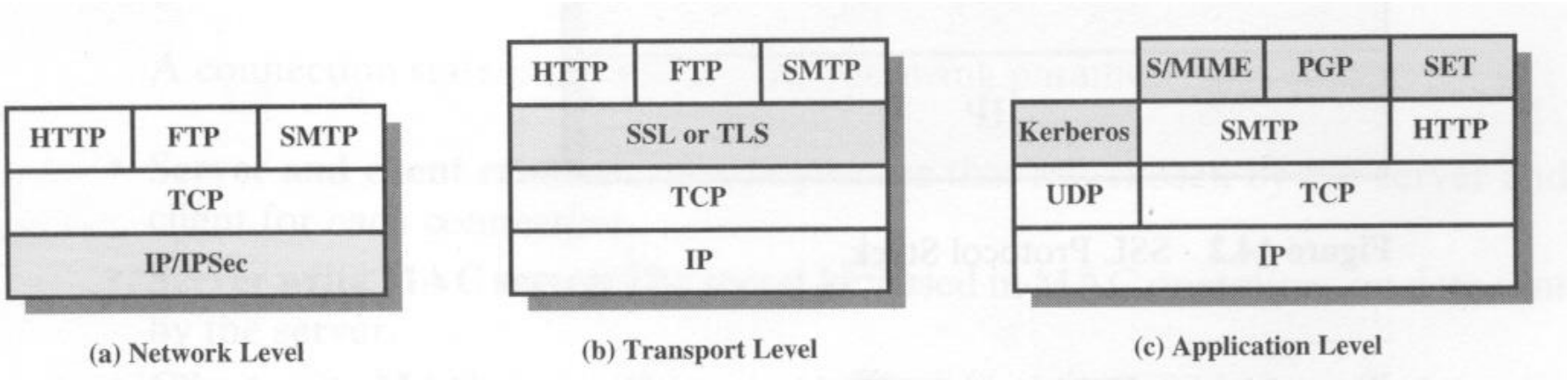
# Chap. 9 IP Security

- IPSec
- VPN (Virtual Private Network)

# Security Approaches

- Security approaches in TCP/IP protocol stack
- IPSec: security features at IP layer
  - Transparent to users and applications
- SSL (or TLS) : security features at transport layer
- Security features at application layer: PGP, S/MIME, SET, …



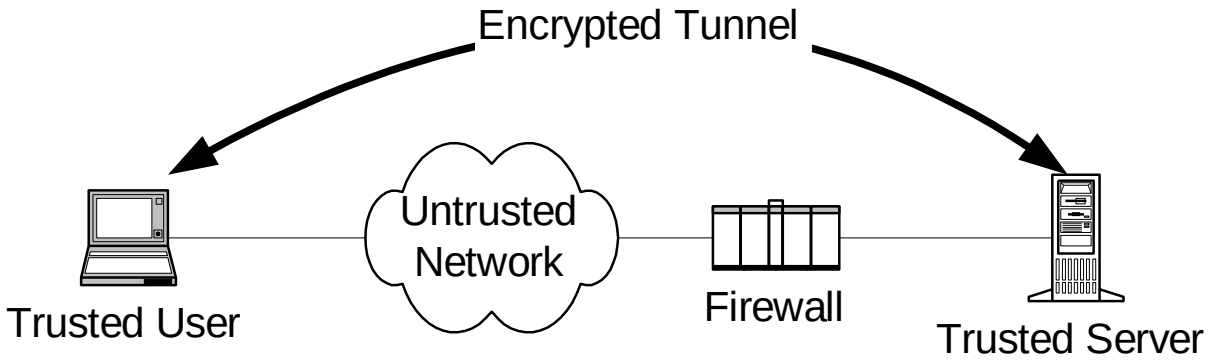
# IP Security Overview

- IP security (IPSec): RFC 1636, 1994
  - Confidentiality service
  - Authentication service
  - Key management
- Application of IPSec
  - VPN over Internet
  - Secure remote access over Internet
  - Enhancing e-Commerce security
  - Secure routing info. exchange among routers

# Virtual Private Networks (VPN)

## What is a VPN?

- a group of two or more computer systems that communicates 'securely' over a public network
- A combination of tunneling, encryption, authentication and access control technologies and services used to carry traffic over an IP network



# Virtual Private Networks (VPN)

- VPN provides
  - Encryption
  - Strong authentication of remote users and hosts
  - Mechanisms for hiding or masking information about the private network topology from potential attackers
- Three basic types:
  - Hardware-based
  - Firewall-based
  - Standalone/Software-based

# IPSec (IP Security)

- IPSec protocols
  - IP Authentication Header (AH)
  - IP Encapsulating Security Payload (ESP)
  - Internet Key Exchange (IKE)

- ESP and AH assume the peers using the protocol have a shared key
  - needs a protocol for distributing keys called Internet Key Exchange (IKE)

# Security Association (SA)

- One-way association b/w sender and receiver that applies security services to the traffic on it
- Defined by:
  - IP destination address
  - Security parameter index (SPI): the index used to select SA under which a received packet will be processed
  - Security protocol identifier: identifies AH or ESP

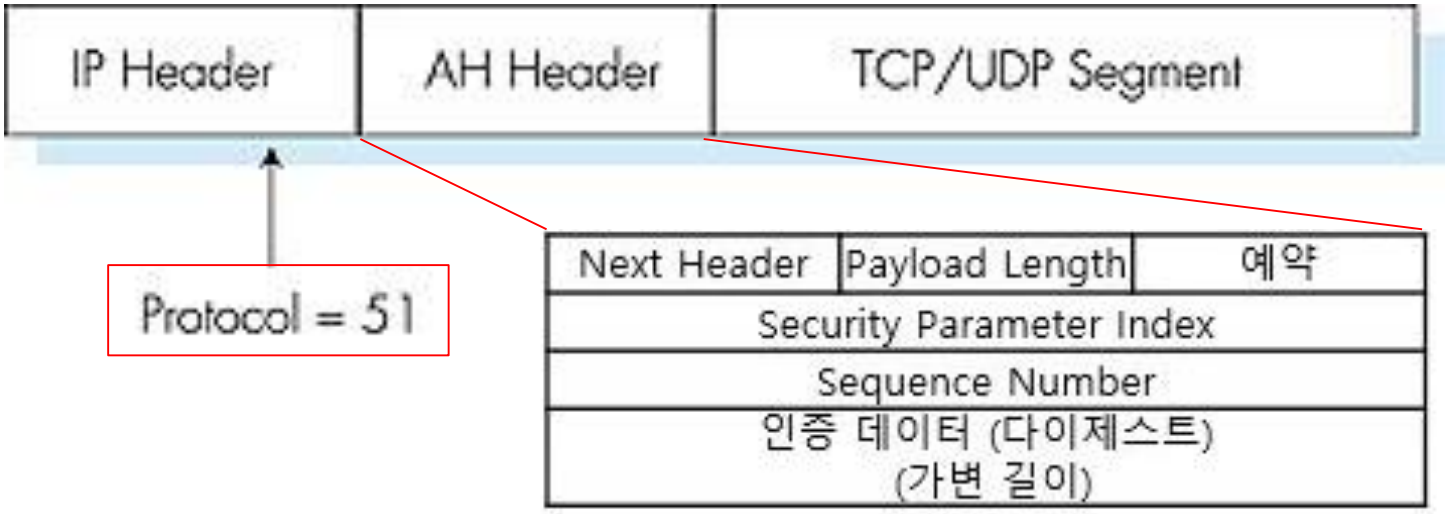
# Security Association

SA parameters

- Packet sequence number counter
- Anti-replay window
- AH information: authentication algorithm, key, key lifetime, etc.
- ESP information: authentication and encryption algorithm, key, IV, key lifetime, etc.
- SA lifetime: after this lifetime, SA must be replaced with a new SA
- IPSec protocol mode: tunnel or transport mode
- Path MTU

# Authentication Header (AH)

- Designed to provide
  - message integrity (authentication)
  - Does not provide confidentiality



# Authentication Header (AH)

- AH header includes:
  - Payload length: length of AH
  - authentication data: signed message digest, calculated over original IP datagram, providing source authentication, data integrity
  - SPI
  - Sequence number (SN): used to protect against replay attacks
  - Next header field: specifies type of data (TCP, UDP, etc.)

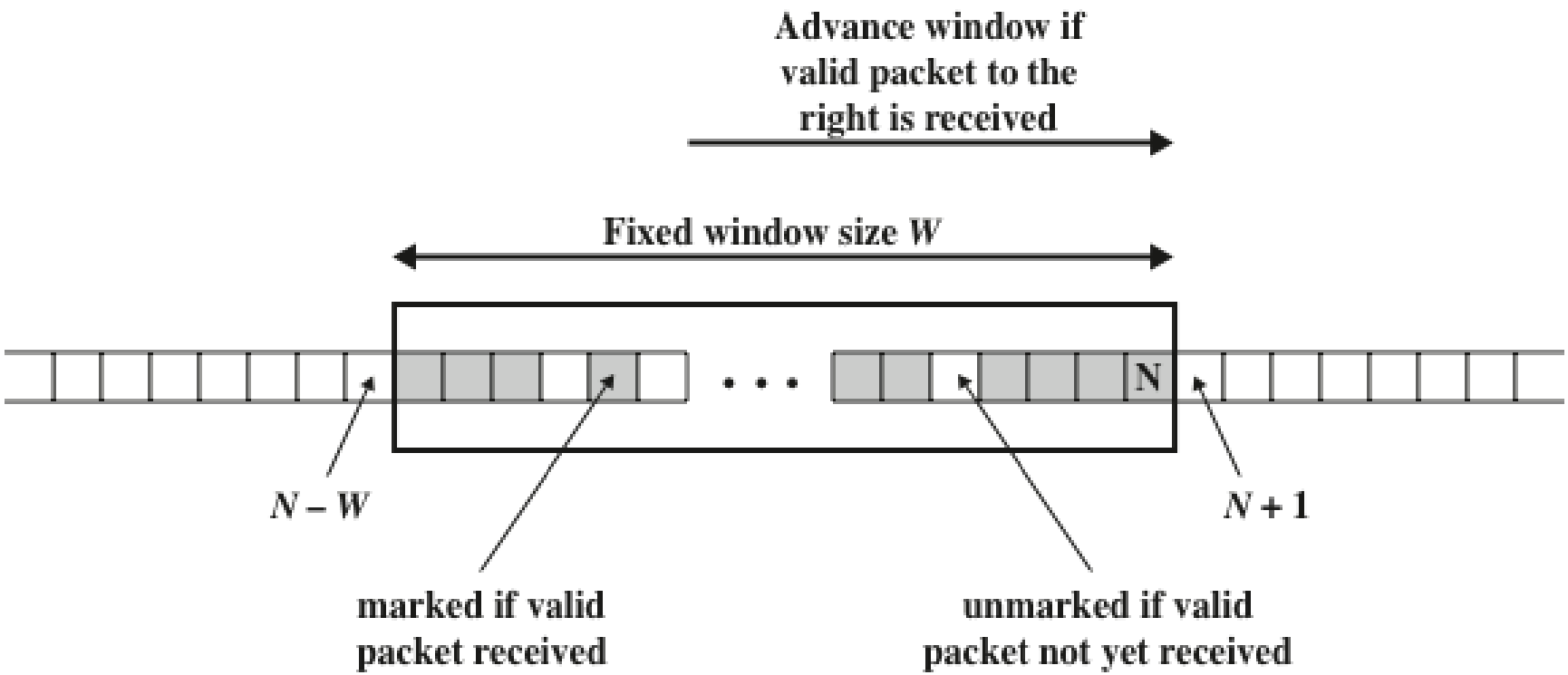
# Authentication Header (AH)

Anti-replay attacks:

- Sender initializes SN counter to 0
- Each time a packet is sent on this SA, sender increments the SN counter
- If the SN counter value overflows, sender terminates the current SA and negotiate a new SA with a new key
- IP packet may be delivered out of order
- Receiver allows packets out of order within a window W (default size of 64)

# Authentication Header (AH)

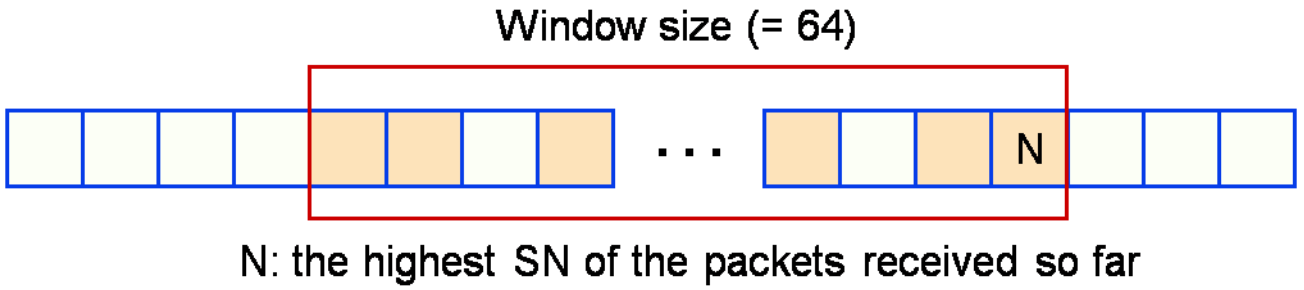
## Anti-replay attacks:



# Authentication Header (AH)

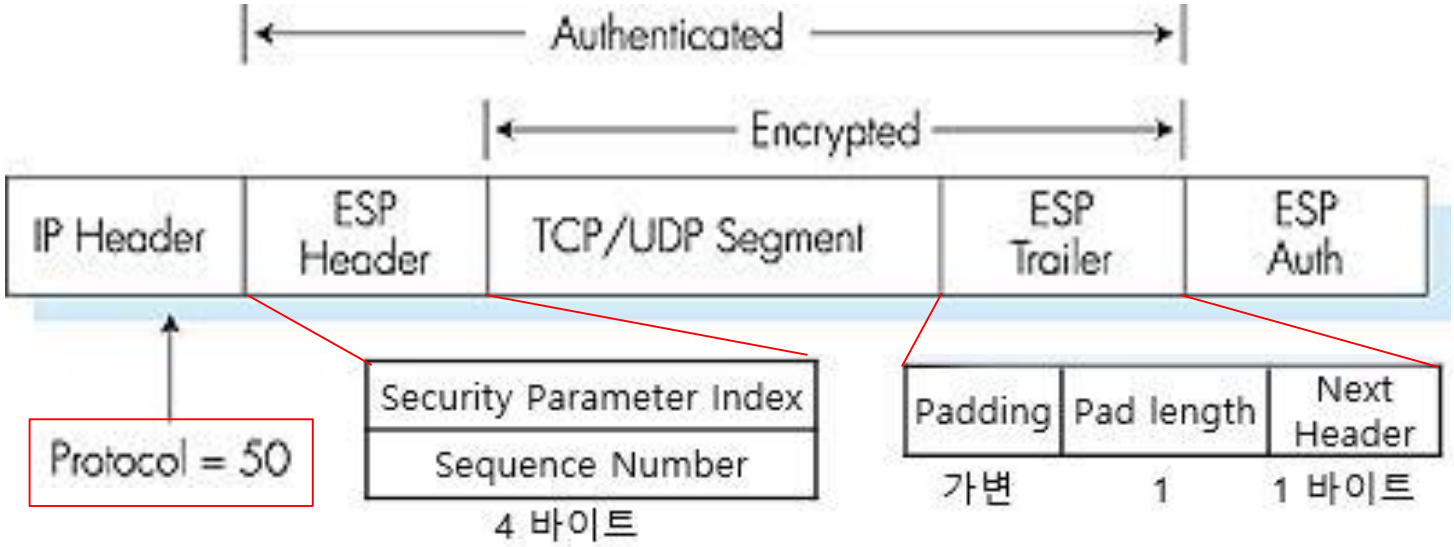
## Anti-replay attacks:

- Input processing (receiver):
  - When SN of the received packet is within the window: check MAC, if correct, mark the window slot
  - When SN of received packet > N: check MAC, if it is correct, mark the window slot and advance the window
  - When SN of the received packet is to the left of the window or MAC is incorrect, discard the packet



# Encapsulating Security Payload (ESP)

- ESP protocol provides
  - Integrity
  - Authentication
  - Confidentiality
- (Data, ESP trailer) encrypted
- Next header field is in ESP trailer
- ESP authentication field is similar to AH authentication field



# IKE (Internet Key Exchange)

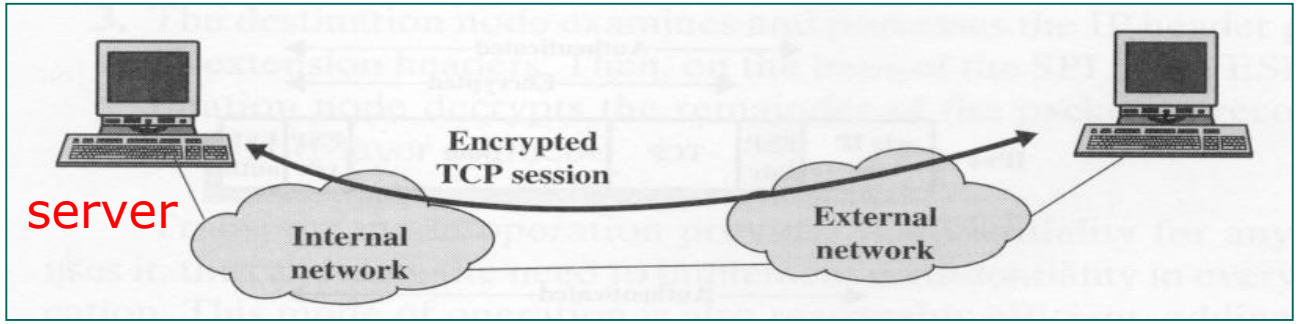
- IKE
  - manual key management: system administrator manually configures each system with keying materials; used in small and static environment
  - automated key management: provides a negotiation method for setting keying materials for SAs automatically; used in large distributed environment
- Based on previous protocols
  - ISAKMP – A framework for authentication and key exchanges, define message formats for key exchanges
  - Oakley: key exchange protocol based on DH algorithm

# IPSec Mode

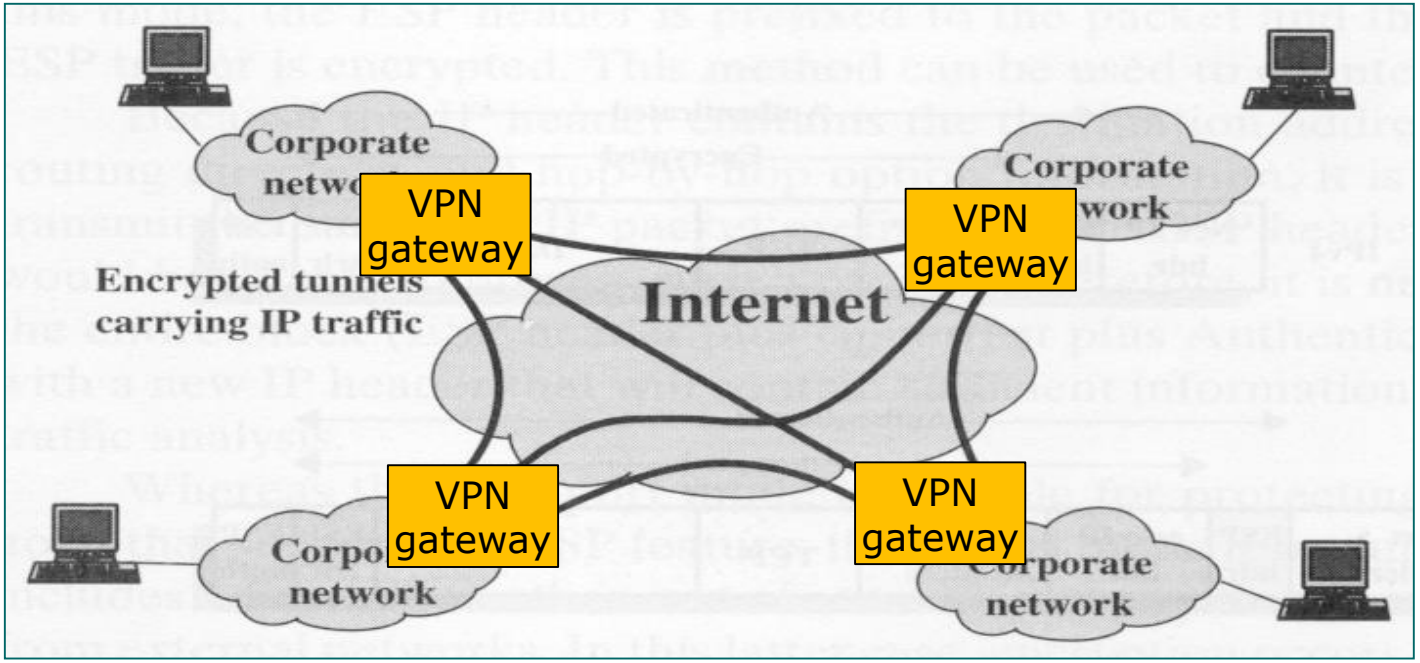
- Transport mode
  - Provides protection to the payload of IP packet
  - remote access: used for end-to-end secure communication between two hosts
- Tunnel mode
  - Provides protection to the entire IP packet
  - The original IP packet is encapsulated into new IP packet including AH or ESP header.
  - VPN: used for secure communications between two IPSec gateways

# IPSec Mode

- Transport mode

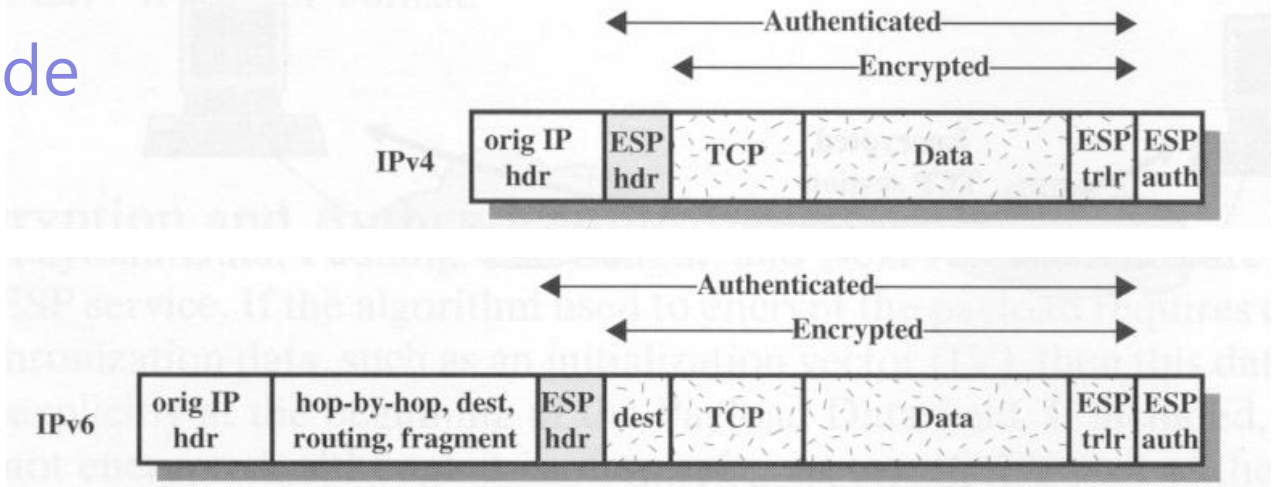



- Tunnel mode



# IPSec Mode: ESP

- Transport mode




- Tunnel mode