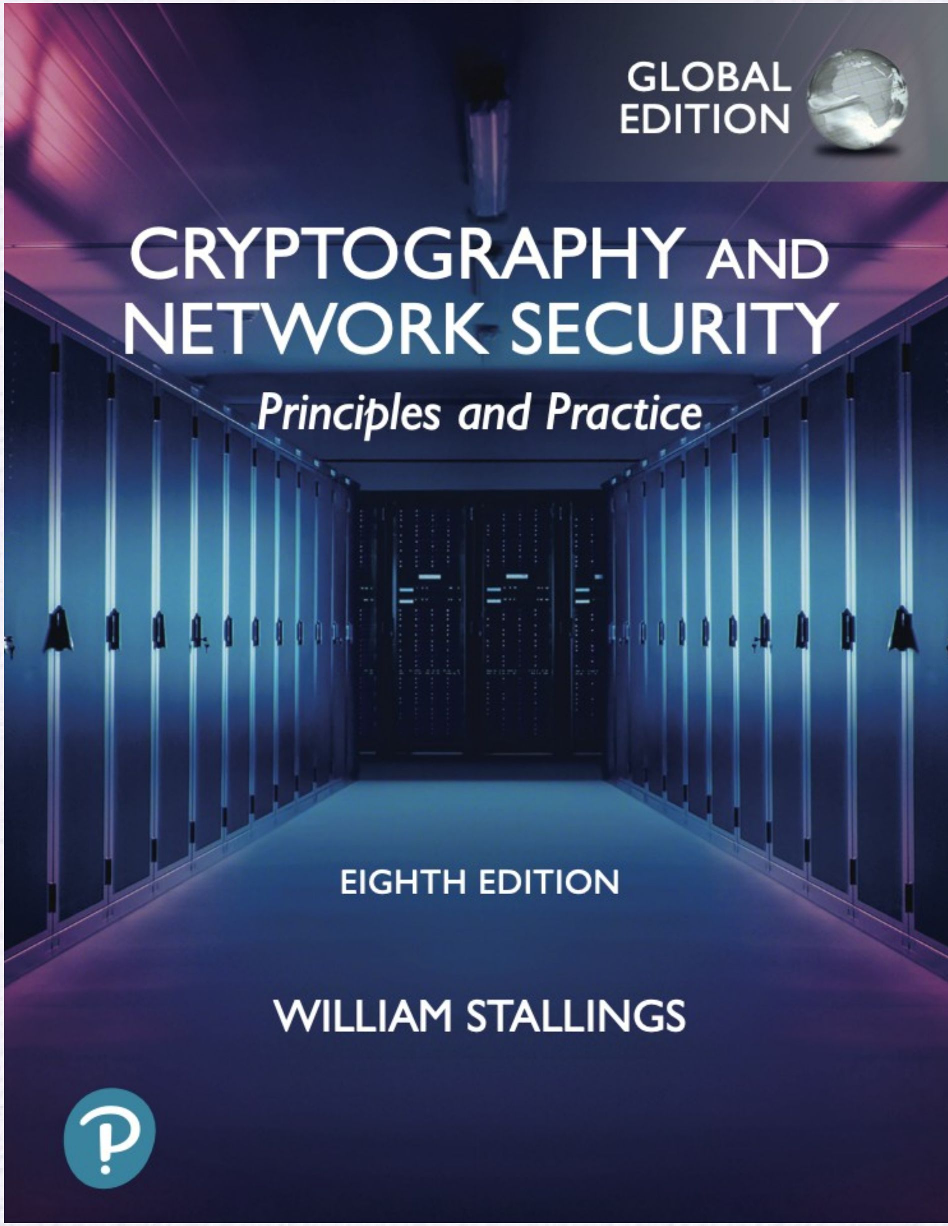
University of Nevada – Reno
Computer Science &
Engineering Department

CS454/654 Reliability and Security of Computing Systems - Fall 2024

Lecture 21

Dr. Batyr Charyyev
bcharyyev.com



CHAPTER 20

IP Security

20.1 IP Security Overview

Applications of IPsec
IPsec Documents
IPsec Services

20.2 IP Security Policy

Security Associations
Security Association Database
Security Policy Database
IP Traffic Processing

20.3 Encapsulating Security Payload

ESP Format
Encryption and Authentication Algorithms
Padding
Anti-Replay Service
Transport and Tunnel Modes

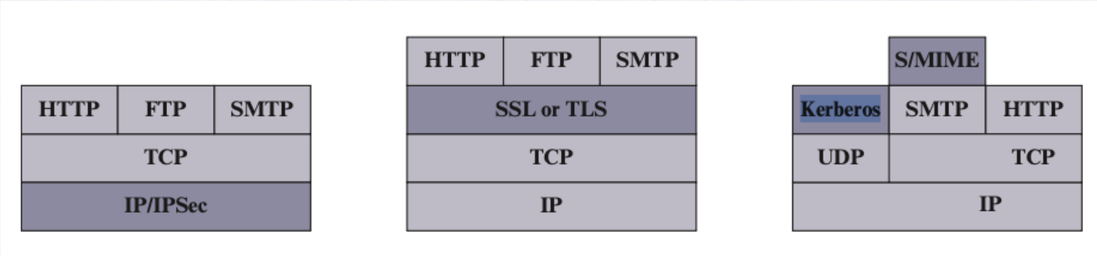
20.4 Combining Security Associations

Authentication Plus Confidentiality
Basic Combinations of Security Associations

20.5 Internet Key Exchange

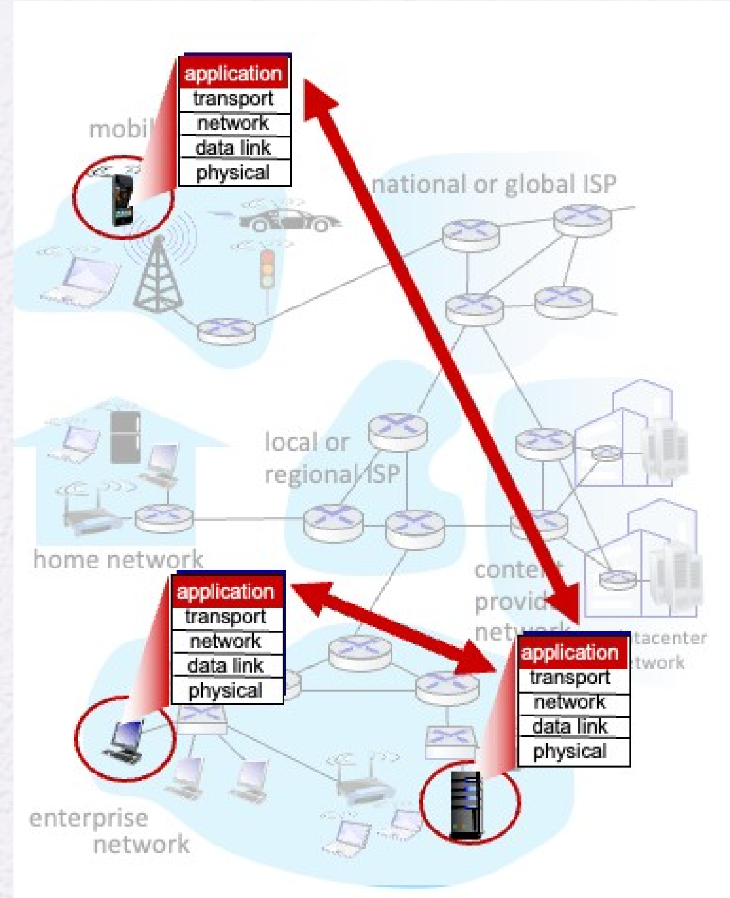
Key Determination Protocol
Header and Payload Formats

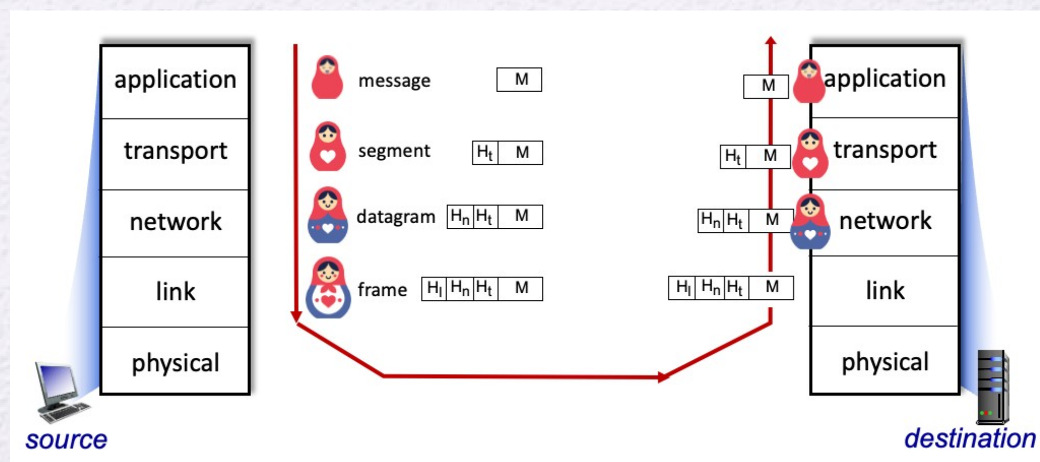
20.6 Key Terms, Review Questions, and Problems



(a) Network level (b) Transport level (c) Application level

TLS: Transport Layer Security
IPSec: IP Security





IPSec

- IPsec provides security services at the IP layer.

- IPsec specification is scattered across dozens of RFCs.
  - **Architecture**: https://datatracker.ietf.org/doc/html/rfc4301
  - **Authentication Header:** https://datatracker.ietf.org/doc/html/rfc4302
  - **Encapsulating Security Payload:** https://datatracker.ietf.org/doc/html/rfc4303
  - **Internet Key Exchange:** https://datatracker.ietf.org/doc/html/rfc7296

- IPsec is not used by default. It is typically utilized when you configure and use a VPN service that relies on IPsec for secure communication.
  - Secure branch office connectivity over the Internet

- Security Associations
- Security Policy Database
- Security Association Database

Security Associations (SA)

- It is like logical connection between sender and receiver.

- Unidirectional, for secure connection in both direction, 2 separate SAs created.

- Identified with 3 parameters.
    - **Security Parameters Index (SPI):** 32-bit identifier.
    - **IP destination address**.
    - **Security Protocol Identifier**: indicates whether association is Authentication Header (AH) or Encapsulating Security Payload (ESP) protocol.
        - AH provides authentication.
        - ESP provides both encryption and authentication.

Security Associations Database (SAD)

- The SAD contains entries for each active SA (Security Association).
  - Each entry holds all the parameters required to define/process the associated SA.

- Key parameters in each SAD entry
  - **Security Parameter Index (SPI):** 32-bit unique identifier for each SA.
  - **Sequence Number Counter (SNC):** 32-bit value, ensures ordered delivery.
  - **Sequence Counter Overflow:** A flag indicating whether overflow of the SNC should generate an auditable event and prevent further transmission of packets on this SA.
  - **Anti-Replay Window:** A mechanism to detect and reject replayed packets.
  - **AH Information**: Details of the Authentication Header (AH) -> authentication algorithm, key, lifetime of key.
  - **ESP Information:** Details of the Encapsulating Security Payload (ESP) -> encryption algorithm, keys, lifetime of key.
  - **Lifetime of the SA:** Defines when the SA expires.
  - **IPsec Protocol Mode**
    - **Tunnel mode:** Encrypts the entire IP packet (used for VPNs)
    - **Transport mode:** Encrypts only the payload of the IP packet.
  - **Path MTU (Maximum Transmission Unit):** Tracks the largest packet size that can be sent without fragmentation.

Security Policy Database (SPD)

- SPD defines how to handle incoming/outgoing IP traffic in relation to security.
  - **Protected** using IPsec (AH or ESP processing).
  - **Bypassed** without IPsec protection.
  - **Discarded** if it doesn't meet security requirements.

- The SPD contains rules (entries) that match subsets of IP traffic to specific SAs or specify that the traffic bypasses IPsec.
- **Selectors** are filters used to match packets to SPD entries.
  - Remote IP Address
  - Local IP Address
  - Next Layer Protocol
  - Local and Remote Ports

Table 20.1 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

Relation: SA – SAD – SPD

- SPD → Determines Traffic Treatment
  - Each packet is checked against the SPD, based on packet's source/destination IPs, ports, and protocols to determine:
    - If it needs IPsec protection.
    - Which SA (if any) it should use.

- Once the SPD determines that traffic requires IPsec, it points to an existing SA in the SAD or triggers the creation of a new SA.

- The SAD provides the operational details for the SA referenced by the SPD.

- SAD, SPD are created and stored locally on your device when you setup your device (install VPN) to use IPSec connection.
  - strongswan -> ipsec
  - https://wiki.strongswan.org/projects/strongswan/wiki/ipseccommand

IP Traffic Processing - Outbound Packets

A block of data from a higher layer (TCP/UDP), is passed down to the IP layer and an IP packet is formed, consisting of an IP header and an IP body. Then the following steps occur:

1. IPsec searches the SPD for a match to this packet.
2. If no match is found, then the packet is discarded and an error message is generated.
3. If a match is found, further processing is determined by the first matching entry in the SPD. If the policy for this pack discarded. If the policy is BYPASS, then th packet is forwarded to the network for tra
4. If the policy is PROTECT, then a search is made of the SAD for a matching entry. If no entry is found, then IKE (Internet Key Exchange) is invoked to create an SA with the appropriate keys and an entry is made in the SA.
5. The matching entry in the SAD determines the processing for this packet. Either encryption, authentication, or both can be performed, and either transport or tunnel mode can be used. The packet is

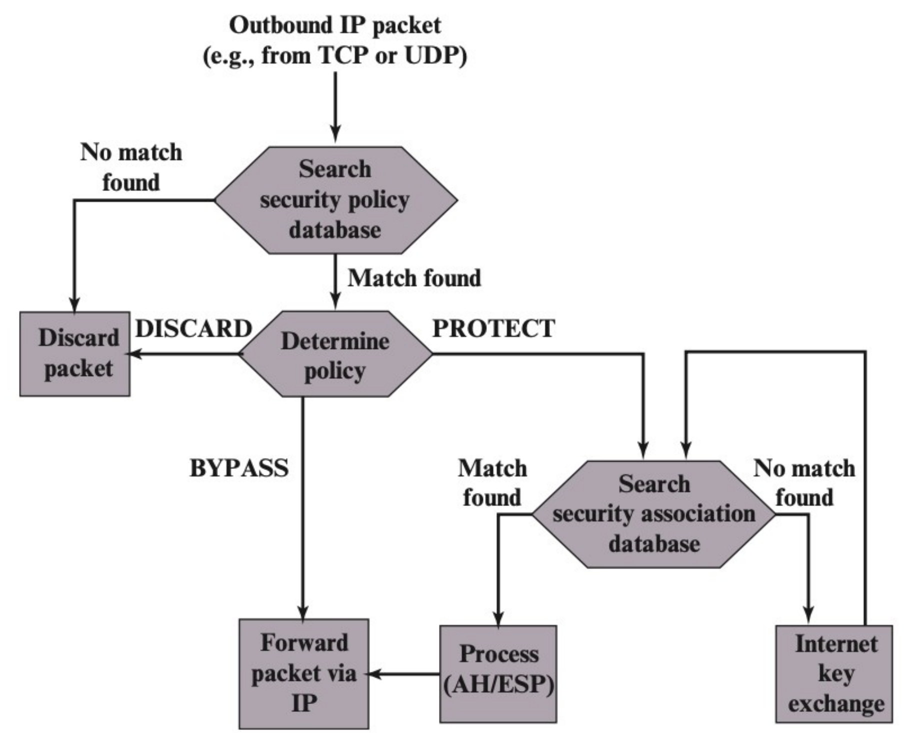


Figure 20.2 Processing Model for Outbound Packets

IP Traffic Processing - Inbound Packets

An incoming IP packet triggers the IPsec processing. The following steps occur:

1. IPsec determines whether this is an unsecured IP packet or one that has ESP or AH headers/trailers, by examining the IP Protocol field (IPv4) or Next Header field (IPv6).

2. If the packet is unsecured, IPsec searches the SPD for a match to this packet. If the first matching entry has a policy of BYPASS, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP. If the first matching entry has a policy of PROTECT or DISCARD, or if there is no matching entry, the packet is discarded

3. For a secured packet, IPsec searches the SAD. If no match is found, the packet is discarded. Otherwise, IPsec applies the appropriate ESP or AH processing. Then, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP.

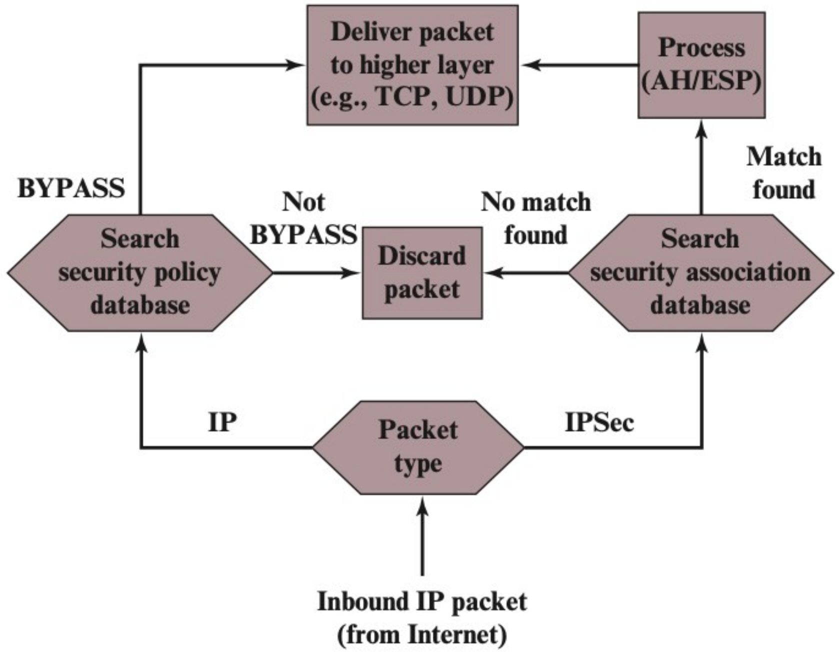


Figure 20.3 Processing Model for Inbound Packets

Security Association (SA)
Security Associations Database (SAD)
Security Policy Database (SPD)
SA – SAD – SPD (Relation)
IP Traffic processing Incoming/Outgoing

Encapsulating Security Payload (ESP)
Transport Mode
Tunnel Mode
Authentication Header (AH) (in comparison to ESP)

Internet Key Exchange

Encapsulating Security Payload (ESP)

- ESP can be used to provide confidentiality, data origin authentication, integrity, an anti-replay service.
- The set of services provided depends on options selected at the time of Security Association (SA) establishment

ESP packet format

- **Security Parameters Index** (32 bits)
- **Sequence Number** (32 bits)
- **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)
- **Pad Length** (8 bits)
- **Next Header** (8 bits): Type of data contained in the payload (TCP, IP)
- **Integrity Check Value** (variable-multiple of 32-bits): computed over the ESP packet minus the

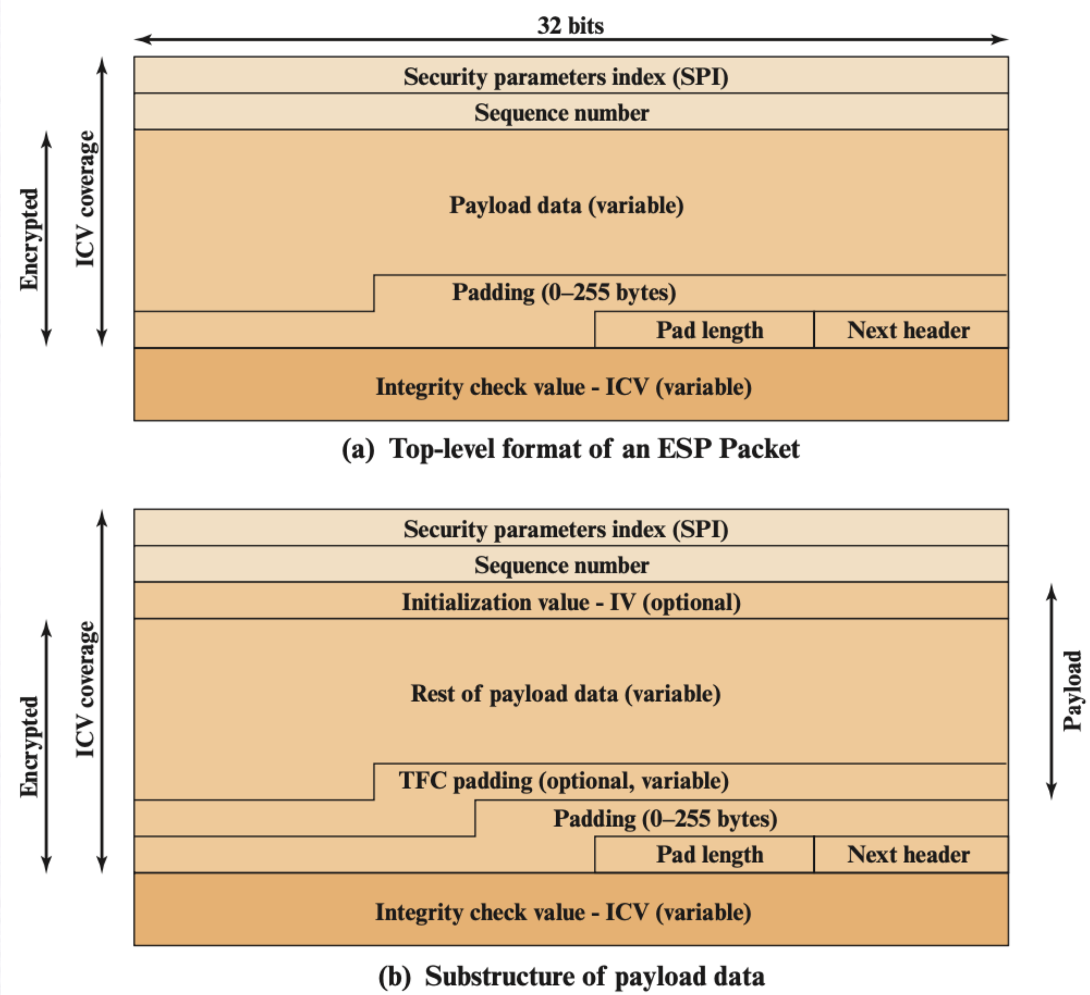


Figure 20.4 ESP Packet Format

Encapsulating Security Payload (ESP)

ESP packet format – additional fields

- Two additional fields may be present in the payload (Figure 20.4b).
- An initialization value (IV), or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP.

- If tunnel mode is being used, then the IPsec implementation may add traffic flow confidentiality (TFC).

- Initialized Vector (IV) is not encrypted.
- ICV is calculated after encryption.
  - Enables quickly reject malicious data by first checking the integrity with ICV and if it is pass then decrypting it. Thus IV is not encrypted.

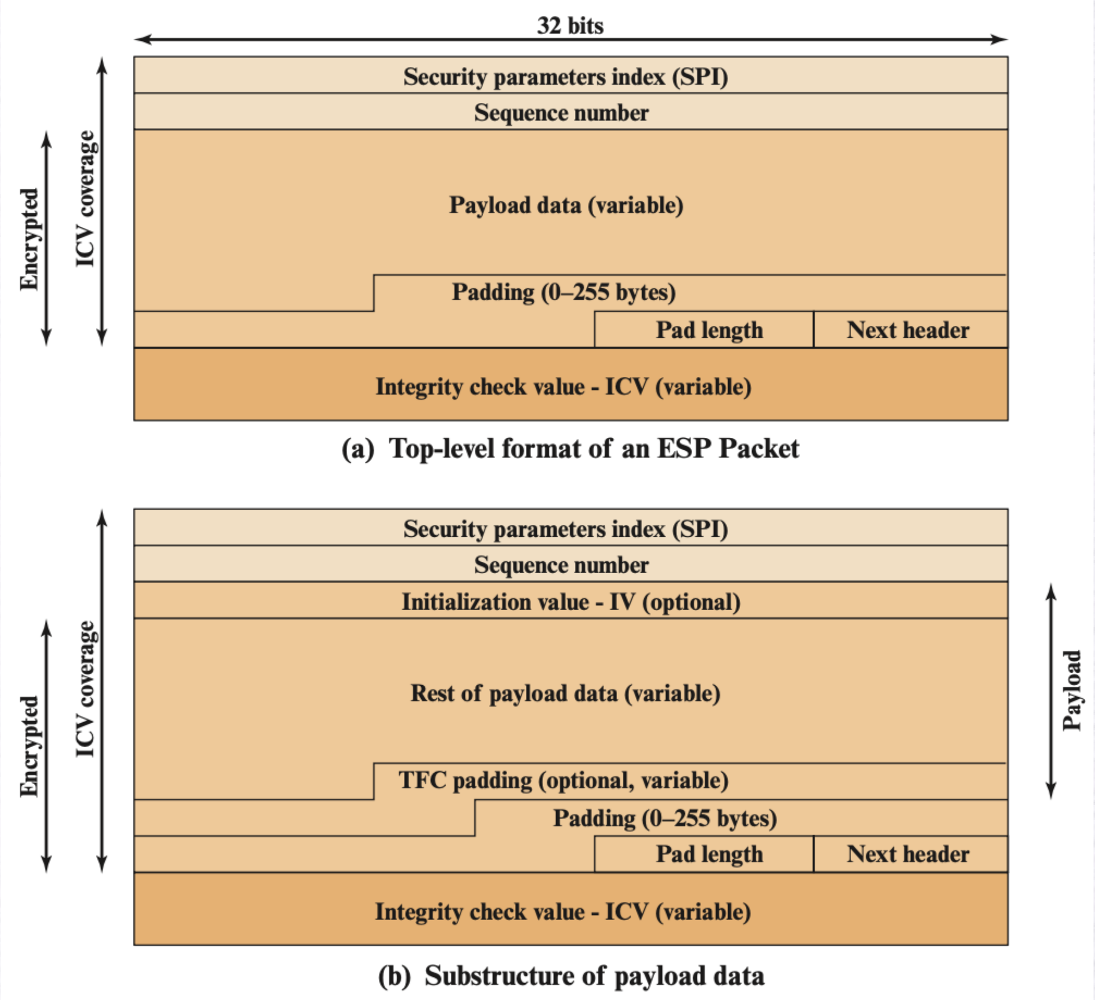


Figure 20.4 ESP Packet Format

- Padding and Pad length to

Transport and Tunnel Modes

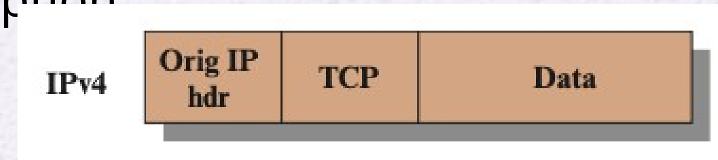
- Both AH and ESP support two modes of use: transport and tunnel mode.

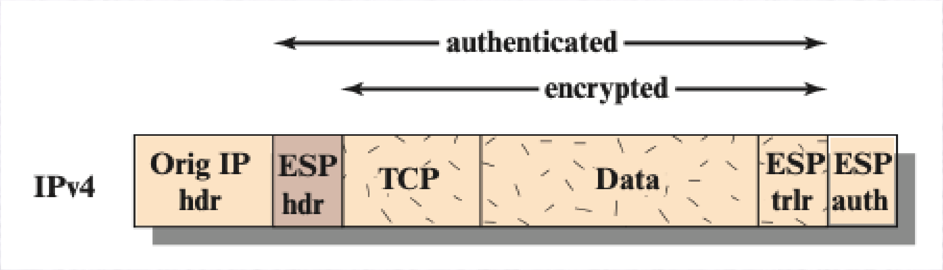
Transport Mode

- Transport mode provides protection primarily for upper-layer protocols (TCP, UDP, ICMP). That is, transport mode protection extends to the payload of an IP packet.

In the context of ESP - provides both encryption and authentication.

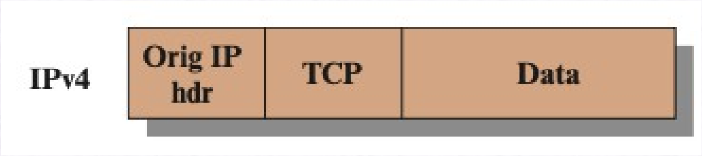
- **ESP header** is inserted right before upper layer protocol header.
- **ESP trailer** (Padding, Pad length, Next header fields) is placed after IP packet.
- If authentication is selected, the ESP Authentication Data field is added after the ESP trailer.
- Coverage - authentication and encryption.
- Notice that Origin IP header is not encrypted thus it enables routing the data to final destination.
- Once data is sent to receiver, based on SA, receiver checks authentication with ESP auth, and then decrypts the data.

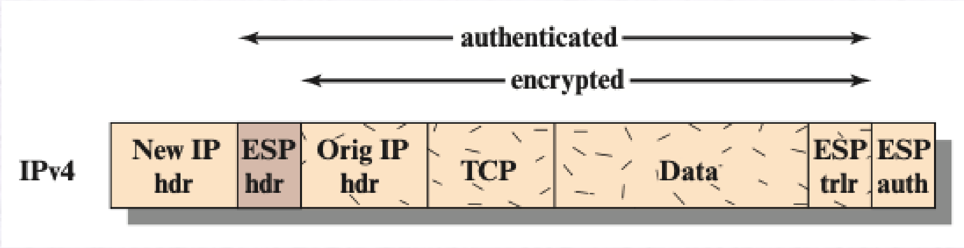




Tunnel Modes

- Tunnel mode provides protection to the entire IP packet.
- No routers along the way are able to examine the inner IP header.
- With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec. The SAs set up by the IPsec software in the firewall or secure router at the boundary of the local network.





Tunnel Modes

1. Initial Packet Generation: Host A creates an IP packet with the destination set to Host B.

- The packet originates from Host A and is sent toward Host B via the network.

2. Processing at the Firewall: The packet reaches a firewall or secure router at the boundary of Host A's network.

- The firewall evaluates whether the packet requires IPsec protection.

3. IPsec Encapsulation: If IPsec is needed, the original packet is encapsulated in a new IP packet.

- Outer IP header: Contains the firewall's IP as the source and the destination firewall's IP as the destination.
- The original packet is encrypted and encapsulated inside.

4. Routing to the Destination Firewall:

- Routing based on outer (firewall) IP

5. Decapsulation at Destination Firewall:

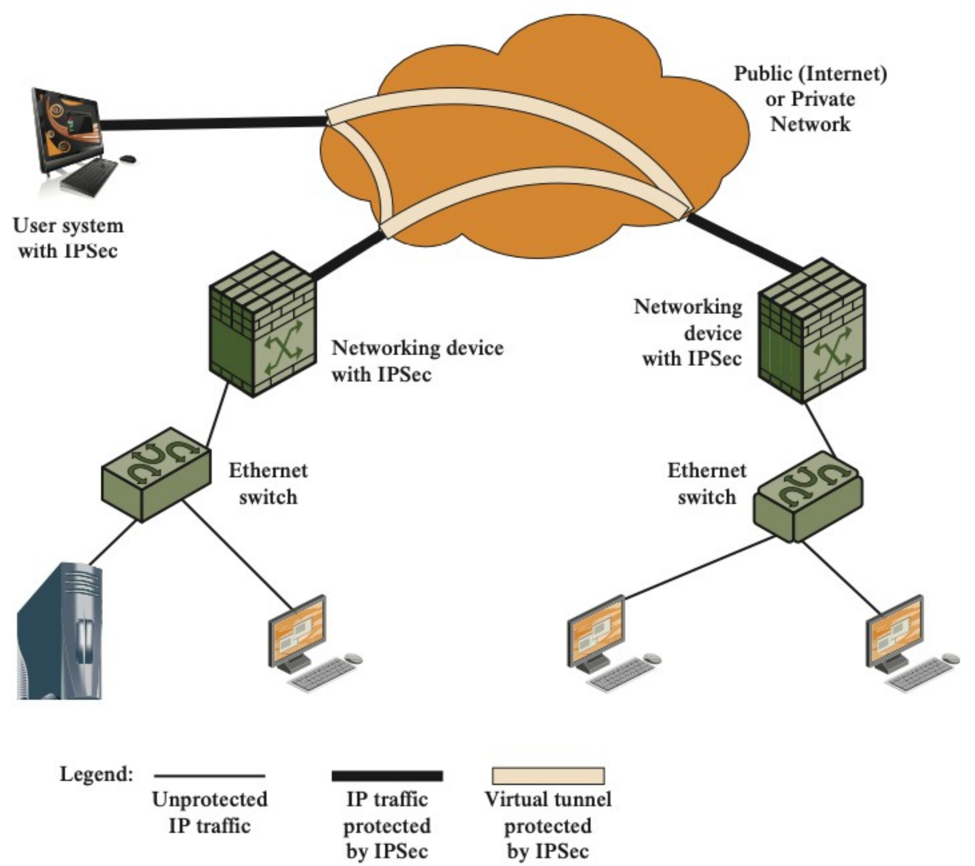
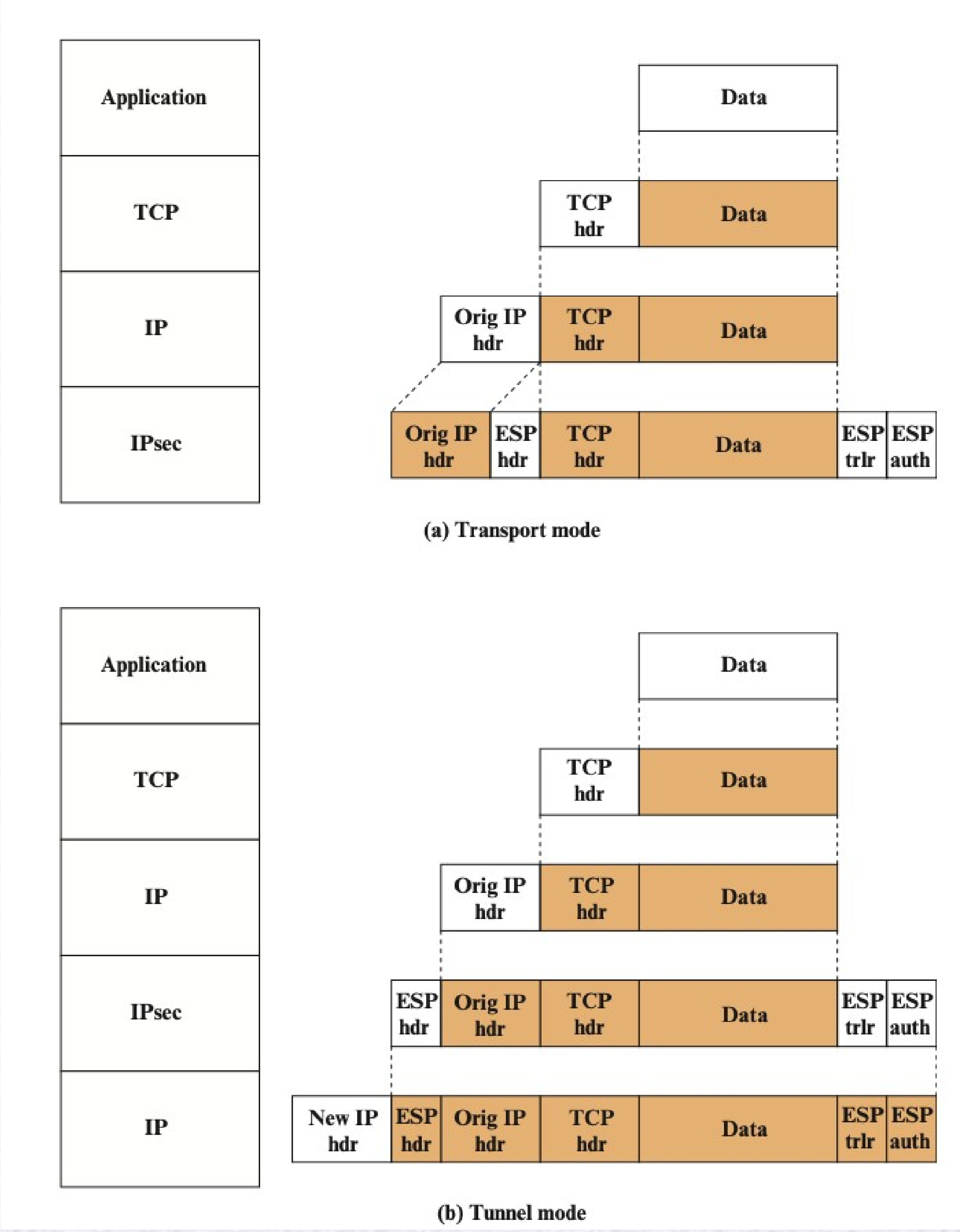


Figure 20.8 Example of Virtual Private Network Implemented with IPsec Tunnel Mode

Transport mode and Tunnel mode comparison

Transport Mode
- Protects connections directly between two hosts (e.g., A and B).
- The original packet header is not encrypted, but the payload is.
- Suitable for scenarios where both hosts support IPsec.

Tunnel Mode
- Protects traffic between security gateways (firewalls) or between a host and a security gateway.
- Entire original packet (header + payload) is encrypted and encapsulated.
- Better for securing networks, as it:
  - Reduces the encryption burden on internal hosts.
  - Simplifies key management by reducing the number of encryption keys.
  - Prevents external traffic



Authentication Header (AH) (in comparison to ESP)

- **AH** is primarily used for integrity, authentication, and anti-replay protection. It does not provide encryption or confidentiality.
- **ESP** provides confidentiality (encryption), integrity, authentication, and anti-replay protection.

AH Transport mode

Original IP Header	AH Header	Payload (Data)

AH Tunnel mode

Outer IP Header	AH Header	Original IP Header	Payload (Data)

ESP Transport mode

~~Outer IP Header~~	ESP Header	Encrypted Payload (Data)	ESP Trailer	ESP Authentication

Original IP Header

ESP Tunnel mode

Outer IP Header	ESP Header	Encrypted Original IP Header + Payload	ESP Trailer	ESP Authentication

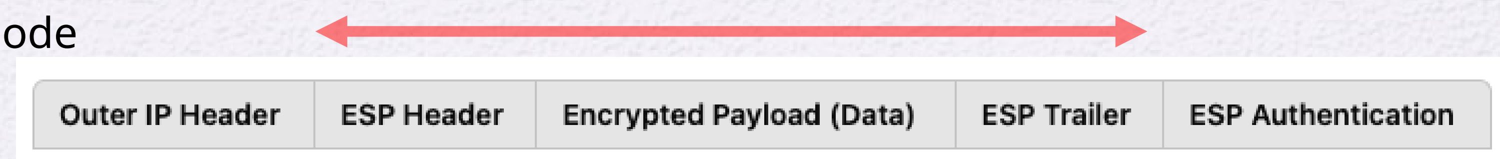
Authentication Header (AH) (in comparison to ESP)

- In terms of **Integrity coverage**
- The authentication code is stored in AH Header for both AH Transport and Tunnel modes

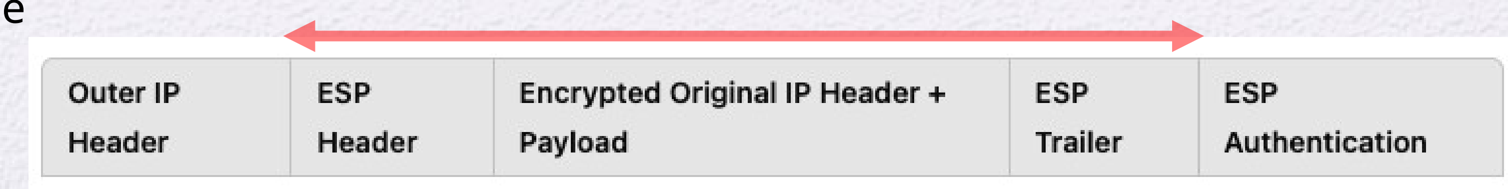
AH Transport mode

AH Tunnel mode

ESP Transport mode



ESP Tunnel mode



Security Association (SA)
Security Associations Database (SAD)
Security Policy Database (SPD)
SA – SAD – SPD (Relation)
IP Traffic processing Incoming/Outgoing

Encapsulating Security Payload (ESP)
Transport Mode
Tunnel Mode
Authentication Header (AH) (in comparison to ESP)

Internet Key Exchange

Internet Key Exchange (IKE)

- Requirement is determining and distributing keys.
- Four keys are required for secure communication – Similar to TLS
  - 2 keys for encryption (sender/receiver)
  - 2 keys for authentication (sender/receiver)

- 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**: 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.
- Uses Diffie–Hellman based approach

Three message types

1. Initial Exchange
2. CREATE_CHILD_SA Exchange
3. Informational Exchange

Data format: Header and Payload

Internet Key Exchange (IKE)

1. **Initial Exchange**

1.1 Negotiating Parameters and Generating Key Material

- Both peers exchange their supported cryptographic algorithms (e.g., encryption, authentication) and agree on a common set.
- Nonces: Random values exchanged to ensure freshness and mitigate replay attacks.
- Diffie–Hellman Values: Exchanged to generate a shared secret, which is used for deriving key material.
- The result of this exchange is the creation of the IKE SA, which protects further communication.

1.2 Authentication and Establishing the First IPsec SA

- Both peers authenticate each other using predefined methods, such as digital signatures, or public-key certificates.
- The authenticated keys derived from the Diffie–Hellman exchange are used to encrypt and authenticate the messages.
- The first IPsec SA is created and stored in the Security Association Database (SADB), allowing secure non-IKE communication (e.g., protecting ordinary data traffic).

Internet Key Exchange (IKE)

1. **Initial Exchange**
2. **CREATE_CHILD_SA Exchange**

- Used when additional IPsec SAs are needed for protecting new traffic flows.
- Each IPsec SA is negotiated independently and added to the Security Association Database (SADB).
- Used to replace an existing SA that is nearing expiration.

Process

1. Initiator Sends CREATE_CHILD_SA Request: Specifies the desired cryptographic algorithms, and other SA parameters.

2. Responder Processes the Request: Selects parameters from the initiator's proposal.

3. Responder Sends CREATE_CHILD_SA Response: Confirms the creation the SA with agreed parameters.

4. SA is Added to the SADB: The newly created SA is stored in the Security Association Database (SADB) for use in protecting traffic.

Internet Key Exchange (IKE)

1. **Initial Exchange**
2. **CREATE_CHILD_SA Exchange**
3. **Informational Exchange**

- Exchange management information, error messages, and notifications.
  - Examples include reporting errors, responding to liveness checks, or updating configuration details.

- Does not create new SAs or modify existing ones.

Internet Key Exchange (IKE)

IKE Header Format

- **Initiator SPI (64 bits):** A unique identifier chosen by the initiator for the SA.
- **Responder SPI (64 bits):** A unique identifier chosen by the responder for the SA.
- **Next Payload (8 bits):** Indicates the type of the first payload in the message. 0 for no more payload.
- **Major and Minor Version (4 bits each):** Specify the version of the IKE protocol in use.
- **Exchange Type (8 bits):** Defines the type of exchange, few examples shown below.
  - Establish SA
  - Information exchange such as error
  - Establish Key parameters
- **Flags (8 bits):** initiator, response, version bits
- **Message ID (32 bits):** used for retransmission control.
  - Each request in an IKE exchange is assigned a unique Message ID. The responder includes the same Message ID in its response to indicate which request it is replying to.
- **Length (32 bits):** Total length of the IKE message, including the header and all payloads.

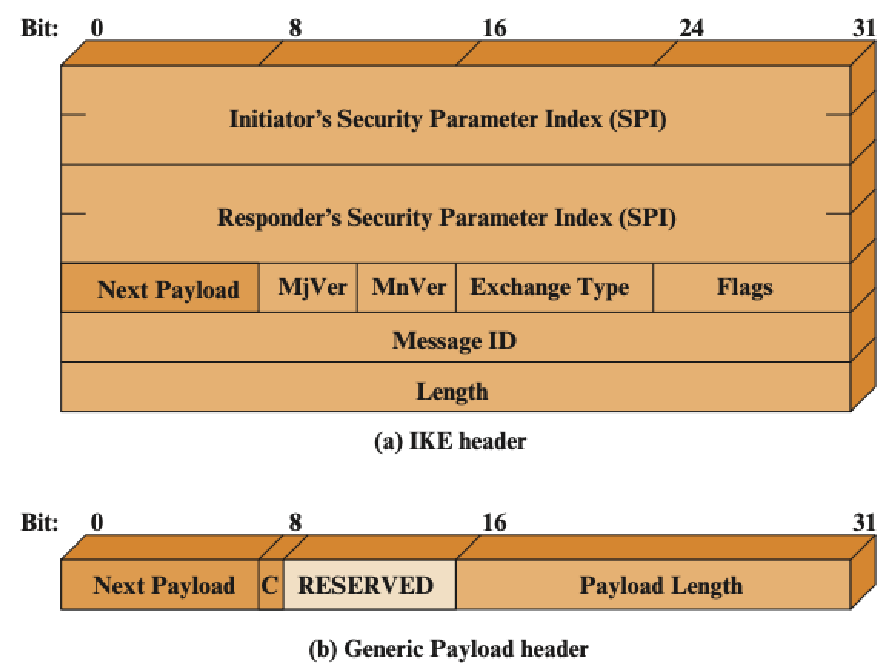


Figure 20.12 IKE Formats

Internet Key Exchange (IKE)

IKE Payload Format

- **Next Payload (8 bits):** Indicates the type of the next payload in the message. 0 for no more payload.
- **Critical bit (1 bit):** has it is own use cases (custom logging, or new security feature)
  - If set to 1, the recipient must reject the message if the payload type is unsupported.
  - If set to 0, the recipient can skip the payload if unsupported.
- **Payload Length:** Length of the payload in bytes, including the generic header.
- **Reserved (8 bits):** For potential future features.

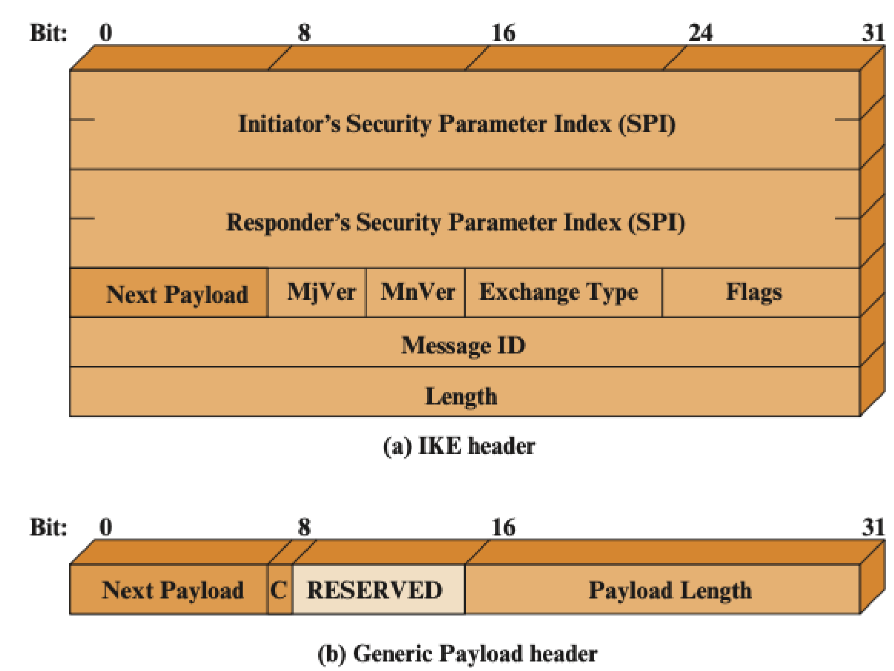


Figure 20.12 IKE Formats

Internet Key Exchange (IKE)

IKE Payload Format

- **Next Payload (8 bits):** Indicates the type of the next payload in the message. 0 for no more payload.
- **Payload Length:** Length of the payload in bytes, including the generic header.

- The actual data for a payload (e.g., nonce in the Nonce Payload) is stored immediately after the generic payload header.

Table 20.3 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

Security Association (SA)
Security Associations Database (SAD)
Security Policy Database (SPD)
SA – SAD – SPD (Relation)
IP Traffic processing Incoming/Outgoing

Encapsulating Security Payload (ESP)
Transport Mode
Tunnel Mode
Authentication Header (AH) (in comparison to ESP)

Internet Key Exchange

Couple other topics

Anti-Replay Service

- The Sequence Number field is designed to stop such attacks.
- When a new SA is established, the sender initializes a sequence number counter to 0. Incremented every time packet is sent.
- If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past 2^{32} - 1 back to zero. Otherwise, there would be multiple valid packets with the same sequence number. If the limit of 2^{32} - 1 is reached, the sender should terminate this SA and negotiate a new SA with a new key.
- We have window of size 64. We we only consider sequence numbers in the range of th

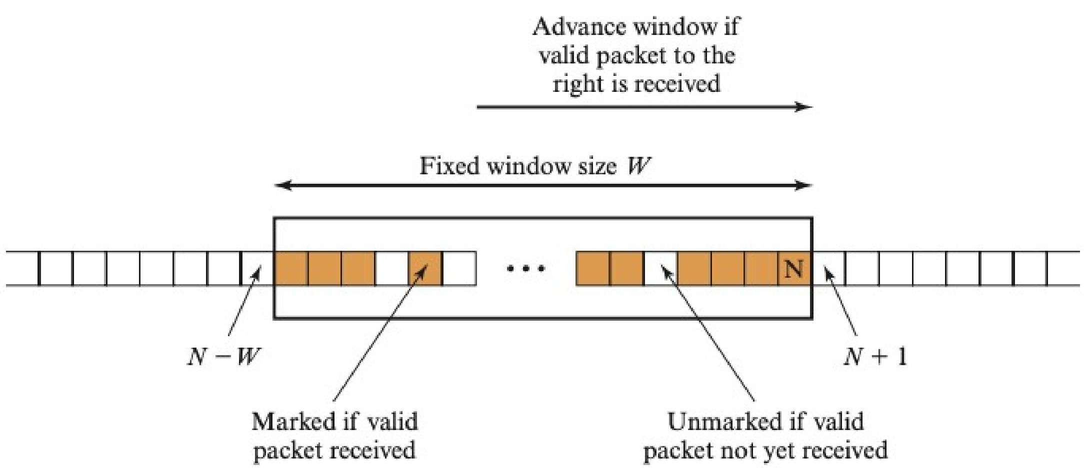


Figure 20.5 Anti-replay Mechanism

Anti-Replay Service

Sequence number processing rule

1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.

2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.

3. If the received packet is to the left of the window or if authentication fails, the packet is discarded; this is an auditable event – basically logged for security analysis.

What is the issue?

- What if we keep getting packets to the right of window?
- Window grows indefinitely?
- **Or do we keep discard sequence numbers to the left of window and keep moving window to left?**

- **Reliability is not responsibility of IPSec**

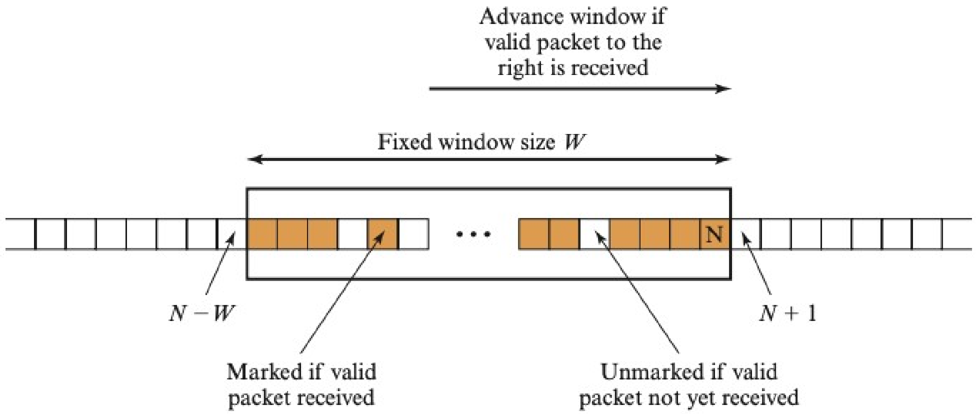


Figure 20.5 Anti-replay Mechanism

Combinations of Security Associations

Security association bundle refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPsec services.

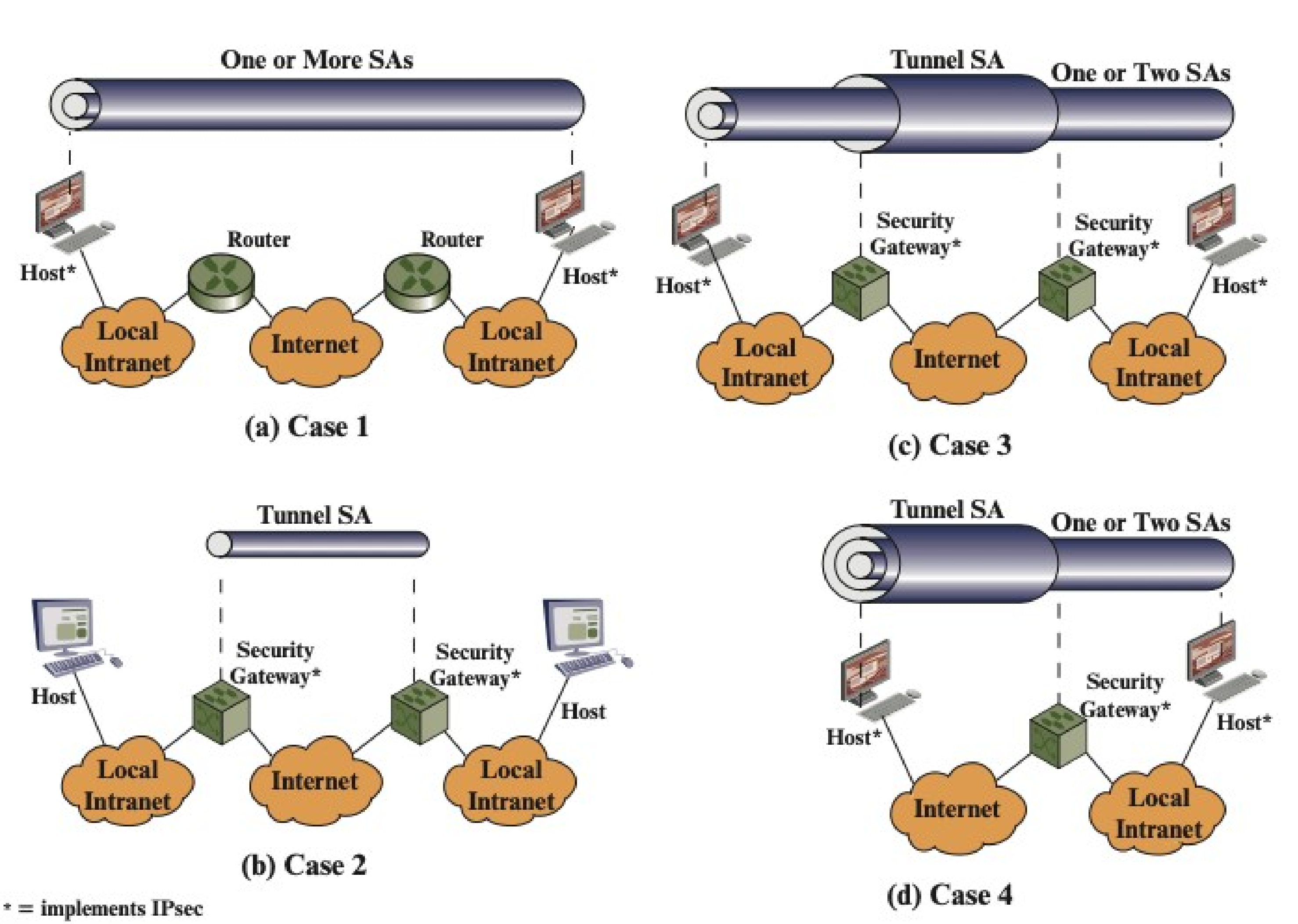


Figure 20.10 Basic Combinations of Security Associations