Information Security

CS3002

Lecture 21

11th November 2024

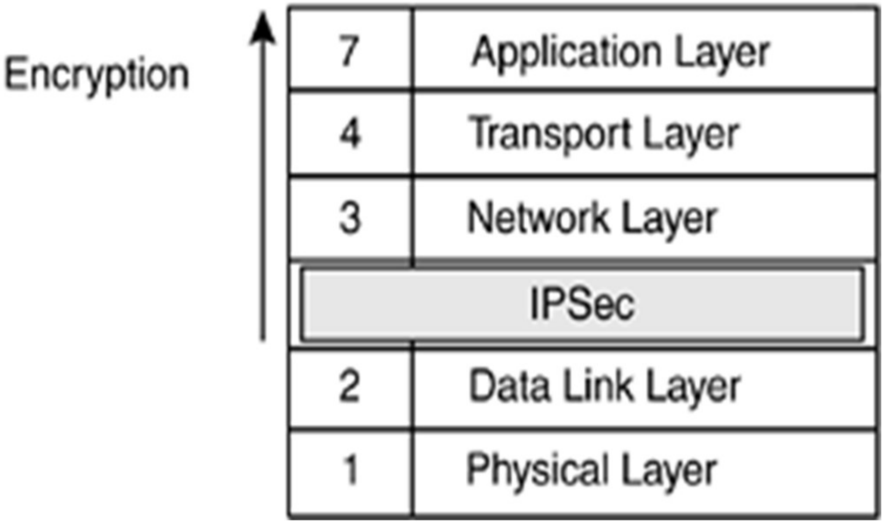
Dr. Rana Asif Rehman

Email: r.asif@lhr.nu.edu.pk

IP Security (IPsec)

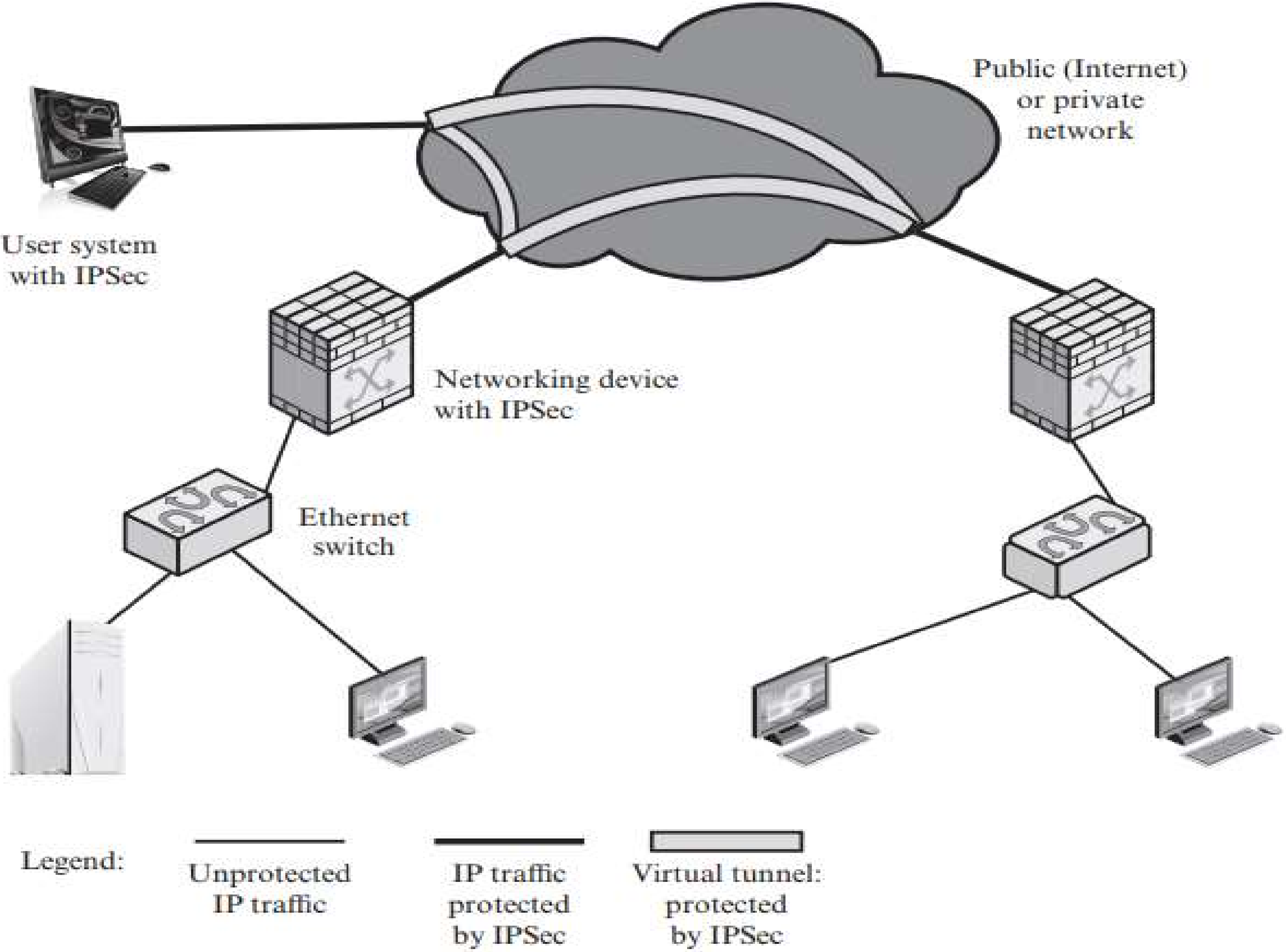
IPsec

- Philosophy of IPsec: implementing security within the operating systems automatically causes applications to be protected without changing applications
- IPsec is within the OS. OS changes, applications and API to TCP don't.



7	Application Layer
4	Transport Layer
3	Network Layer
IPSec	
2	Data Link Layer
1	Physical Layer

An IPsec VPN Scenario



IPsec

- Security at layer 3
- IPsec ensures:
  - Confidentiality, integrity, and authenticity
- Allows secure communication over the Internet
- Independent from the application or higher protocols
- Network-layer security instead of application-layer security
  - Compatible with schemes providing security at the application layer
    - Can be applied simultaneously

IPsec

- Further advantages:
  - Can be applied to all network traffic
  - Routers/firewalls vendors can implement it (Can't implement SSL)
  - Transparent to the applications
  - Transparent to the users
- Limitations:
  - Limited to IP Addresses
  - Has no concept of application users

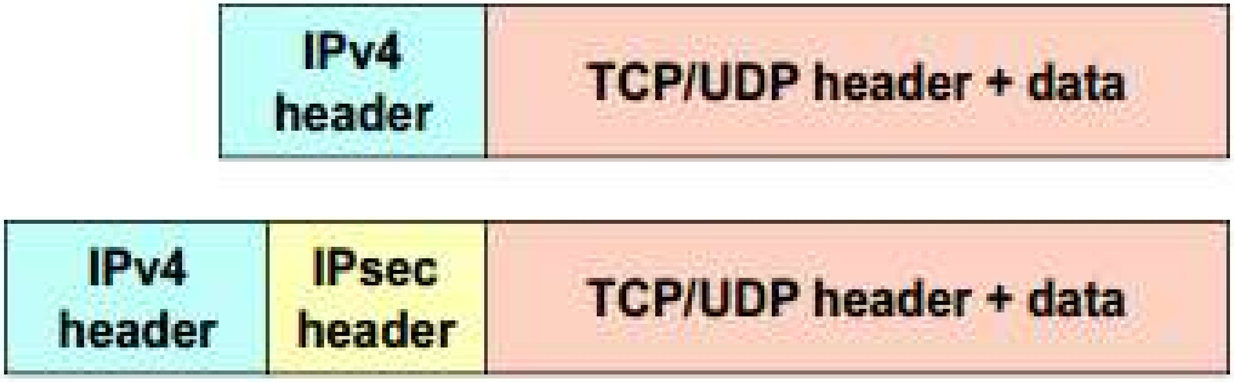
IPsec

- Two Modes
  - Transport Mode 1
  - Tunnel Mode 2

The IP header remains in plaintext, exposing sensitive routing information.

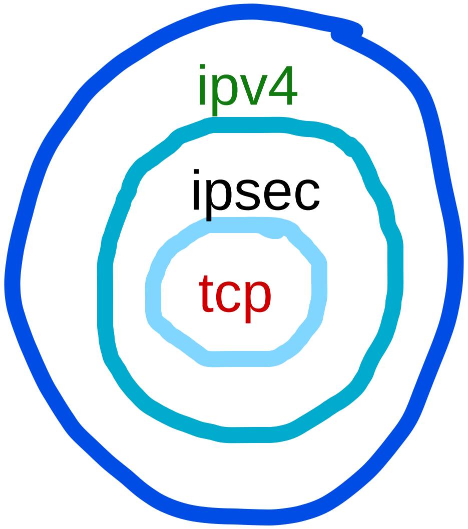
1. Transport Mode

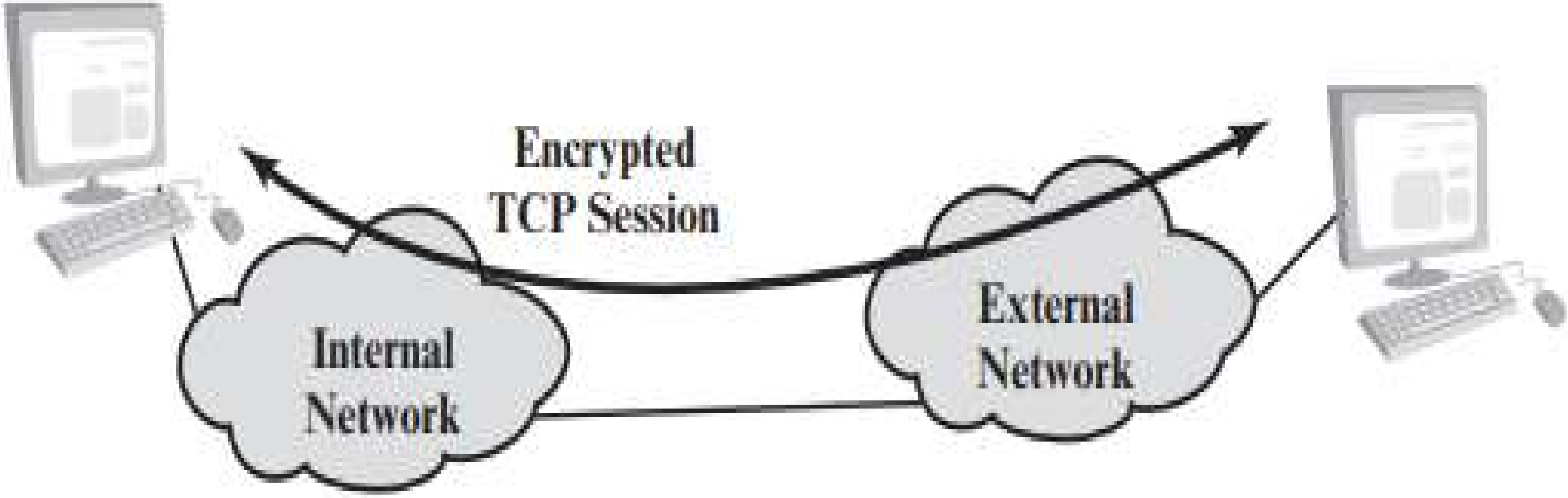
- Used for end-to-end security, that is used by hosts, not gateways (exception: traffic for the gateway itself e.g: SNMP, ICMP)
- Pro: computationally light
- Con: no protection of header variable fields



Encrypts only the payload of the IP packet, leaving the header

Transport Mode





(a) Transport-level security

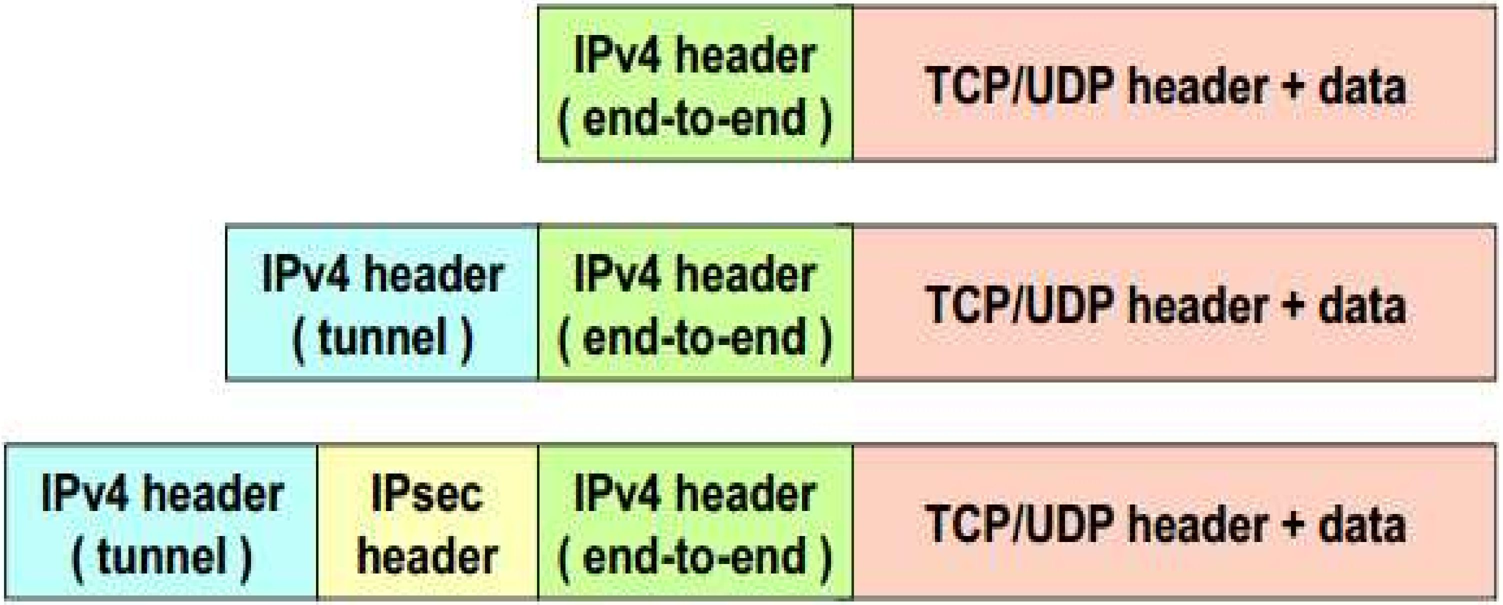
Primarily for end-to-end communication between devices (hosts)
Computationally lighter: Processes less data, as the header is not encrypted.
Suitable for applications like host-to-host communication (e.g., between two PCs).
Example: Used for protecting traffic such as SNMP or ICMP for the gateway itself.

Encrypts the entire IP packet, including the payload and the original header, and then encapsulates it in a new IP packet with a new header

2. Tunnel Mode

- Used to create a VPN, usually by gateways
- Gateway-to-gateway mode
- Pro: protection of header variable fields
- Con: computationally heavy

Requires more resources due to full packet encryption.

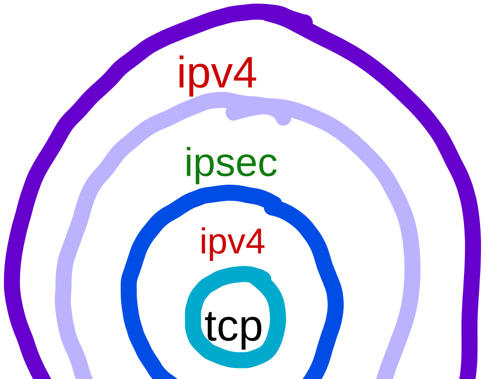


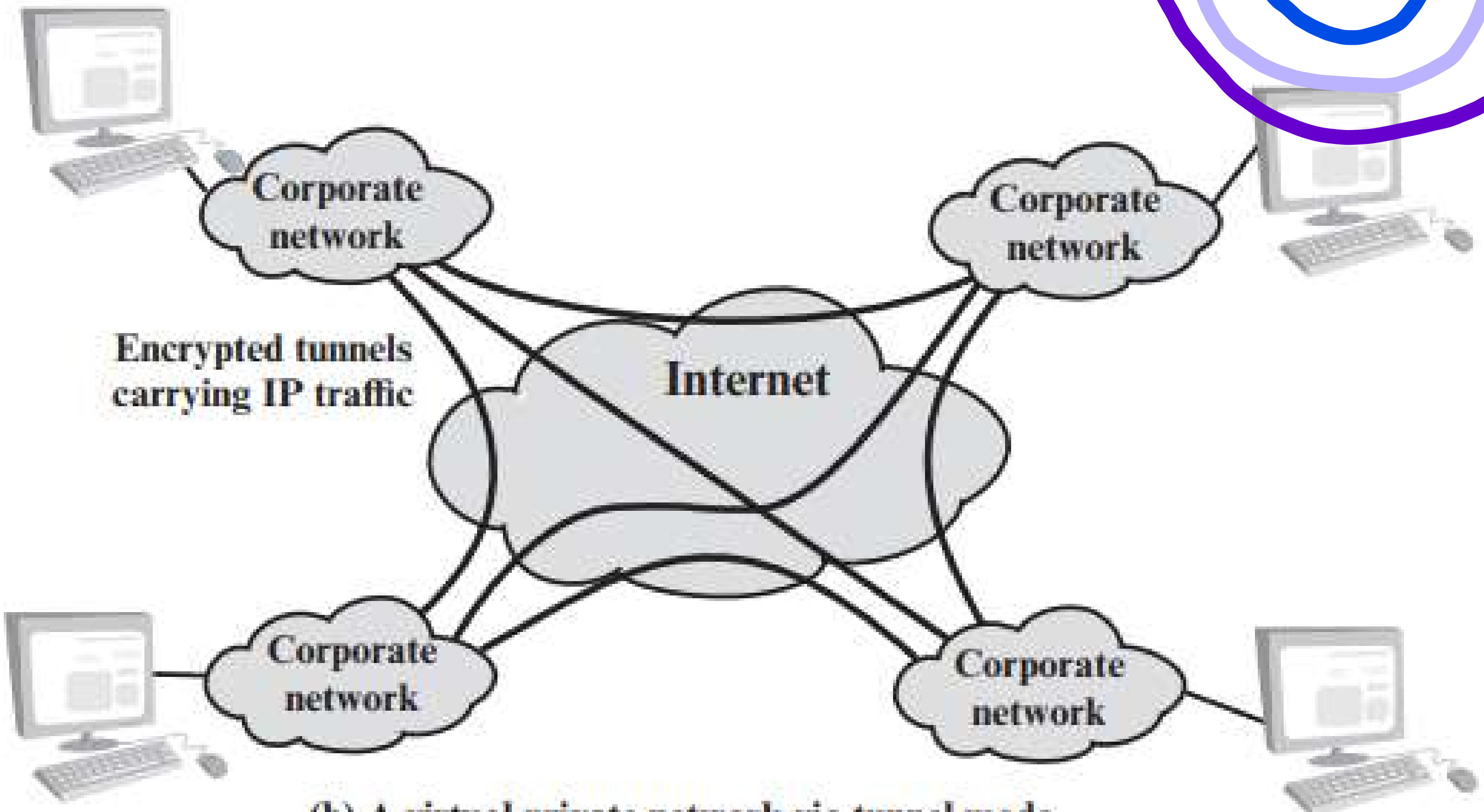
IPv4 header (end-to-end) | TCP/UDP header + data

IPv4 header (tunnel) | IPv4 header (end-to-end) | TCP/UDP header + data

IPv4 header (tunnel) | IPsec header | IPv4 header (end-to-end) | TCP/UDP header + data

Tunnel Mode





(b) A virtual private network via tunnel mode

Applications of IPsec

- Secure connection among different branches of the same company
  - Virtual Private Network (VPN)

- Secure remote access to an Intranet through the (insecure) Internet
  - Allows secure remote workers

- Secure communication between peers

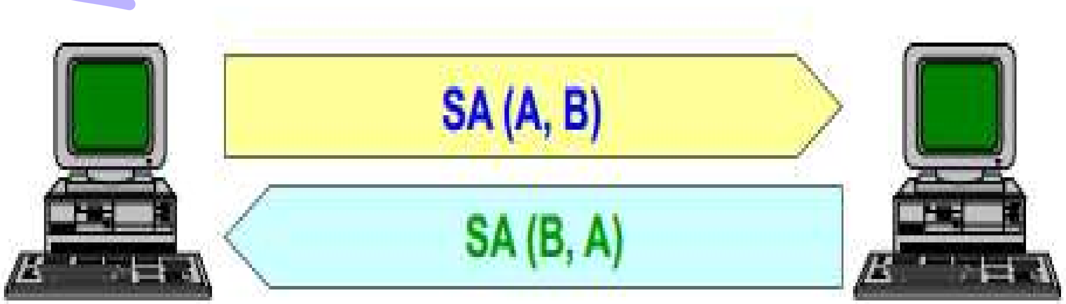
- Adding security for electronic commerce applications

IPsec Overview

- IETF architecture for L3 security in IPv4 / IPv6:
- Definition of two specific packet types:
  - AH (Authentication Header) 1
    - for integrity, authentication, no replay
    - Use is IPsecv3 for backward compatibility
    - Not used in new applications
  - ESP (Encapsulating Security Payload) 2
    - for confidentiality, integrity, authentication, no replay
- Protocol for key exchange:
  - IKE (Internet Key Exchange) ★

Security Association (SA)

- Establishment of shared security attributes between sender and receiver to support secure communication
- Usually considered unidirectional
- Contain all the information required for execution of various network security services
- Three SA identification parameters
  - Security parameter index (SPI)
  - IP destination address
  - Security protocol identifier (i.e. AH/ESP)
- Two SA are needed to get complete protection of a bidirectional packet flow in IPsec

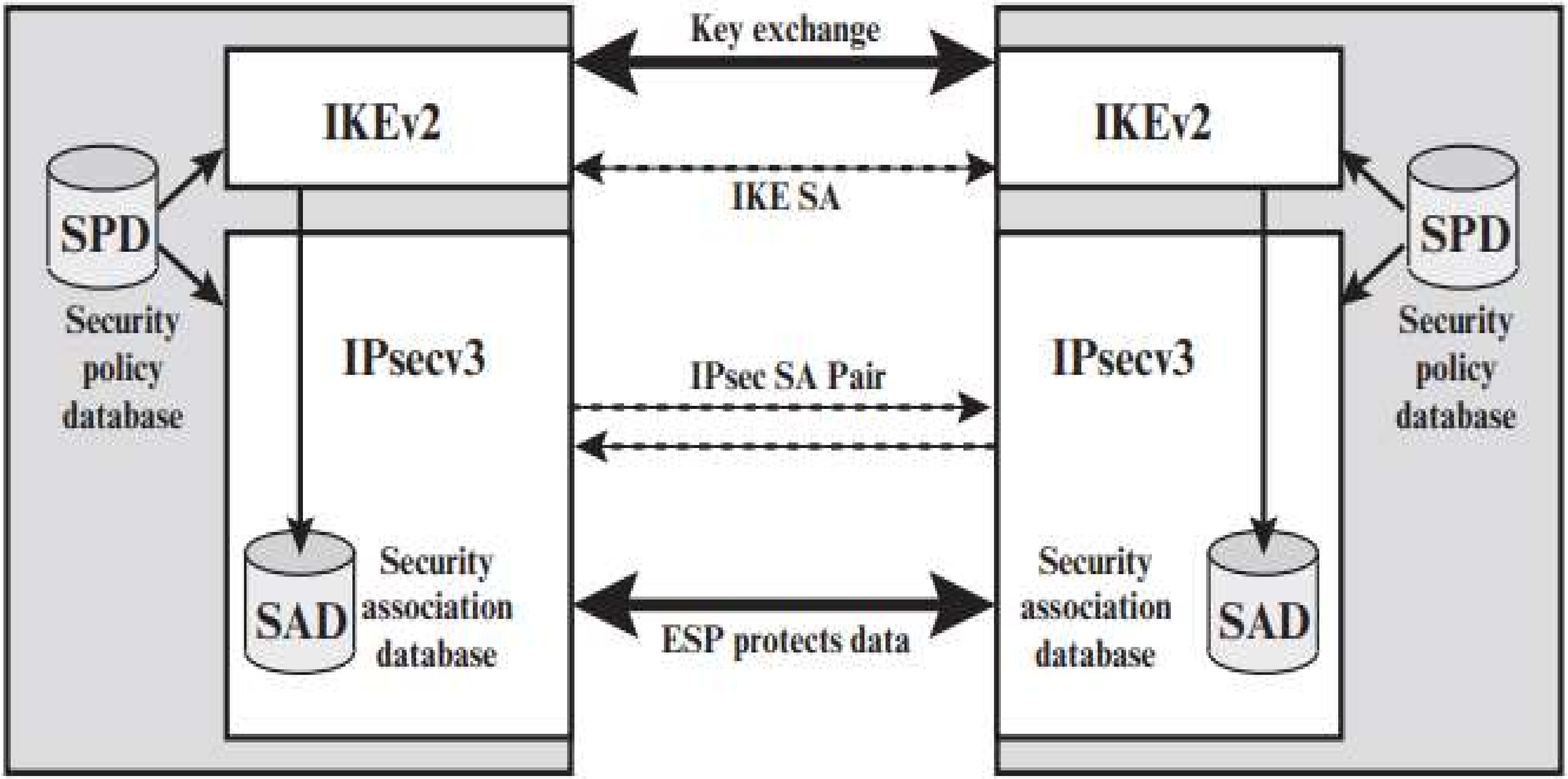


IPsec Local Databases

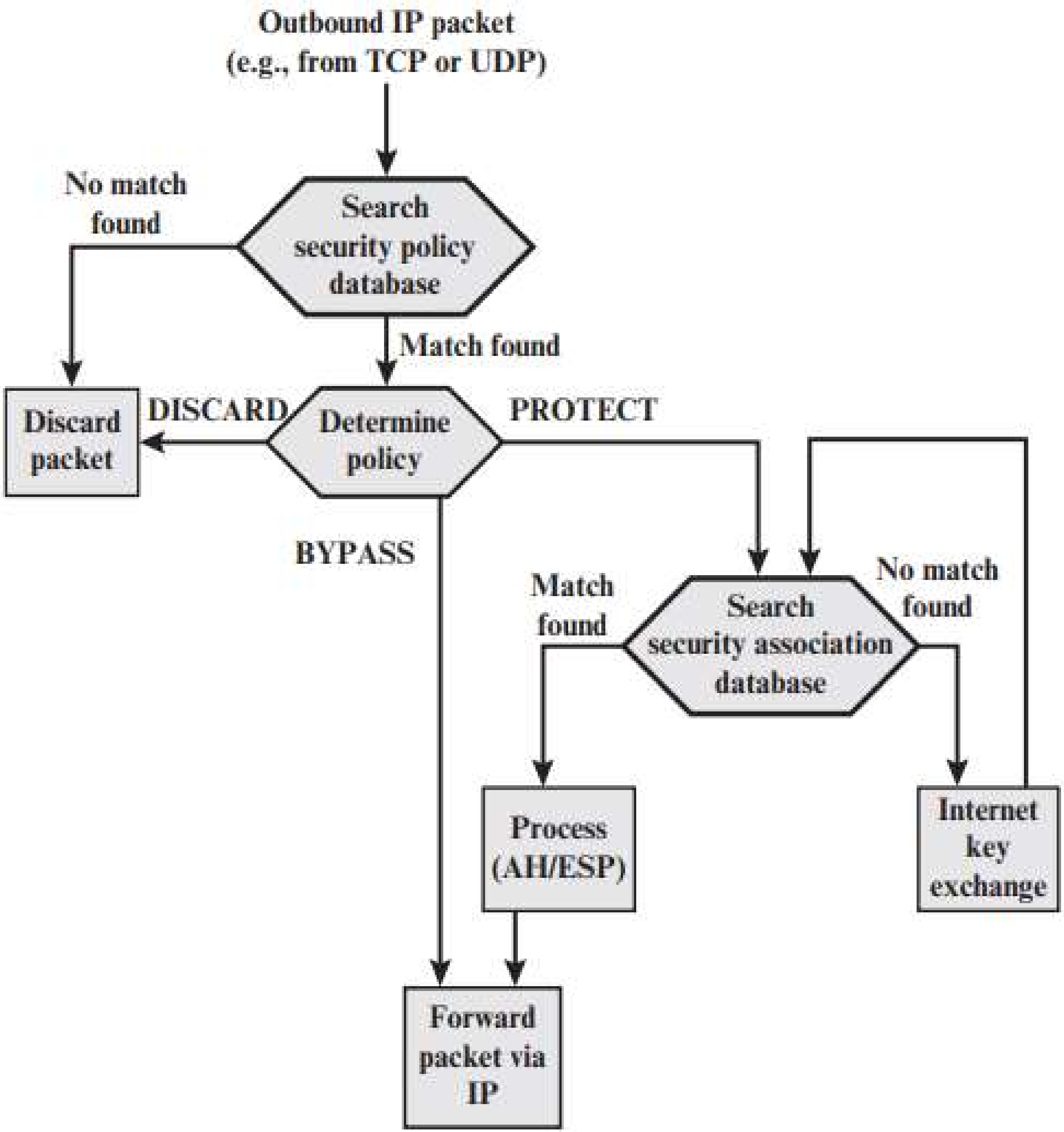
- SAD (SA Database)
  - list of active SA and their characteristics (algorithms, keys, parameters)
  - maintained by user-processes

- SPD (Security Policy Database)
  - list of security policies to apply to the different packet flows
  - 1 a-priori configured (e.g. manually) or connected to an automatic
    2 system (e.g. ISPS, Internet Security Policy System)

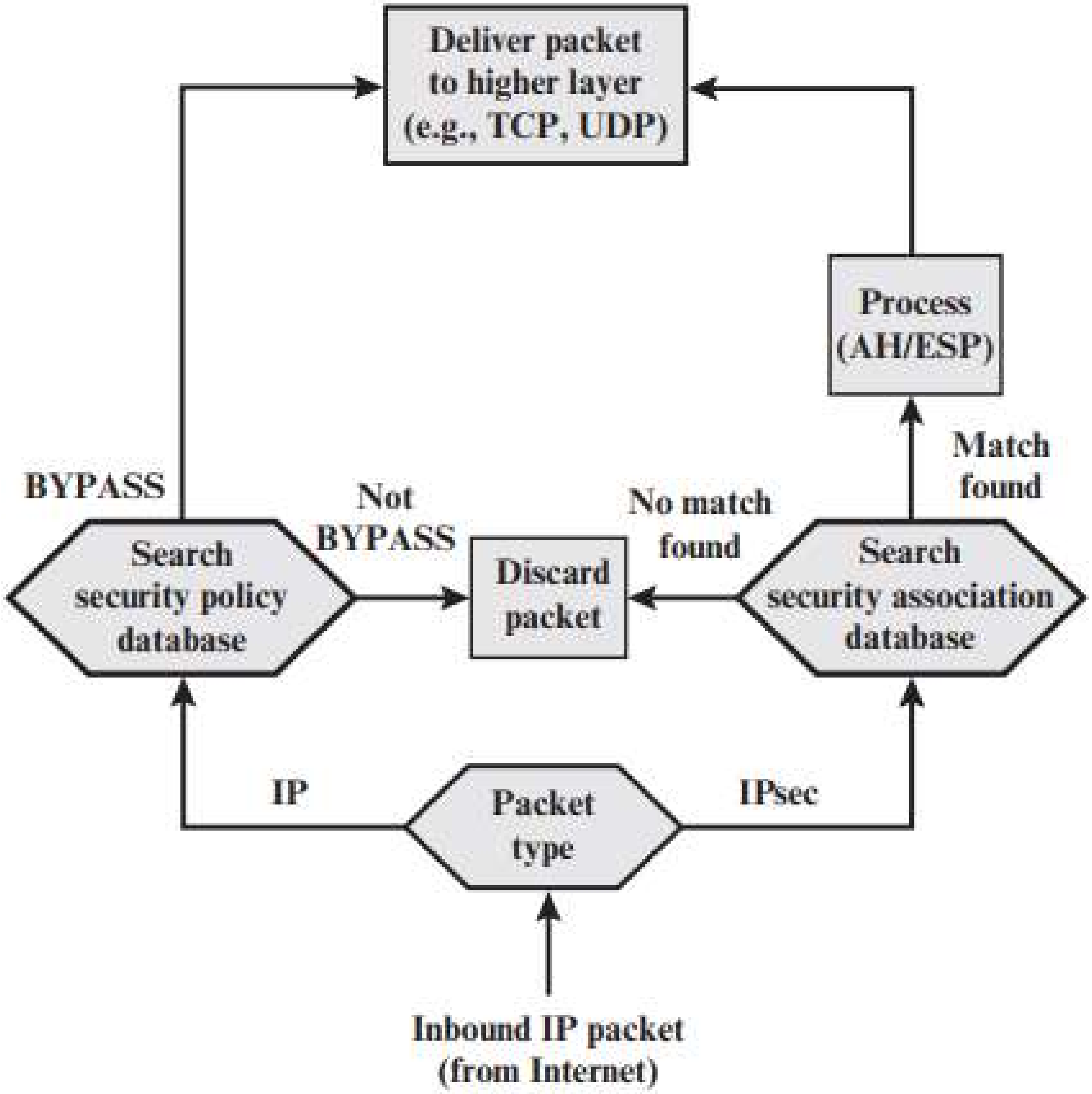
IPsec Architecture



IP Traffic Processing (Outbound Packets)



IP Traffic Processing (Inbound Packets)

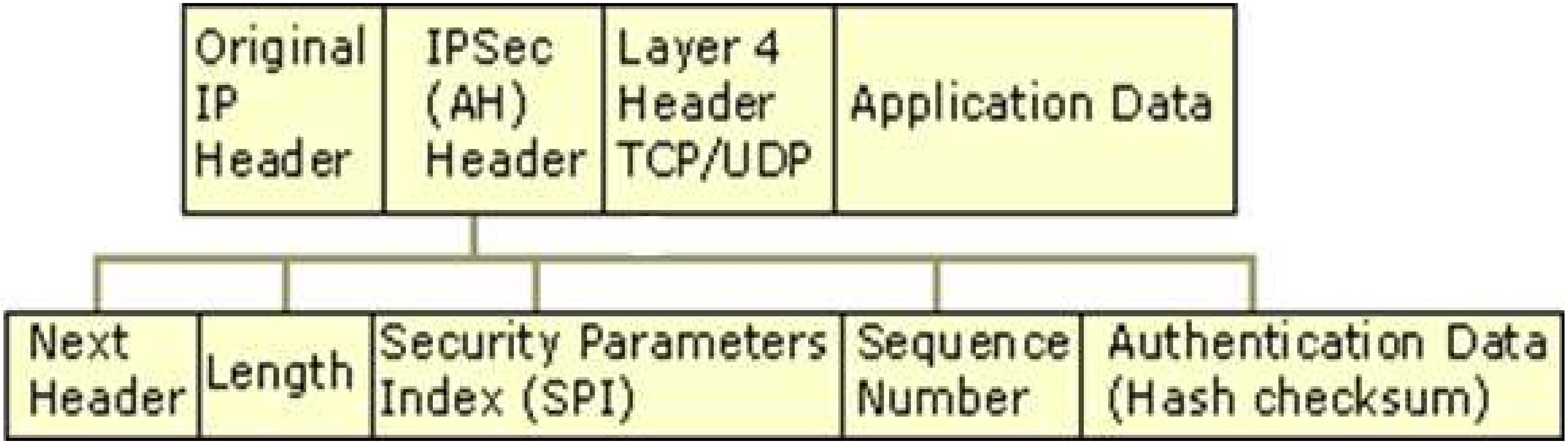

Deliver packet to higher layer (e.g., TCP, UDP)
Process (AH/ESP)
Match found
BYPASS
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
Packet type
IPsec
Inbound IP packet (from Internet)

do

AH

- Authentication Header
- Mechanism (first version, RFC-1826):
  - data integrity and sender authentication
  - compulsory support of keyed-MD5 (RFC-1828)
  - optional support of keyed-SHA-1 (RFC-1852)
- Mechanism (second version, RFC-2402):
  - data integrity, sender authentication and protection from replay attack
  - HMAC-MD5
  - HMAC-SHA-1

AH Packet

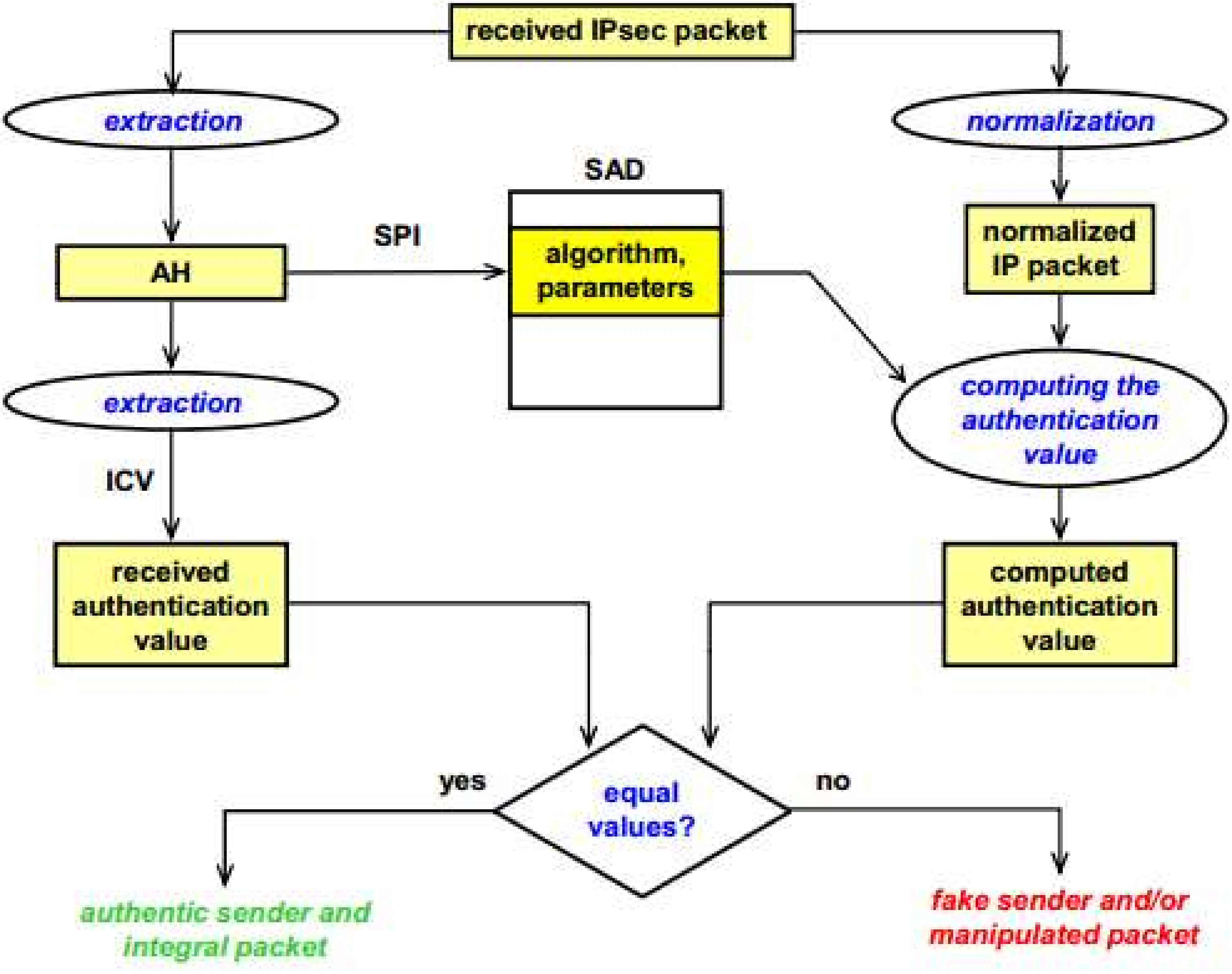


Original IP Header	IPSec (AH) Header	Layer 4 Header TCP/UDP	Application Data

Next Header	Length	Security Parameters Index (SPI)	Sequence Number	Authentication Data (Hash checksum)

- Next header: identifies the nature of the payload (TCP/UDP)
- Length: Indicates the length of the AH header
- SPI: Identifies the correct security association for the communication
- Sequence Number: Provides anti-replay protection for the SA
- Auth. Data: contains the Integrity Check Value (ICV) that is used to verify the integrity of the message. The receiver calculates the hash value and checks it against this value (calculated by the sender) to verify integrity.

AH Verification



received IPsec packet

extraction

normalization

SAD

SPI

AH

algorithm, parameters

normalized IP packet

extraction

computing the authentication value

ICV

received authentication value

computed authentication value

yes

equal values?

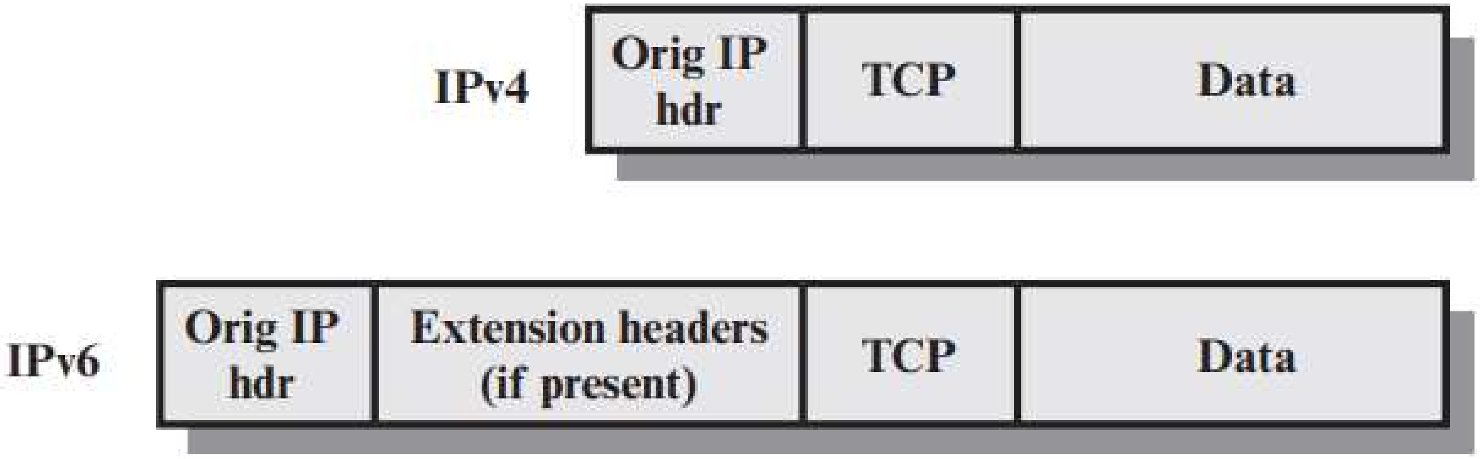
no

authentic sender and integral packet

fake sender and/or manipulated packet

ESP

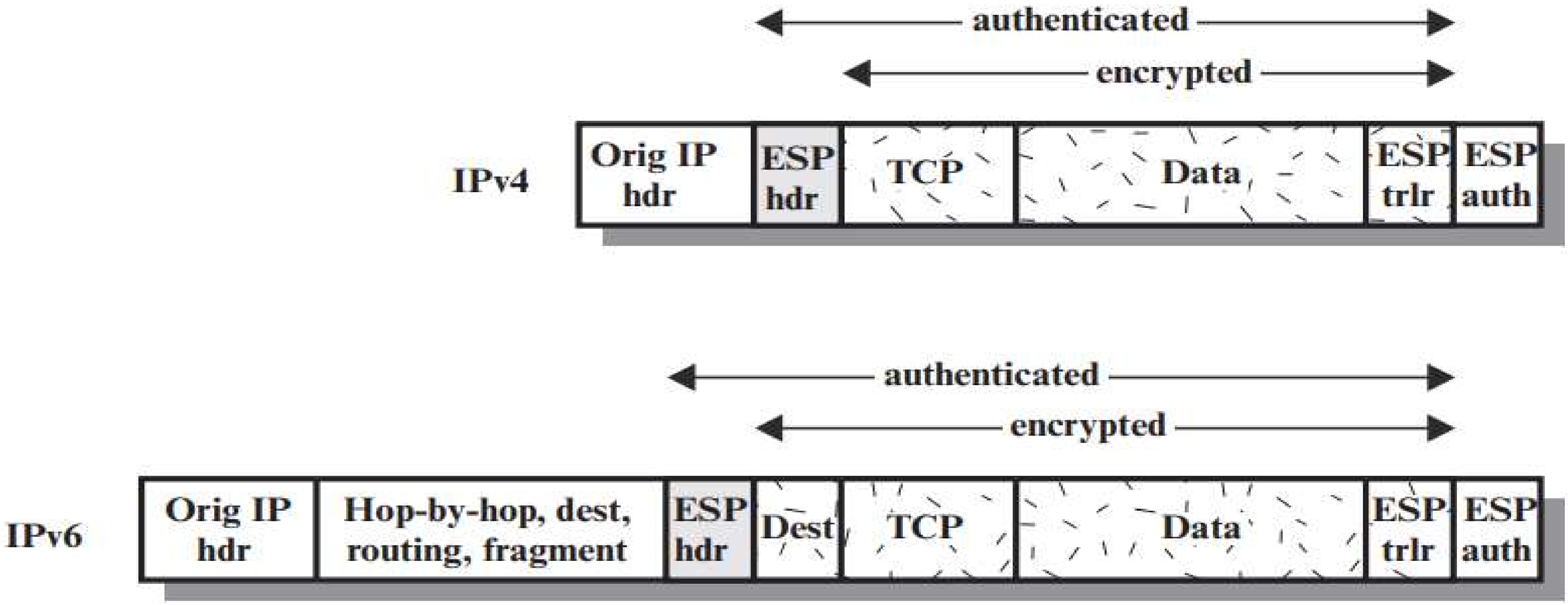
- Encapsulating Security Payload (ESP)
- First version (RFC-1827) gave only confidentiality
  - base mechanism: DES-CBC (RFC-1829)
- Second version (RFC-2406):
  - provides confidentiality & authentication (but not the IP header, so the coverage is not equivalent to that of AH)



(a) Before Applying ESP

ESP in Transport Mode

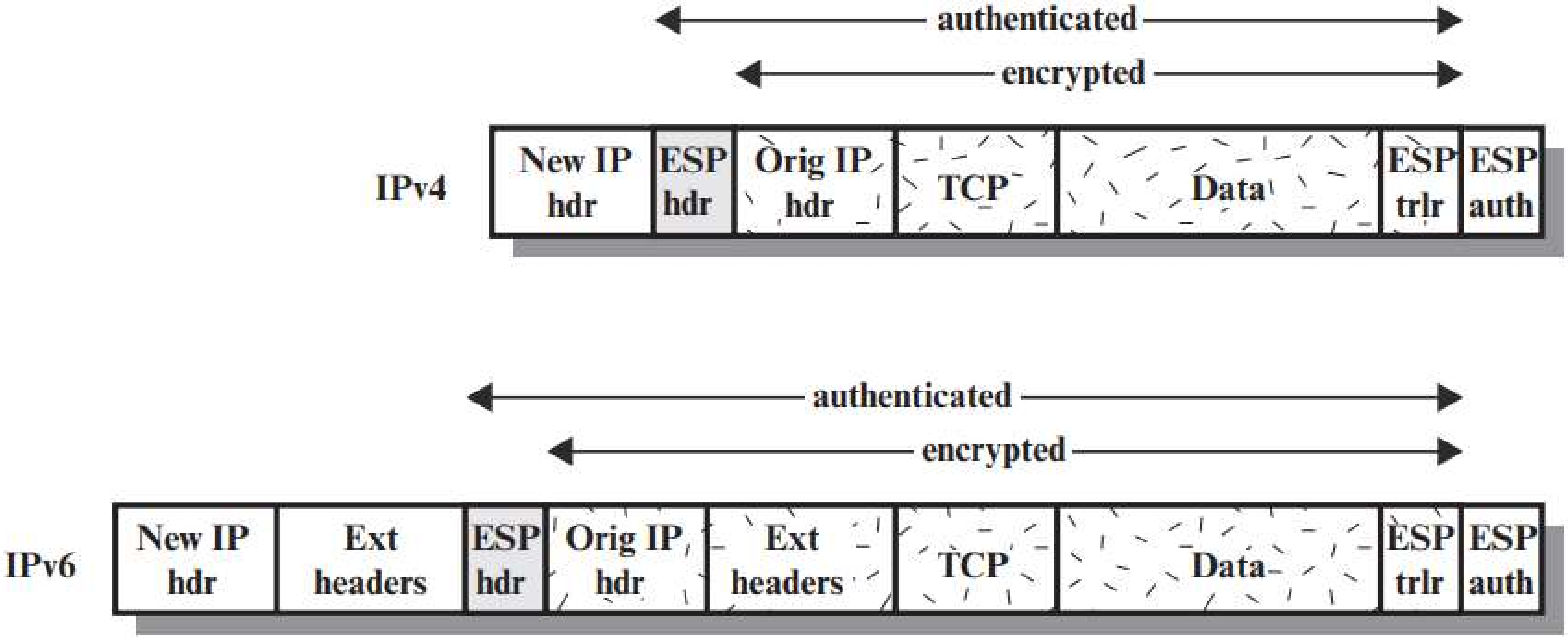
- Pro: the payload is hidden (including info needed for QoS or intrusion detection)
- Con: the header remains in clear



(b) Transport Mode

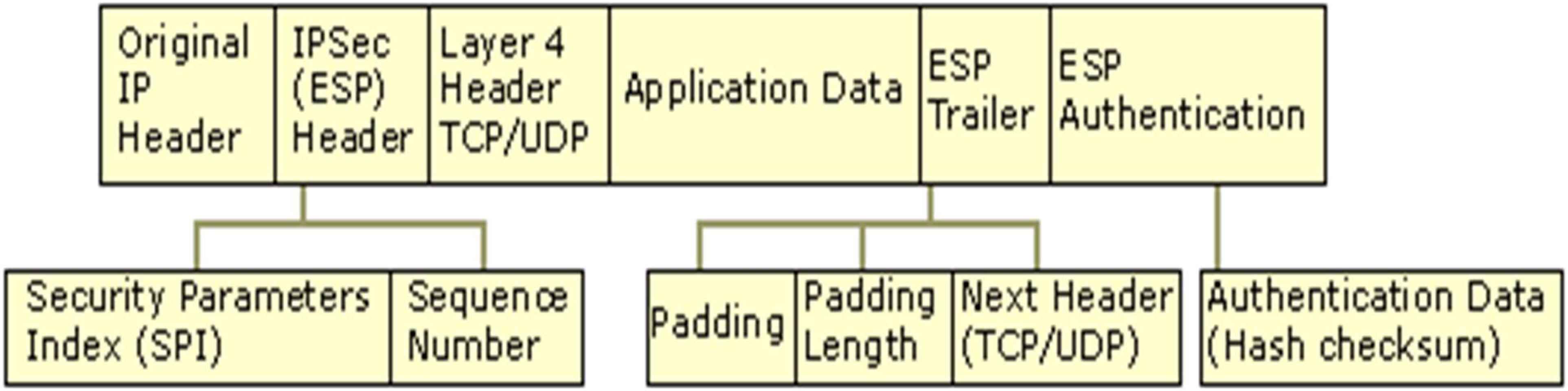
ESP Tunnel Mode

- Pro: hides both the payload and (original) header
- Con: larger packet size



(c) Tunnel Mode

ESP Packet



Original IP Header | IPSec (ESP) Header | Layer 4 Header TCP/UDP | Application Data | ESP Trailer | ESP Authentication

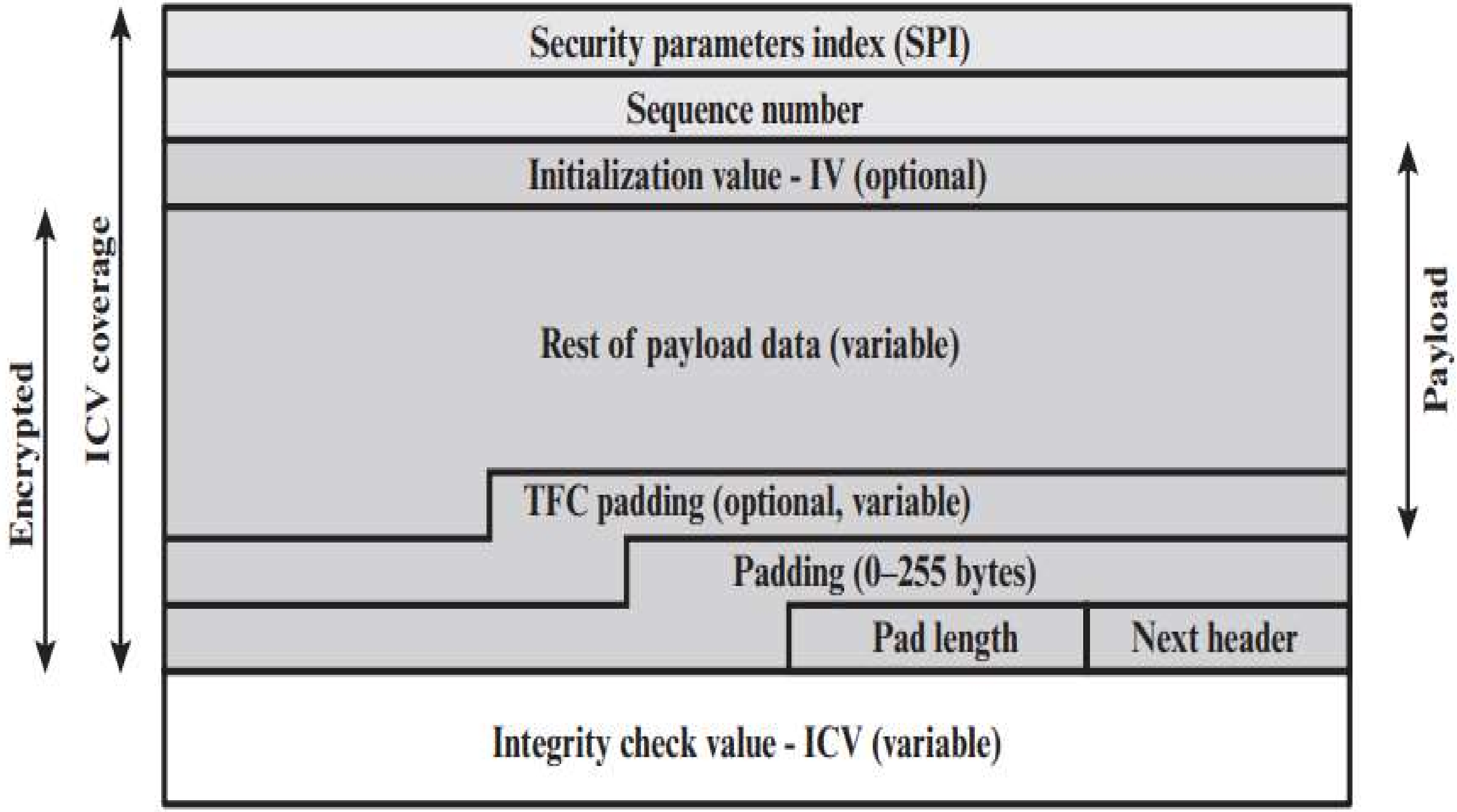
Security Parameters Index (SPI) | Sequence Number

Padding | Padding Length | Next Header (TCP/UDP)

Authentication Data (Hash checksum)

- SPI: Identifies the correct security association for the communication
- Sequence number: Provides anti-replay protection for the SA
- Next header: Identifies the nature of the payload (TCP/UDP)
- Auth. Data: Contains the Integrity Check Value (ICV), and a message authentication code that is used to verify the sender's identity and message integrity. The ICV is calculated over the ESP header, the payload data and the ESP trailer
- Initialization Vector (IV): optional. Is after the Sequence number

ESP Packet: Encryption & Authentication


Security parameters index (SPI)
Sequence number
Initialization value - IV (optional)
Rest of payload data (variable)
TFC padding (optional, variable)
Padding (0–255 bytes)
Pad length
Next header
Integrity check value - ICV (variable)
Encrypted
ICV coverage
Payload