V	Network security: Electronic Mail Security: Pretty good privacy- S/MIME. IP Security: Architecture- authentication Header- Encapsulating Security payload- Combining Security associations- Key management.	7	20 %

IP Security

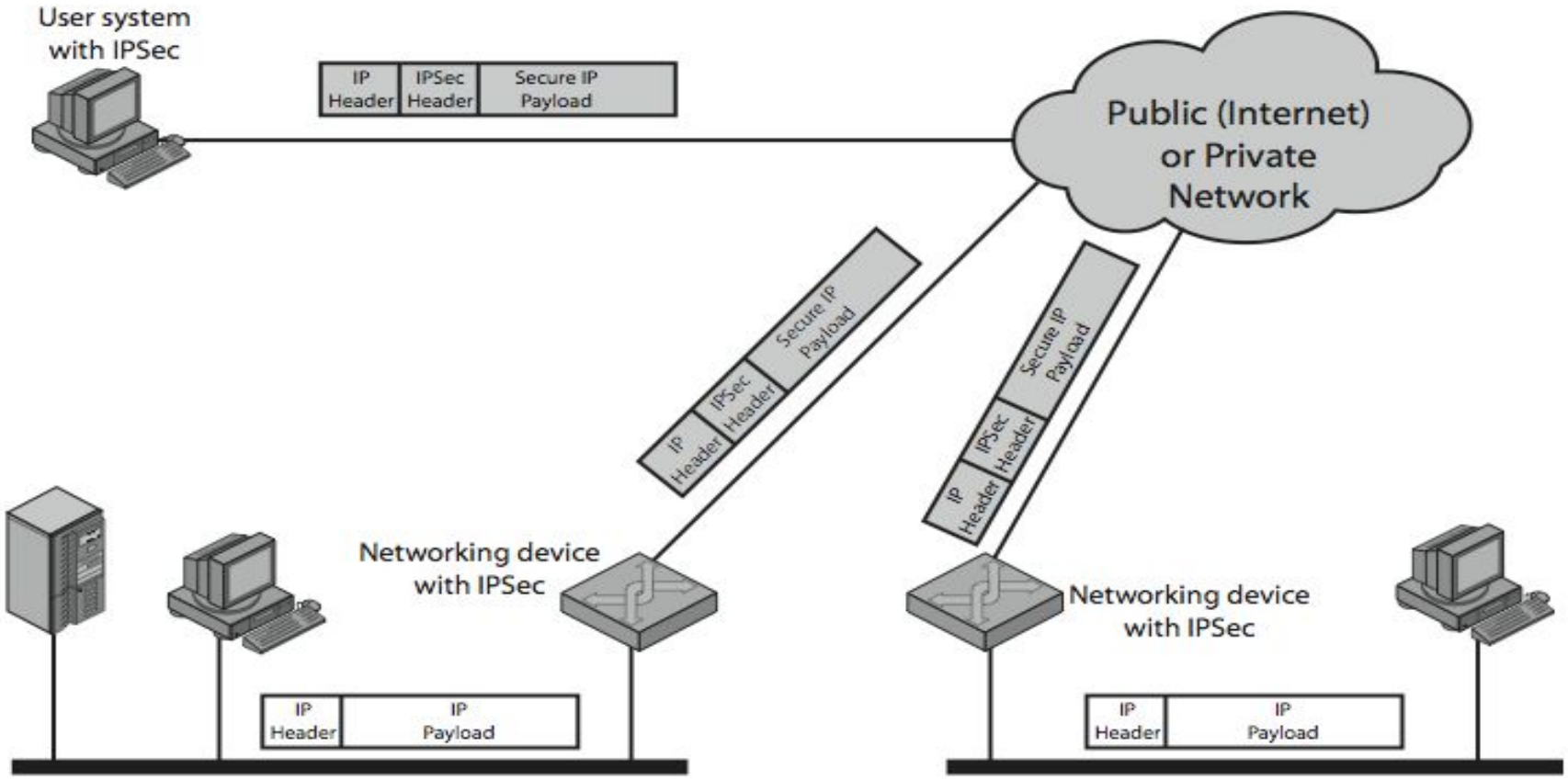
- IPsec (Internet Protocol Security) is a framework that helps us to protect IP traffic on the network layer. Why? because the IP protocol itself doesn't have any security features at all. IPsec can protect our traffic with the following features:
- **Confidentiality**: by encrypting our data, nobody 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.

- **What is IPsec used for?**
- IPsec is used for protecting sensitive data, such as financial transactions, medical records and corporate communications, as it's transmitted across the network.
- It's also used to secure virtual private networks (VPNs), where IPsec tunneling encrypts all data sent between two endpoints.
- IPsec can also encrypt application layer data and provide security for routers sending routing data across the public internet. IPsec can also be used to provide authentication without encryption -- for example, to authenticate that data originated from a known sender.

IPSec Applications

- Secure branch office connectivity over the internet.
- Secure remote access over the internet.
- Establishing extranet and intranet connectivity with partners.
- Enhancing electronic commerce security.

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
- 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
- Secures routing architecture

IP Security Architecture

- IPSec specification consists of numerous documents
- Mandatory in IPv6, optional in IPv4
- Have two security header extensions:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

- **Components of IP Security –**
  It has the following components:

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 provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentialitv.

- **Internet Key Exchange (IKE) –**
  It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.
- The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.
- The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
- Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5.

IPSec Services

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

IP Security Policy

- A security policy is applied to each IP packet that transits from a source to a destination
- IPsec policy is determined primarily by the interaction of two databases,
  - The security association database (SAD)
  - The security policy database (SPD)

Security Associations

- A one-way relationship between sender & receiver that affords security for traffic flow
- Each SA is uniquely identified by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- Has a number of other parameters
  - seq no, AH & EH info, lifetime etc

Security Association Database

- Sequence Number Counter
- Sequence Counter Overflow
- Anti-replay window
- AH information
- ESP information
- Lifetime of this SA
- IPSec protocol mode
- Path MTU (Maximum Transmission Unit)

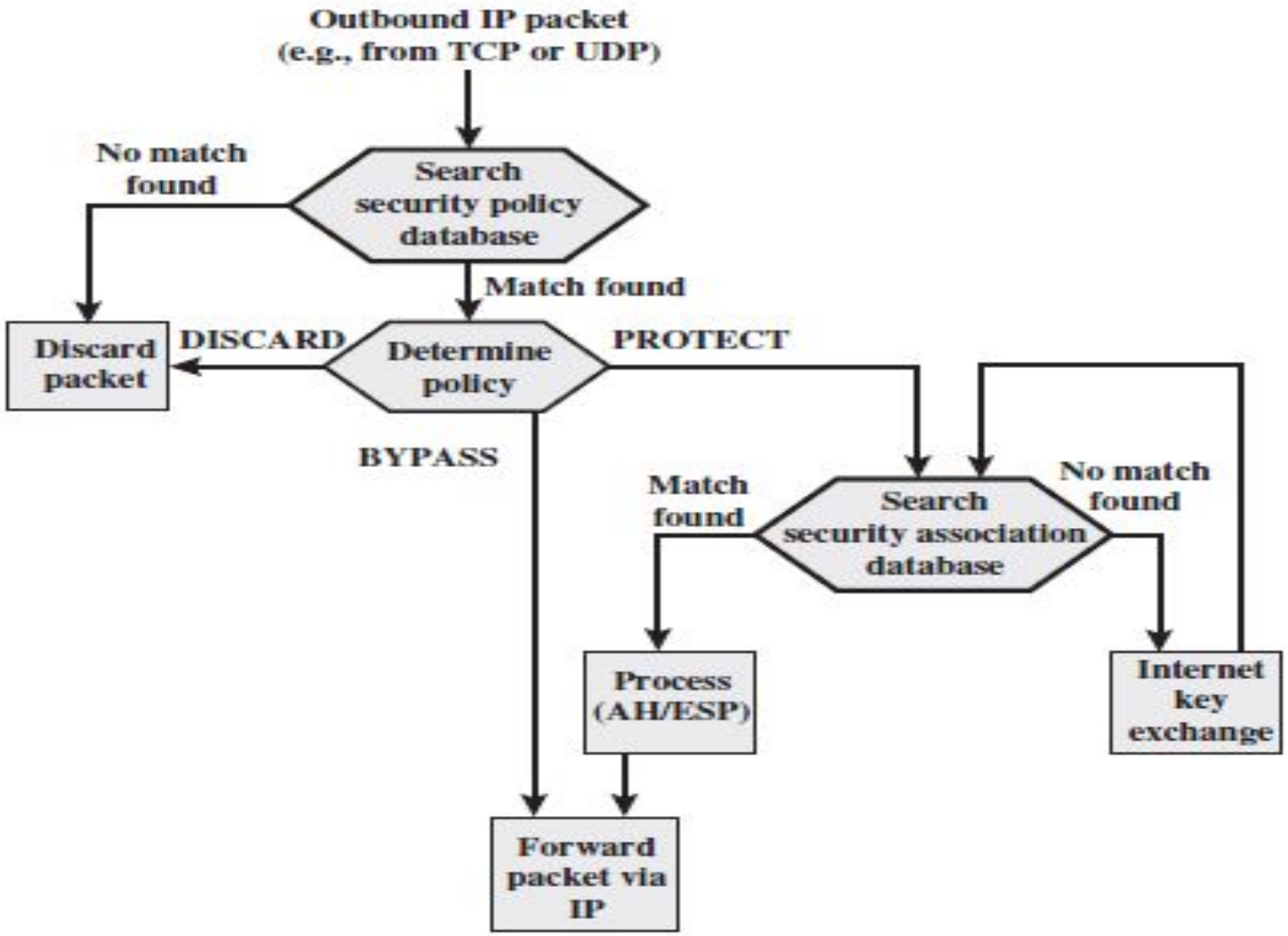
Security Policy Database

- IPSec provides good flexibility in discriminating between the traffic
  - that needs IPSec protection and
  - that is allowed to bypass IPSec
- Security Policy Database (SPD) entry called **selectors** are used to filter outgoing traffic for a particular SA

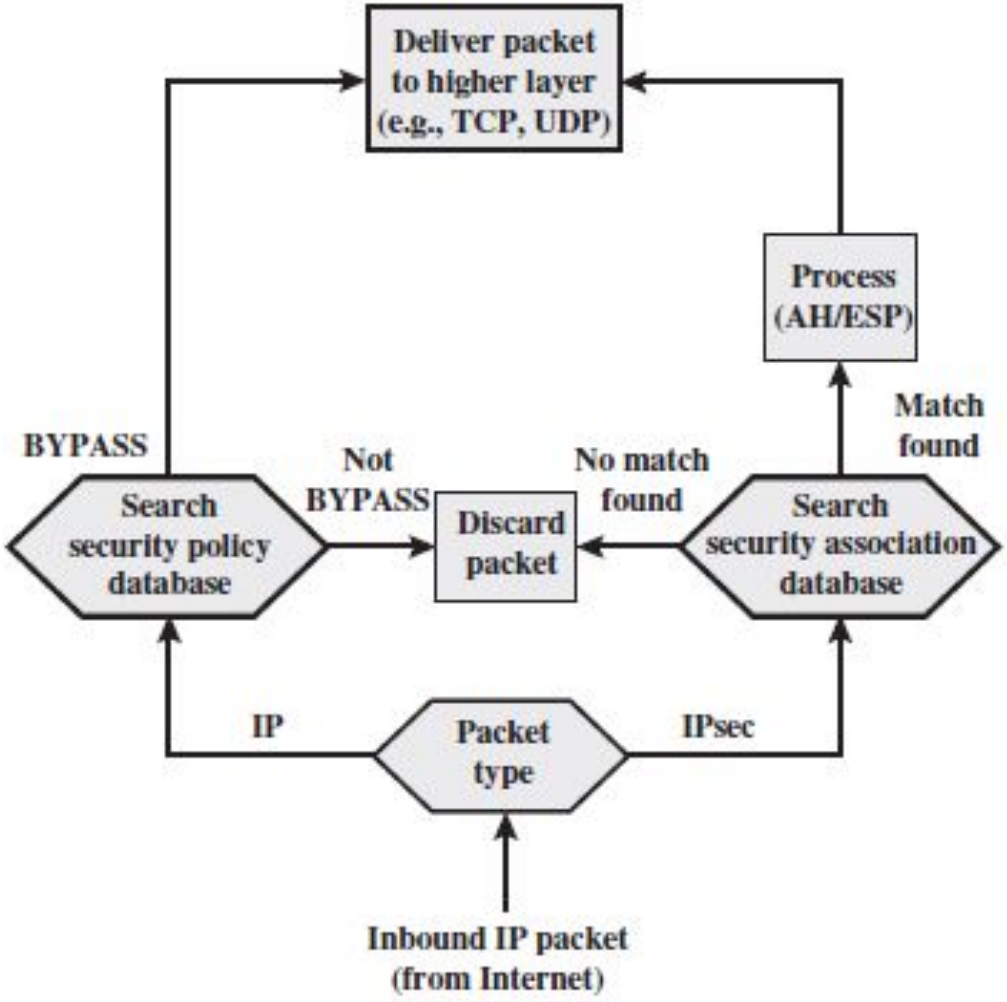
Security Policy Database Selectors

- Destination IP Address
- Source IP Address
- UserID
- Next Layer Protocol: The IP protocol header (IPv4, IPv6, or IPv6 Extension
- Source and Destination Ports

IP Traffic Processing : Outbound Packets



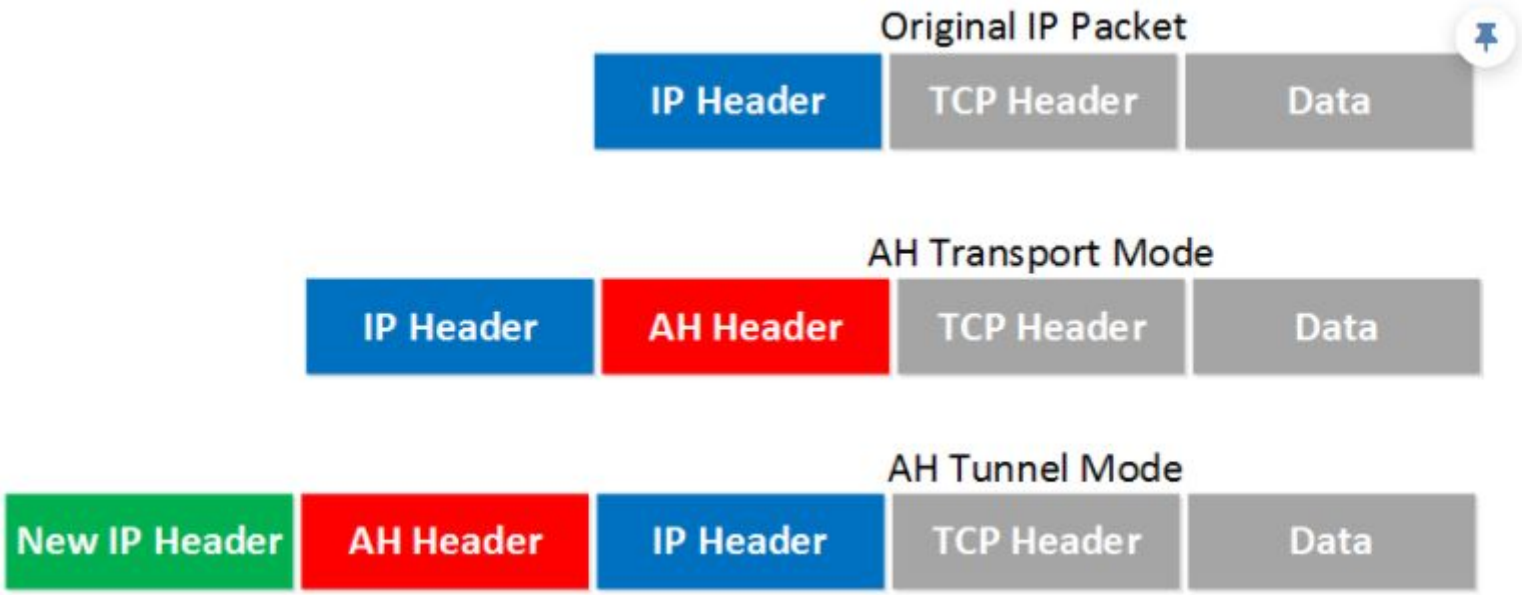
IP Traffic Processing : Inbound Packets



IPSec Protocol Mode

- Transport mode
- Tunnel mode

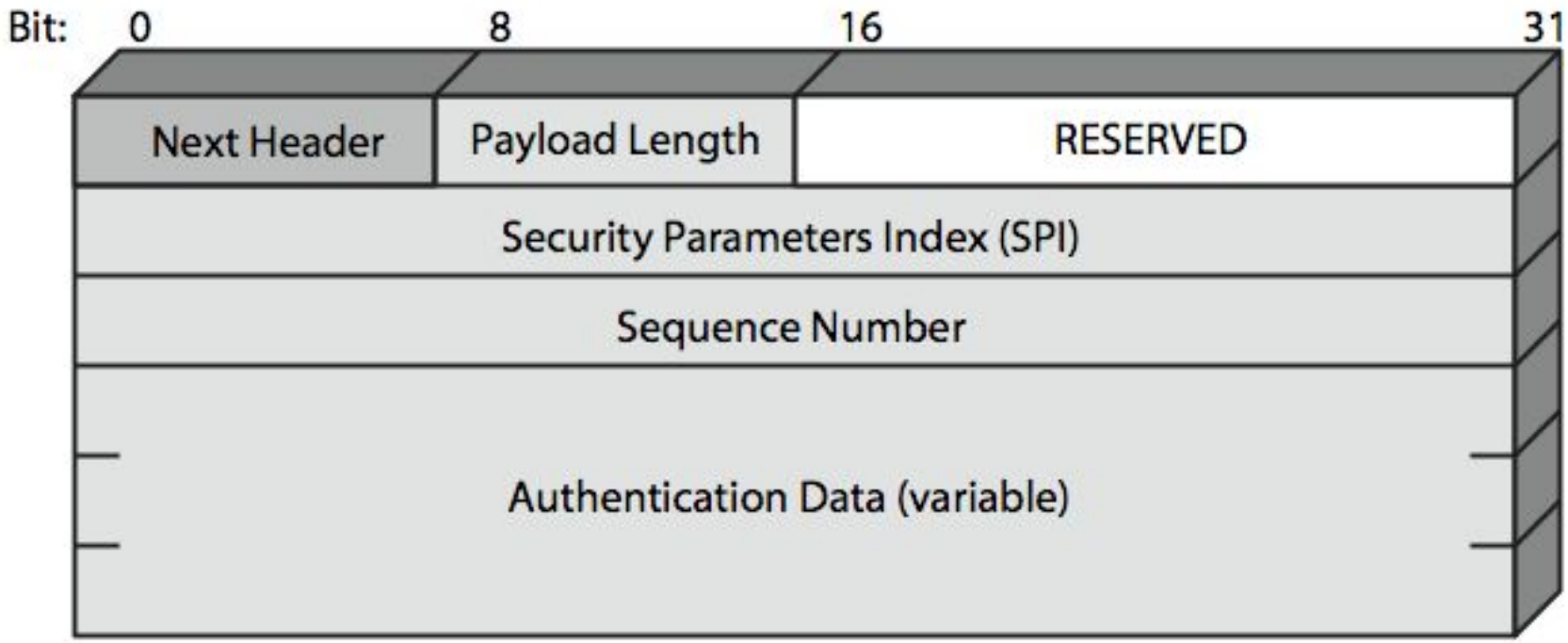
- The main difference between the two is that with transport mode we will use the **original IP header** while in tunnel mode, we use a new **IP header**. Here's an example to help you visualize this:



Authentication Header (AH)

- Provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - 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



Anti-Replay Service

- Sender uses a sequence number starting from 0
- For each packet, seq no is incremented and places on the Sequence Number field.
- Once the max value is reached, a new SA is negotiated with new key

Anti-replay Window

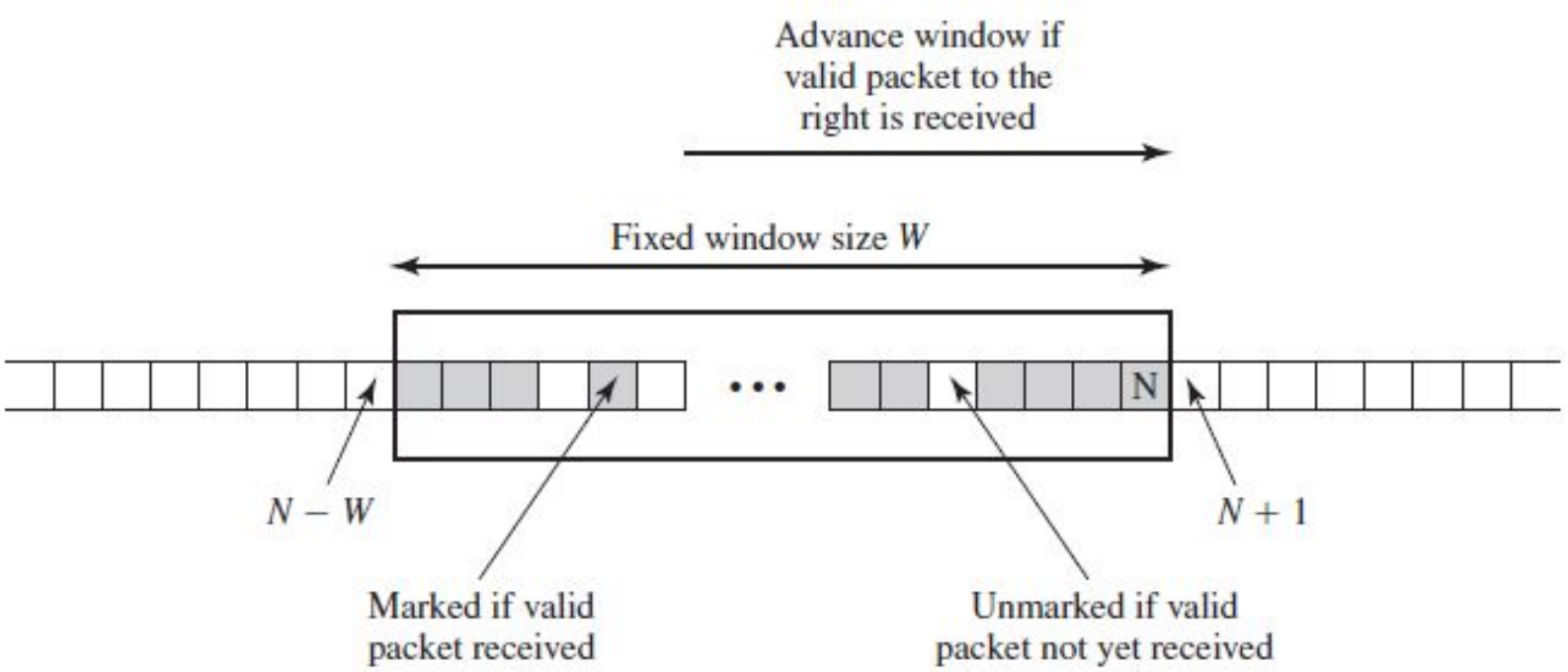
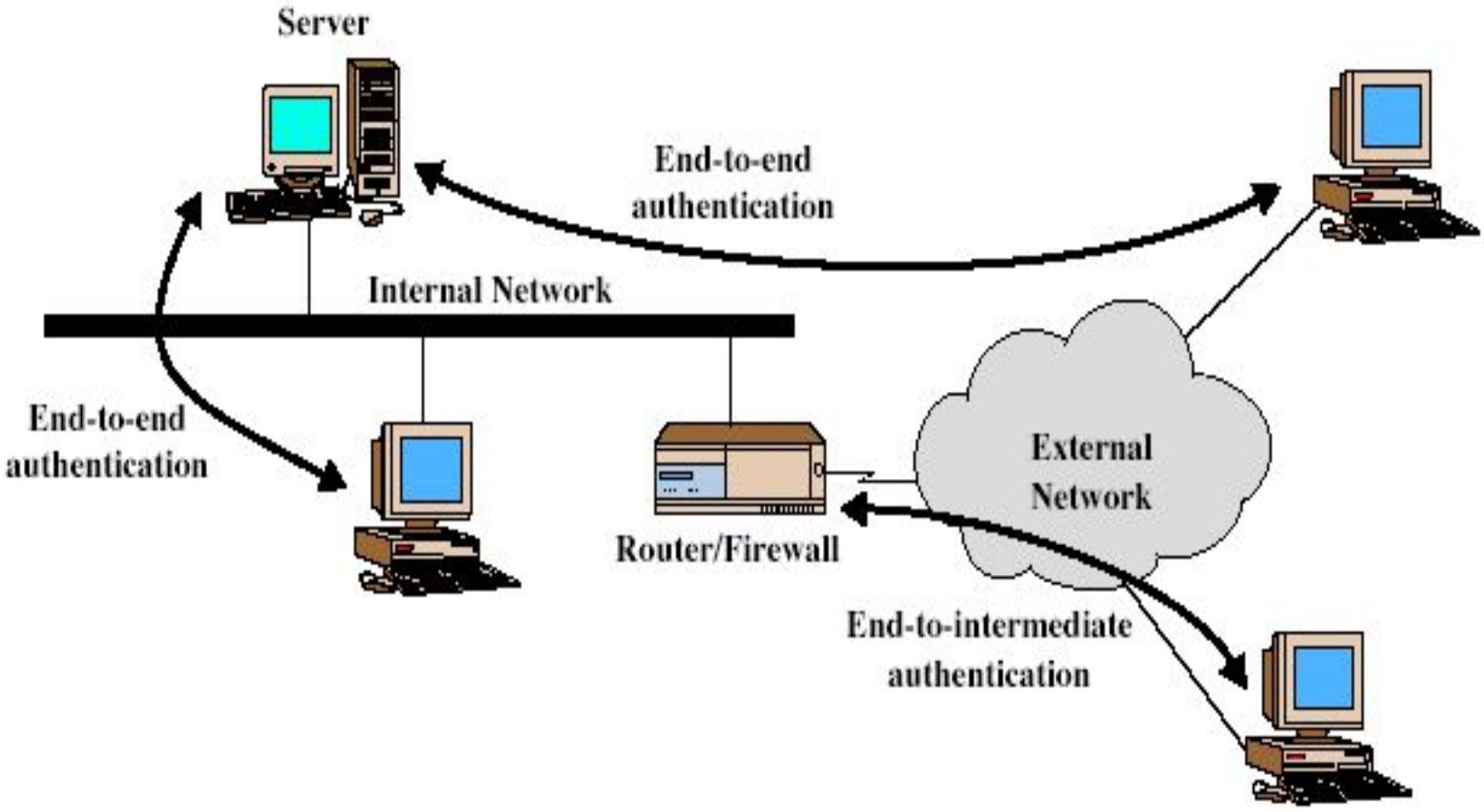


Figure 19.6 Anti-replay Mechanism

Integrity Check Value

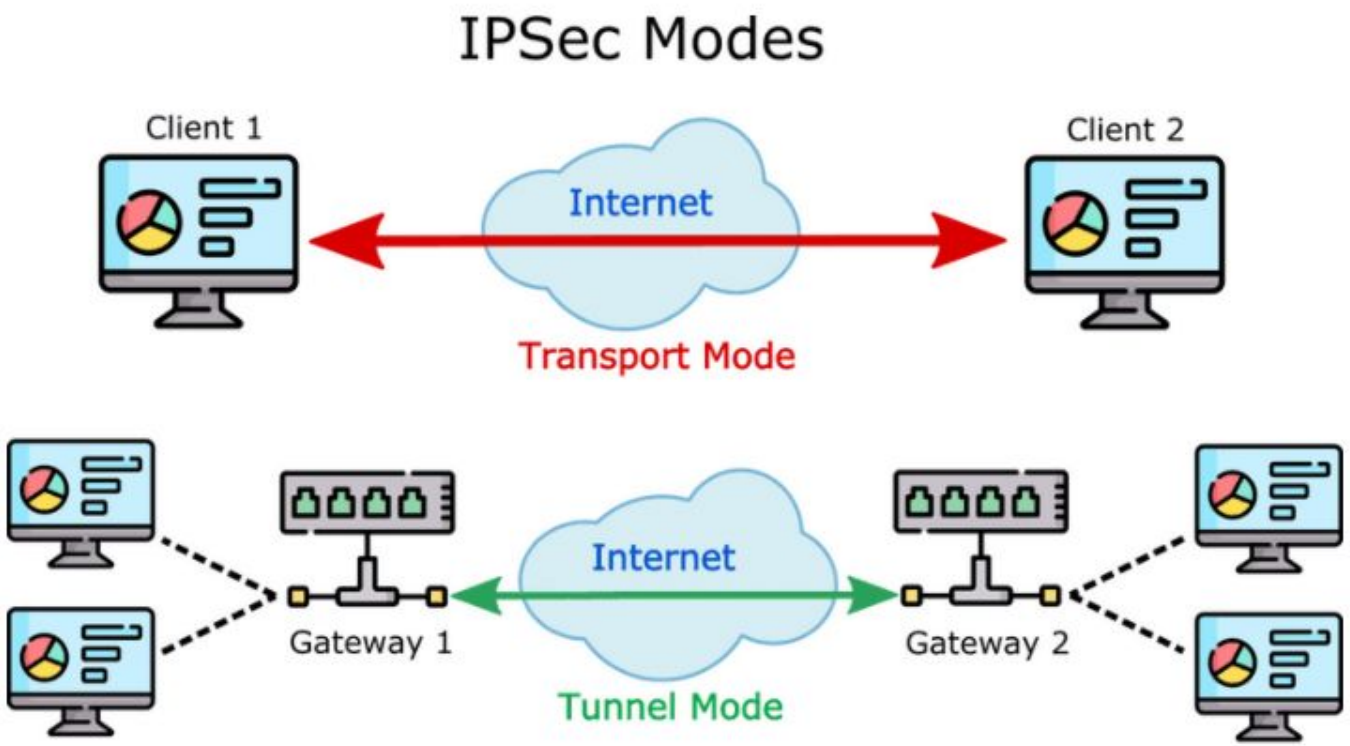
- The Authentication Data field holds a value called Integrity Check Value ICV is a MAC

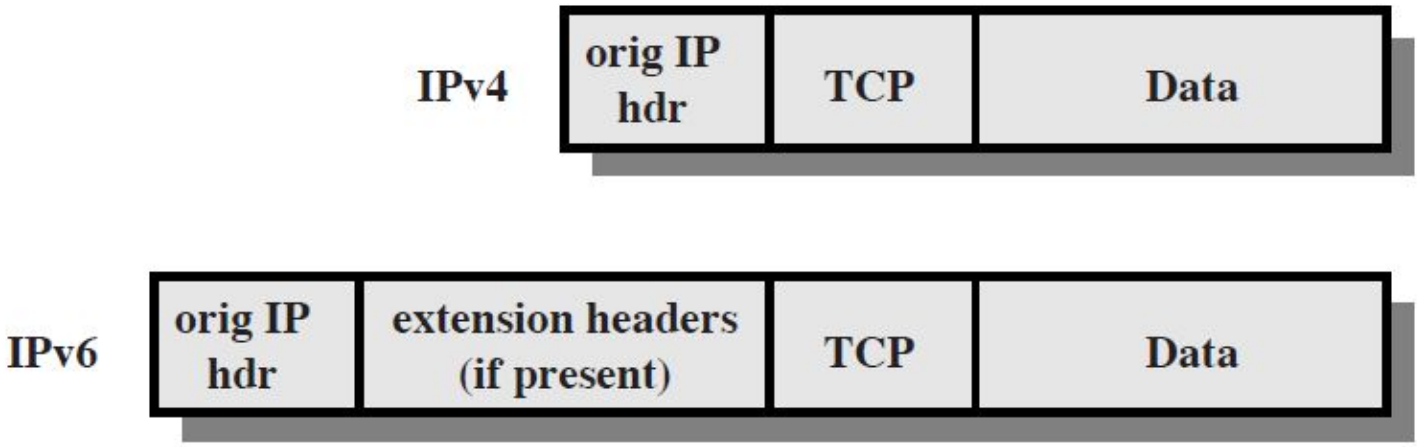
Transport & Tunnel Modes



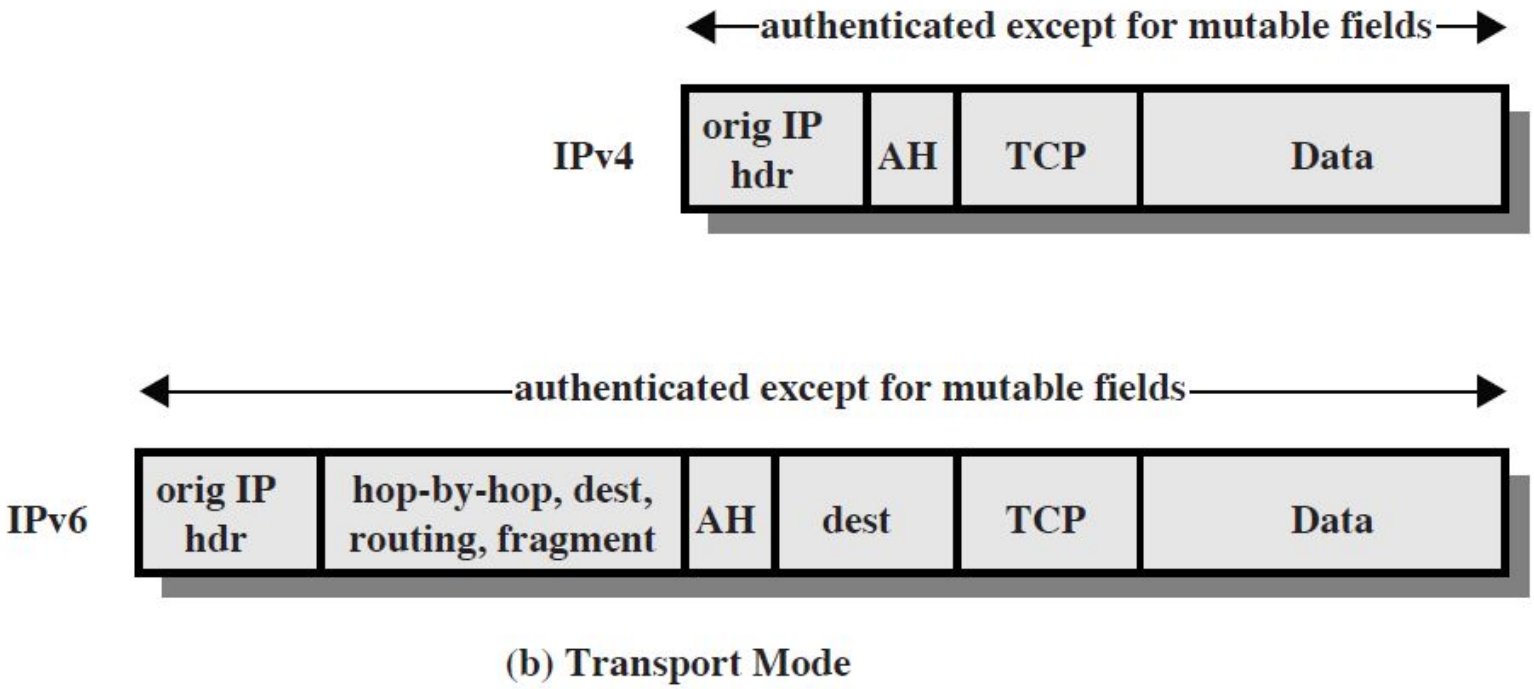
- **Tunnel Mode**
- In tunnel mode, the entire original IP packet is encapsulated to become the payload of a new IP packet.
- Additionally, a new IP header is added on top of the original IP packet. Since a new packet is created using the original information, tunnel mode is useful for protecting traffic between different networks.
- An additional advantage of this mode is that it makes it very easy to establish a "tunnel" between two secure IPsec gateways.
- These IPsec gateways in turn can connect two different networks securely. Using secure IPsec proxies like the ones shown in the diagram below can be very useful

- **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 between two hosts that previously established a secure IPsec tunnel.
- Since a new IP header isn't created, the process used by transport mode is less complex than tunnel mode:

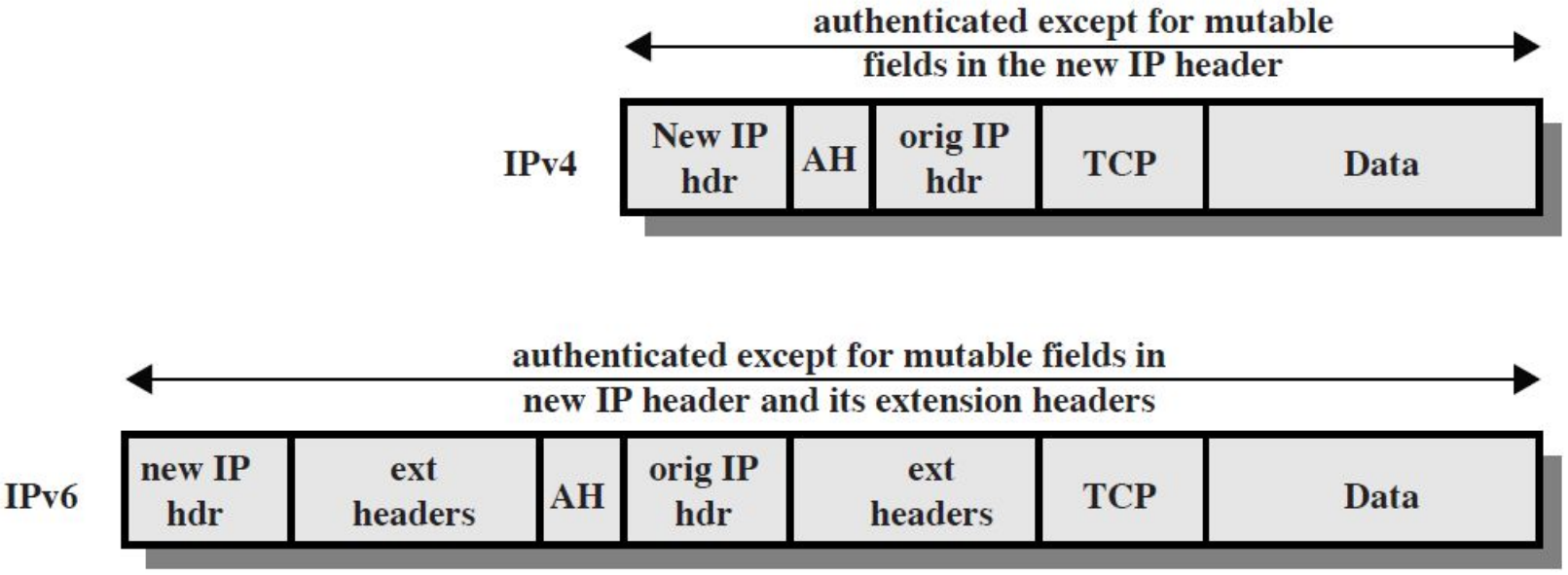

IPSec Modes
Client 1
Client 2
Internet
Transport Mode
Gateway 1
Internet
Gateway 2
Tunnel Mode



(a) Before Applying AH



(b) Transport Mode

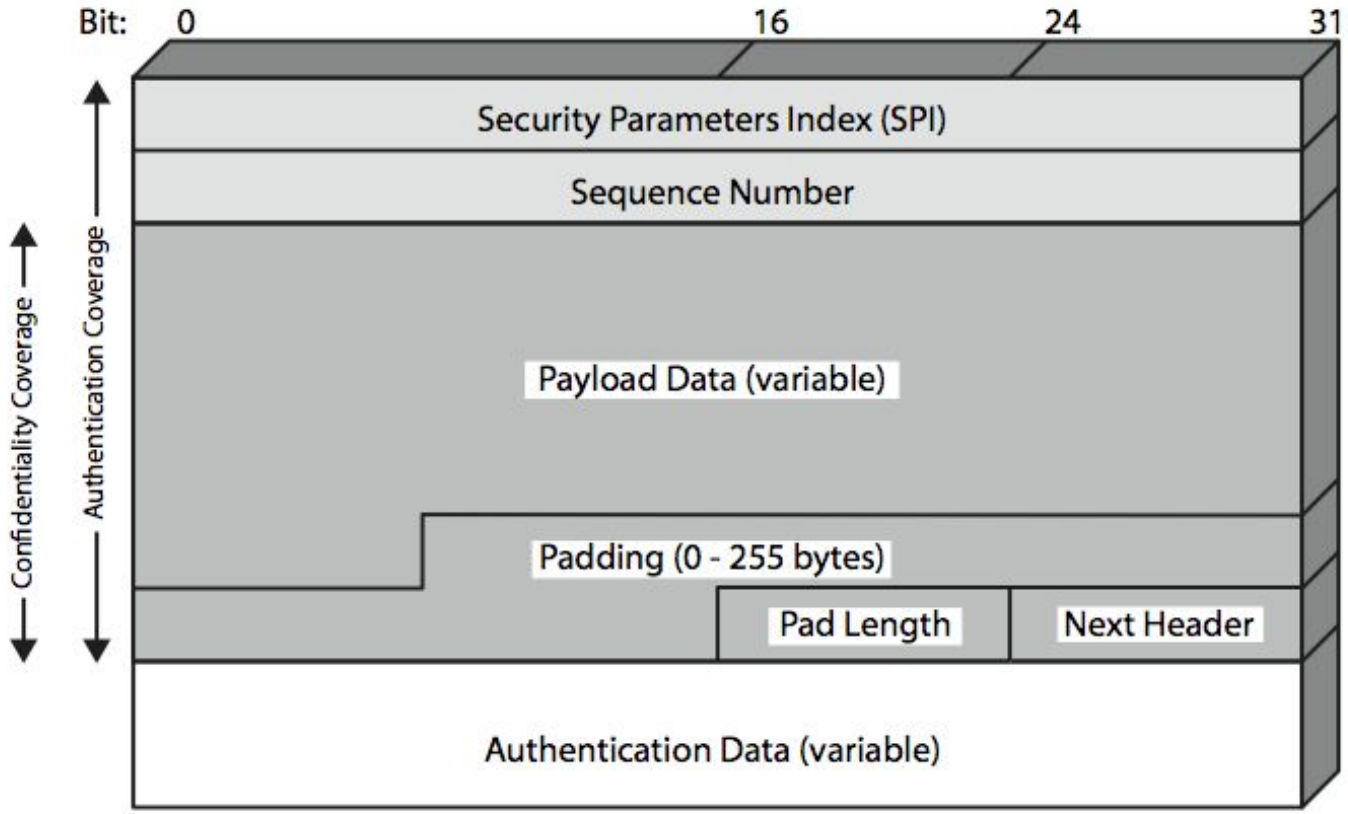


(c) Tunnel Mode

Encapsulating Security Payload (ESP)

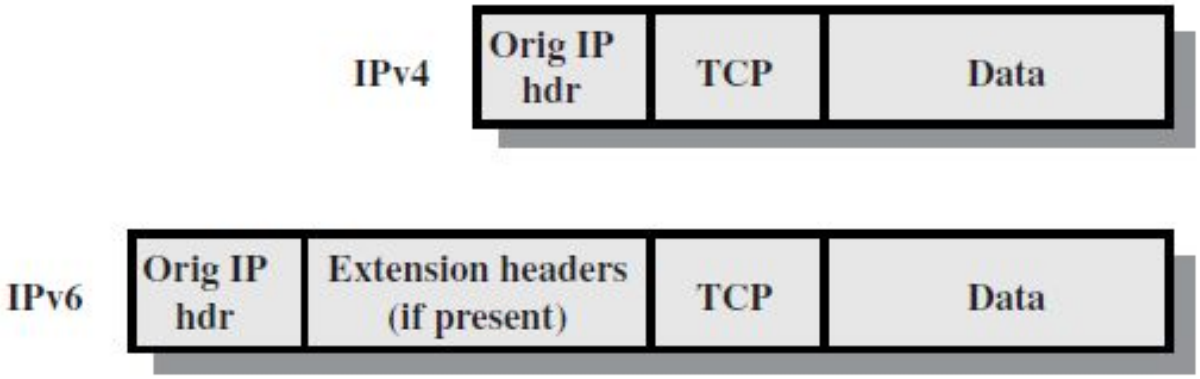
- Provides message content confidentiality & limited traffic flow confidentiality
- Can optionally provide the same authentication services as AH
- Supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - padding needed to fill block size, fields, for traffic flow

Encapsulating Security Payload

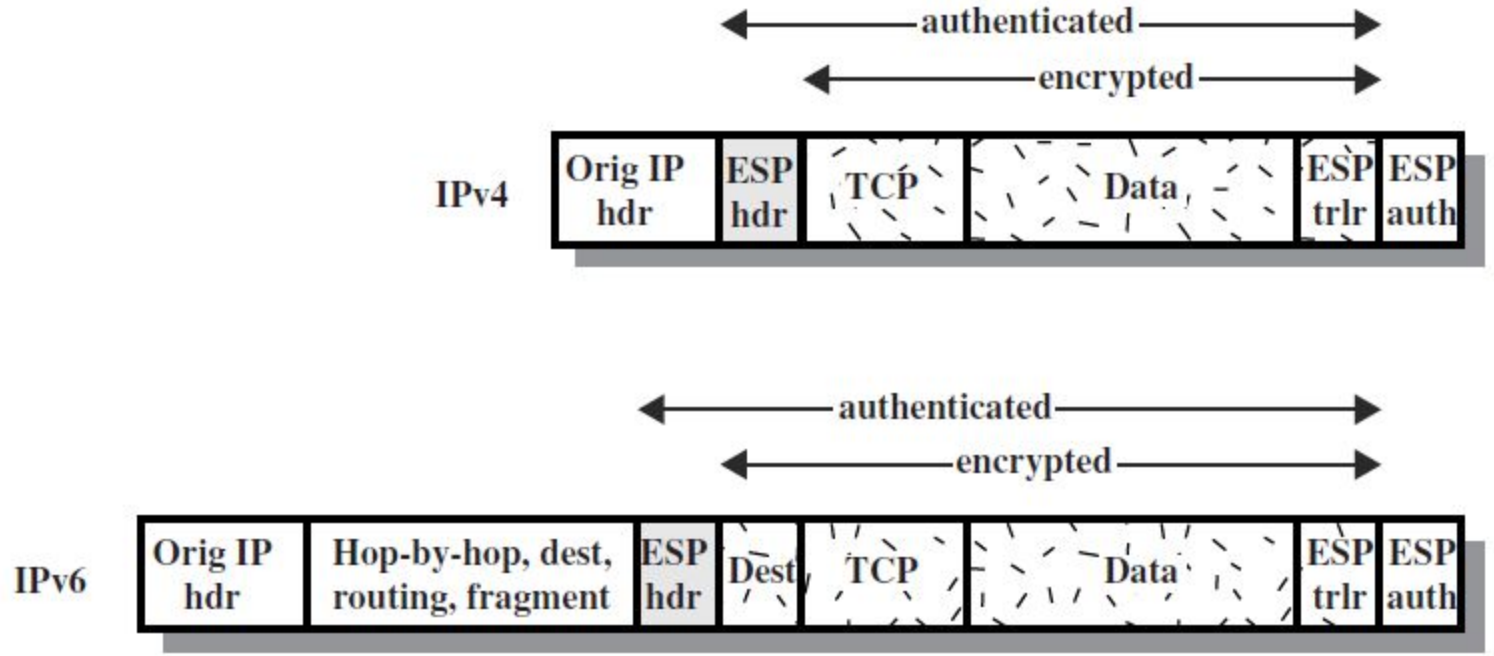


Transport vs Tunnel Mode ESP

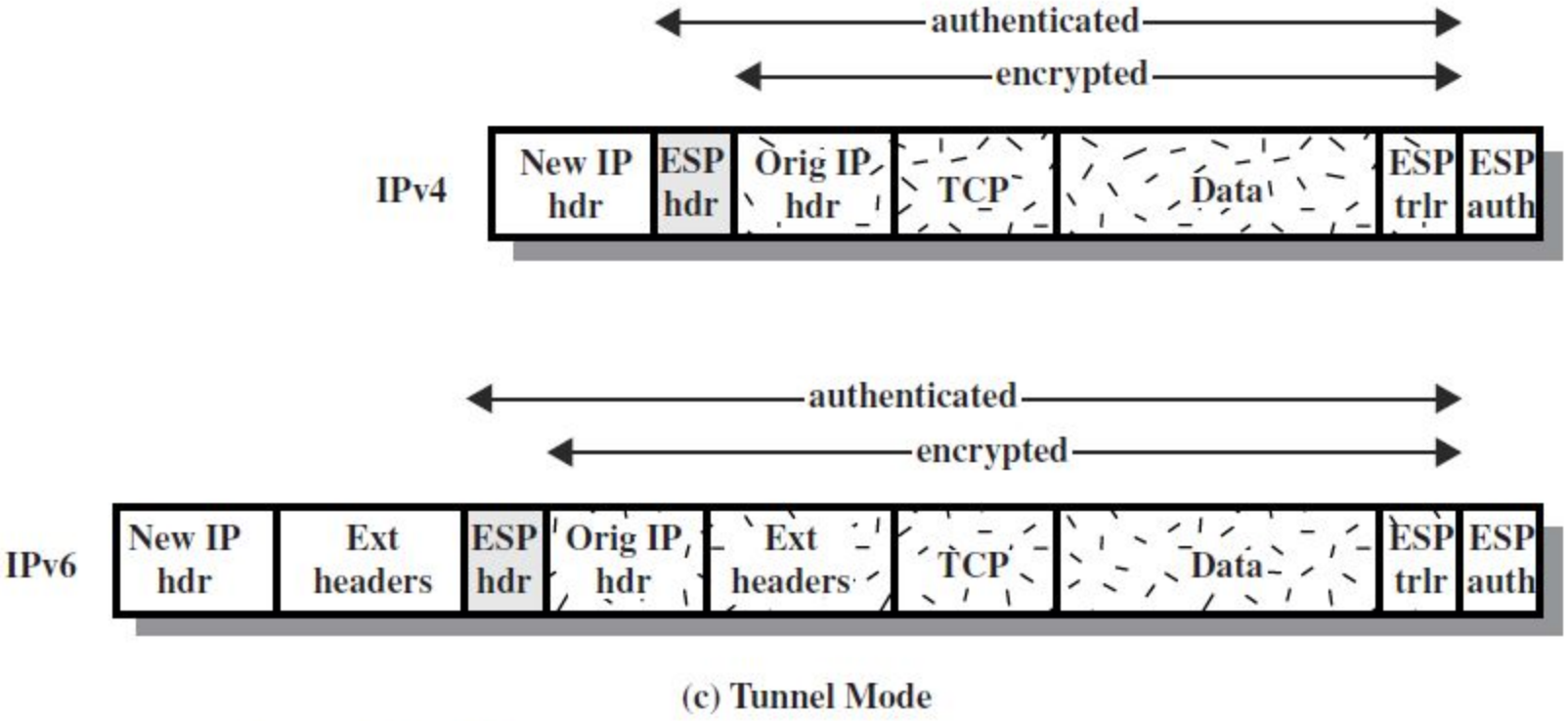
- Transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- Tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security



(a) Before Applying ESP



(b) Transport Mode



(c) Tunnel Mode

Figure 19.8 Scope of ESP Encryption and Authentication

Combining security associations

Combining Security Associations

- 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.

The SAs in a bundle may terminate at different endpoints or at the same endpoints

- An individual SA can implement either the AH or ESP protocol but not both
- Sometimes both are required, plus transport and tunnel modes
- For that, multiple SAs must be employed for the same traffic flow Called ***Security Association Bundle***

Combining Security Associations

Security associations may be combined into bundles in two ways:

1. Transport adjacency
   - applying AH and ESP to the same IP packet without tunneling(Tunneling is **a protocol that allows for the secure movement of data from one network to another.**)
2. Iterated tunneling
   - multiple layers of security protocols through IP tunneling

Combining Security Associations: Authentication Plus Confidentiality

Approaches to combine Encryption and authentication on IP Packets:

- ESP with Authentication option
- Transport Adjacency
- Transport-Tunnel Bundle

ESP with Authentication option

- Transport mode ESP
- Tunnel mode ESP

For both cases, authentication applies to the ciphertext rather than the plaintext

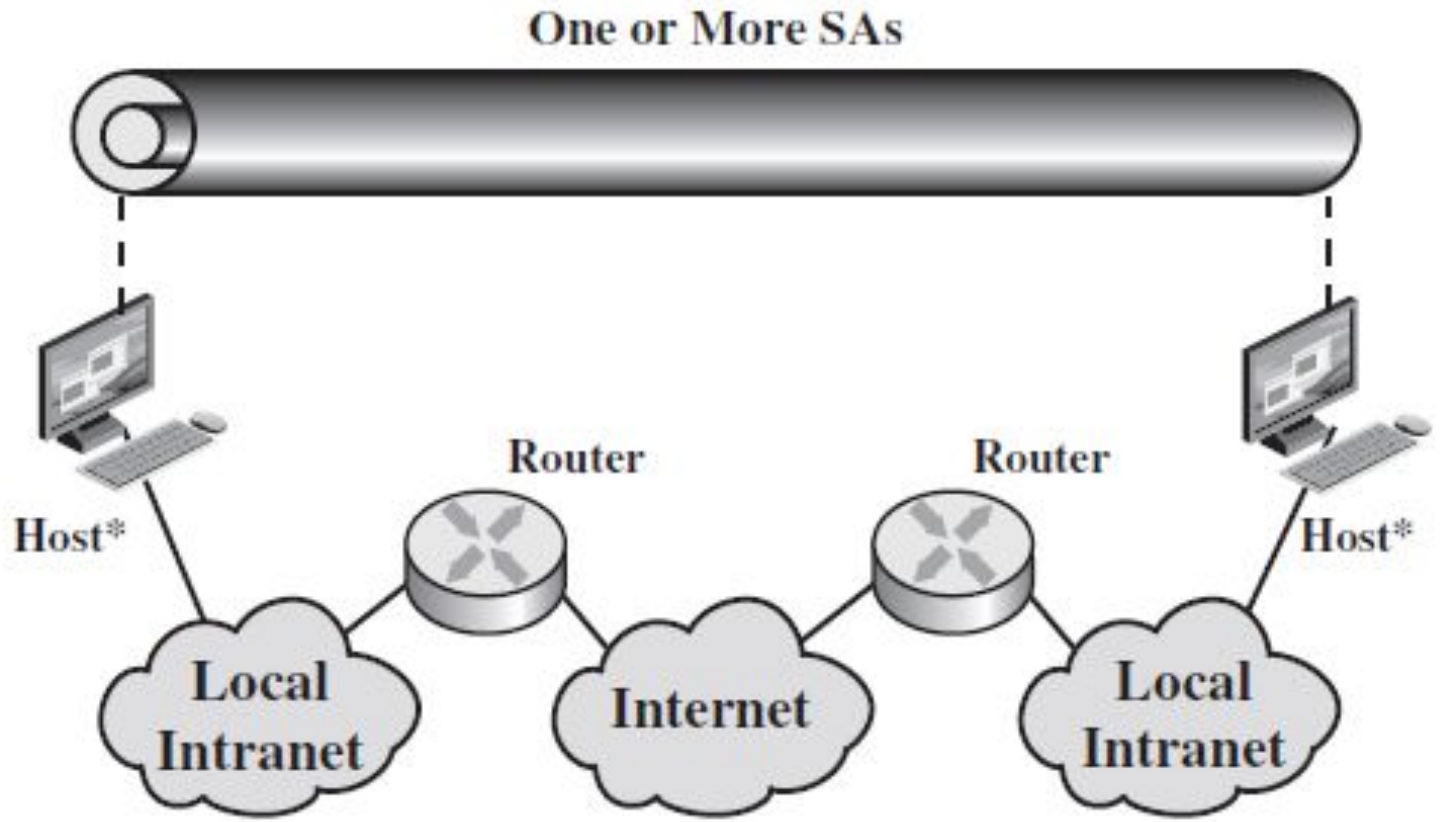
Transport Adjacency

- Two bundled transport SAs are used
- With the inner being an ESP SA and the outer being an AH SA

Transport-Tunnel Bundle

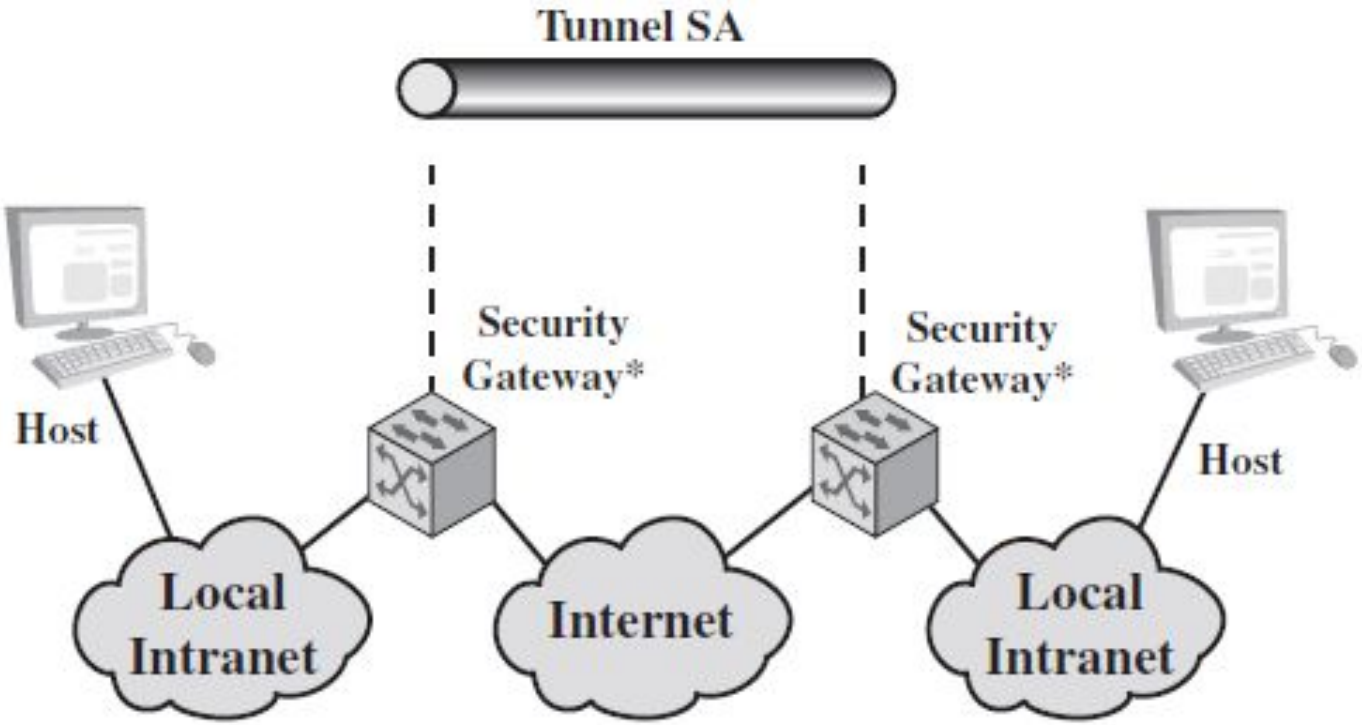
- A bundle consisting of an inner AH transport SA and an outer ESP tunnel SA.
- Authentication is applied to the IP payload plus the IP header
- The resulting IP packet is then processed in tunnel mode by ESP

Basic Combinations of Security Associations



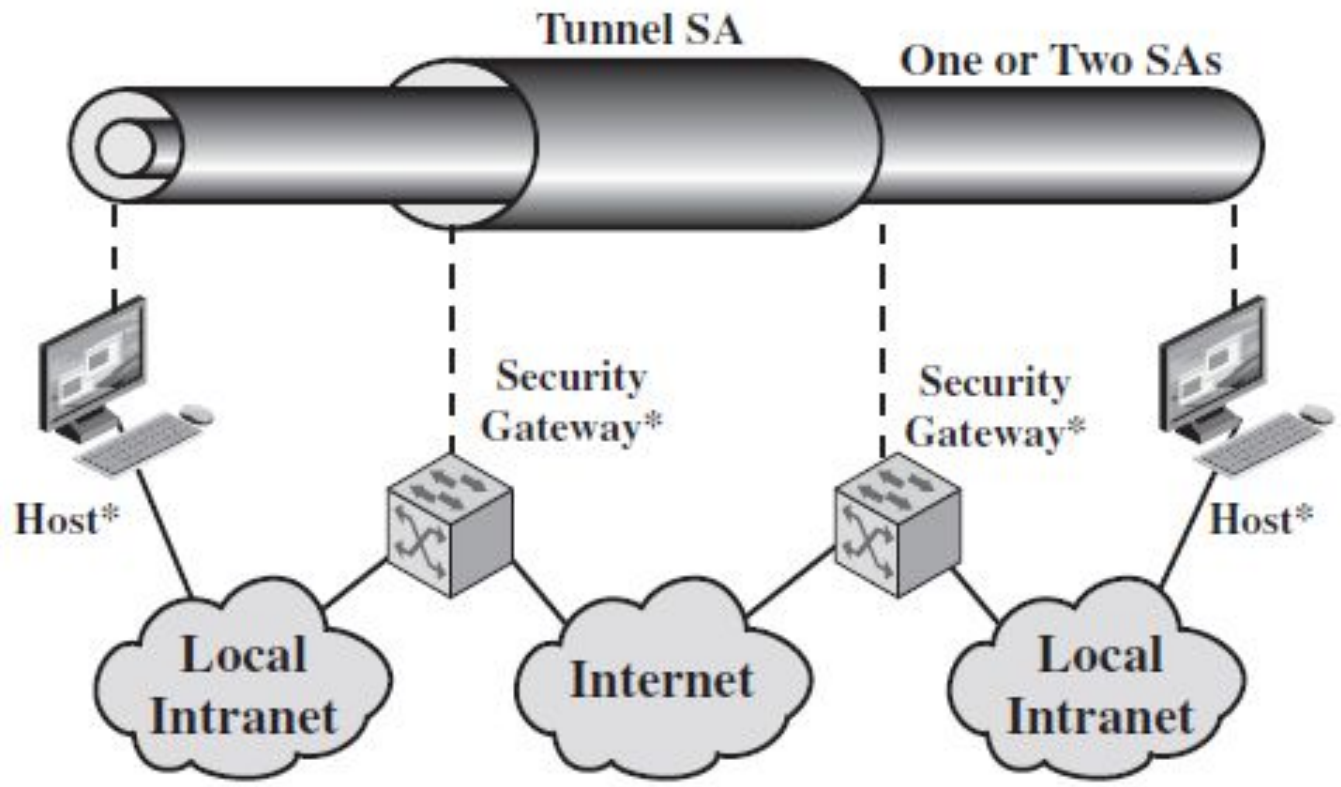
(a) Case 1

Basic Combinations of Security Associations



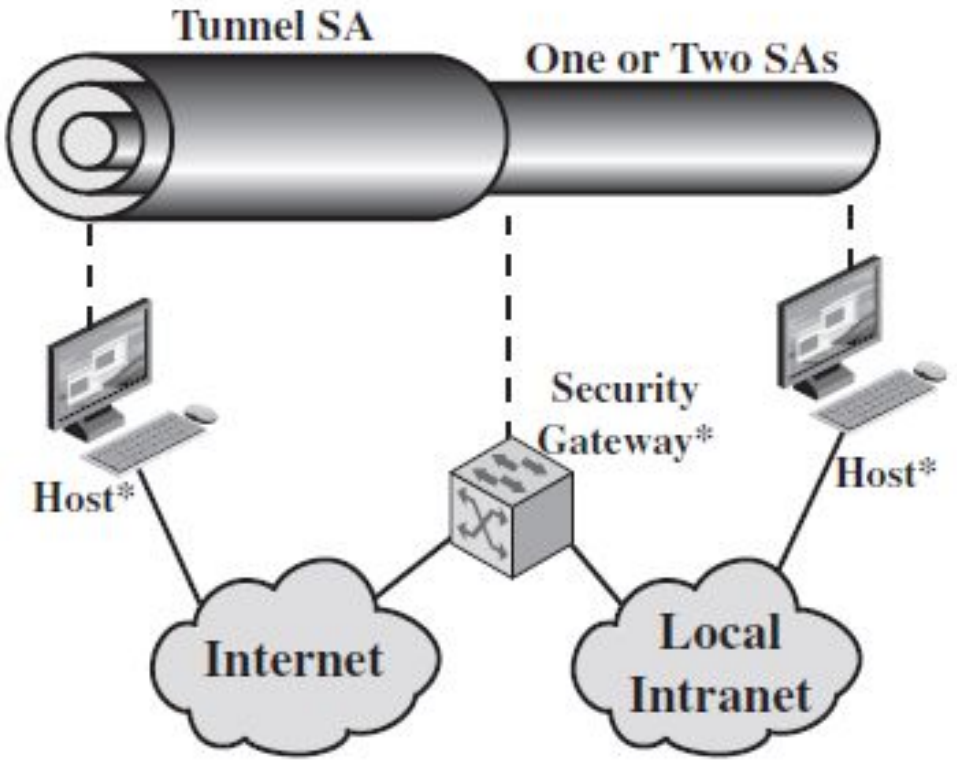
(b) Case 2

Basic Combinations of Security Associations



(c) Case 3

Basic Combinations of Security Associations



(d) Case 4

Case 1. All security is provided between end systems that implement IPsec.

For any two end systems to communicate via an SA, they must sharetheappropriate-ate secret keys. Among the possible combinatio ns are

a. AH in transport mode

b. ESP in transport mode

c. ESP followed by AH in transport mode (an ESP SA inside an AH SA)

d. Any one of a, b, or c inside an AH or ESP in tunnel mode

We have already discussed how these various combinations can be usedtosupport authentication, encryption, authentication before encr yption, and authentication after encryption.

- **Case 2.** Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec. This case illustrates simple virtual private network support. The security architecture document specifies tha t only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required, because the IPsec services apply to the entire inner packet

Case 3. This builds on case 2 by adding end-to-end security. The same combi- nations discussed for cases 1 and 2 are allowed here. The gateway-to-gateway tunnel provides either authentication, confidentiality, or both for all traffic between end systems. When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality. Individual hosts can implement any additional IPsec ser- vices required for given applications or given users by means of end-to-end SAs.

- **Case 4.** This provides support for a remote host that uses the Internet to reach an organization's firewall a nd then to gain access to some server or workstation behind the firewall. Only tunnel mode is required be tween the remote host and the firewall. As in case 1, one or two SAs may be used between the r emote host and the local host.

KEY MANAGEMENT

Key Management

- The key management portion of IPsec involves the determination and distribution of secret keys
- The IPsec Architecture document mandates support for two types of key management:
  - Manual
  - Automated

- Manual: A system administrator manually configures each system with its own keys and with the keys of other communicating systems. This is practical for small, relatively static environments.
- Automated: An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration

Key Management

- The automated key management protocol for IPsec is referred to as ISAKMP/Oakley
- It consists of the following elements:
  - Oakley Key Determination Protocol
  - Internet Security Association and Key Management Protocol (ISAKMP)

Oakley Key Determination Protocol

- A key exchange protocol based on the Diffie-Hellman algorithm with added security
  - Advantages of Diffie-Hellman
    - Secret keys are created only when needed
    - The exchange requires no pre-existing infrastructure
  - Weaknesses to Diffie-Hellman
    - Does not provide information on identities of the parties
    - Subject to a man-in-the-middle attack
    - Computationally intensive: clogging attack

Oakley Features

1. It employs cookies to thwart clogging attacks
2. It enables the two parties to negotiate a *group; this, specifies the* global parameters of the Diffie-Hellman
3. It uses nonces to ensure against replay attacks.
4. It enables the exchange of Diffie-Hellman public key values.
5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

Ans: Oakley Authentication Method

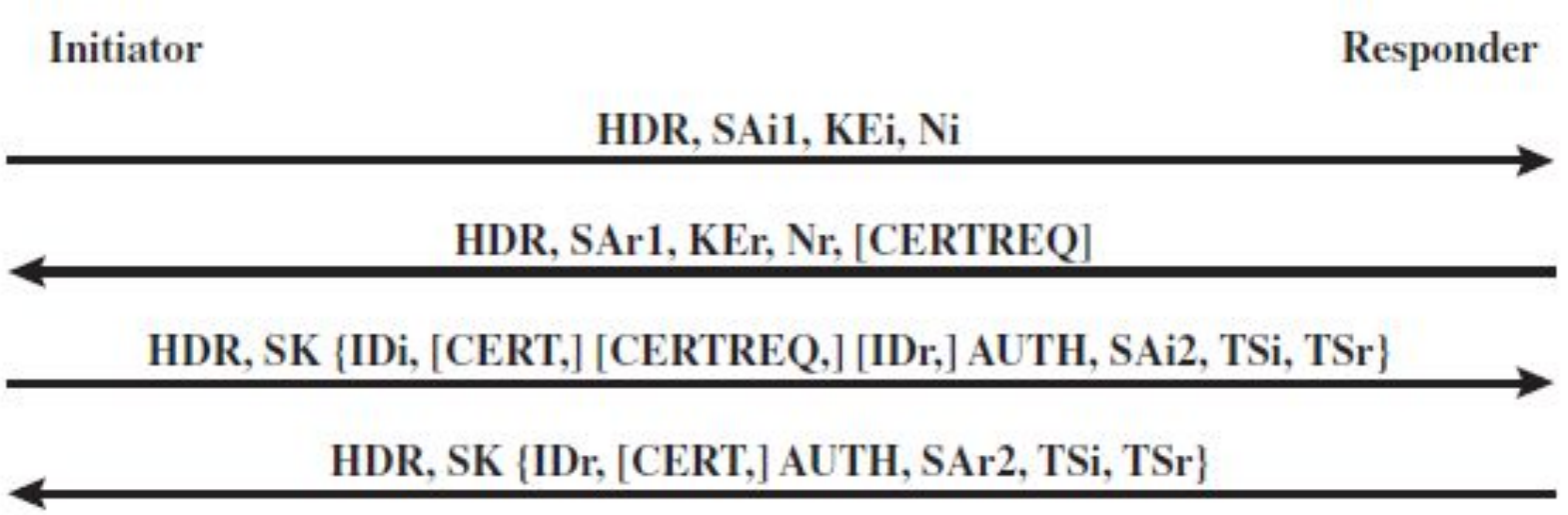
Three different authentication methods can be used with Oakley:

1) **Digital Signatures:** The exchange is authenticated by signing a mutually obtainable hash; each party encrypts the hash with its private key. The hash is generated over important parameters, such as user IDs and nonces.
2) **Public-Key Encryption:** The exchange is authenticated by encrypting parameters such as IDs and nonces with the sender's private key.
3) **Symmetric-Key Encryption:** A key derived by some out-of-band mechanism can be used to authenticate the exchange by symmetric encryption of exchange parameters.

IKE v2 Exchanges

- The IKEv2 protocol involves the exchange of messages in pairs

IKE v2: Initial Exchanges

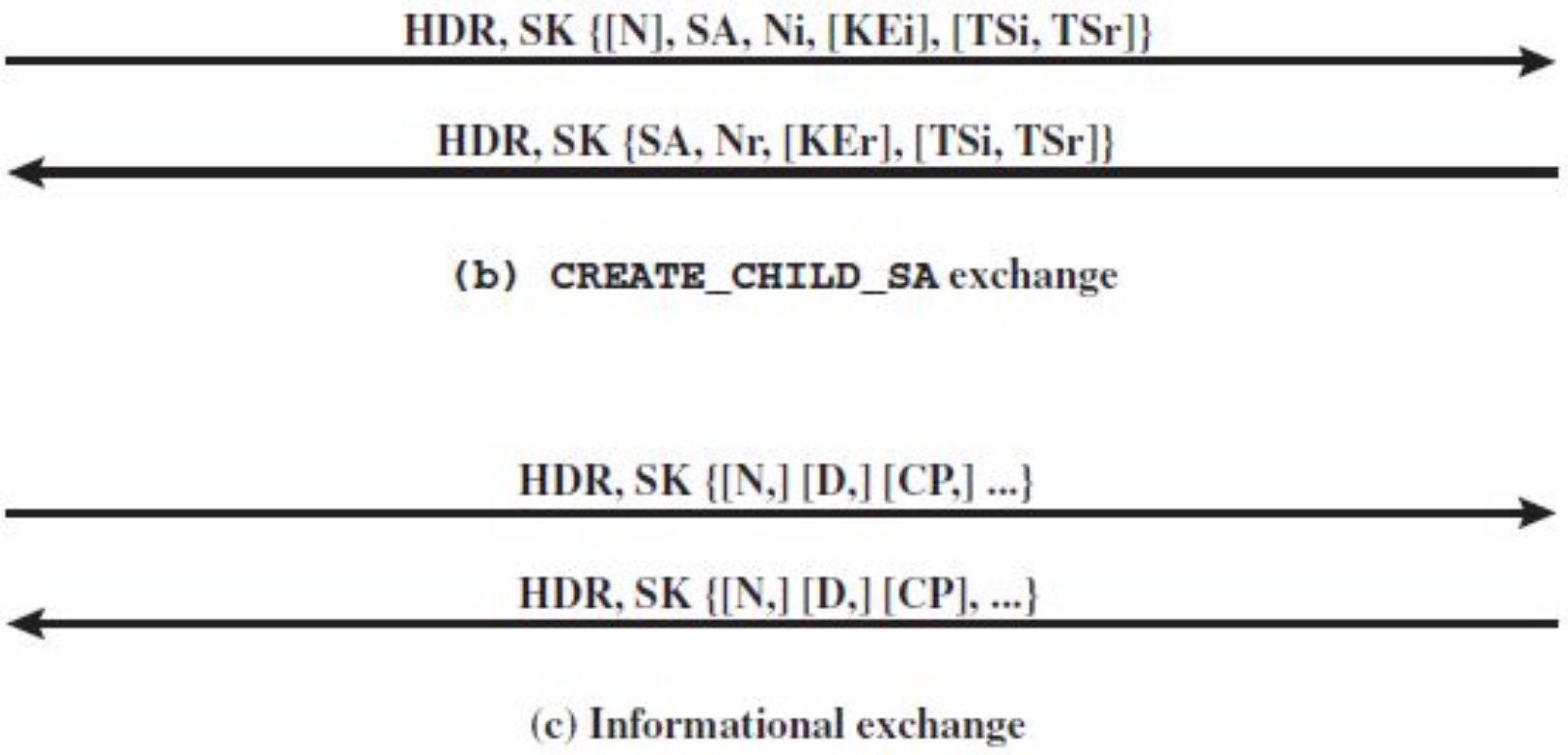


(a) Initial exchanges

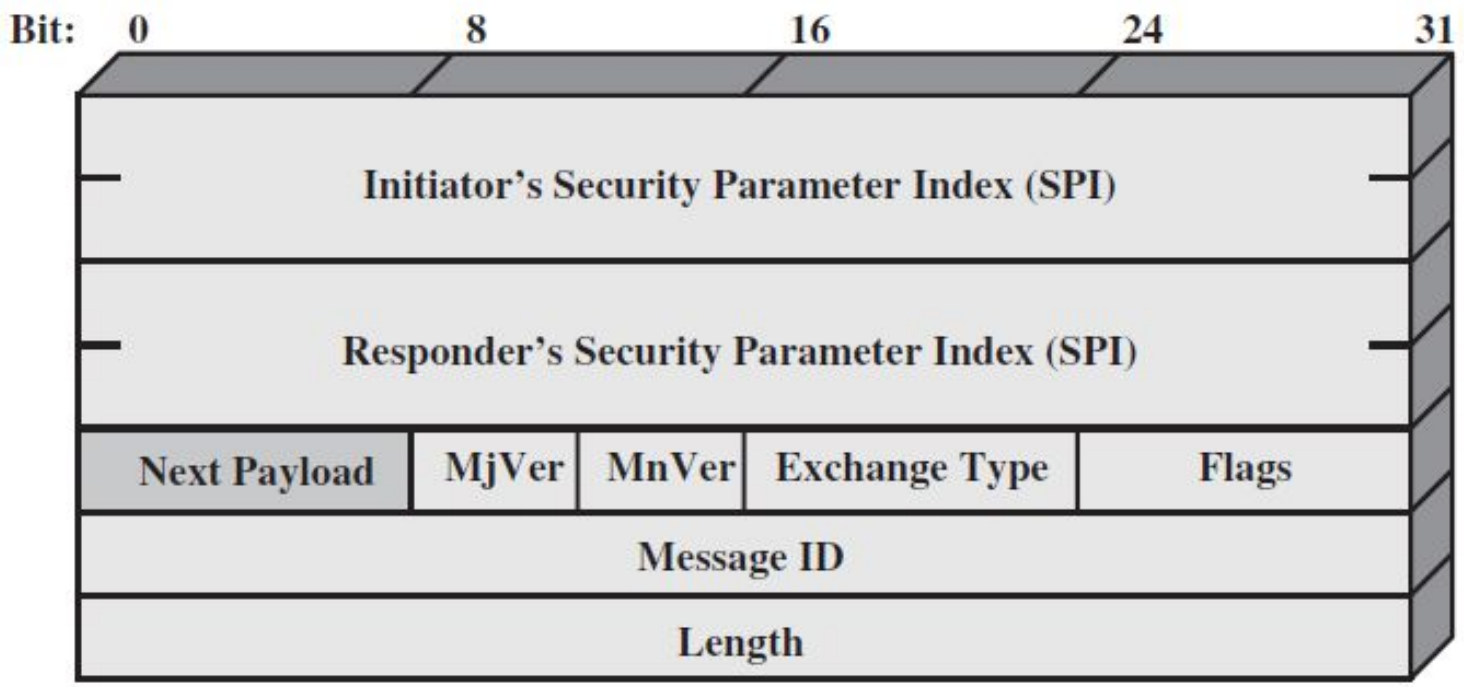
HDR = IKE header
SAx1 = offered and chosen algorithms, DH group
KEx = Diffie-Hellman public key
Nx= nonces
CERTREQ = Certificate request
IDx = identity
CERT = certificate

SK {...} = MAC and encrypt
AUTH = Authentication
SAx2 = algorithms, parameters for IPsec SA
TSx = traffic selectors for IPsec SA
N = Notify
D = Delete
CP = Configuration

IKE v2 Further Exchanges



IKE Header Format

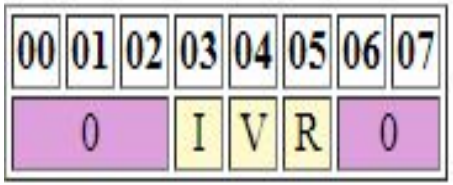


(a) IKE header

- **Initiator SPI.** 8 bytes.
  A value chosen by the initiator to identify a unique IKE security association. This value MUST NOT be cleared to zero.
- **Responder SPI.** 8 bytes.
  A value chosen by the responder to identify a unique IKE security association. This value MUST be cleared to zero in the first message of an IKE Initial Exchange (including repeats of that message including a cookie) and MUST NOT be zero in any other message.
- **Next payload.** 8 bits.
  Indicates the type of payload that immediately follows the header.

- **Major ver.** 4 bits.
  Indicates the major version of the IKE protocol to use.
- **Minor ver.** 4 bits.
  Indicates the minor version of the IKE protocol to use.
- **Exchange type.** 8 bits.
  Indicates the type of exchange being used. This constrains the payloads sent in each message and orderings of messages in an exchange.

- **Flags.** 8 bits.
  Indicates specific options that are set for the message. The presence of options is indicated by the appropriate bit in the flags field being set.



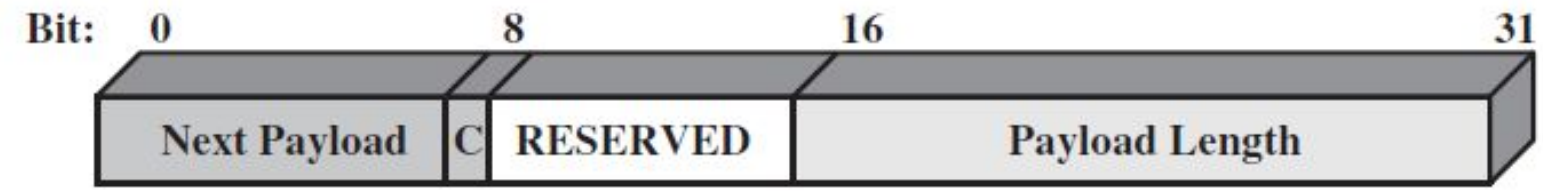
I, Initiator. 1 bit.
Indicates the message was sent by the initiator if set.

V, Version. 1 bit.
Indicates that the sender is capable of speaking a higher major version number of the protocol than the one indicated in the major version number field. Implementations of IKEv2 must clear this bit when sending and MUST ignore it in incoming messages.

R, Response. 1 bit.
Indicates that this message is a response to a message containing the same message ID. This bit MUST be cleared in all request messages and MUST be set in all responses. An IKE endpoint MUST NOT generate a response to a message that is marked as being a response.

IKE Payload Types

- All IKE payloads begin with the same generic payload header



(b) Generic Payload header

IKE Payload Types

Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message