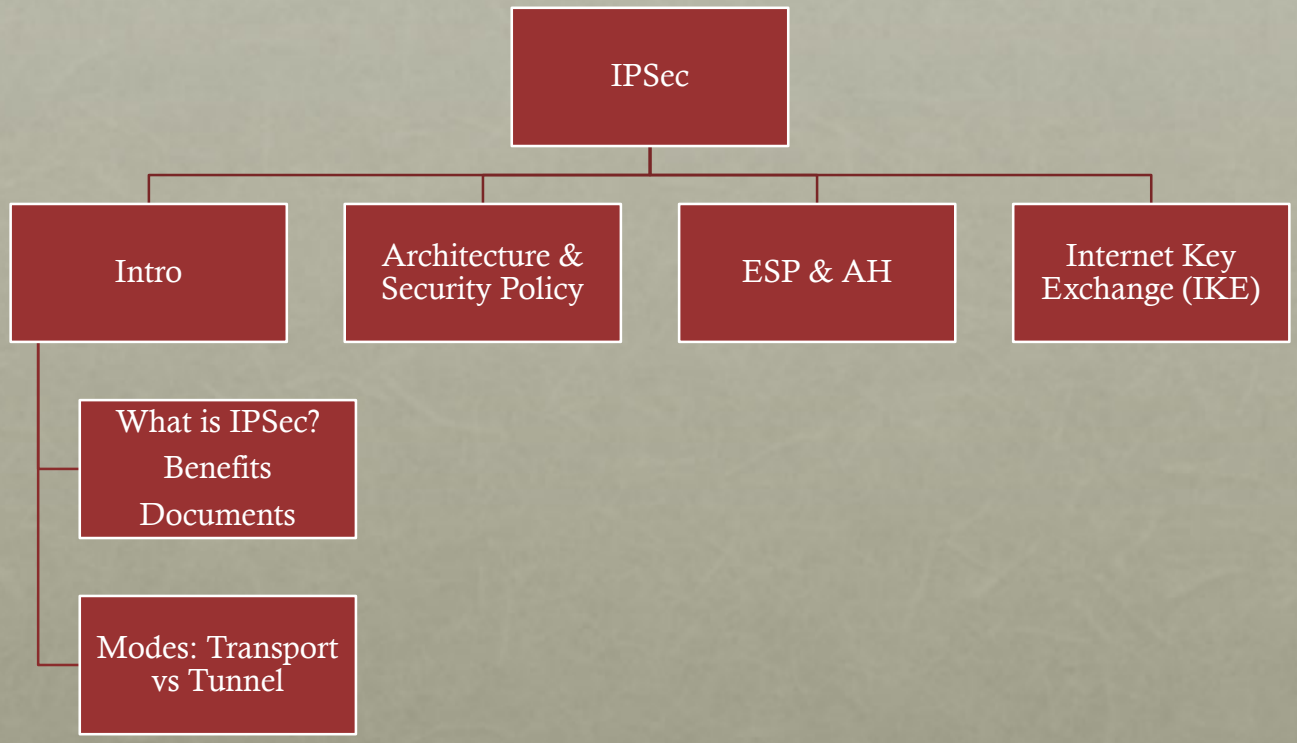
CHAPTER 9

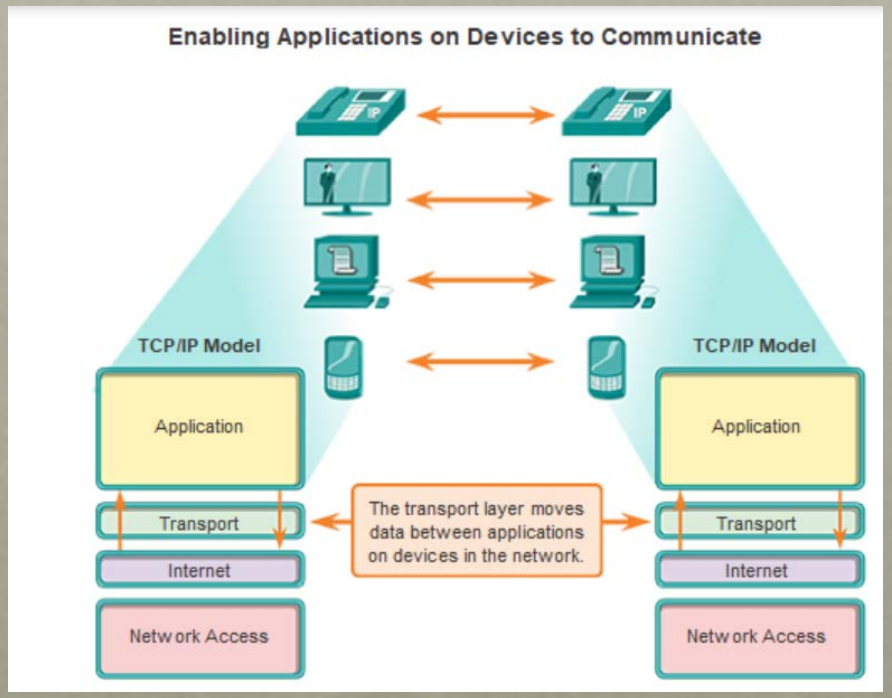
IP Security

OUTLINE

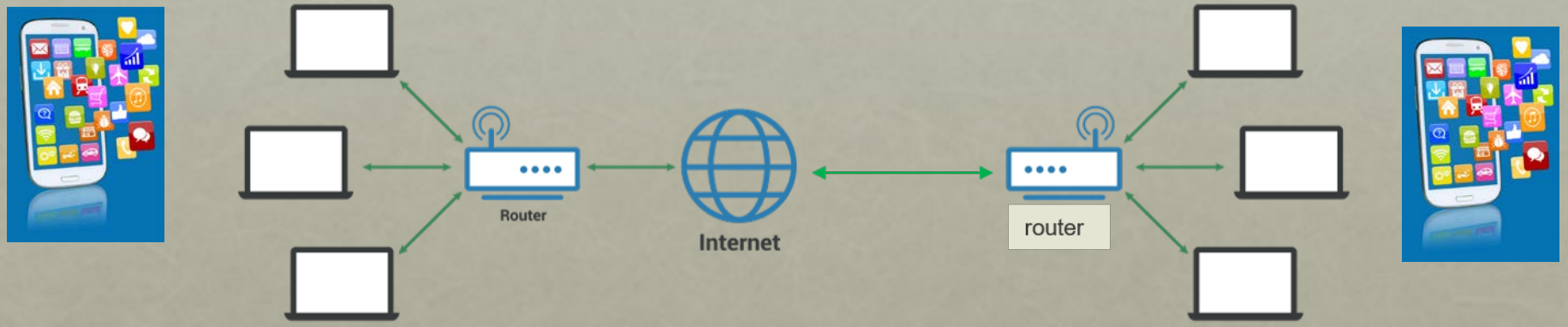

IPSec
Intro
Architecture & Security Policy
ESP & AH
Internet Key Exchange (IKE)
What is IPSec?
Benefits
Documents
Modes: Transport vs Tunnel

INTRO

- Network Access Layer
  - Provides a physical device to a physical device connection
- Network Layer
  - Provides a host to host to network to network connection
- Transport Layer
  - Provides application end-point to application end-point connection



WHY DO WE NEED SECURITY IN THE NETWORK LAYER?



Application Layer
Transport Layer
Network Layer
Network Access

Network Layer
Network Access

Network Layer
Network Access

Application Layer
Transport Layer
Network Layer
Network Access

SECURITY IN EVERY LAYER!!!

- **Network access security protocols:**
  - Security within the LAN between STA and AP
  - The data sent from the STA to the AP will be encrypted only between the STA and the AP.
  - cipher text received by the AP will be converted back to plaintext and transferred over the network backbone.
- Hence, we need security in higher layer to secure data as they travel between APs from source to destination.
- **IPSec works in the network layer** to secure data (create a secure tunnel) between two hosts (host to host), networks (AP to AP), or host to network.
- **Transport layer security protocols** secure data (create a secure tunnel) between two endpoint applications.
- **Kerberos work within the application layer** to authenticate users and distribute secret keys.

IP SECURITY OVERVIEW

- RFC 1636
  - "Security in the Internet Architecture"
  - Issued in 1994 by the Internet Architecture Board (IAB)
  - Identifies key areas for security mechanisms
    - Need to secure the network infrastructure from unauthorized monitoring and control of network traffic
    - Need to secure end-user-to-end-user traffic using authentication and encryption mechanisms
  - IAB included authentication and encryption as necessary security features in the next generation IP (IPv6)
    - The IPsec specification now exists as a set of Internet standards

BENEFITS OF IPSEC

Some of the benefits of IPsec:

1. When IPsec is implemented in a firewall or a router, it provides strong **security that can be applied to all traffic crossing the perimeter**. Traffic within a company or workgroup does not incur the overhead of security-related processing
2. **IPsec in a firewall is resistant to bypass** if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization
3. IPsec is below the transport layer (TCP, UDP) and so **is transparent to applications**. Hence, there is no need to change software on a user or server system when IPsec is implemented in the firewall or router
4. **IPsec can be transparent to end users**, hence, there is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization
5. **IPsec can provide security for individual users if needed**, this is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications

APPLICATIONS OF IPSEC

- IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet

Examples include:

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

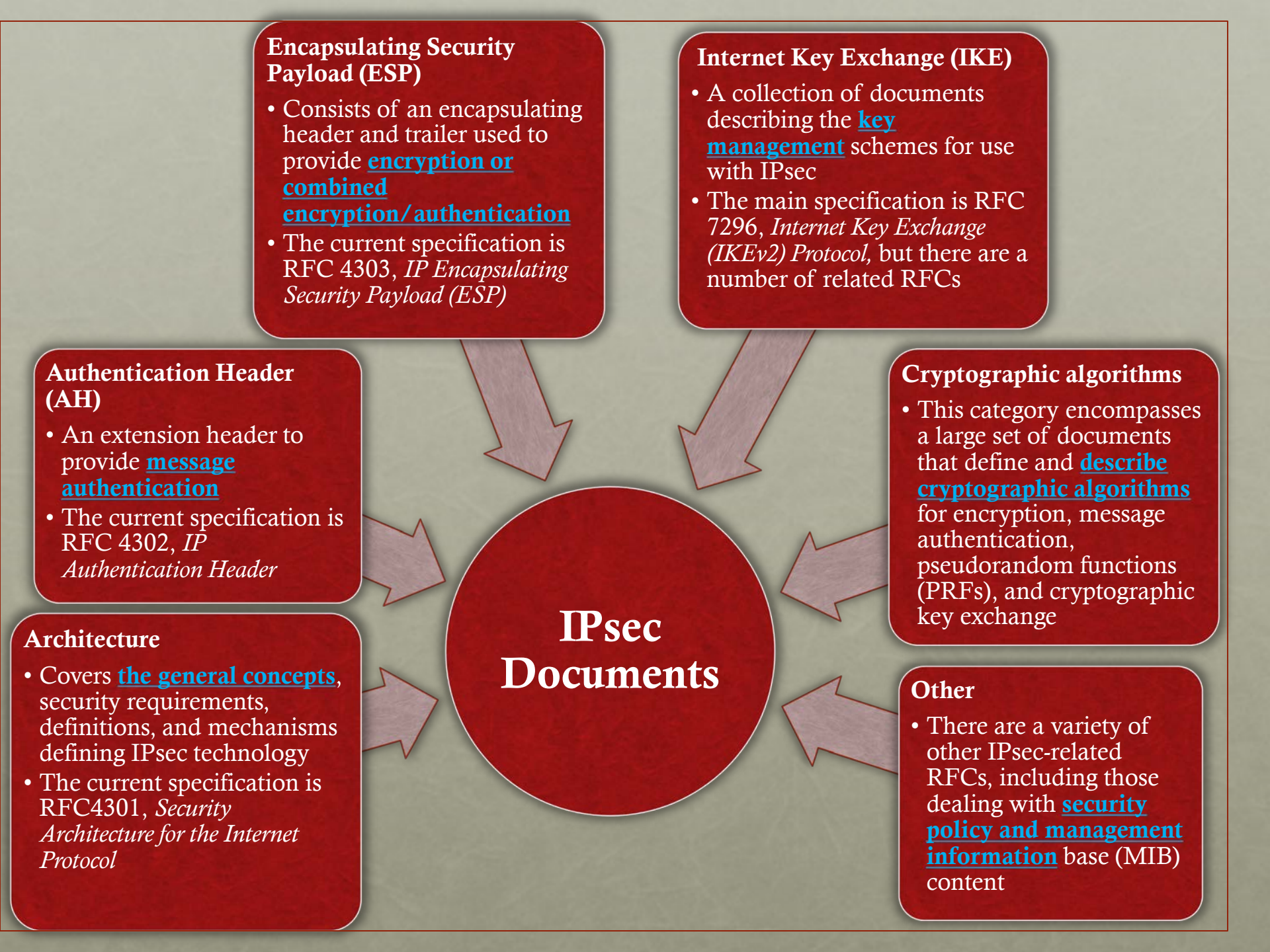
- Principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level
  - Thus all distributed applications (remote logon, client/server, e-mail, file transfer, Web access) can be secured

ANOTHER EXAMPLE: ROUTING APPLICATIONS

- IPsec can play a vital role in the routing architecture required for internetworking

IPsec can assure that:

- **A router advertisement comes from an authorized router**
- **A router seeking to establish a neighbor relationship with a router in another routing domain is an authorized router**
- **A redirect message comes from the router to which the initial IP packet was sent**
- **A routing update is not forged**


Encapsulating Security Payload (ESP)
• Consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication
• The current specification is RFC 4303, IP Encapsulating Security Payload (ESP)
Internet Key Exchange (IKE)
• A collection of documents describing the key management schemes for use with IPsec
• The main specification is RFC 7296, Internet Key Exchange (IKEv2) Protocol, but there are a number of related RFCs
Authentication Header (AH)
• An extension header to provide message authentication
• The current specification is RFC 4302, IP Authentication Header
Cryptographic algorithms
• This category encompasses a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange
IPsec Documents
Architecture
• Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology
• The current specification is RFC4301, Security Architecture for the Internet Protocol
Other
• There are a variety of other IPsec-related RFCs, including those dealing with security policy and management information base (MIB) content

TRANSPORT MODE VS. TUNNEL MODE

Transport mode: Host to Host

Tunnel mode: Host to Network or Network to Network

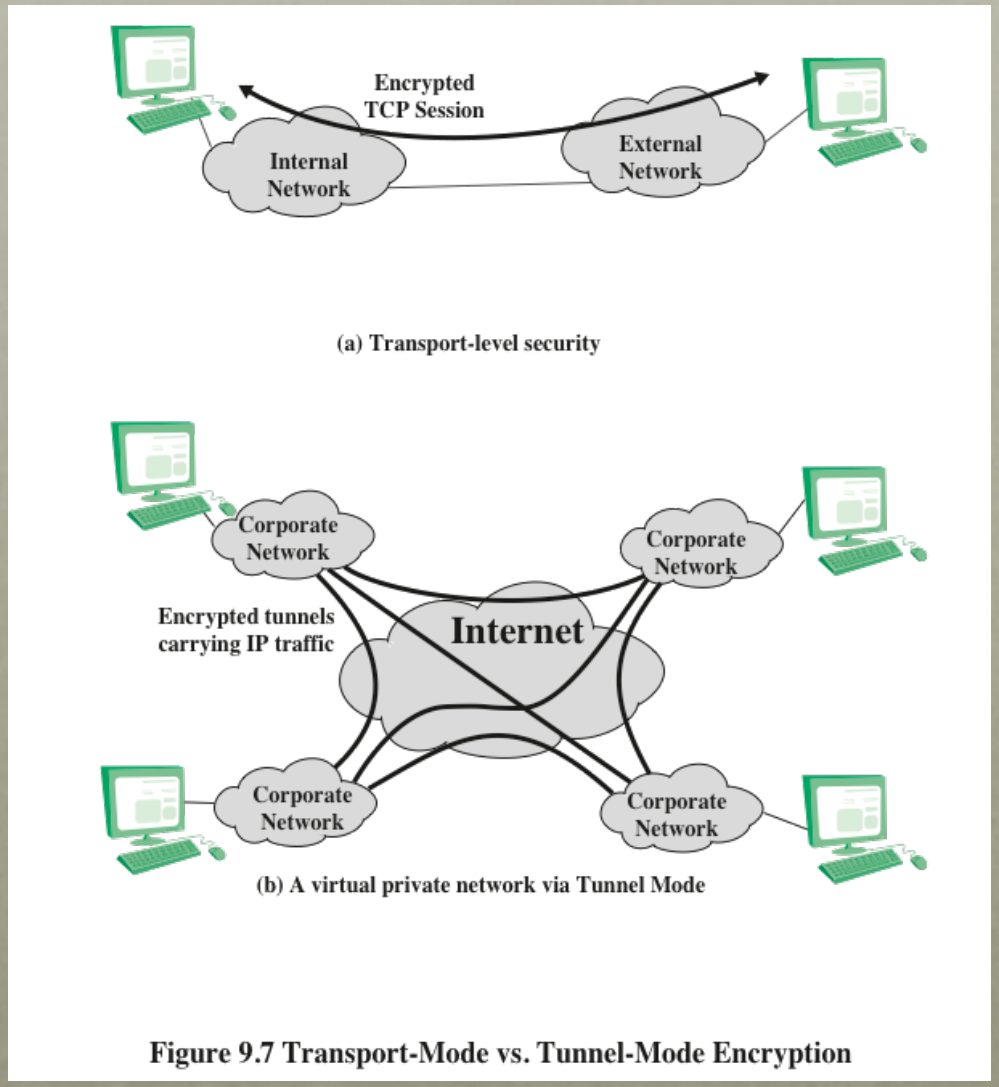
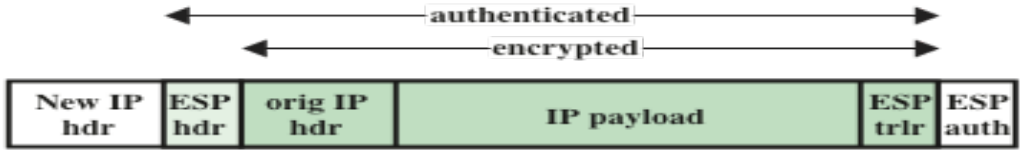
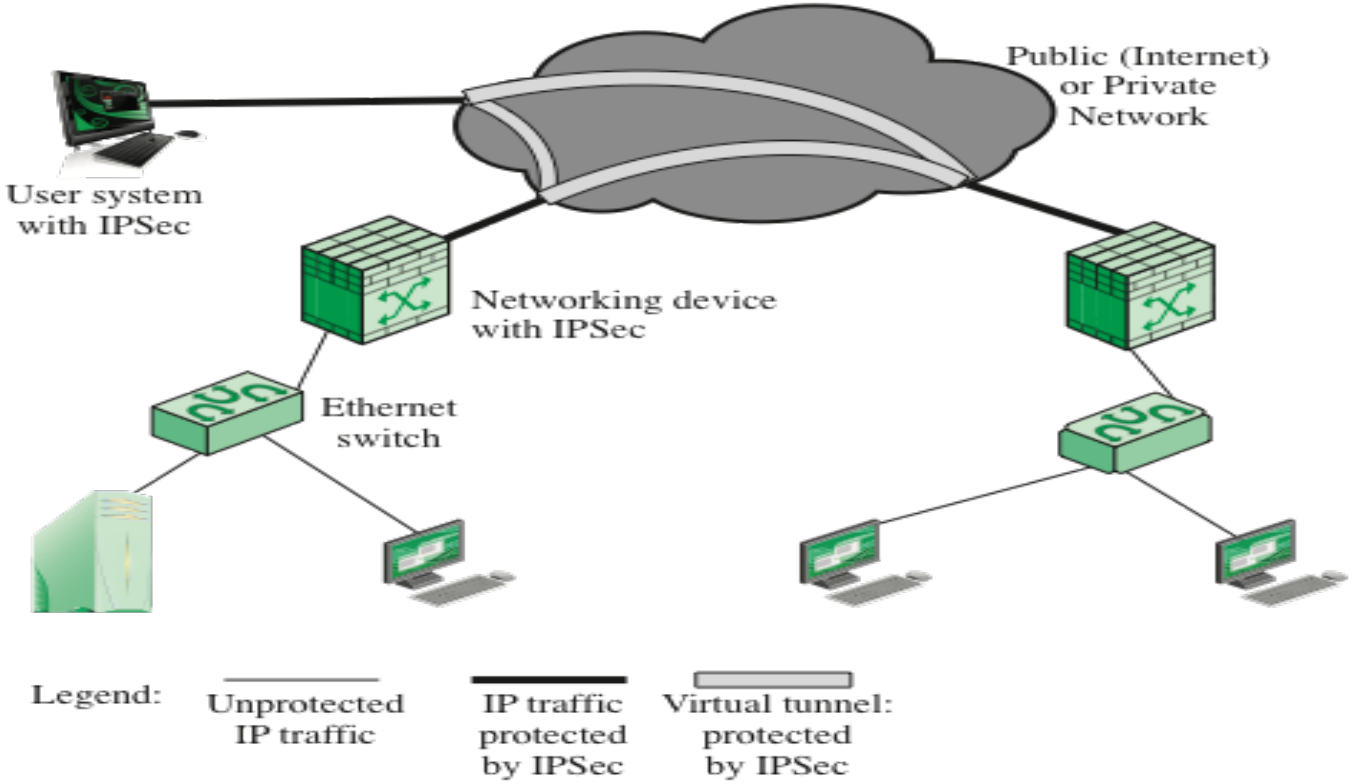


Figure 9.7 Transport-Mode vs. Tunnel-Mode Encryption



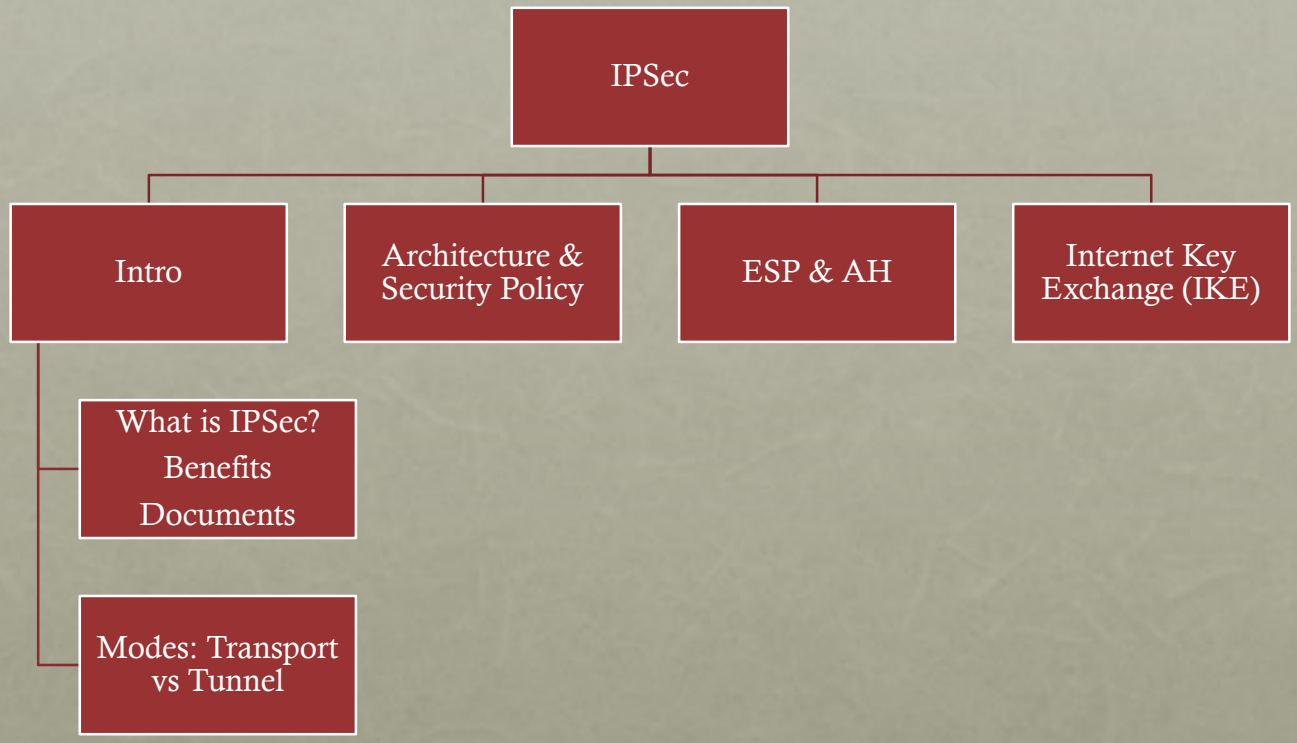
(a) Tunnel-mode format



(b) Example configuration

Figure 9.1 An IPSec VPN Scenario

OUTLINE


IPSec
Intro
Architecture & Security Policy
ESP & AH
Internet Key Exchange (IKE)
What is IPSec?
Benefits
Documents
Modes: Transport vs Tunnel

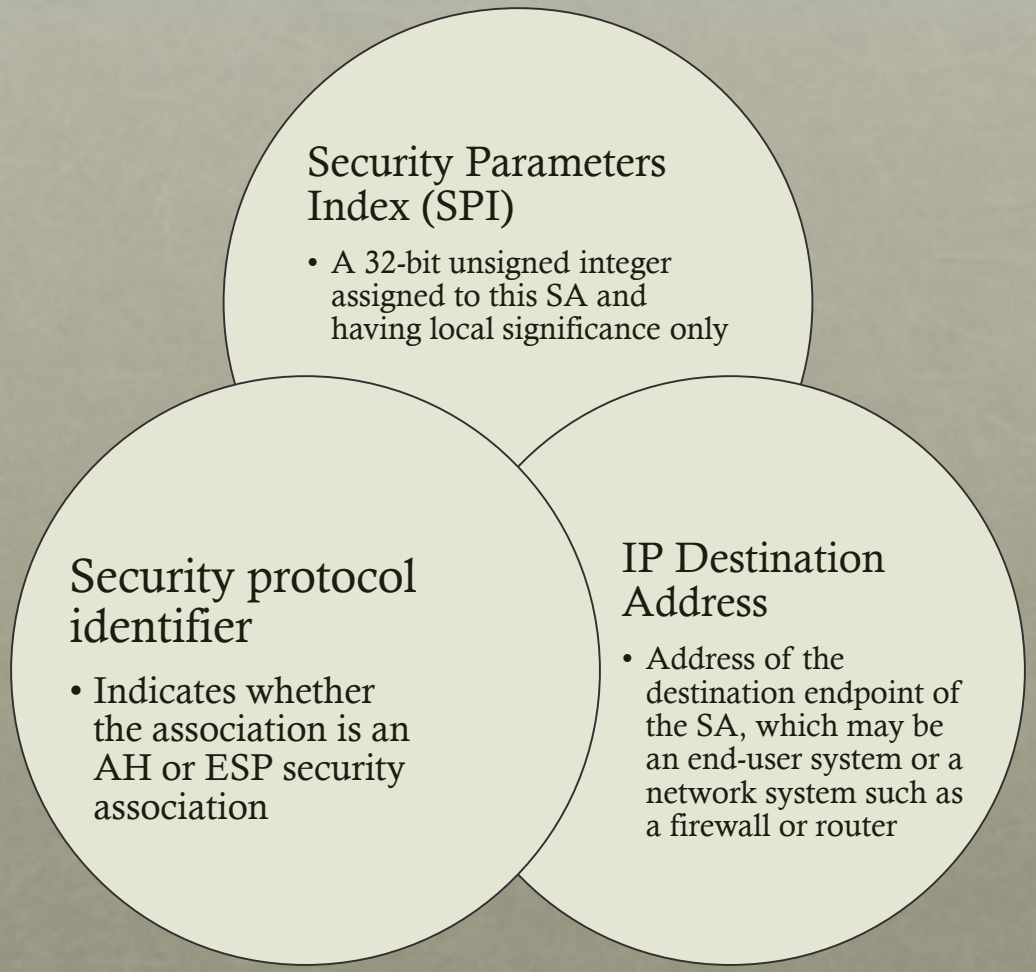
ARCHITECTURE OF IPSEC

- For security in the Network Layer we must provide the three services:
  - Confidentiality,
  - Integrity, and
  - Authentication
- IPSec Comprises:
  - IKE → for key management, policy agreement and security association establishment
  - ESP → confidentiality
  - AH → Integrity and message authentication

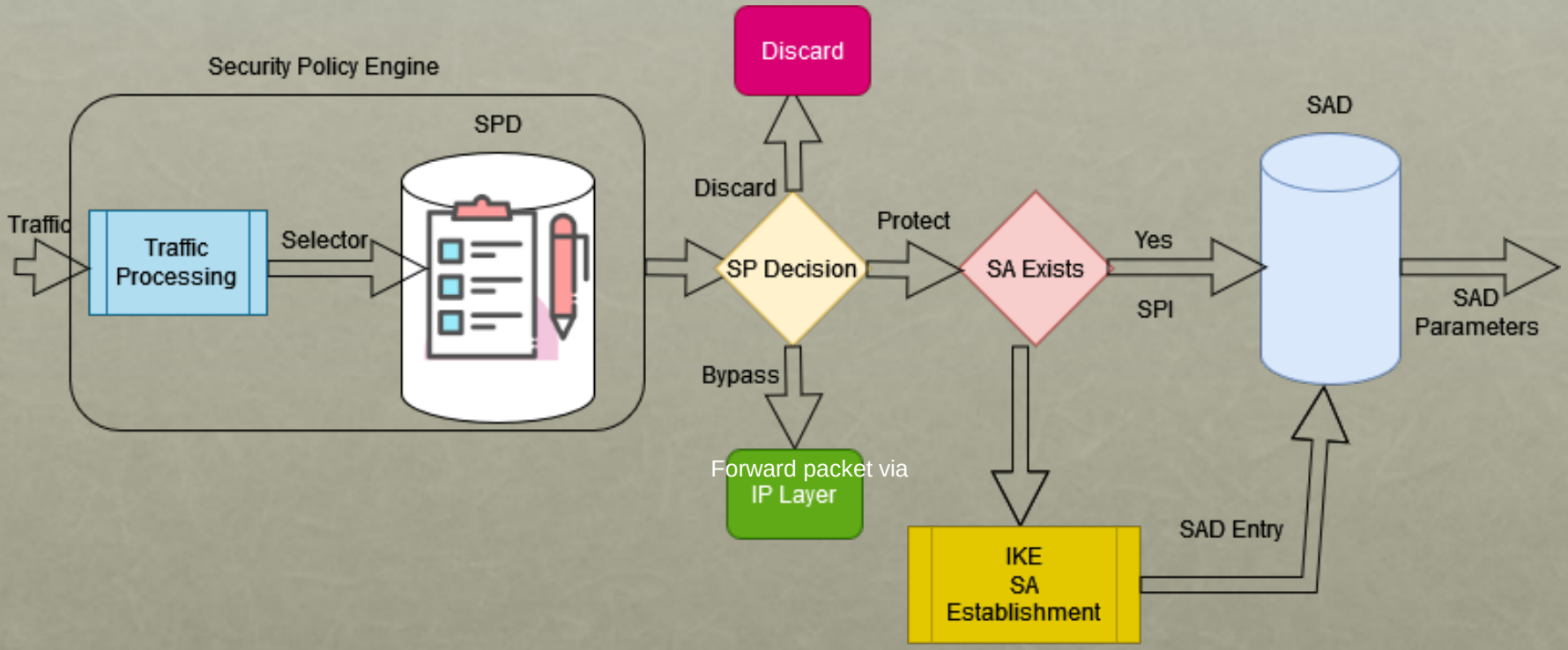
SECURITY ASSOCIATION (SA)

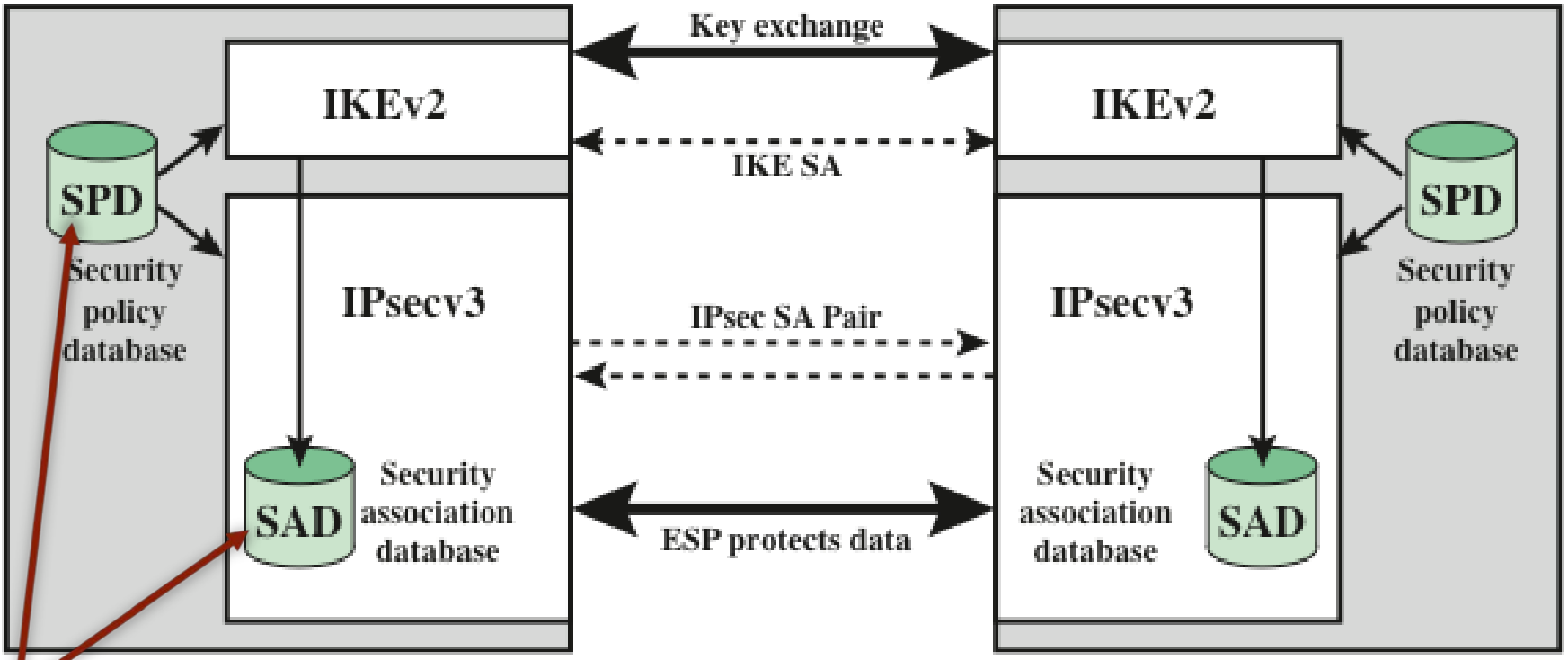
- A one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it
- In any IP packet, the SA is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP)

Uniquely identified by three parameters:



IPSEC PROCESS OVERVIEW





- **IPSec Policy** is determined by the interaction of these two databases
- For each security policy, we have a set of **security parameters**
- These **security parameters** are saved in the SAD as an entry
- The identifier of this entry is the SPI

SECURITY POLICY DATABASE (SPD)

- The means by which IP traffic is related to specific SAs
  - Contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic
- In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry
  - Each SPD entry is defined by a set of IP and upper-layer protocol field values called ***selectors***
  - These are used to filter outgoing traffic in order to map it into a particular SA

SPD ENTRIES

- The following **selectors** determine an SPD entry:

Remote IP address	Local IP address	Next layer protocol	Name	Local and remote ports
This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address	This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address	The IP protocol header includes a field that designates the protocol operating over IP	A user identifier from the operating system	These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port
The latter two are required to support more than one destination system sharing the same SA	The latter two are required to support more than one source system sharing the same SA		Not a field in the IP or upper-layer headers but is available if IPsec is running on the same operating system as the user	

Table 9.2
Host SPD Example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Security Association Database (SAD)

- Defines the parameters associated with each SA
- Normally defined by the following parameters in a SAD entry:
  - Security parameter index
  - Sequence number counter
  - Sequence counter overflow (using the initial sequence number and the max counter value, we can define a lifetime of the SA in terms of number of allowed packets. Once this number is reached, we may need to renew the SA.)
  - Anti-replay window
  - AH information
  - ESP information
  - Lifetime of this security association (as in actual times, mins, hours, …, etc.)
  - IPsec protocol mode (i.e. Tunnel, transport).
  - Path MTU

ESP ANTI-REPLAY SERVICE

- **Three Possible options when receiving a new packet:**
  - **A packet with a sequence number inside the window is received**
    - The packet has been authenticated and its sequence number is marked as "Not Received"
      - → outcome: place the packet in the corresponding position and mark this position as "received".
    - The packet has been authenticated and its sequence number is marked as "Received"
      - → outcome: discard the packet and raise an alert flag
  - **A Packet with a sequence number < N –W**
    - Discard and raise an alert flag
  - **A Packet with a sequence number > N**
    - If the packet is authenticated,
      - Place the packet in the corresponding position,
      - Mark the position as received
      - Advance the window to the new position

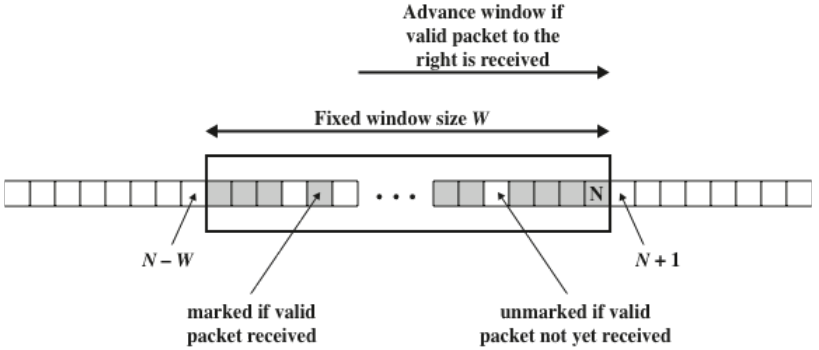


Figure 9.6 Anti-Replay Mechanism

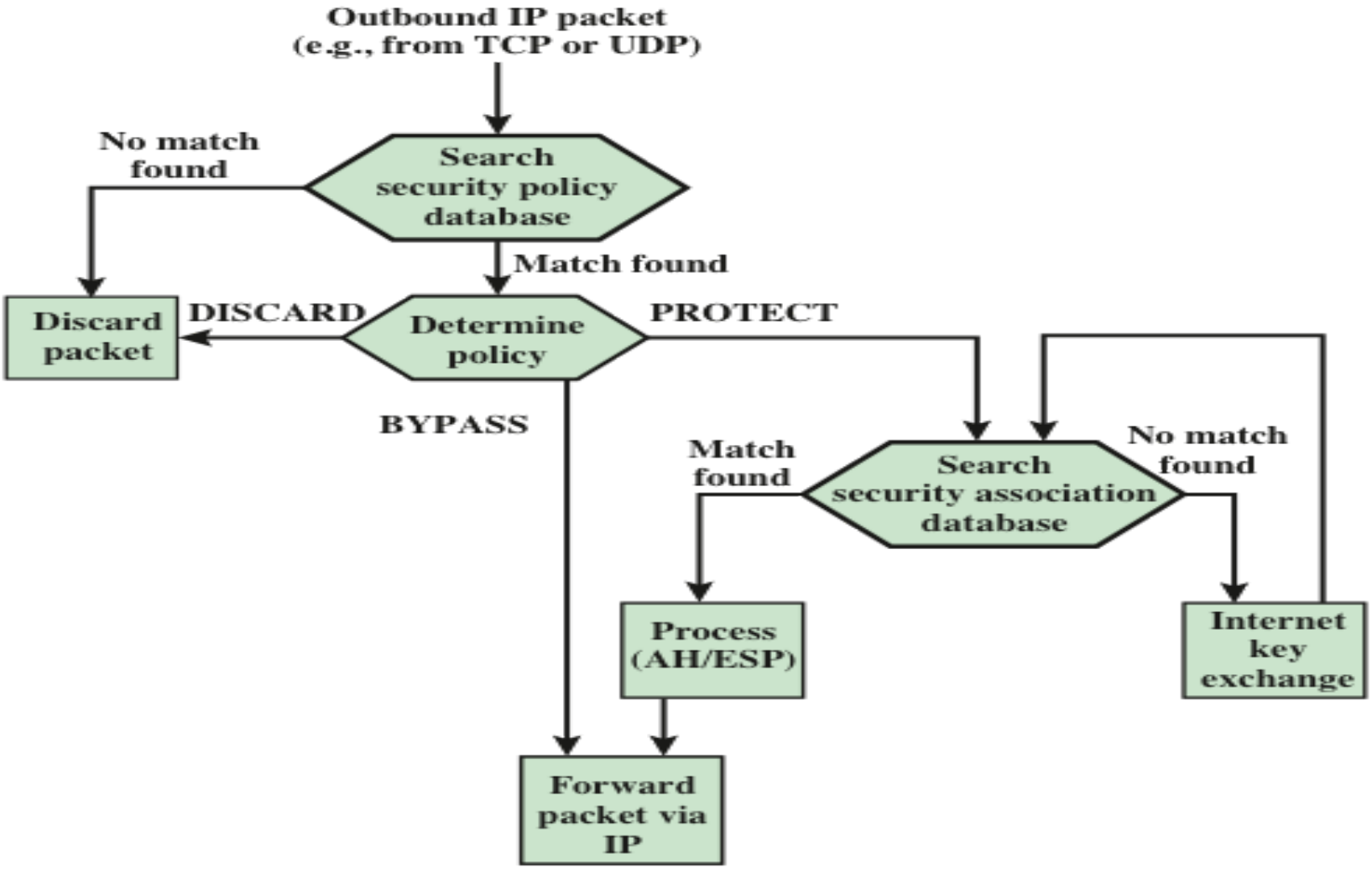


Figure 9.3 Processing Model for Outbound Packets

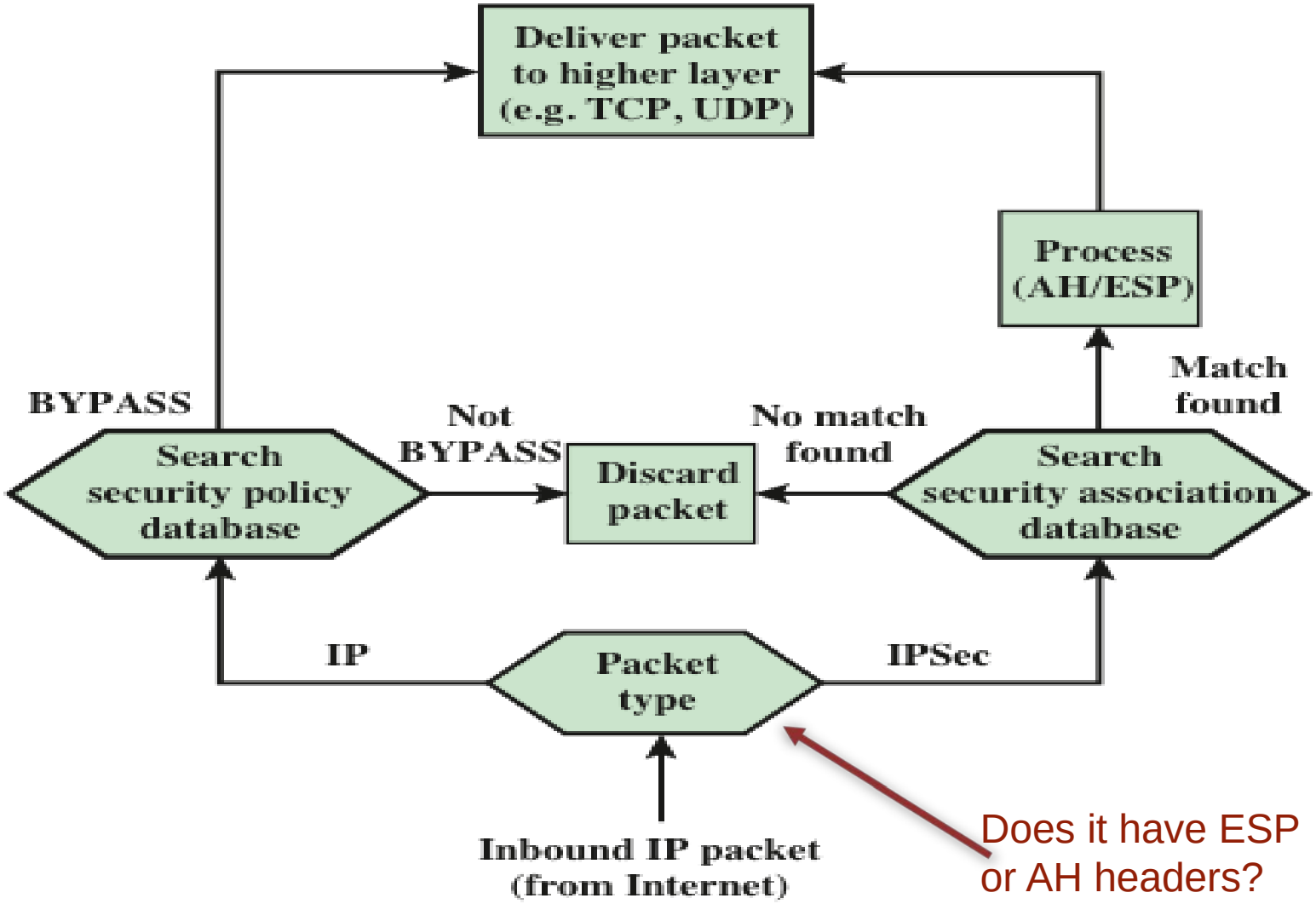
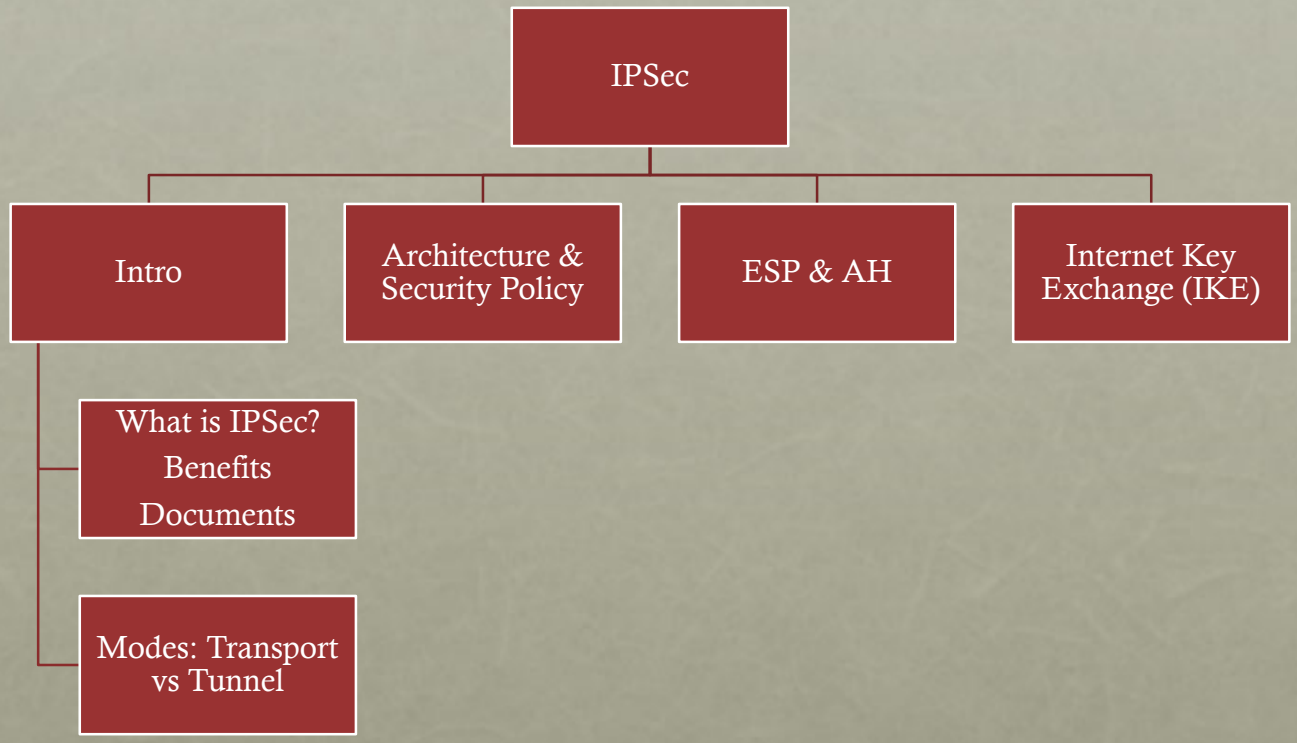


Figure 9.4 Processing Model for Inbound Packets

OUTLINE


IPSec
Intro
Architecture & Security Policy
ESP & AH
Internet Key Exchange (IKE)
What is IPSec?
Benefits
Documents
Modes: Transport vs Tunnel

ESP HEADER & TRAILER STRUCTURE

- ESP can provide:
  - **Confidentiality**
  - **Connectionless integrity** (IPSec inherits the characteristics of the IP layer, hence it is also connectionless and works on a packet-by-packet basis)
  - **Anti-replay service** (sequence number and anti-replay window)
  - **Partial traffic flow confidentiality** (through padding)
- Which services are provided depends on
  - Options selected at the time of SA
- ESP header includes fields before payload (SPI and Sequence number)
- ESP trailer includes fields after payload (padding, pad length, next header, and optionally ICV)

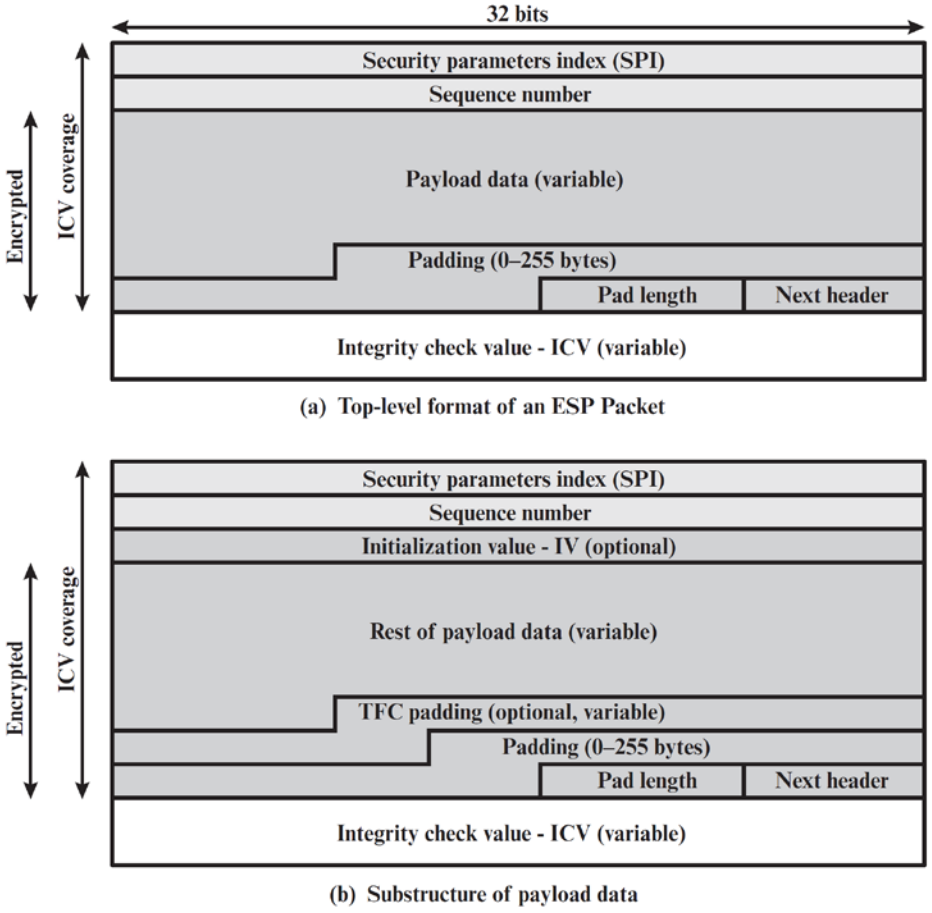


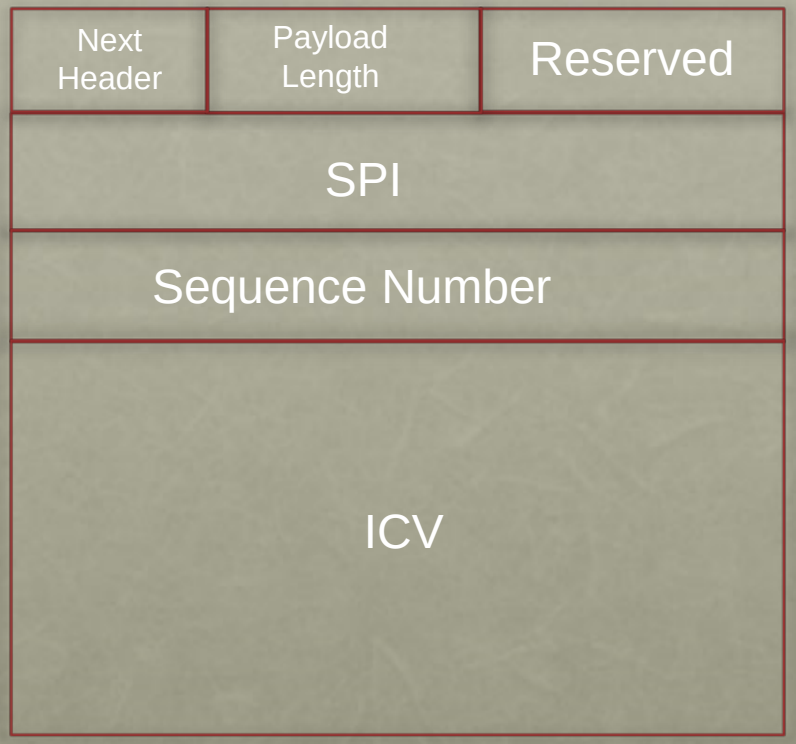
Figure 9.5 ESP Packet Format

Padding can be used for:

- Data alignment, e,g., encryption and hashing require a specific size of data for each block
- Alignment of the ESP header to a 32-bit word
- Traffic flow confidentiality

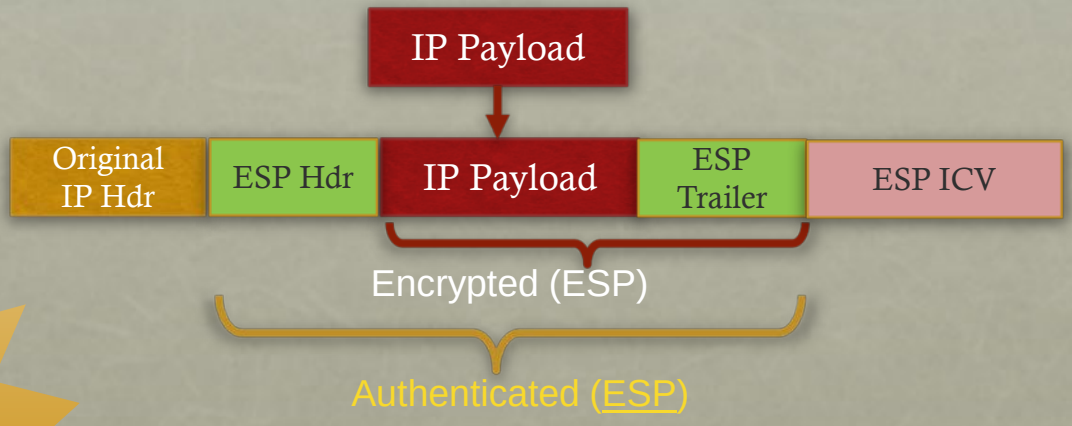
AH HEADER STRUCTURE

- AH can provide
  - Data integrity
  - ICV is integrity check value (equivalent to message authentication code (MAC)).
- Note SPI is included in both the headers of ESP and AH.



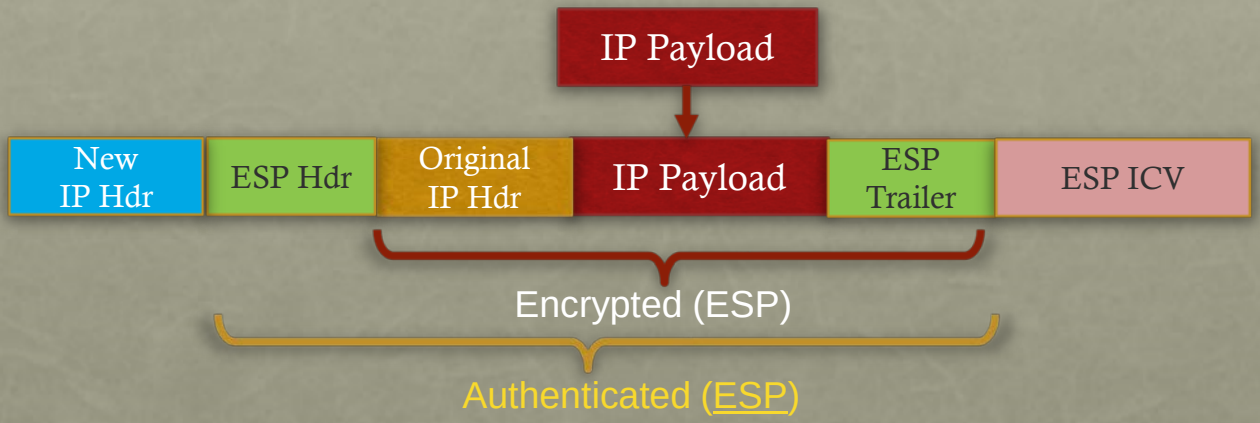
ESP FOR ENCRYPTION + AUTHENTICATION

Transport Mode

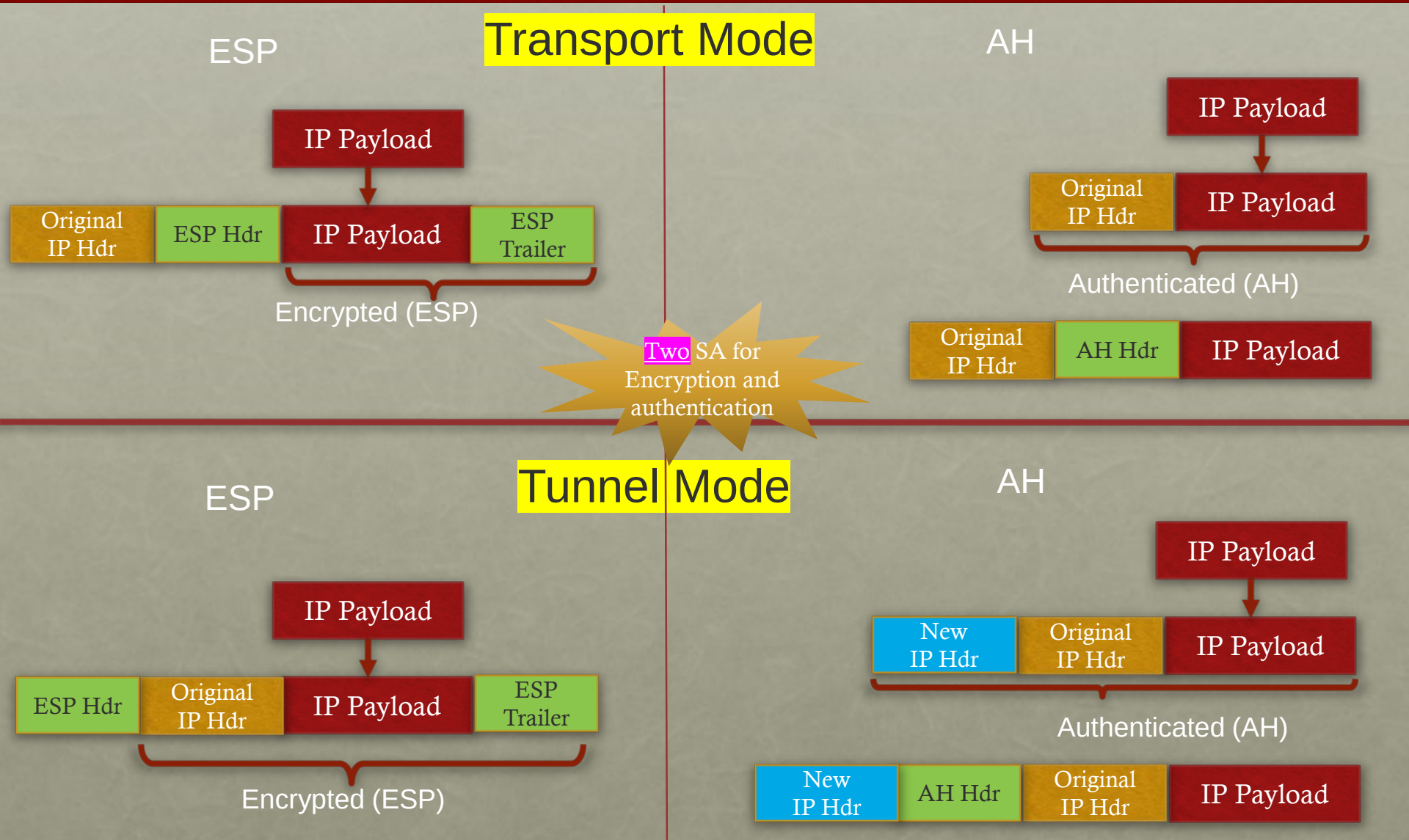


Single SA for Encryption and authentication

Tunnel Mode



ESP FOR ENCRYPTION ONLY & AH FOR AUTHENTICATION



AH TRANSPORT MODE VS TUNNEL MODE

The original IP header gets Authenticated!!!

Is this good or bad?

- Both
- Good because we authenticate more fields
- Bad: because of NAT!!!
  - NAT at the AP will change the private IP to the corresponding Public IP
  - However, **the sent ICV** was calculated based on **private IP.**
  - At the receiving end, the ICV will be **calculated** based on the **public** IP.
  - The sent ICV and Calculated ICV will not match!!!

TRANSPORT AND TUNNEL MODES

Transport Mode

- Provides protection primarily for upper-layer protocols
- Examples include a TCP or UDP segment or an ICMP packet
- **Typically used for end-to-end communication between two hosts**
- **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

Tunnel Mode

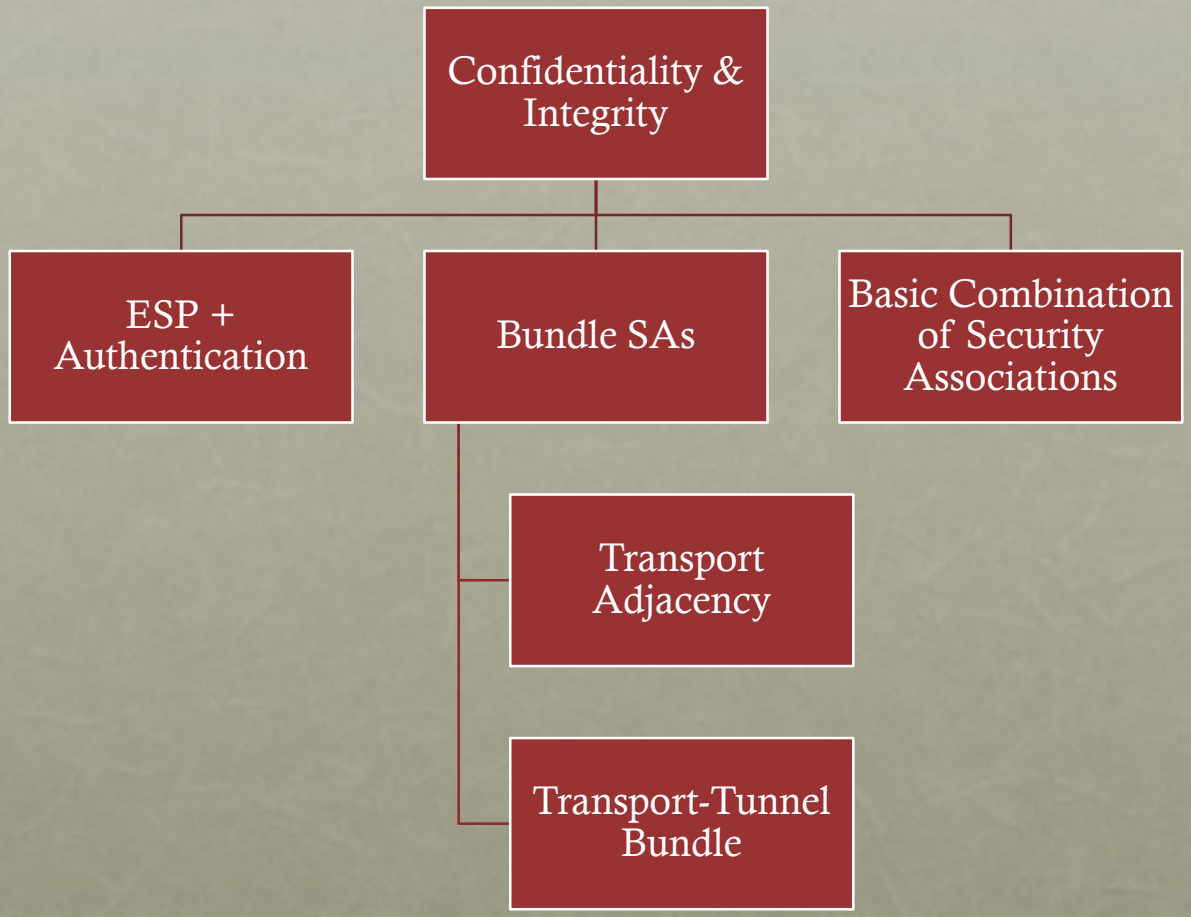
- **Provides protection to the entire IP packet**
- **Used when one or both ends of a security association (SA) are a security gateway**
- A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec
- **ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header**
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header

Table 9.1- Tunnel Mode and Transport Mode Functionality

Table 9.1 Tunnel Mode and Transport Mode Functionality

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

POSSIBLE WAYS TO PROVIDE CONFIDENTIALITY AND INTEGRITY



ESP + AUTHENTICATION

TRANSPORT MODE VS. TUNNEL MODE

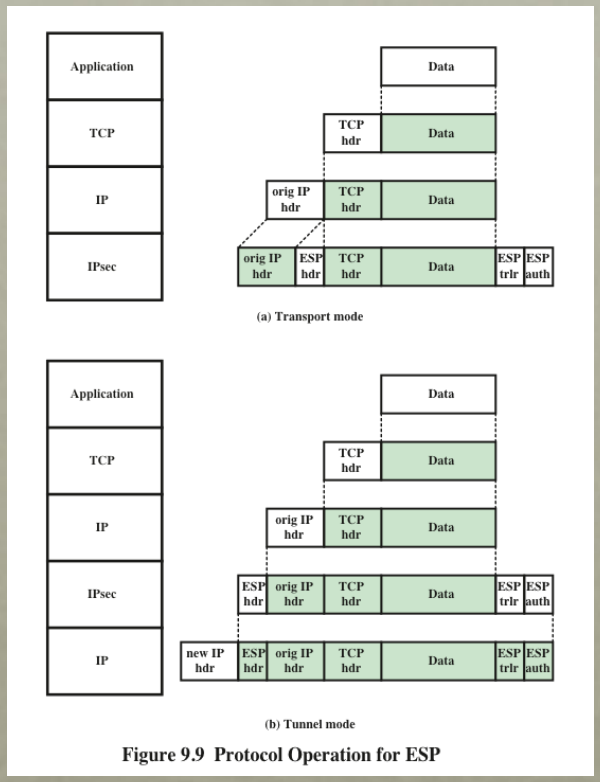
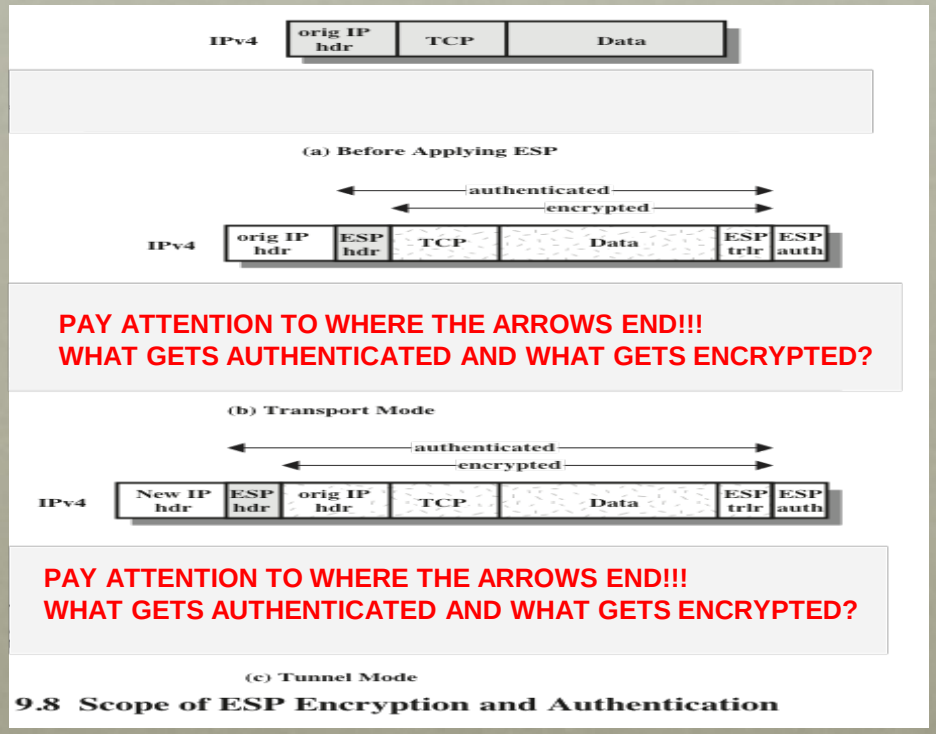


Figure 9.9 Protocol Operation for ESP



9.8 Scope of ESP Encryption and Authentication

Transport mode ESP

- Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected

Tunnel mode ESP

- Authentication applies to the entire IP packet delivered to the outer IP destination address and authentication is performed at that destination
- The entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination

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

ESP + AUTHENTICATION
TRANSPORT MODE VS. TUNNEL MODE

Why do we encrypt the ESP trailer but not the ESP header?

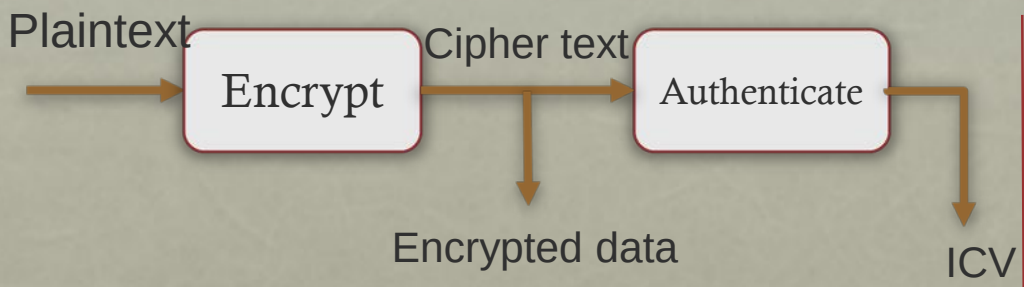
- The **ESP Trailer** includes the padding, which is consider part of the payload
- We cannot encrypt the **ESP Header** since it has the SPI.
  - We need to communicate this SPI to the receiving end such that it can look up its own SAD and grab all needed parameters to decrypt the data including the secret key.
  - If the SPI encrypted, then the receiving end won't be able to look up its own SAD.
  - Moreover, SPI is the agreement serial number that identifies the SAD entry. It is only meaningful to the two communicating parties.
- In transport mode, "Original IP header" is not encrypted
- In tunnel mode, , "New IP header" is not encrypted
- This is to facilitate routing the packet across the network.
- In both modes: outer IP header does NOT get authenticated → this is one key difference when using the bundle mode

BUNDLE SAs

- Using two distinct security associations for encryption and authentication
- Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA.
- In this case, ESP is used without its authentication option.
- Because the inner SA is a transport SA, encryption is applied to the IP payload.
- Two options:
  - Transport Adjacency bundle
  - Transport-Tunnel bundle

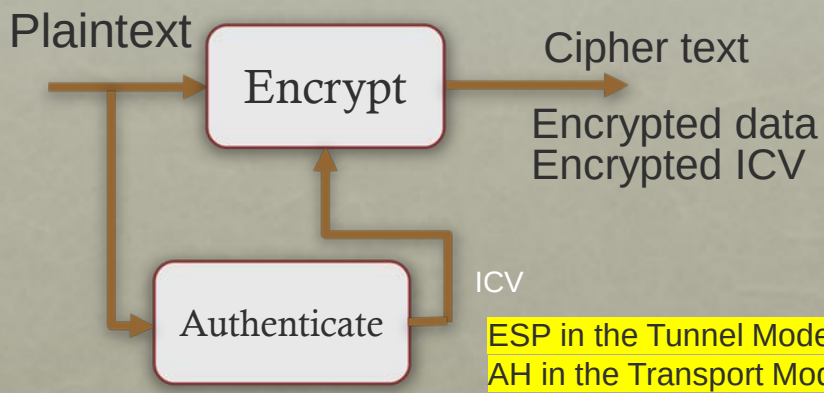
TRANSPORT ADJACENCY VS. TRANSPORT TUNNEL BUNDLE

Transport Adjacency



ESP in the Transport Mode
AH in the Transport Mode

Transport-Tunnel Bundle



ESP in the Tunnel Mode
AH in the Transport Mode

Which one is better?

Preferable when?

- Rapid detection and rejection of bogus packets → ICV is computed on the cipher text → no need to decrypt to authenticate
- Parallel processing of packets: decryption and integrity checking could happen in parallel

Preferable when?

- It may be desirable to store the authentication information with the message at the destination for later use.
- If the Authentication method does not use key in the process, the authenticated data will be encrypted

TRANSPORT ADJACENCY

- Another way to apply authentication after encryption is to use **two bundled transport SAs**, with the inner being an ESP SA and the outer being an AH SA
  - In this case ESP is used without its authentication option
  - Encryption is applied to the IP payload
  - AH is then applied in transport mode
  - **Advantage** of this approach when *compared to ESP + Authentication* is that the authentication covers more fields
  - **Disadvantage** is the overhead of two SAs versus one SA

TRANSPORT-TUNNEL BUNDLE

- The use of authentication prior to encryption might be preferable for several reasons:
  - It is impossible for anyone to intercept the message and alter the authentication data without detection
  - It may be desirable to store the authentication information with the message at the destination for later reference
- One approach is to use 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
    - The result is that the entire authenticated inner packet is encrypted and a new outer IP header is added

BASIC COMBINATION

- The IPsec Architecture document lists four examples of combinations of SAs.
- The lower part of each case in the figure represents the physical connectivity of the elements; the upper part represents logical connectivity via one or more nested SAs.
- Each SA can be either AH or ESP.
- For host-to-host SAs, the mode may be either transport or tunnel; otherwise it must be tunnel mode.

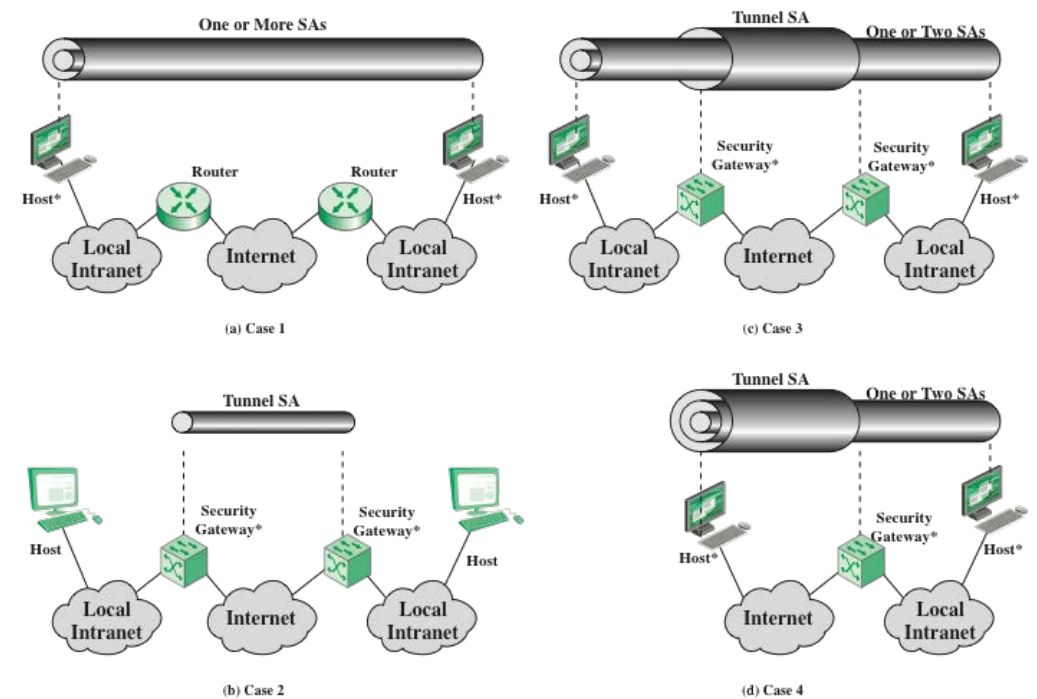
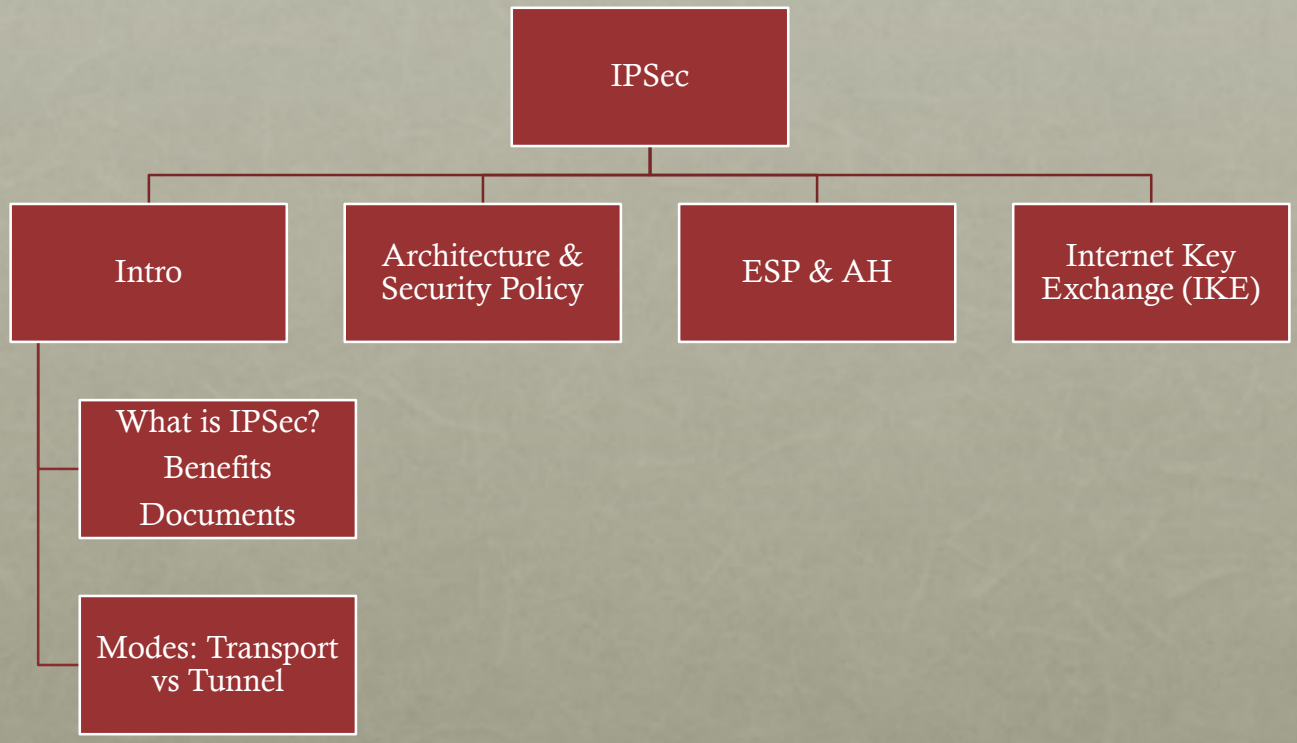


Figure 9.10 Basic Combinations of Security Associations

OUTLINE


IPSec
Intro
Architecture & Security Policy
ESP & AH
Internet Key Exchange (IKE)
What is IPSec?
Benefits
Documents
Modes: Transport vs Tunnel

INTERNET KEY EXCHANGE

- The key management portion of IPsec involves the determination and distribution of secret keys
  - A typical requirement is four keys for communication between two applications
    - Transmit and receive pairs for both integrity and confidentiality

The IPsec Architecture document mandates support for two types of key management:

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

- Enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration

ISAKMP/OAKLEY

- The default automated key management protocol of IPsec
- Consists of:
  - Internet Security Association and Key Management Protocol (ISAKMP) → IKE Phase 1
    - Provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes
    - Consists of a set of message types that enable the use of a variety of key exchange algorithms
  - Oakley Key Determination Protocol → IKE Phase 2
    - A key exchange protocol based on the Diffie-Hellman algorithm but providing added security
    - Generic in that it does not dictate specific formats

Weaknesses of Diffie-Hellman

- It does not provide information about the identities of the parties
- Subject to man-in-the-middle attack
- Computationally intensive
  - Vulnerable to **clogging attack**: an opponent requests a high number of keys. The victim spends considerable computing resources doing useless modular exponentiation rather than real work
- IKE Key determination is designed to retain the advantages of Diffie-Hellman while countering its weaknesses.

FEATURES OF IKE KEY DETERMINATION

- Algorithm is characterized by five important features:

1. It employs a mechanism known as cookies to thwart clogging attacks
2. It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange
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

HOW CLOGGING IS MITIGATED?

- Cookies exchange before engaging in the Diffie-Hellman Key generation
- **The cookie :**
  - Must depend on the specific parties
  - Must not be possible for anyone other than the issuing entity to generate the cookies that will be accepted by that entity.
  - The cookie generation and verification method must be fast. The cookie is not even stored locally.
- **The recommended method is:**
  - Perform fast hashing over:
    - The IP source and destination addresses
    - UDP source and destination ports, and
    - Locally generated secret value
- **How it works?**
  - A receives a request from a legitimate user B to generate a Diffie-Hellman Key
  - Before A gets engaged in the process of the generation of the Key, it generates a cookie and sends it to B.
  - The cookie will be delivered through the network to the legitimate user B
    - If B's IP address was forged by an Attacker C, the cookie will not be delivered to C and B will just ignore the cookie and will not respond to A.
    - If B is indeed the user who initiated the request, B will send the same cookie back to A. A will then verify that this cookie is indeed valid and that he is the creator of the cookie. A can then gets engaged in the key generation process.

Features of IKE key determination

- Why do we use nonces?
  - To mitigate anti-replay attack during IKE key determination phase
- Which authentication techniques are used?
  - Digital certificates
  - Public key encryption
  - Symmetric key encryption

IKEv2 Exchange

Initial Exchange:

- **First Message**: I sends to R **(IKE_SA_INIT),** which contains:
  - offered encryption and message integrity algorithms,
  - Diffie-Hellman public Keys,
  - and nonces.
- **Second Message:** R responds to I with (IKE_SA_INIT),
  - chosen encryption and message integrity algorithms,
  - Diffie-Hellman Keys,
  - nonces, and
  - **Certificate request**

- **NOTE**,
  - by the end of this step, both I and R have created a secret key and all following messages are encrypted, and
  - **ONE SA (IKE SA) FOR CONTROL MESSAGES HAS BEEN ESTABLISHED**
- **Third and Fourth Messages (IKE_AUTH)**:
  - Initiators and responder's identities, certificates (optional), SA parameters are exchanged
  - Validate the identity
- **NOTE**,
  - by the end of these two steps, users have been authenticated, and
  - **ONE SA (IPSEC SA) FOR communication between the peers**

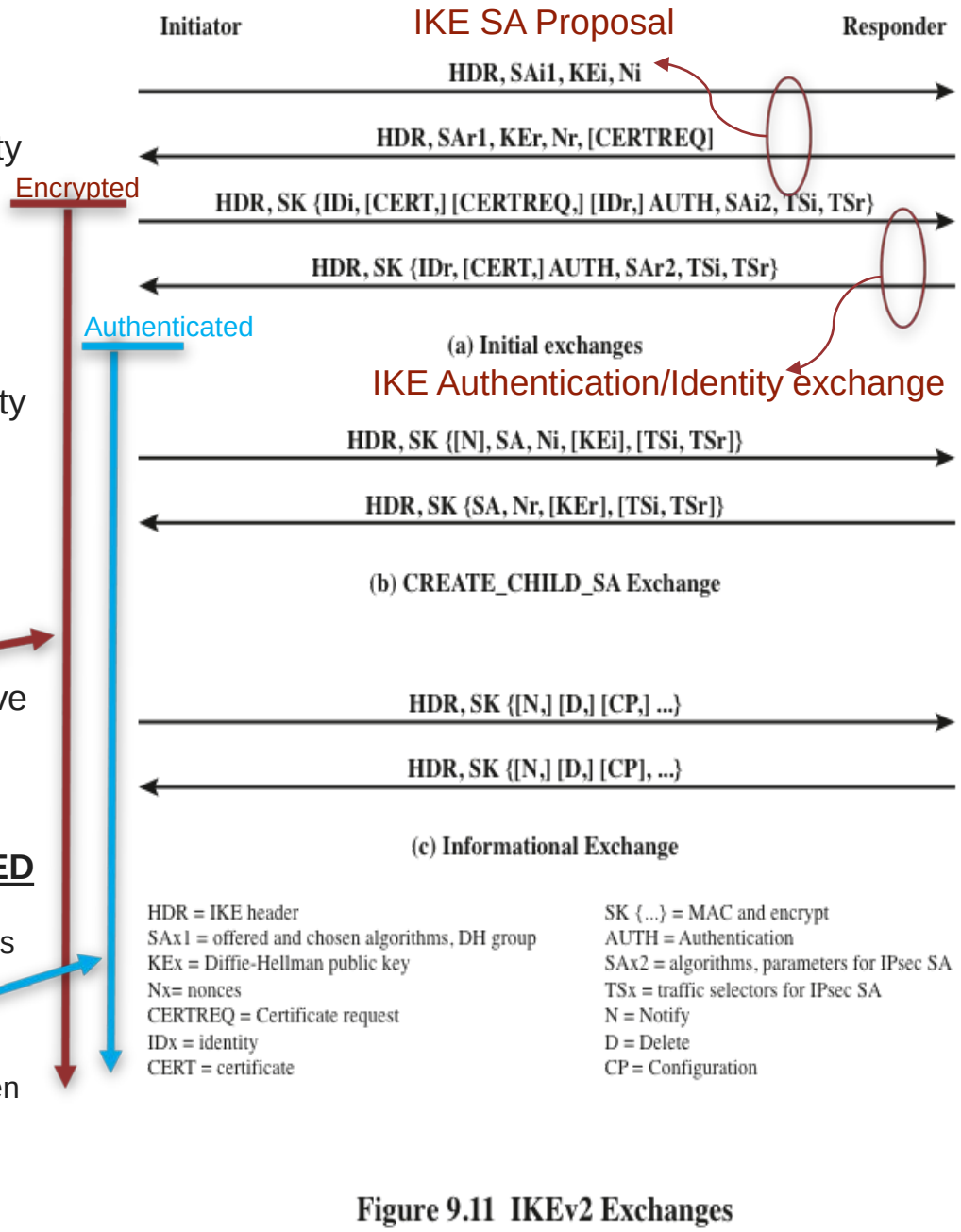


Figure 9.11 IKEv2 Exchanges

IKEv2 Exchange

Create Child SA :

- Used to create new additional child SA to using a new tunnel.
- New Diffie-Hellman values and message authentication parameters are exchanged
- Why do we need to create child SA?
  - Create SAs for ESP and AH
    - That is why you see traffic selector negotiations **AGAIN** in this step
  - We can also use them for:
    - Rekey both IKE SAs → create a new SA and delete the old one
  - And
    - Compatible with IKEv1
- **Informational Exchange:**
  - Maintenance Exchange control information related to deleting the tunnel or change in the configuration or a notification as in the case of detecting a past packet outside the anti-replay window.

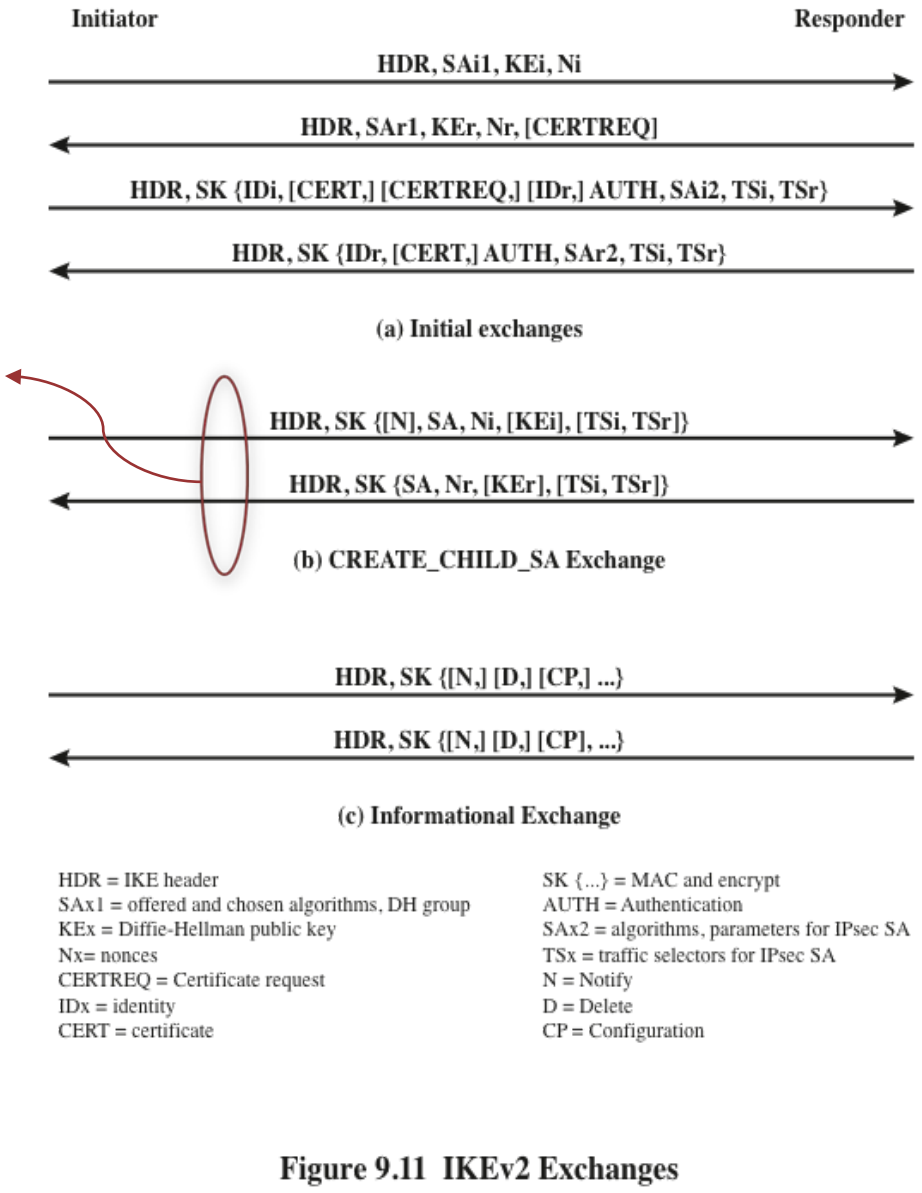
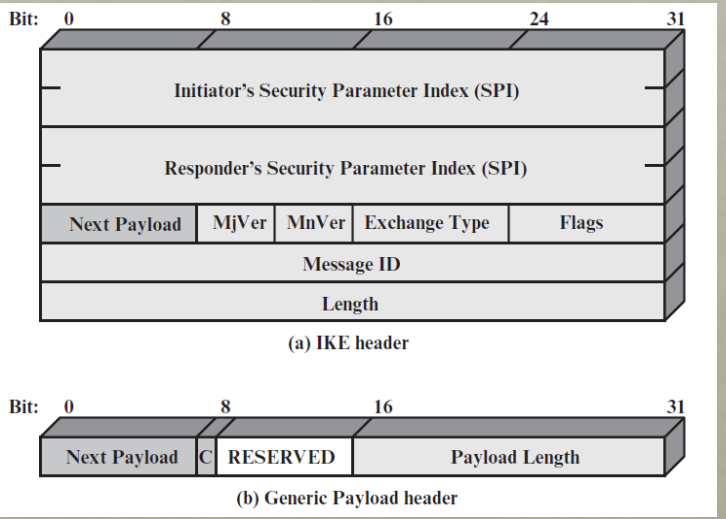


Figure 9.11 IKEv2 Exchanges

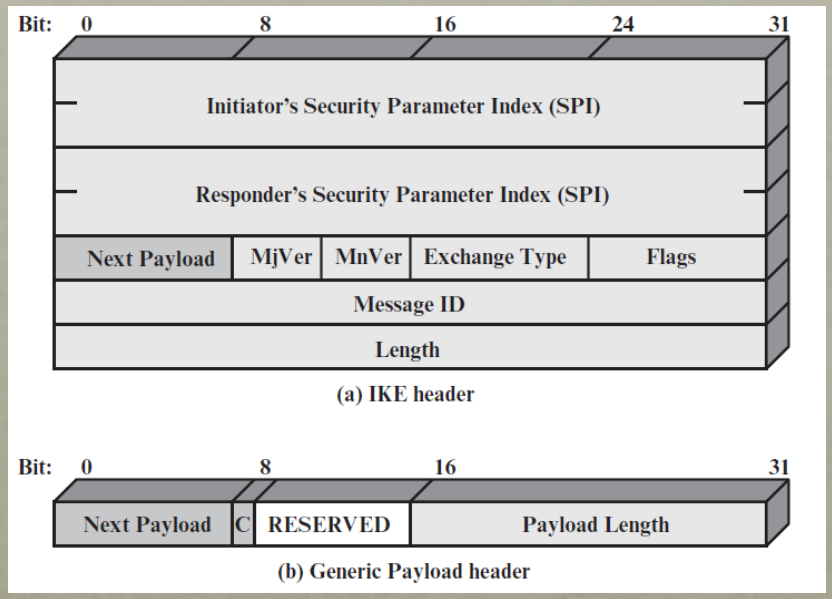
IKE HDR AND PAYLOAD

- IKE message consists of a HDR and a payload
- Initiator SPI: chosen by the initiator
- Responder SPI: chosen by the responder
- Next Payload: Type of the first payload
- Major and minor version
- Exchange type:
  - IKE_SA_INIT, CREATE_CHILD_SA, or INFORMATIONA
- Flags: only 3 flags defined
  - Initiator bit: indicates whether this bit is sent by the SA initiator
  - Version bit: indicates whether the transmitter is capable of using a higher major version number than the one currently indicated.
  - Response bit: indicates whether this is a response to a message containing the same message ID.
- Length: length of the total message (header plus payloads)
- Types of payload: proposal, transforms, attributes, key exchange , identification, certificate, authentication, nonce, notify delete, configure, vendor ID, traffic selector, EAP payload, Encrypted data.



IKE HDR AND PAYLOAD

- IKE payload:
  - Next payload:
    - 0 if this is the last payload
    - Payload length
    - Critical bit:
      - It is set to 0:
        - if the sender wants the recipient to skip this payload if it does not understand the payload type code in the next payload field of the previous payload.
      - It is set to 1
        - if the sender wants the recipient to reject the entire message if it does not understand the payload type code.



SUMMARY

- IP security overview
  - Applications of IPsec
  - Benefits of IPsec
  - Routing applications
  - IPsec documents
  - IPsec services
  - Transport and tunnel modes
- IP security policy
  - Security associations
  - Security association database
  - Security policy database
  - IP traffic processing
- Cryptographic suites
- Encapsulating security payload
  - ESP format
  - Encryption and authentication algorithms
  - Anti-replay service
  - Transport and tunnel modes
- Combining security associations
  - Authentication plus confidentiality
  - Basic combinations of security associations
- Internet key exchange