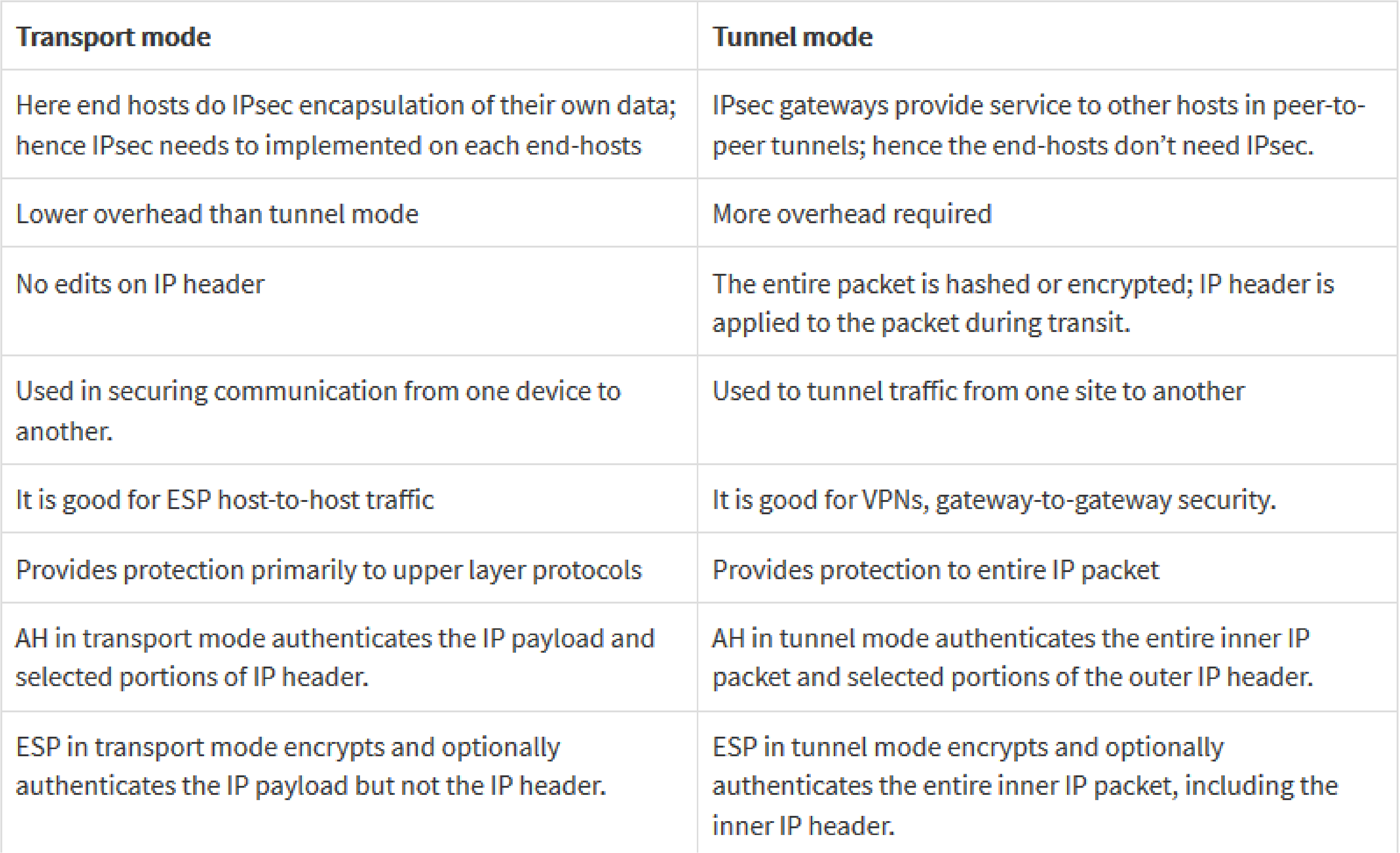
Transport vs Tunnel Mode ESP



(a) Transport-level security



(b) A virtual private network via Tunnel Mode

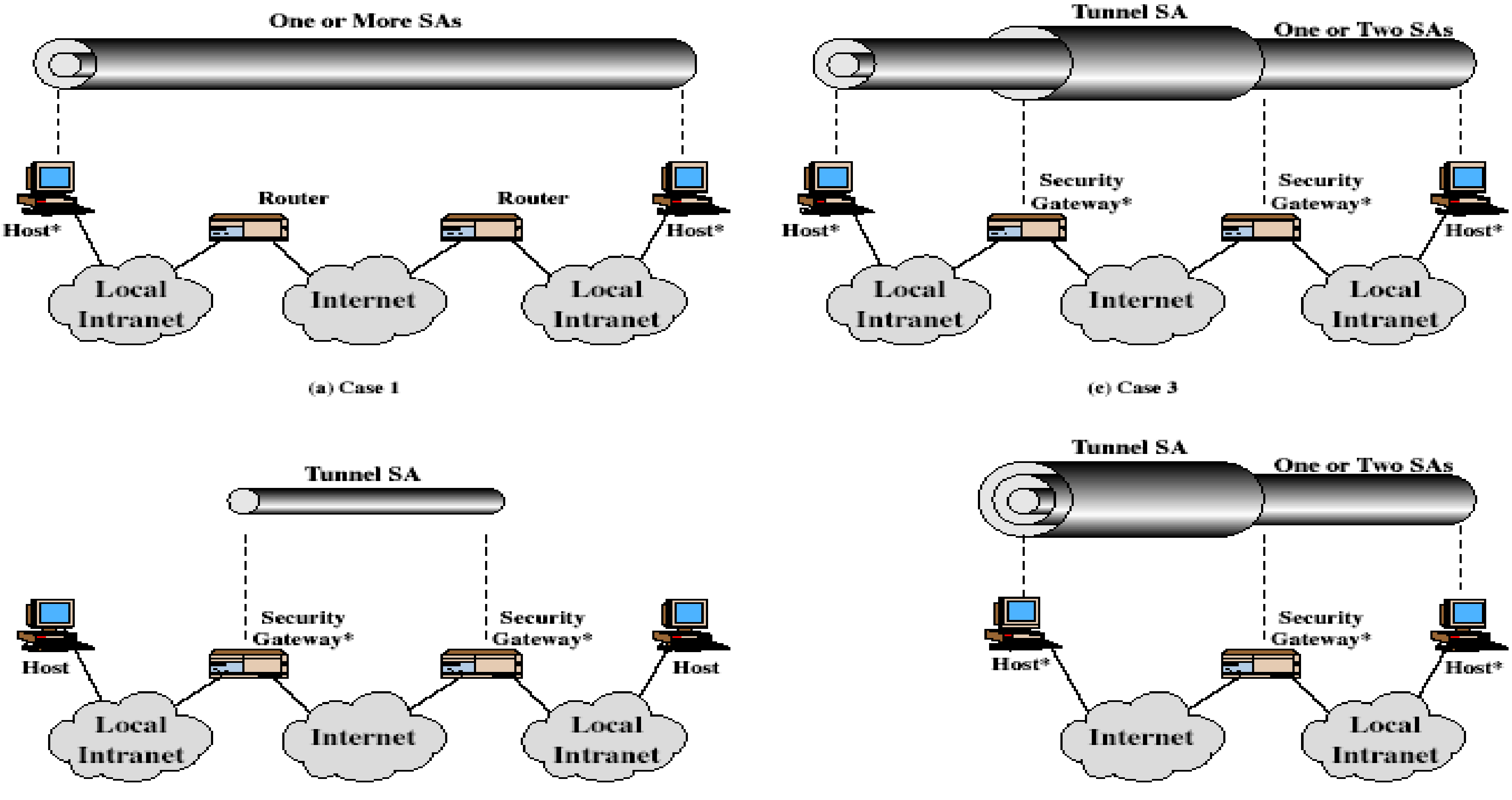


Transport mode	Tunnel mode
Here end hosts do IPsec encapsulation of their own data; hence IPsec needs to implemented on each end-hosts	IPsec gateways provide service to other hosts in peer-to-peer tunnels; hence the end-hosts don't need IPsec.
Lower overhead than tunnel mode	More overhead required
No edits on IP header	The entire packet is hashed or encrypted; IP header is applied to the packet during transit.
Used in securing communication from one device to another.	Used to tunnel traffic from one site to another
It is good for ESP host-to-host traffic	It is good for VPNs, gateway-to-gateway security.
Provides protection primarily to upper layer protocols	Provides protection to entire IP packet
AH in transport mode authenticates the IP payload and selected portions of IP header.	AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.
ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.	ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.

Combining Security Associations

- SA’s can implement either AH or ESP
- to implement both need to combine SA’s -form a security association bundle
- The term *security association bundle* refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPSec services.
- have 4 cases

Combining Security Associations



(a) Case 1

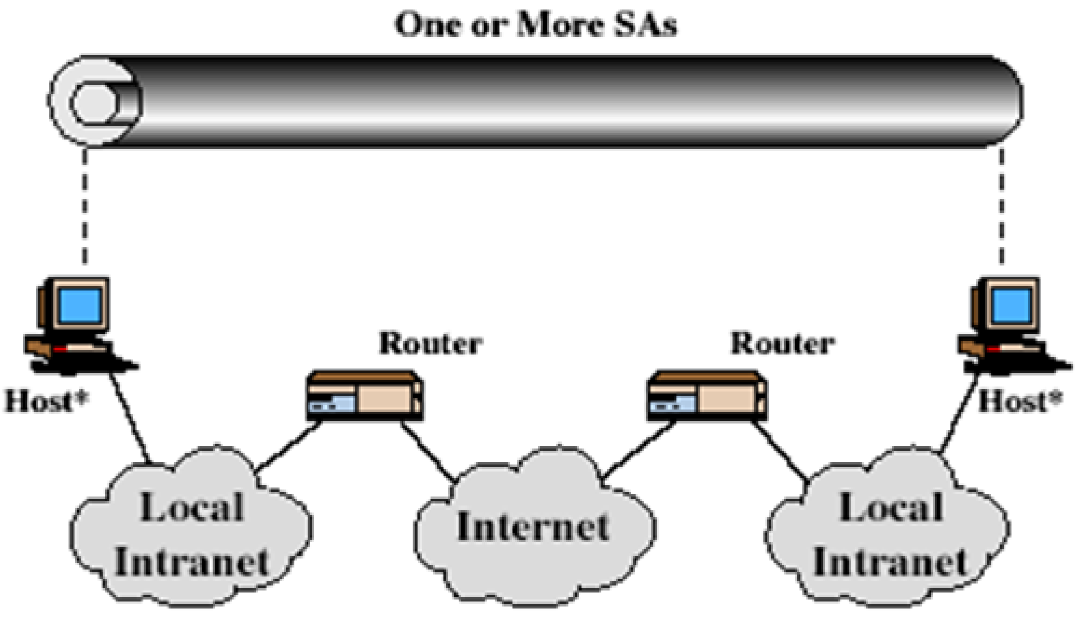
(c) Case 3

(b) Case 2

(d) Case 4

* Implements IPsec

Case 1

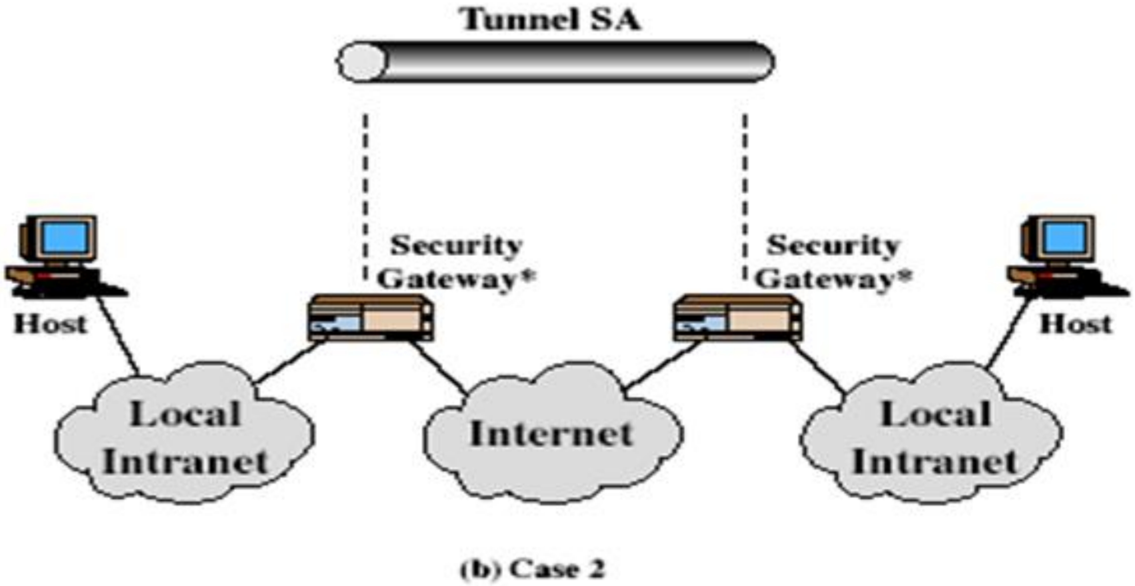


(a) Case 1

- Security between end systems that provide Ipsec

  -Must share appropriate secret keys; Any possible combination
  - AH/ESP in Tr. Mode
  - ESP followed by AH in Tr. Mode (ESP SA inside AH SA)
  - Any above in tunnel mode

Case 2

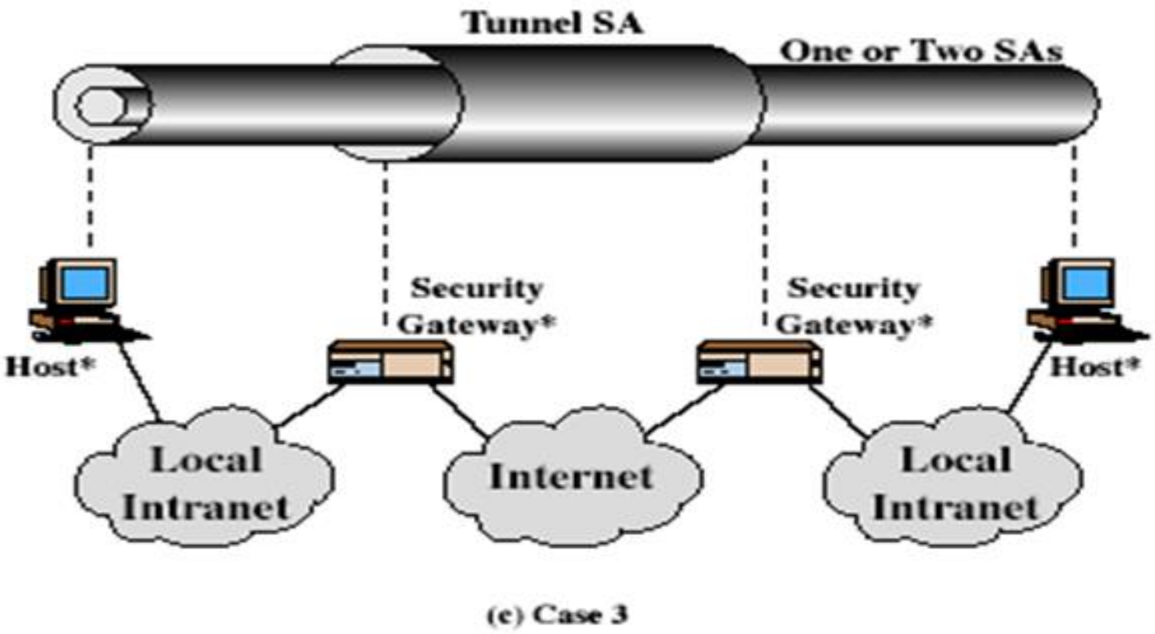


(b) Case 2

- Simple VPN support; Security only between gateways & no hosts Implement Ipsec;

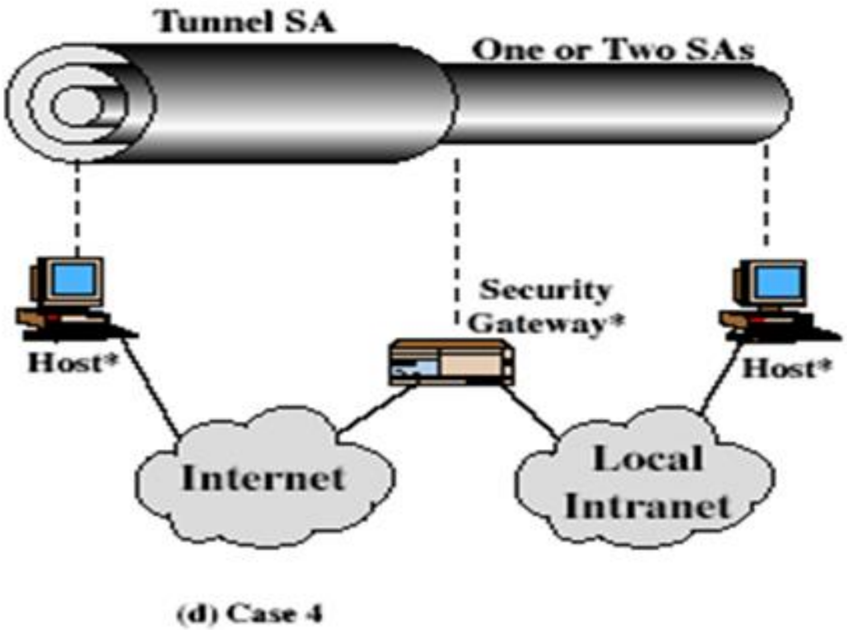
No need of nested tunnels because IPsec services apply to the entire inner packet

Case 3



- Builds on case 2 by adding end-to-end security
- Gateway-to-gateway tunnel provides authentication and/or confidentiality

Case 4



(d) Case 4

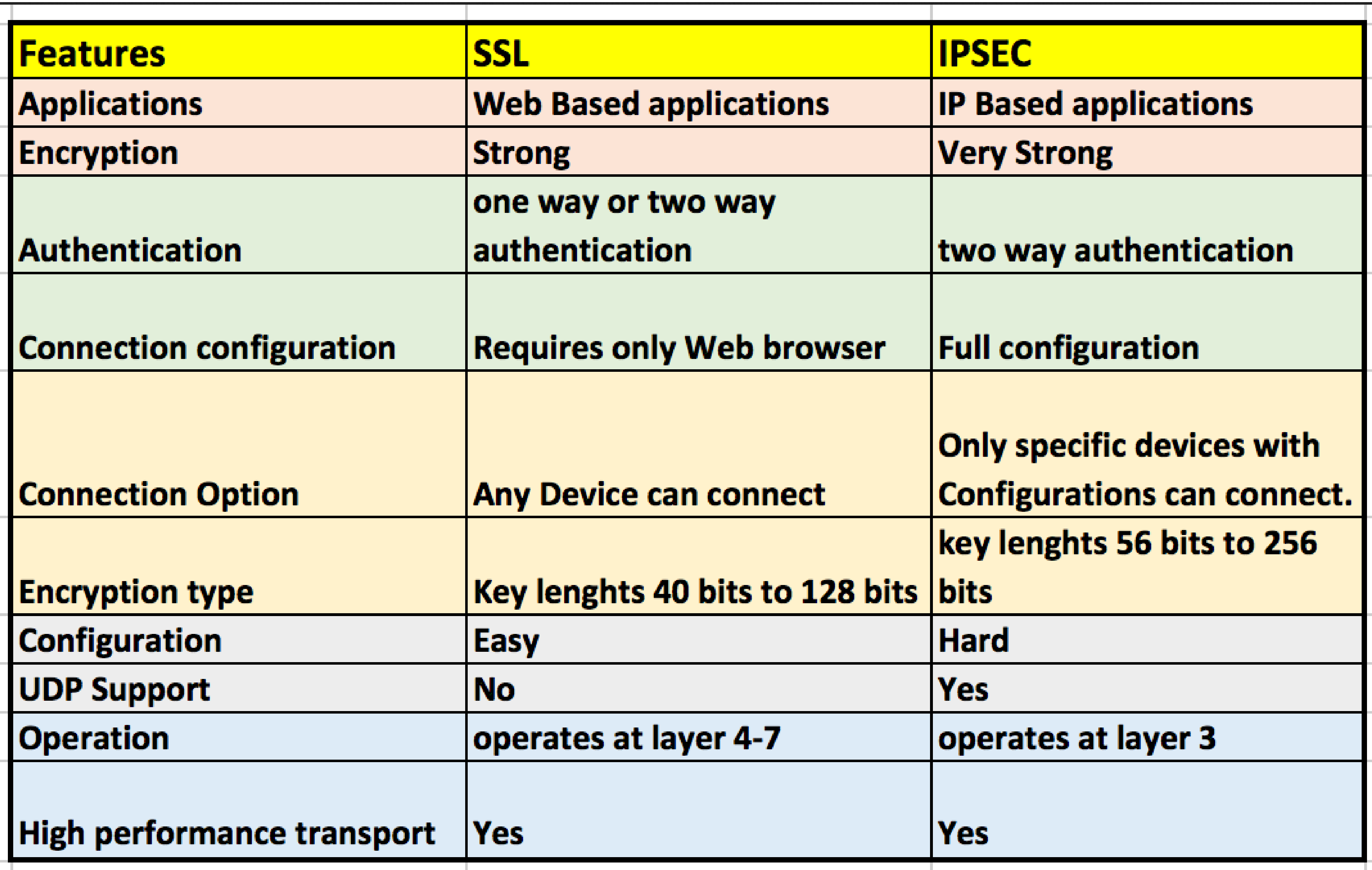
- Provides support (tunnel mode) for remote host that uses Internet to reach an organization’s firewall

Key Management

- handles key generation & distribution of secret keys
- typically need 2 pairs of keys
  - Transmit & receive pairs for AH & ESP
- manual key management
  - Sys admin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large distributed systems
  - has Oakley & ISAKMP elements

Oakley Key Determination Protocol: Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security.

Internet Security Association and Key Management Protocol (ISAKMP): ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats for negotiation of security attributes.



Features	SSL	IPSEC
Applications	Web Based applications	IP Based applications
Encryption	Strong	Very Strong
Authentication	one way or two way authentication	two way authentication
Connection configuration	Requires only Web browser	Full configuration
Connection Option	Any Device can connect	Only specific devices with Configurations can connect.
Encryption type	Key lenghts 40 bits to 128 bits	key lenghts 56 bits to 256 bits
Configuration	Easy	Hard
UDP Support	No	Yes
Operation	operates at layer 4-7	operates at layer 3
High performance transport	Yes	Yes

Summary

- Question Bank
- IPSec security framework including
  - AH

  ESP

  - Security Association Concept and Combination Types/Cases

  - Comparison of Transport and Tunnel Mode