

IP Security

Dr. Arjan Durresi
Louisiana State University
Baton Rouge, LA 70810
Durresi@csc.lsu.edu

These slides are available at:

<http://www.csc.lsu.edu/~durresi/csc4601-07/>



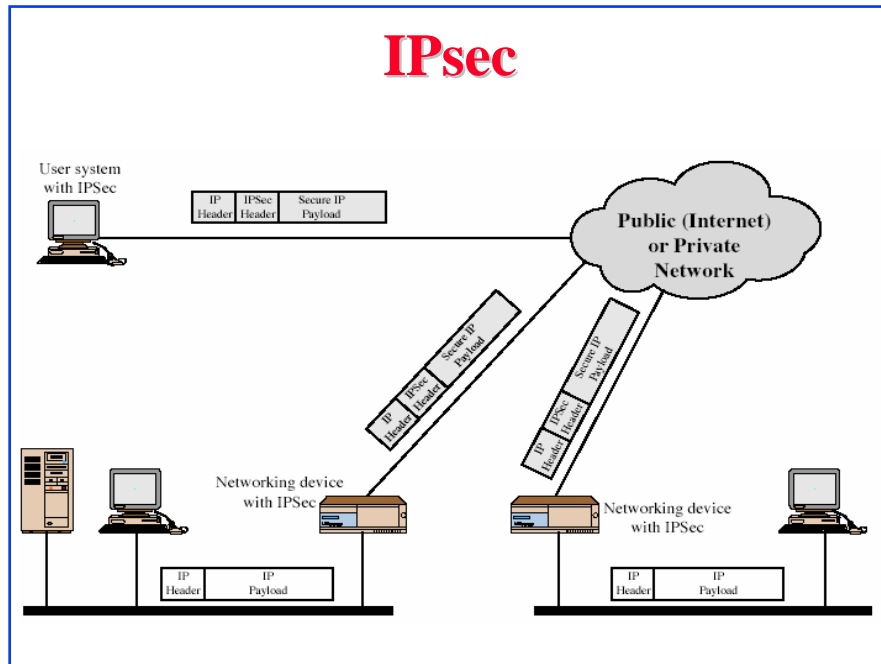
- ❑ Objectives
- ❑ IPSec architecture & concepts
- ❑ IPSec authentication header
- ❑ IPSec encapsulating security payload

IPSEC Objectives

- ❑ IPsec – IETF standard for real-time communication security
- ❑ Band-aid for IPv4
 - Spoofing a problem
 - Not designed with security or authentication in mind
- ❑ IP layer mechanism for IPv4 and IPv6
 - Not all applications need to be security aware
- ❑ Can be transparent to users

IPsec

- ❑ General IP Security mechanisms
- ❑ Provides
 - authentication
 - confidentiality
 - key management
- ❑ Applicable to use over LANs, across public & private WANs, & for the Internet



Benefits of IPsec

- ❑ In a firewall/router provides strong security to all traffic crossing the perimeter
- ❑ Is resistant to bypass
- ❑ Is below transport layer, hence transparent to applications
- ❑ Can be transparent to end users
- ❑ Can provide security for individual users if desired

IPsec Services

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

Architecture & Concepts

- ❑ Specification is quite complex
- ❑ Mandatory in IPv6, optional in IPv4
- ❑ Host or gateway implementation
- ❑ Tunnel vs. Transport mode
- ❑ Security association (SA) – cryptographically protected connection
 - Security parameter index (SPI)
 - Security policy database (SPD)
 - SA database (SAD)
 - SPI + destination address define SA
- ❑ Encapsulating security payload (ESP)
- ❑ Authentication header (AH)

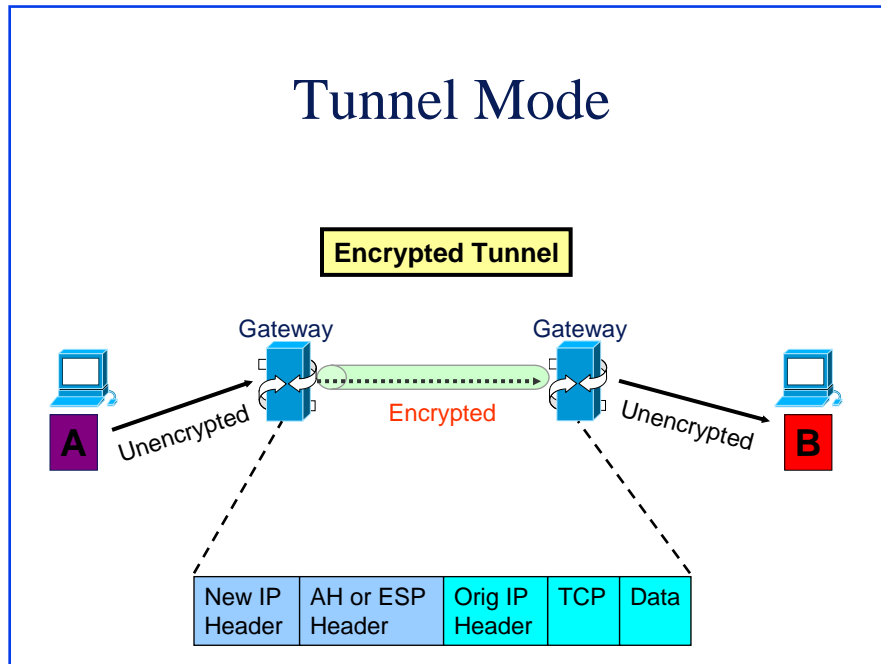
Authentication Header – AH Encapsulating Security Payload - ESP

- ❑ AH (RFC 2406) and ESP (RFC 2402) are the two types of IPsec headers
- ❑ AH – Integrity only
- ❑ ESP – Integrity + Encryption
- ❑ Is AH necessary?
- ❑ AH protects some IP header fields too
- ❑ If IP payload is encrypted (ESP) firewalls and routers cannot check TCP cannot check layer 4 ports.

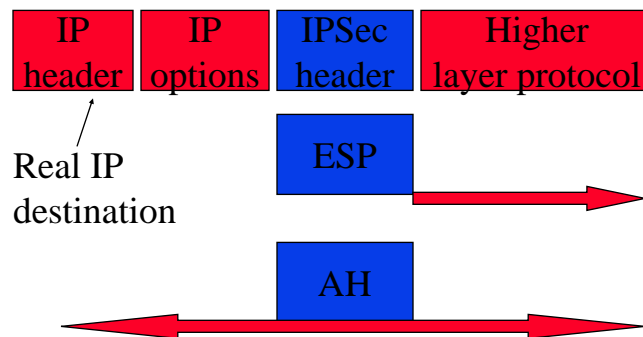
Hosts & Gateways

- ❑ Hosts can implement IPsec to :
 - Other hosts in transport or tunnel mode
 - Gateways with tunnel mode
- ❑ Gateways to gateways - tunnel mode

Tunnel Mode

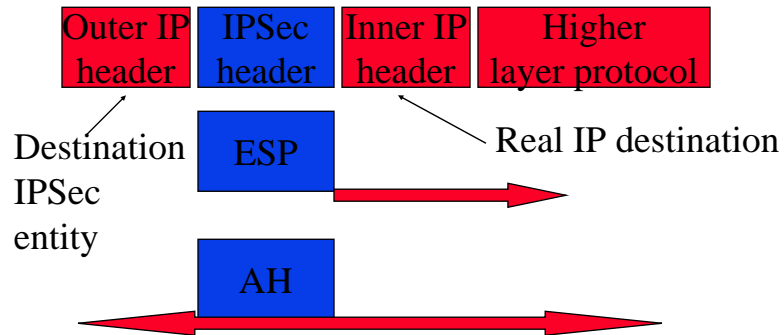


Transport Mode



- ❑ ESP protects higher layer payload only. Encryption and/or integrity protection
- ❑ AH can protect IP headers as well as higher layer payload – integrity protection only
- ❑ Is AH really needed?

Tunnel Mode



- ESP applies only to the tunneled packet
- AH can be applied to portions of the outer header

Tunnel and Transport Mode

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

The same packet might have multiple layers of IPsec (ESP and AH) headers and might be multiply-encrypted.

Network Address Translation

- ❑ NAT – share IPv4 addresses. Translates internal IP addresses to globally unique IP addresses
- ❑ IPsec tunnel and transport cannot work with NAT
- ❑ Firewalls vs. End-to-end security
- ❑ IPsec tunnel
 - NAT wants to update the IP address inside the encrypted data, but it does not have the key.
- ❑ IPsec transport
 - IP address is included in the computation of TCP or UDP checksum

Security Association - SA

- ❑ A one-way relationship between sender & receiver that affords security for traffic flow
- ❑ Defined by 3 parameters:
 - Security Parameters Index (SPI)
 - IP Destination Address
 - Security Protocol Identifier – indicates AH or ESP assoc.
- ❑ Has a number of other parameters
 - seq no, AH & ESP info, lifetime etc
- ❑ Have a database of Security Associations
- ❑ Determine IPsec processing for senders
- ❑ Determine IPsec decoding for destination
- ❑ SAs are not fixed! Generated and customized per traffic flows

Security Parameters Index - SPI

- ❑ Can be up to 32 bits large
- ❑ The SPI allows the destination to select the correct SA under which the received packet will be processed (according to the agreement with the sender)
 - The SPI is sent with the packet by the sender
- ❑ SPI + Dest IP address + IPSec Protocol (AH or ESP) uniquely identifies a SA

SA Database - SAD

- ❑ Holds parameters for each SA
 - Sequence number Counter - 32 bit
 - Lifetime of this SA
 - AH and ESP information
 - Tunnel or transport mode
- ❑ Every host or gateway participating in IPSec has their own SA database

SA Bundle

- ❑ More than 1 SA can apply to a packet
- ❑ Example: ESP does not authenticate new IP header.
How to authenticate?
 - Use SA to apply ESP w/out authentication to original packet
 - Use 2nd SA to apply AH

Security Policy Database - SPD

- ❑ What traffic to protect?
- ❑ Has incoming traffic been properly secured?
- ❑ Policy entries define which SA or SA Bundles to use on IP traffic
- ❑ Each host or gateway has their own SPD
- ❑ Index into SPD by Selector fields
 - Dest IP, Source IP, Transport Protocol, IPSec Protocol, Source & Dest Ports, ...

SPD Entry Actions

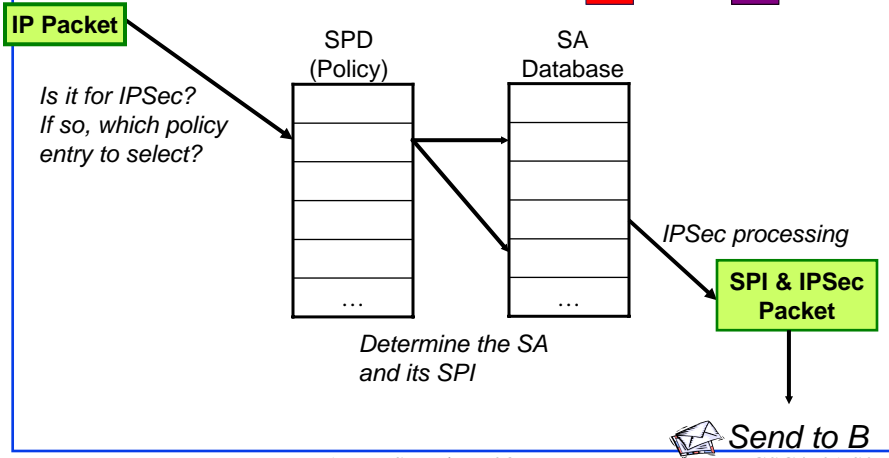
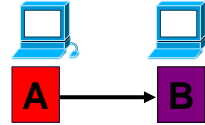
- ❑ Discard
 - Do not let in or out
- ❑ Bypass
 - Outbound: do not apply IPSec
 - Inbound: do not expect IPSec
- ❑ Protect – will point to an SA or SA bundle
 - Outbound: apply security
 - Inbound: check that security must have been applied

SPD Protect Action

- ❑ If the SA does not exist...
 - Outbound processing: use IKE to generate SA dynamically
 - Inbound processing: drop packet

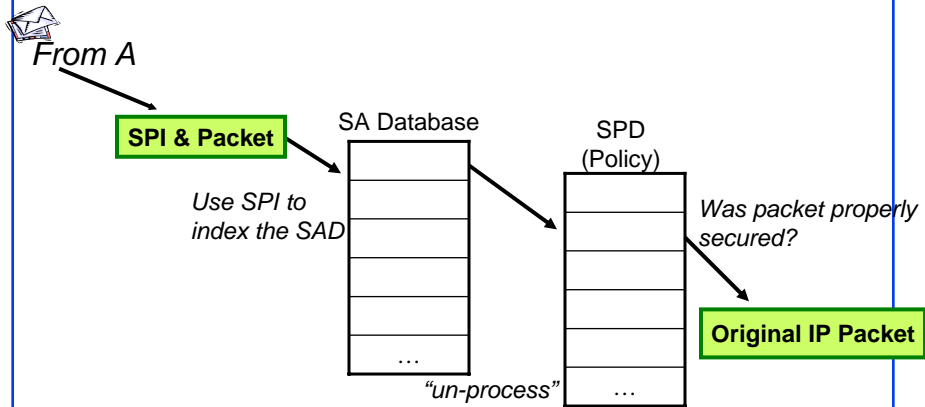
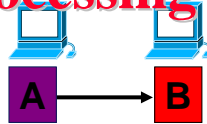
Outbound Processing

Outbound packet (on A)



Inbound Processing

Inbound packet (on B)



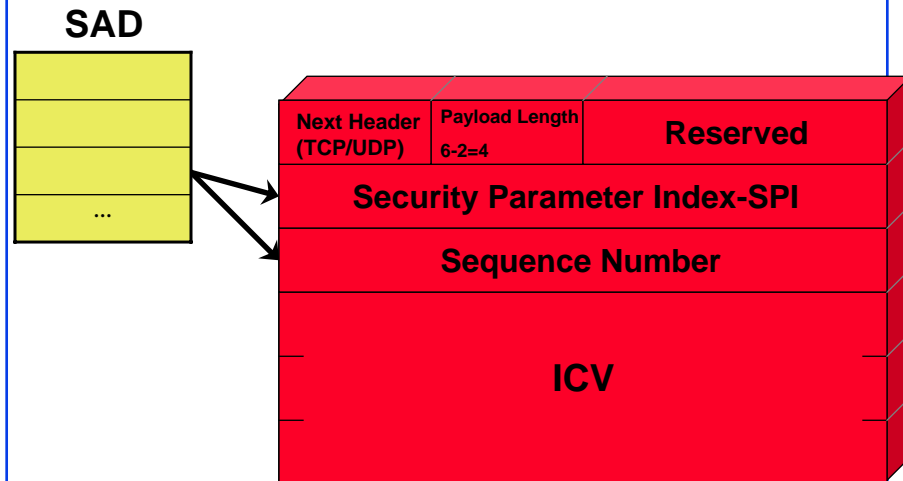
Authenticated Header

- ❑ Data integrity
 - Entire packet has not been tampered with
- ❑ Authentication
 - Can “trust” IP address source
 - Use Message Authentication Code (MAC) to authenticate
- ❑ Anti-replay feature
- ❑ Integrity check value

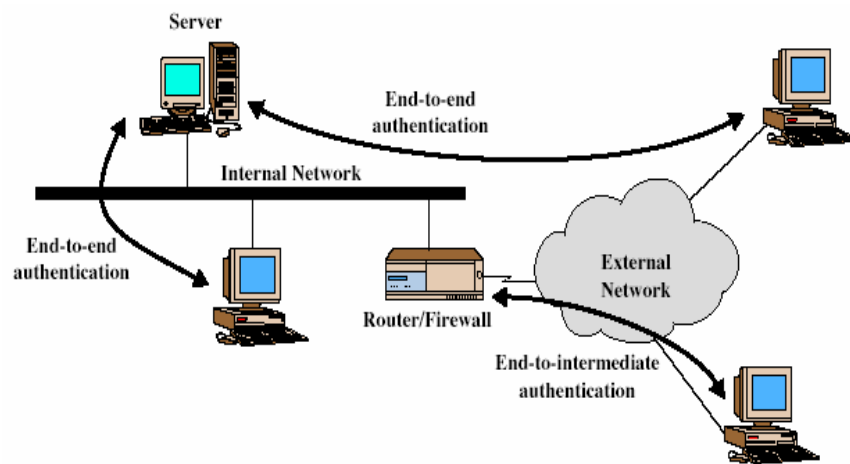
Integrity Check Value - ICV

- ❑ Message authentication code (MAC) calculated over
 - IP header field that do not change or are predictable such as Source Address, Internet Header Length
 - IPSec protocol header minus where the ICV value goes
 - Upper-level data
- ❑ Code may be truncated to first 96 bits

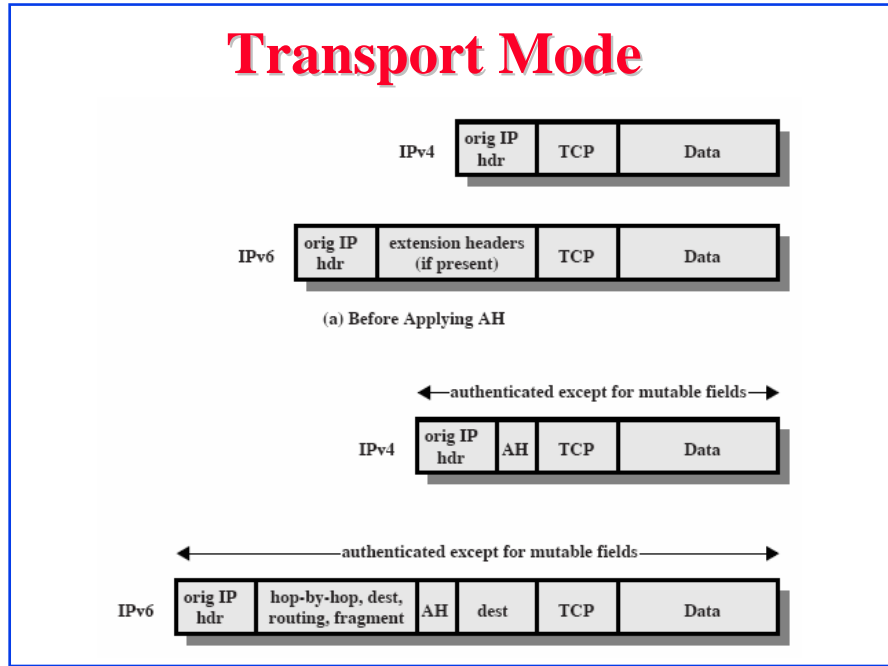
IPSec Authenticated Header



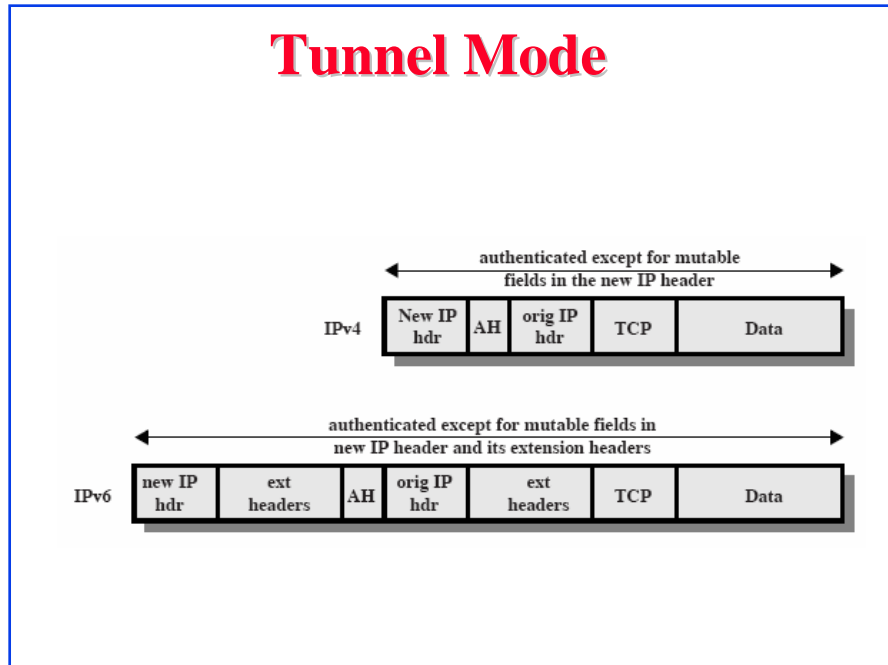
End-to-end vs. End-to-Intermediate Authentication



Transport Mode



Tunnel Mode



Encapsulated Security Protocol - ESP

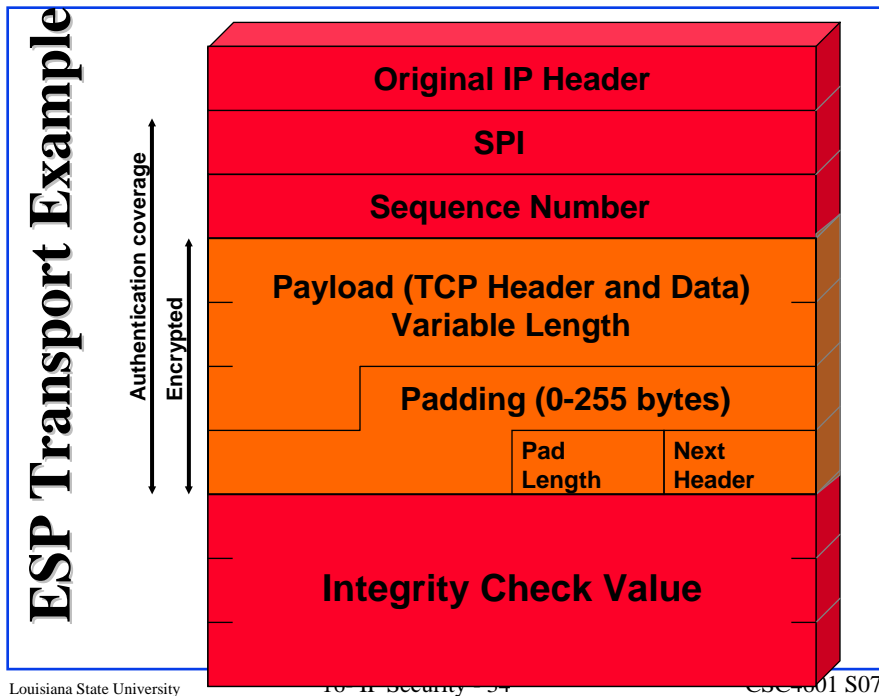
- ❑ Confidentiality for upper layer protocol
- ❑ Traffic flow confidentiality
- ❑ Data origin authentication and connectionless integrity (optional)

Outbound Packet Processing

- ❑ Form ESP payload
- ❑ Pad as necessary
- ❑ Encrypt result [payload, padding, pad length, next header]
- ❑ Apply authentication
 - Allow rapid detection of replayed/bogus packets
 - Allow potential parallel processing - decryption & verifying authentication code

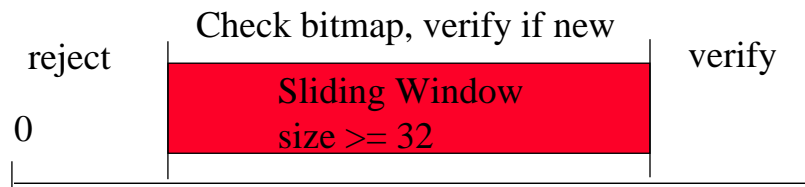
Outbound Packet Processing...

- ❑ Sequence number generation
 - Increment then use
 - With anti-replay enabled, check for rollover and send only if no rollover
 - With anti-replay disabled, still needs to increment and use but no rollover checking
- ❑ ICV calculation
 - ICV includes whole ESP packet minus *authentication data* field
 - Implicit padding of '0's between *next header* and *authentication data* is used to satisfy block size requirement for ICV algorithm



Inbound Packet Processing

- ❑ Sequence number checking
 - Anti-replay is used only if authentication is selected
 - Sequence number should be the first ESP check on a packet upon looking up an SA
 - Duplicates are rejected!



Anti-replay Feature

- ❑ Optional
- ❑ Information to enforce held in SA entry
- ❑ Sequence number counter - 32 bit for outgoing IPsec packets
- ❑ Anti-replay window
 - 32-bit
 - Bit-map for detecting replayed packets

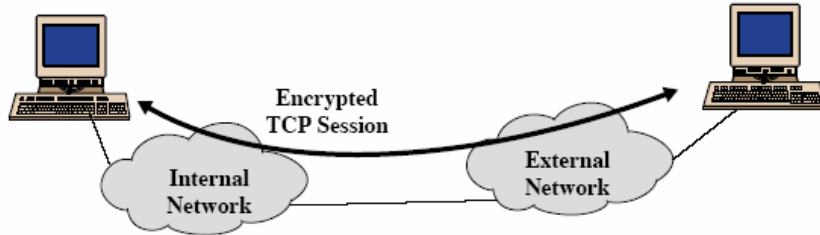
Anti-replay Sliding Window

- ❑ Window should not be advanced until the packet has been authenticated
- ❑ Without authentication, malicious packets with large sequence numbers can advance window unnecessarily
 - Valid packets would be dropped!

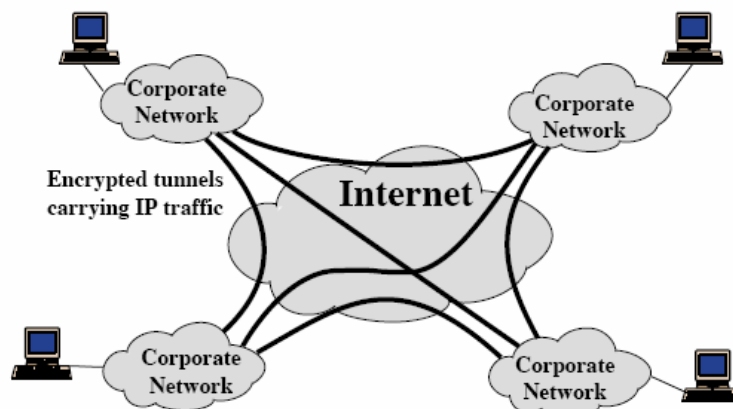
Inbound Packet Processing...

- ❑ Packet decryption
 - Decrypt quantity [ESP payload, padding, pad length, next header] per SA specification
 - Processing (stripping) padding per encryption algorithm; In case of default padding scheme, the padding field SHOULD be inspected
 - Reconstruct the original IP datagram
- ❑ Authentication verification (option)

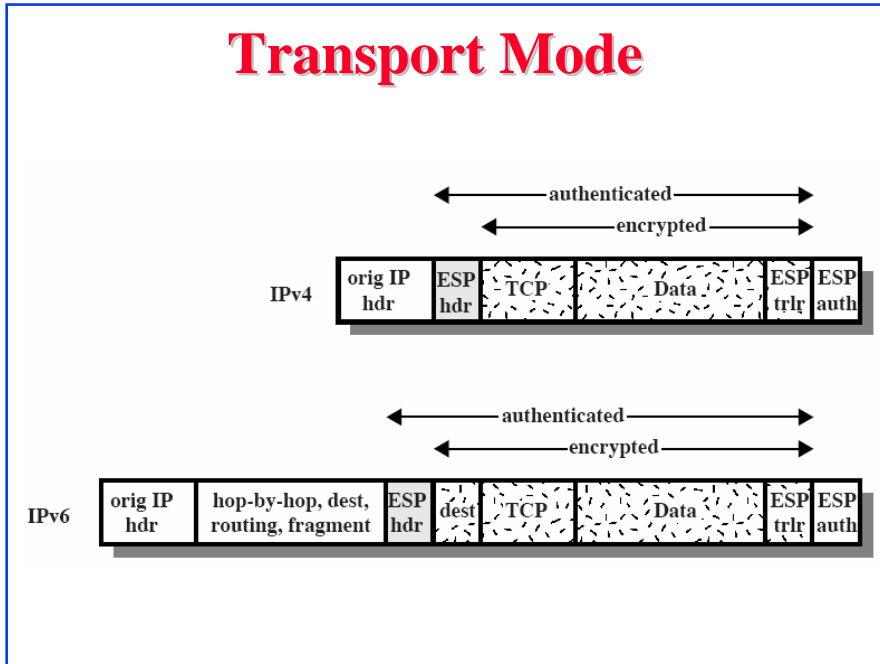
Transport Mode



Tunnel Mode

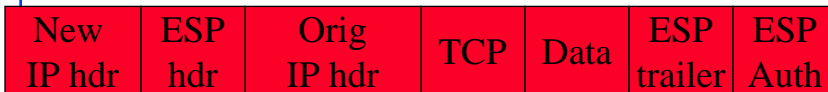


Transport Mode

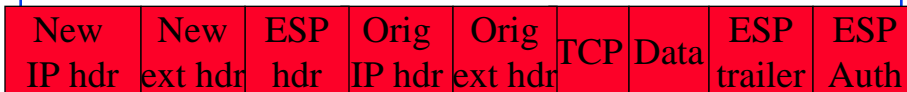


ESP Processing - Header Location...

IPv4



IPv6



- Tunnel mode IPv4 and IPv6

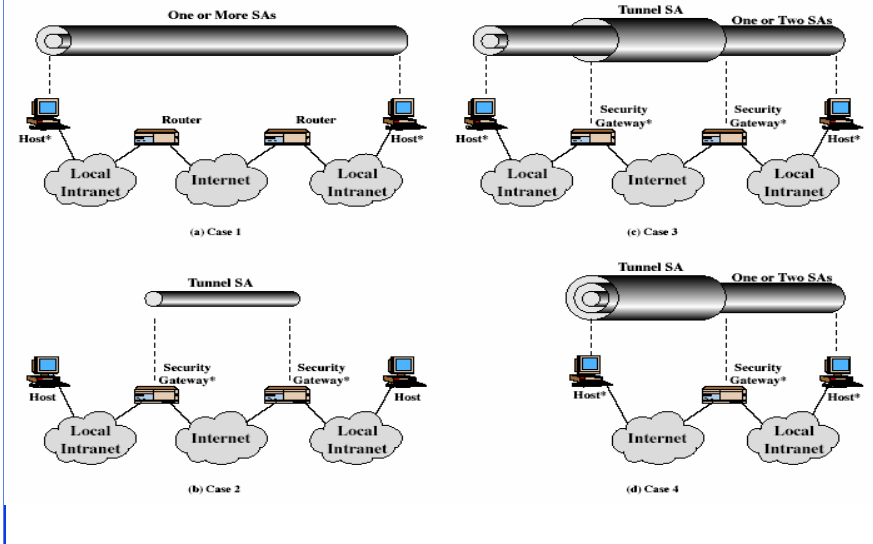
Transport vs Tunnel Mode ESP

- ❑ 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

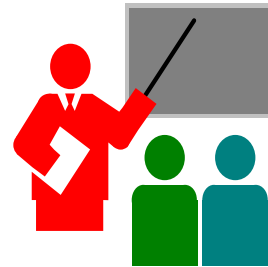
Combining Security Associations

- ❑ SA's can implement either AH or ESP
- ❑ To implement both need to combine SA's
 - form a security bundle
- ❑ Have 4 cases (see next)

Combining Security Associations



Summary



- ❑ Objectives
- ❑ IPsec architecture & concepts
- ❑ IPsec authentication header
- ❑ IPsec encapsulating security payload