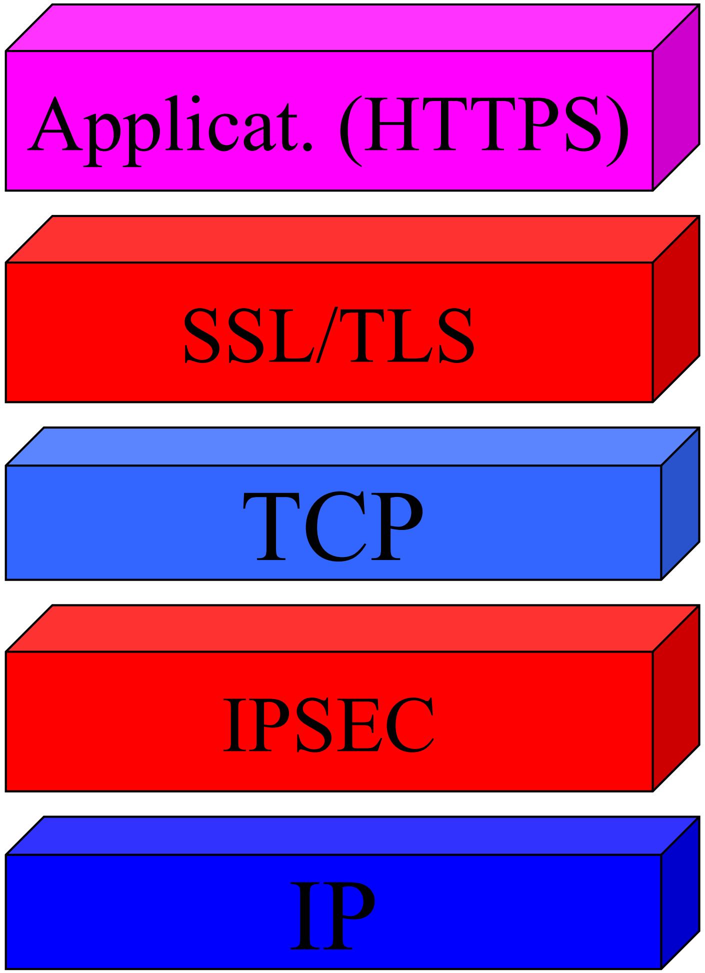
Cryptography and Network Security

IPSEC

Security architecture and protocol stack



Secure applications: PGP, HTTPS, S-HTTP, SFTP, …

or

Security down in the protocol stack

- SSL between TCP and application layer
- IPSEC between TCP and IP

Why not security on datagrams?

- Protect IP packets at each hop (there is a shared key among two routers that are connected by a link)
- Good: all traffic is encrypted (including IP headers)
- Bad:
  - Cooperation among router is required
  - Significant computational effort (when a router receives a packet decodes it, then encodes it for next hop)

IP Security

- there exist several application specific security mechanisms
  - e.g. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- it is important to have a security protocol that can be used by all applications
- IP security: security between IP and TCP

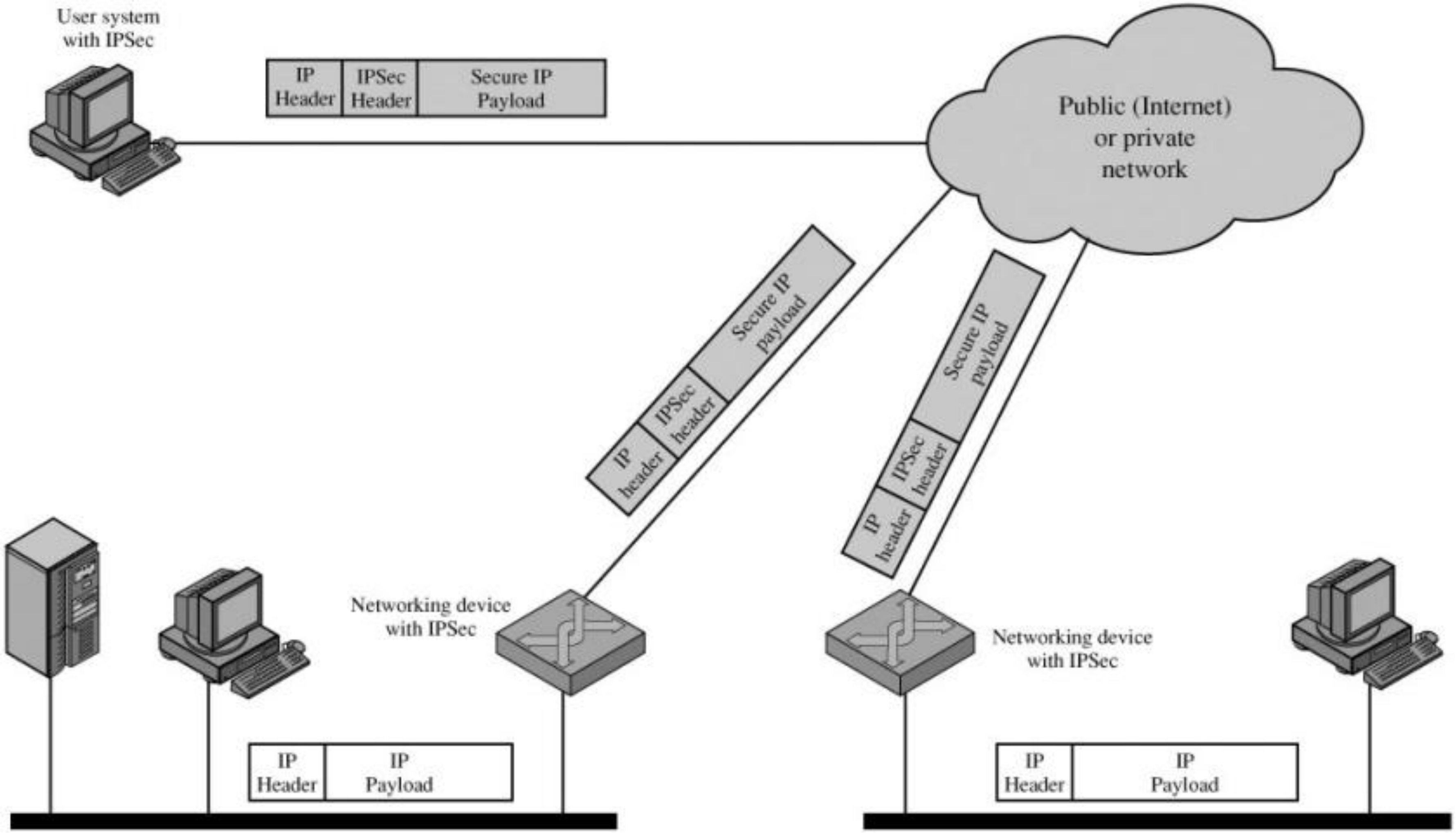
IPSec

- IP Security mechanism provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs & for the Internet
- Very complicated & articulated specification (many docs...)
- was mandatory, then optional, in IPv6
  - optional in IPv4

RFC 6434 (2011) "IPv6 Node Requirements"

Previously, IPv6 mandated implementation of IPsec and recommended the key management approach of IKE. This document updates that recommendation by making support of the IPsec Architecture [RFC4301] a SHOULD for all IPv6 nodes.

IPSec



payload = actual data carried by the headers

Benefits of IPSec

- 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 (allows to realize Virtual Private Networks)
- can provide security for individual users if desired

Practical applications of IPSec

- Secure branch office connectivity over the Internet
  - A company can build a secure virtual private network over the Internet or over a public WAN
- Secure remote access over the Internet
  - An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network

Practical applications of IPSec

- Establishing extranet and intranet connectivity with partners
  - IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism
- Enhancing electronic commerce security
  - Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security

Practical applications of IPSec

- The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level
- All distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured
  - also routing protocols could benefit

security features

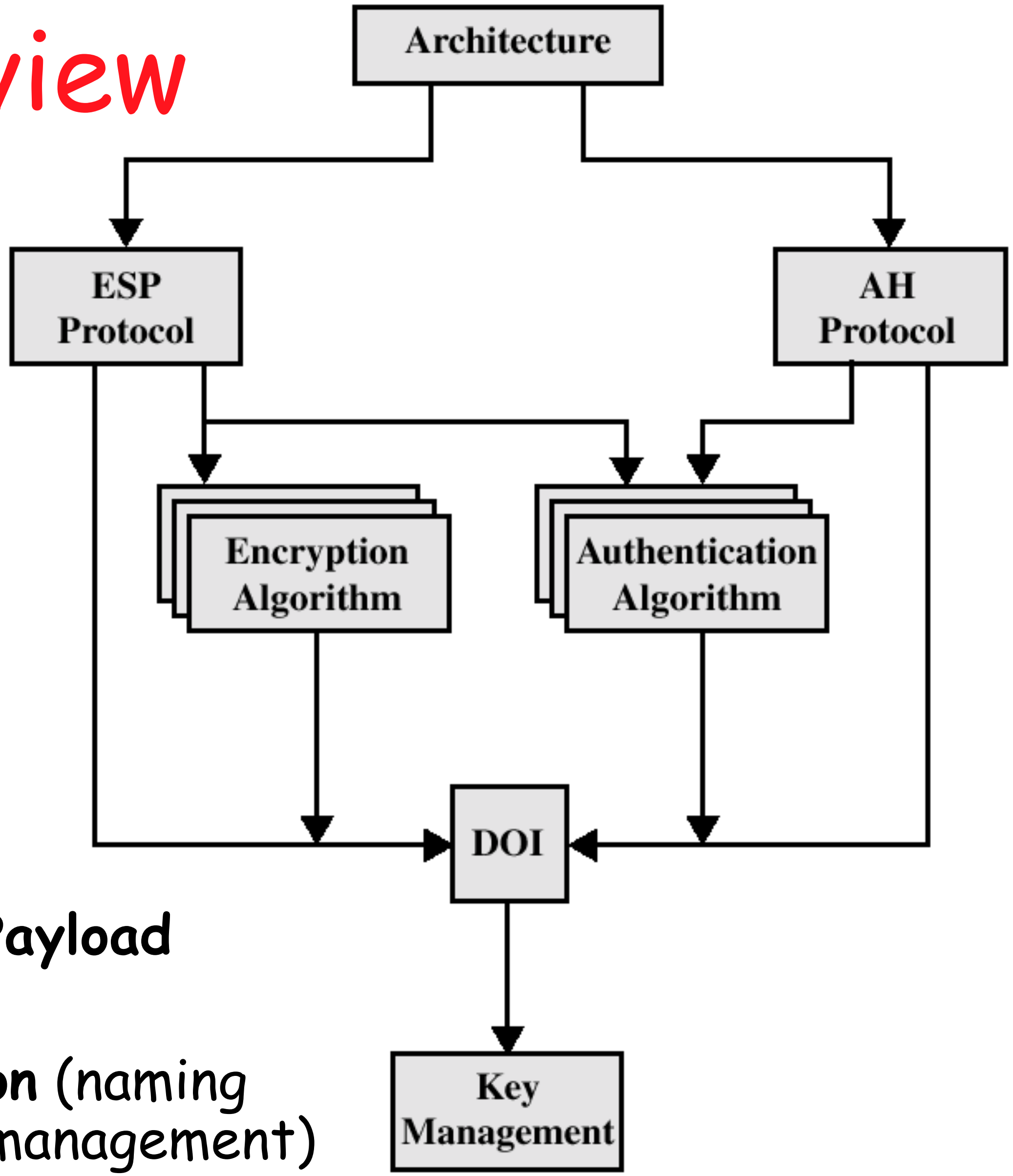
- implemented as extension headers that follow the main IP header
  - Authentication Header (AH) is the extension header for authentication
  - Encapsulating Security Payload (ESP) is the extension header for encryption

IPSec Documents

The most important (1998):

- RFC 2401: An overview of a security architecture
- RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
- RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
- RFC 2408: Specification of key management capabilities

IPSec document overview

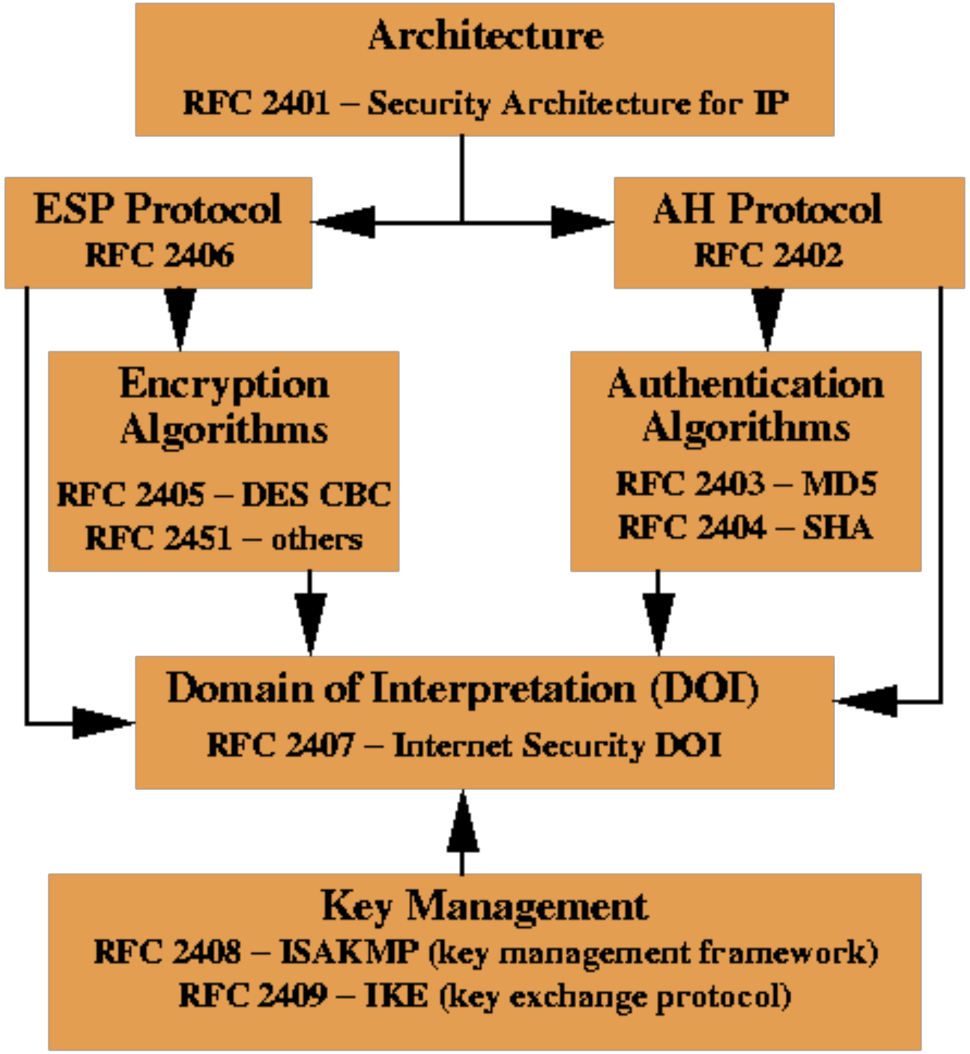


ESP = Encapsulating Security Payload

AH = Authentication Header

DOI = Domain of Interpretation (naming conventions, related to keys management)

IPsec Document Roadmap



IPSec Services

- **Access control**
  - prevents unauthorized use of a resource (computing cycles, data, network, bandwidth etc.)
- **Connectionless integrity**
  - detects modification of an individual IP datagram
- **Data origin authentication**
  - verifies the identity of the claimed source of data
- **Rejection of replayed packets**
  - a form of partial sequence integrity
- **Confidentiality (encryption)**
- **Limited traffic flow confidentiality**
  - *traffic flow confidentiality* = concealing source and destination addresses, message length, or frequency of communication

services provided by AH and ESP protocols

- For ESP, two cases: with and without the authentication option
- Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols

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

Security Associations

- A security association (SA) is a one-way relationship between sender & receiver that affords security for traffic flow
  - logical group of security parameters, that ease the sharing of information to another entity
- There is a database of Security Associations (SADB)
  - according to RFC 2401, each interface for which IPsec is enabled requires nominally separate inbound vs. outbound databases, because of the directionality
- Identified by 3 main parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier (AH or ESP)

SA, continued 1

- bi-directional traffic → flows secured by 2 SAs
- choice of encryption and authentication algorithms (from a defined list) left to IPsec administrator
- protection for outgoing packet determined by
  - Security Parameter Index (SPI)
    - conceptually similar to TCP port number
    - it enables the receiving system to select the SA under which a received packet will be processed
  - destination address in packet header
- similar procedure for incoming packets, where IPsec gathers decryption and verification keys from SADB

SA, continued 2

- For multicast, SA is provided for the group, and is duplicated across all authorized receivers of the group.
- There may be more than one SA for a group, using different SPIs, thereby allowing multiple levels and sets of security within a group.
- Note that the relevant standard does not describe how the association is chosen and duplicated across the group; it is assumed that a responsible party will have made the choice.

SA's parameters

- Sequence Number Counter
  - 32-bit value used to generate the Sequence Number field in AH or ESP headers
- Sequence Counter Overflow
  - flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA
- Anti-Replay Window
  - used to determine whether an inbound AH or ESP packet is a replay

SA's parameters

- AH Information
  - Authentication algorithm, keys, key lifetimes, and related parameters being used with AH
- ESP Information
  - Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP

SA's parameters

- Lifetime of This Security Association
  - A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur
- IPSec Protocol Mode
  - Tunnel, transport, or wildcard
- Path MTU
  - Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables

Security Policy Database and SA selectors

- Entries in the Security Policy Database (SPDB) discriminate traffic: either IPSec protection, or bypass IPSec
  - each entry is defined by a set of IP and upper-layer protocol field values, called *selectors*
  - each entry points to an SA for that traffic (in general, it is possible a many-to-many relationship)
- Selectors are used to filter traffic in order to map it into a particular SA. Outbound processing obeys the following general sequence for each IP packet:
  1. Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry, which will point to zero or more SAs.
  2. Determine the SA (if any) for this packet and its associated SPI
  3. Do the required IPSec processing (i.e., AH or ESP processing)

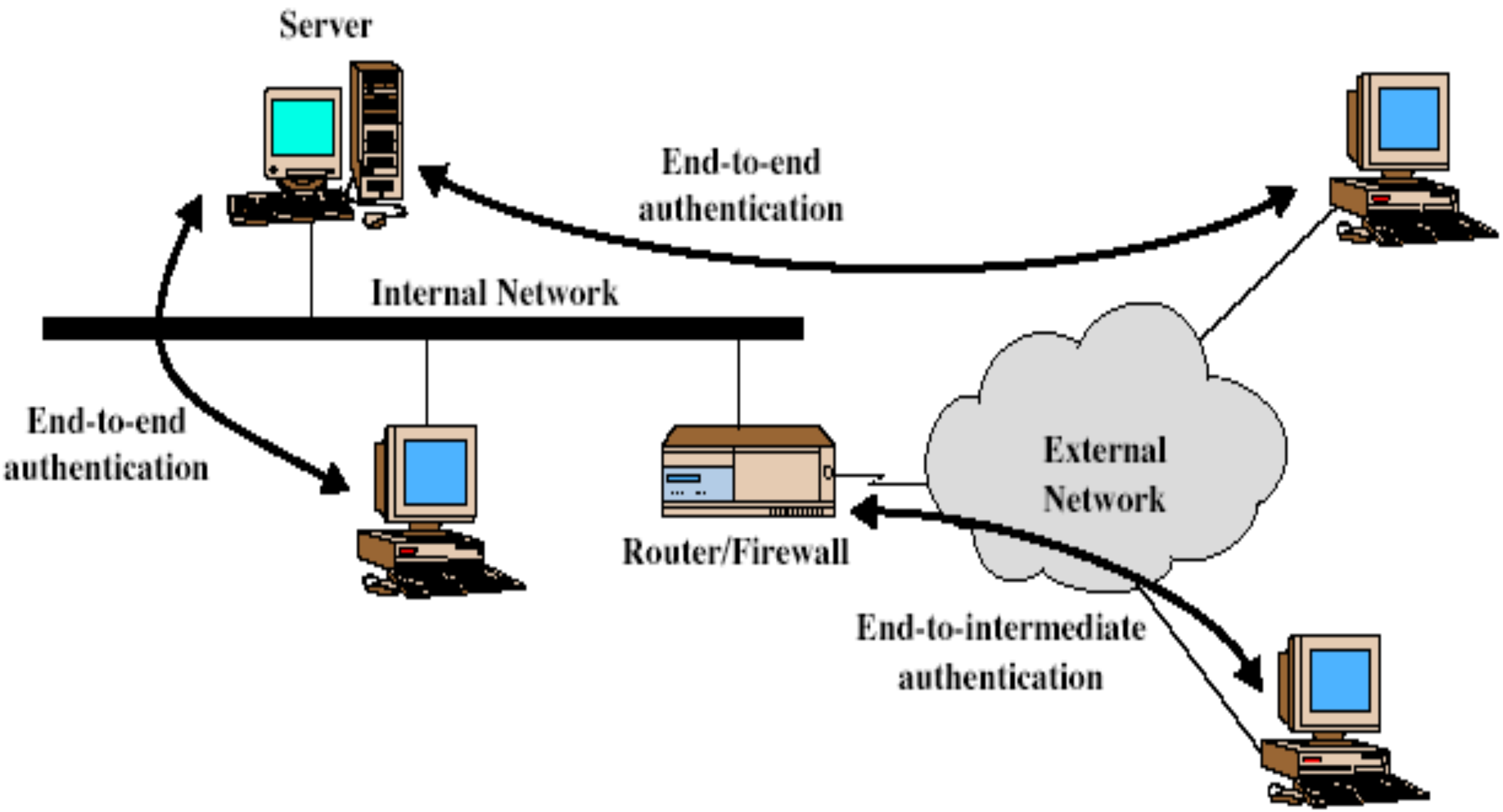
SA selectors

- **Destination IP Address**
  - a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address
- **Source IP Address**
  - a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address
- **UserID**
  - a user identifier from the operating system
  - 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
- **Data Sensitivity Level**
  - used for systems providing information flow security (e.g., *secret* or *unclassified*)
- **Transport Layer Protocol**
  - from IPv4 or IPv6, may be an individual protocol number, a list of protocol numbers, or a range of protocol numbers
- **Source and Destination Ports**
  - may be individual TCP/UDP port values, an enumerated list of ports, or a wildcard port

SADB vs SPDB

- SPDB specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or a security gateway
- SADB is a security association table, containing parameters of the security associations

Transport & Tunnel Modes



Transport mode summary

- Transport mode: original IP header not touched; IPsec information added between IP header and packet body
  - IP header | IPsec | $\underbrace{\text{[packet]}}_{\text{protected}}$
  - Most logical when IPsec used end-to-end

Tunnel mode summary

- <u>Tunnel mode</u>: keep original IP packet intact but protect it; add new header information outside
  - $\text{New IP header} \mid \underbrace{\text{IPsec} \mid \underbrace{[\text{ old IP header} \mid \text{packet }]}_{\text{encrypted}}}_{\text{authenticated}}$
  - Can be used when IPSec is applied at intermediate point along path (e.g., for firewall-to-firewall traffic)
    - Treat the link as a secure tunnel
  - Results in slightly longer packet

Transport mode

- Used for host-to-host communications
- Only payload (the data you transfer) of IP packet is encrypted and/or authenticated
- Routing is intact, since the IP header is neither modified nor encrypted
  - however, when the authentication header is used, the IP addresses cannot be translated (NAT), as this will invalidate the hash value

Transport mode, continued

- Transport and application layers are always secured by hash, so they cannot be modified in any way (for example by translating the port numbers)
- A means to encapsulate IPsec messages for NAT traversal has been defined (see RFCs 3715, 3947, 3948), describing the NAT-T mechanism

Tunnel mode

- The entire IP packet (data and IP header) is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header.
- Tunnel mode is used to create Virtual Private Networks (VPN) for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access), and host-to-host communications (e.g. private chat)

Transport & tunnel modes

Tunnel & Transport Mode Functionality

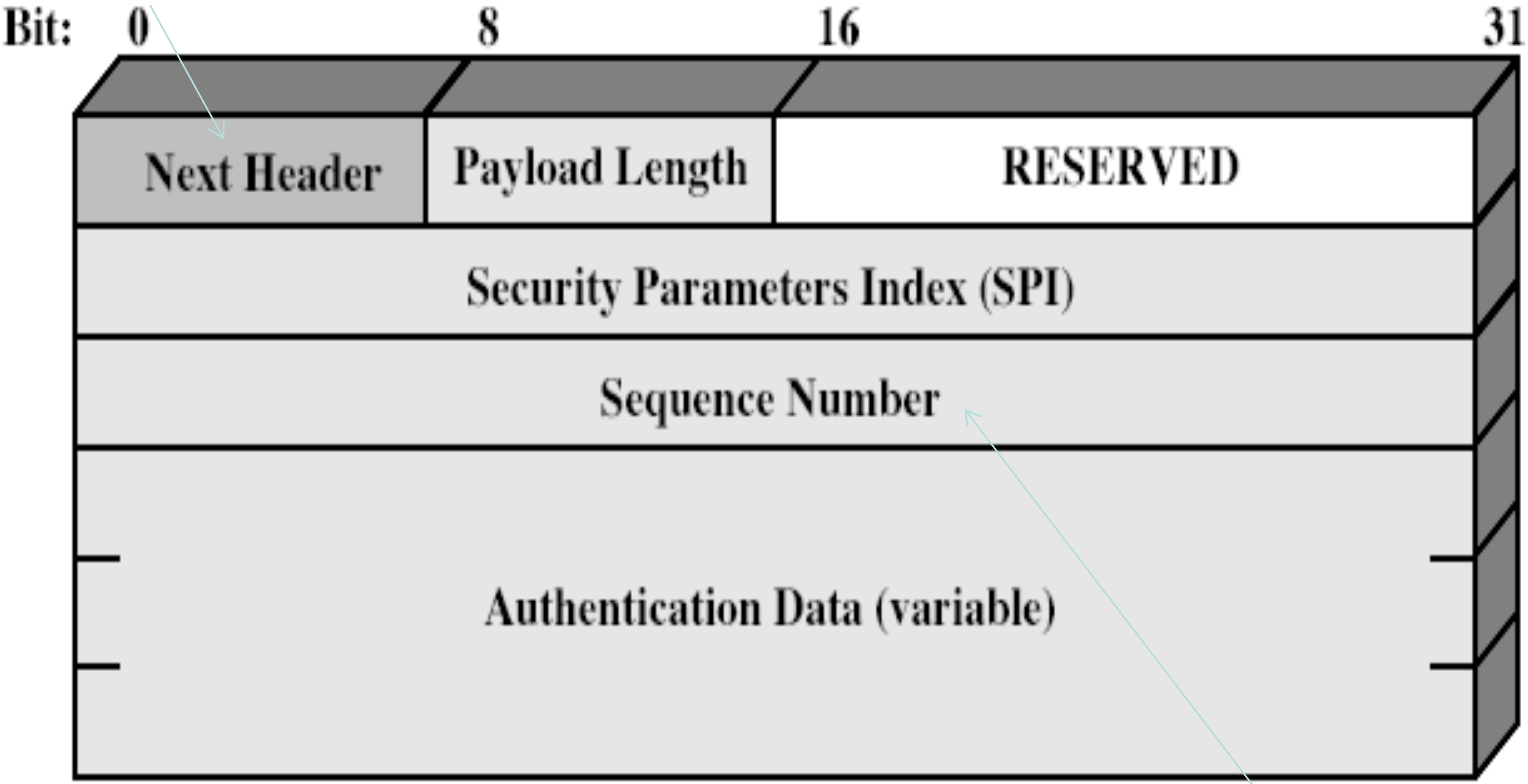
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 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.

Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- does not provide support for confidentiality
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- users must share a secret key

Authentication Header

higher level protocol,
e.g. TCP



not restarting

AH protocol

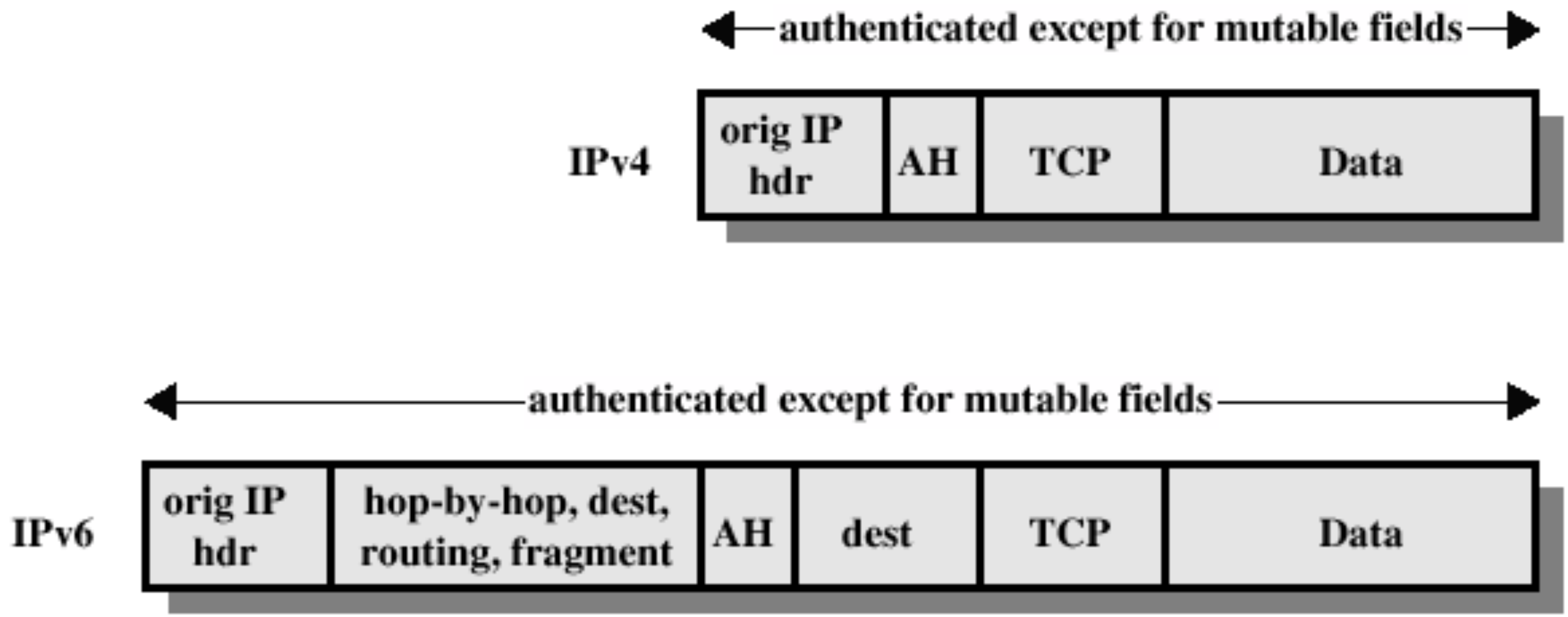
- AH protects the IP payload and all header fields of an IP datagram except for mutable fields
  - In IPv4, mutable (and therefore unauthenticated) IP header fields include TOS, Flags, Fragment Offset, TTL and Header Checksum.
- AH operates directly on top of IP, using IP protocol number 51

HMAC (from RFC 2104)

- **H**(·) be a cryptographic hash function
  - e.g., MD5, SHA-1
- *K* be a secret key padded to the right with extra zeros to the block size of the hash function
- *m* be the message to be authenticated
- // denote concatenation
- ⊕ denote exclusive or (XOR)
- opad be the outer padding (0x5c5c5c…5c5c, one-block-long hexadecimal constant)
- ipad be the inner padding (0x363636…3636, one-block-long hexadecimal constant)

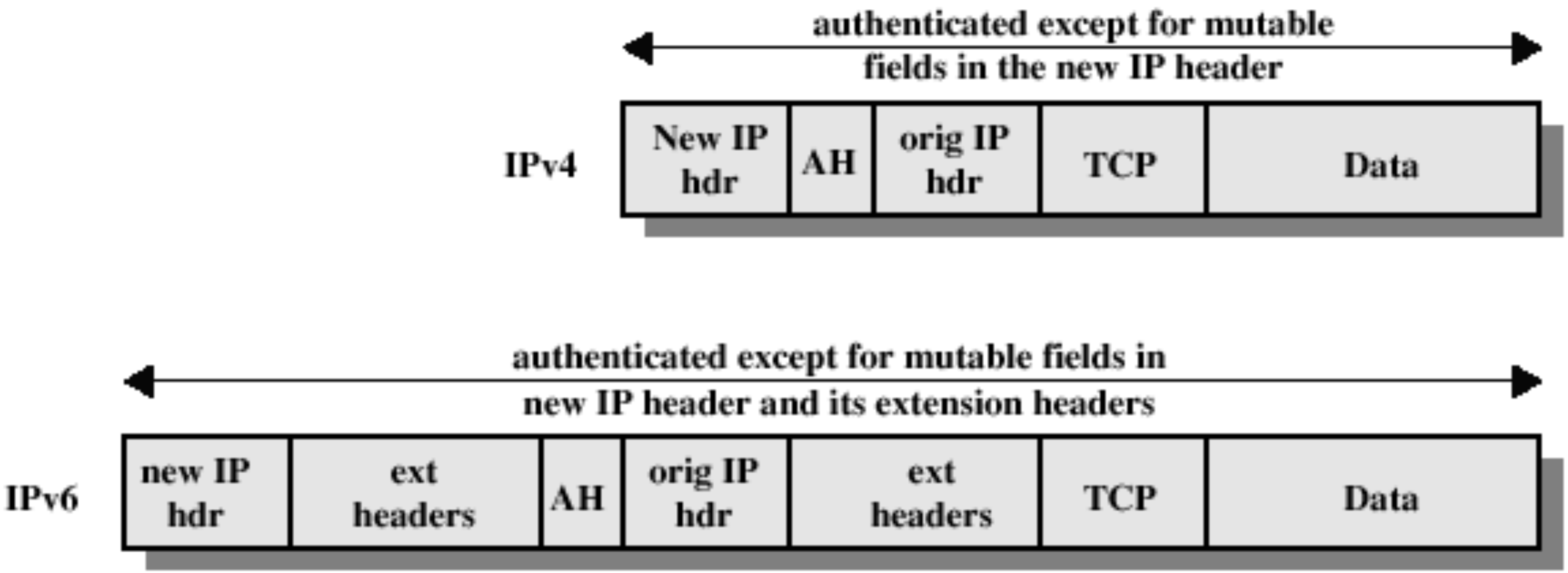
$$\mathbf{HMAC}(K,m) = \mathbf{H}((K \oplus \mathrm{opad}) \;//\; \mathbf{H}((K \oplus \mathrm{ipad}) \;//\; m))$$

Authentication Header (AH): transport mode



Note that only part of the header is authenticated

Authentication Header (AH): tunnel mode

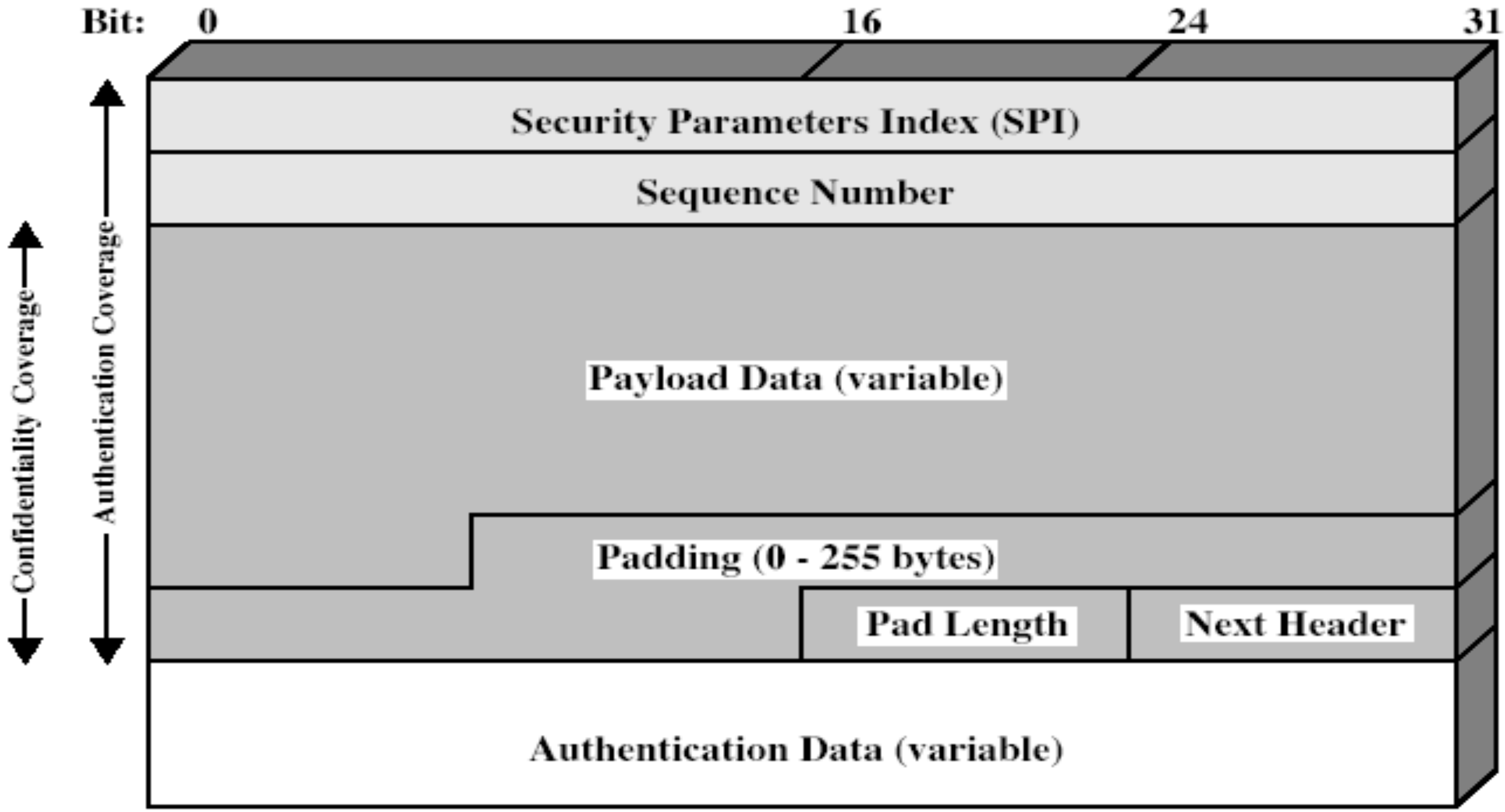


Note that only part of the header is authenticated

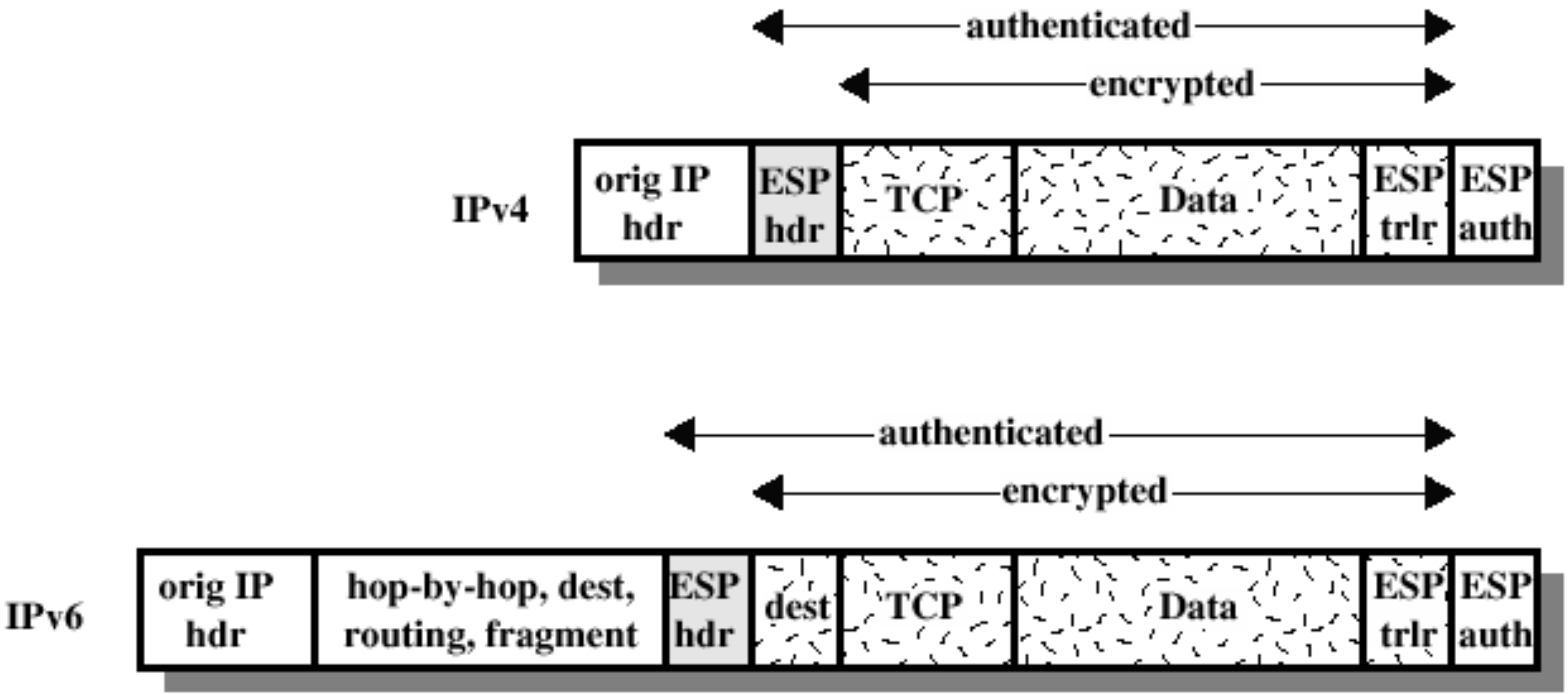
Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - AES, DES, Triple-DES, Blowfish etc
  - CBC most common
  - padding to meet blocksize of the packet
  - HMAC (same as AH)

Encapsulating Security Payload

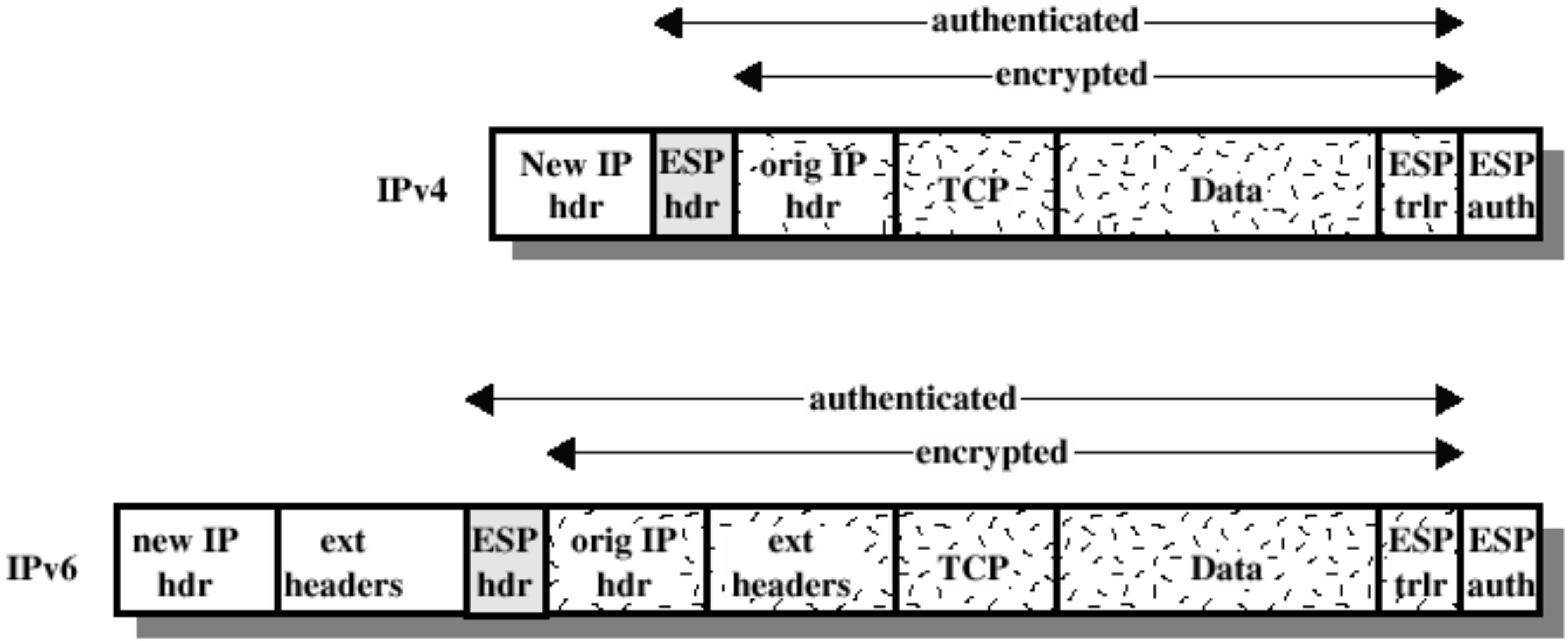


ESP - encoding and authentication: Transport mode



(a) Transport Mode

ESP - encoding and authentication: Tunnel mode

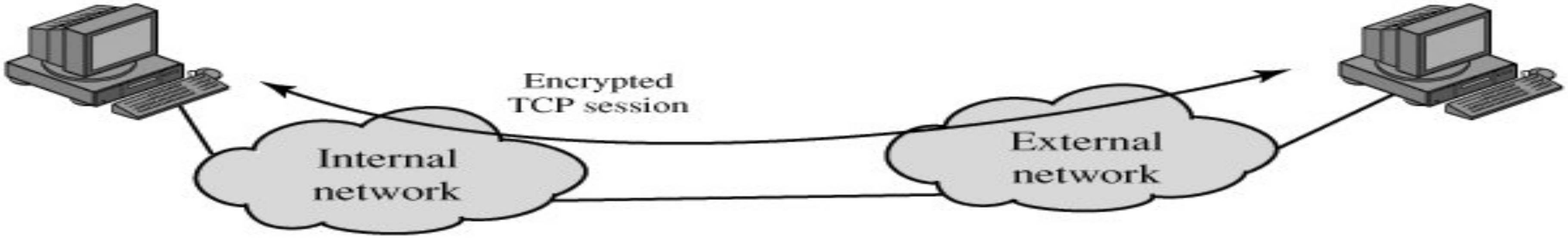


(b) Tunnel Mode

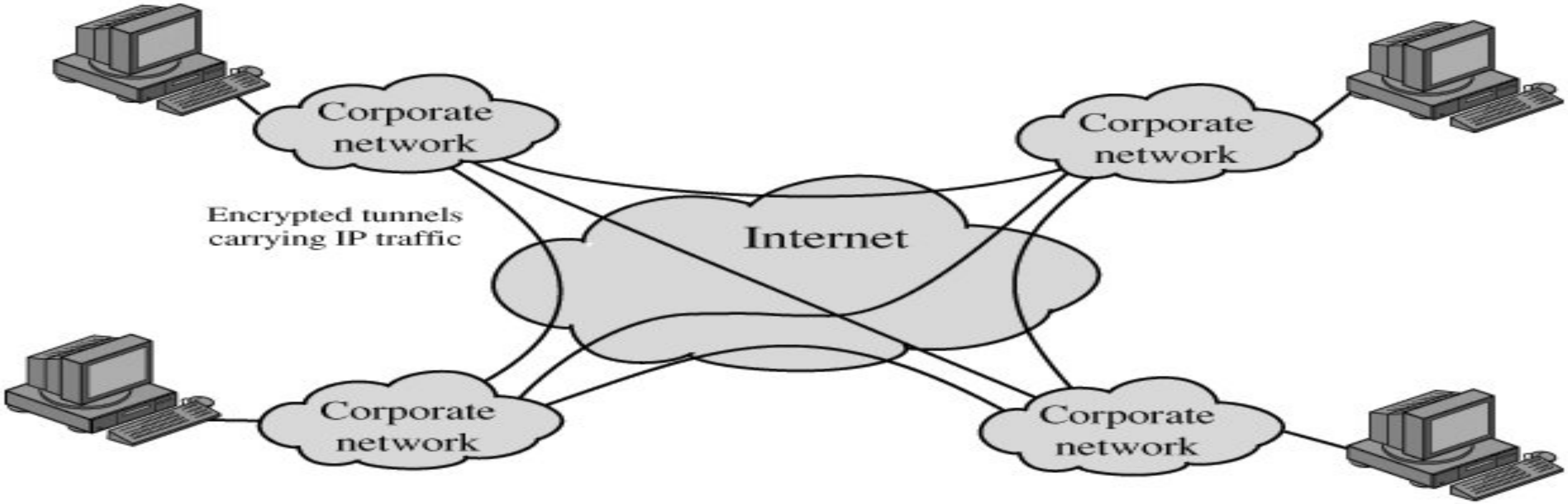
Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - adversary can try traffic analysis
  - good for host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - slow
  - good for VPNs (Virtual Private Networks, gateway to gateway security)

Transport vs Tunnel Mode ESP



(a) Transport-level security

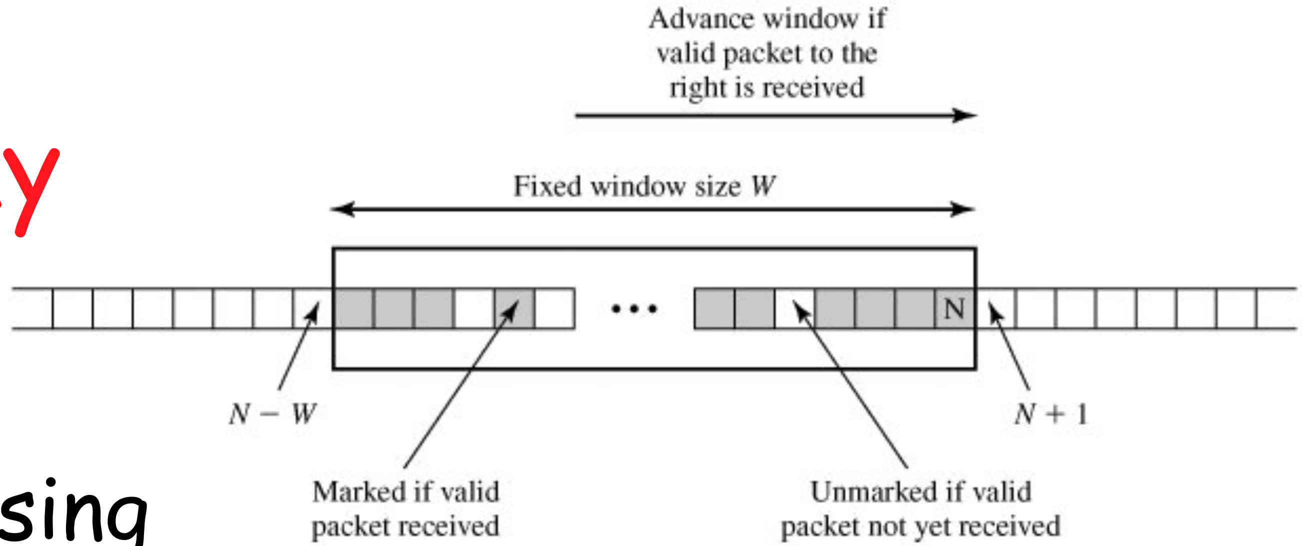


(b) A virtual private network via tunnel mode

Anti-Replay Service

- when new SA is established, sender initializes a sequence number counter to 0
- for each packet sent on this SA, sender increments the counter and places the value in the Sequence Number field
  - the first value to be used is 1
  - 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 packets with the same sequence number
  - if the limit of $2^{32} - 1$ is reached, sender should terminate this SA and negotiate a new SA with a new key
- IP does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered
- receiver should implement window of size W, with a default of W = 64: right edge of window represents highest sequence number, N, so far received for a valid packet
- for any packet with a sequence number in [N – W + 1, N] that has been properly authenticated, the corresponding slot in the window is marked

Anti-replay



inbound processing

1. if received packet falls within window and is new, then MAC is checked; if check OK, then corresponding slot in window is marked
2. if packet is to the right of the window and is new, then MAC is checked; if OK, window is advanced and the corresponding slot in the window is marked
3. if packet is to the left of the window, or if authentication fails, packet is discarded; this is an auditable event

Combining Security Associations

- SAs can implement either AH or ESP
- to implement both need to combine SAs and form a security bundle; two ways:
  - transport adjacency
    - applying more than one protocol to same IP packet, without tunneling
    - only one level of combination, further nesting yields no added benefit
  - iterated tunneling
    - application of multiple layers of security effected through IP tunneling
    - allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPsec site along the path
- the two approaches can be combined, for example, by having a transport SA between hosts travel part of the way through a tunnel SA between security gateways

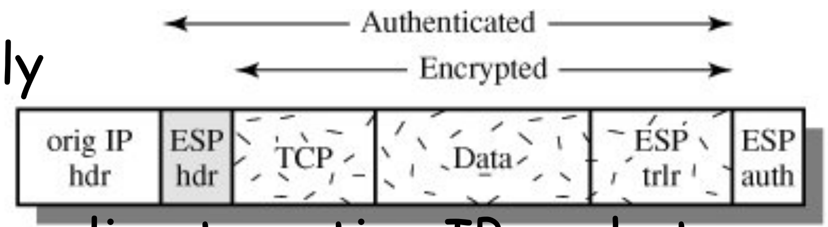
Authentication plus confidentiality

Encryption and authentication can be combined in order to transmit a packet that has both confidentiality and authentication. Several approaches:

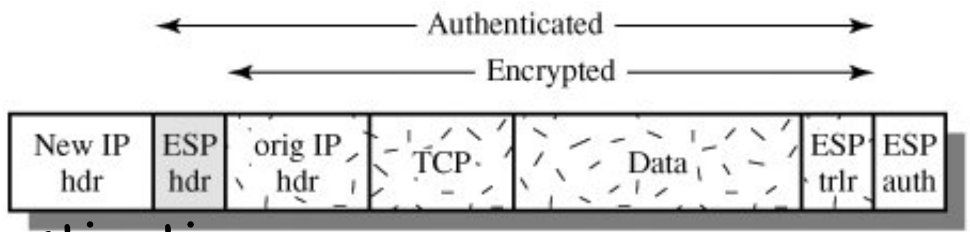
- ESP with authentication option
- Transport adjacency
- Transport-tunnel bundle

ESP with authentication option

- user first applies ESP to data to be protected, then appends the authentication data field. Two subcases:
  - **Transport mode ESP** Authentication and encryption apply to IP payload delivered to the host, but IP header not protected



  - **Tunnel mode ESP** Authentication applies to entire IP packet delivered to outer IP destination address and authentication is performed at that destination. Entire inner IP packet is protected by the privacy mechanism, for delivery to the inner IP destination

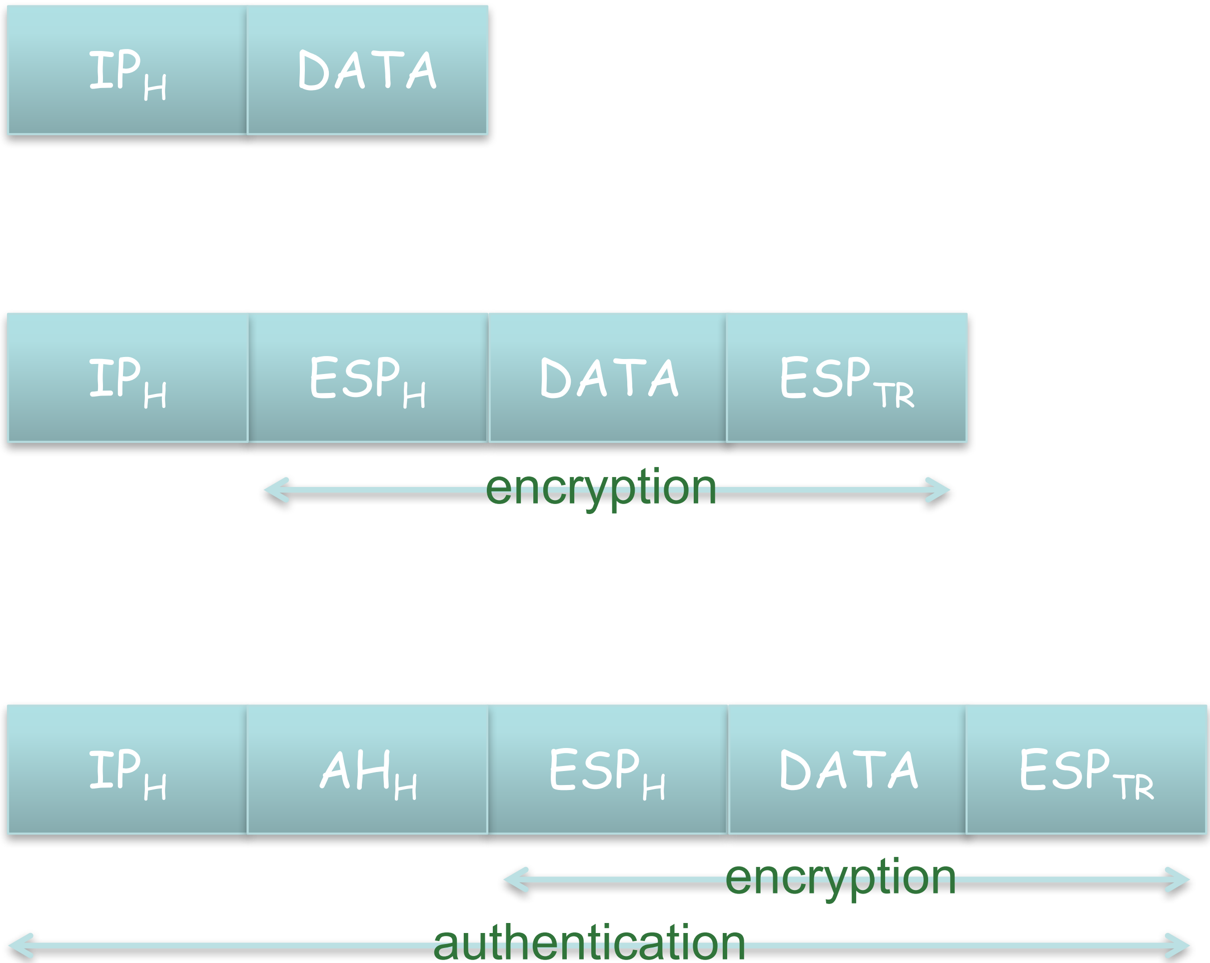


- *For both cases, authentication applies to the ciphertext rather than the plaintext (authentication after encryption)*

Transport adjacency

- still authentication after encryption
- two bundled **transport** SAs
  - inner = ESP (no authentication)
  - outer = AH
- encryption is applied to IP payload and resulting packet is IP header + ESP
- AH is then applied in transport mode, so that authentication covers the ESP + original IP header (except for mutable fields)
- advantage over ESP + authentication: *authentication covers more fields*, including source and destination IP addresses
- disadvantage: overhead (two SAs versus one SA)

Transport adjacency



What about authentication first?

authentication prior to encryption might be *preferable* for two reasons

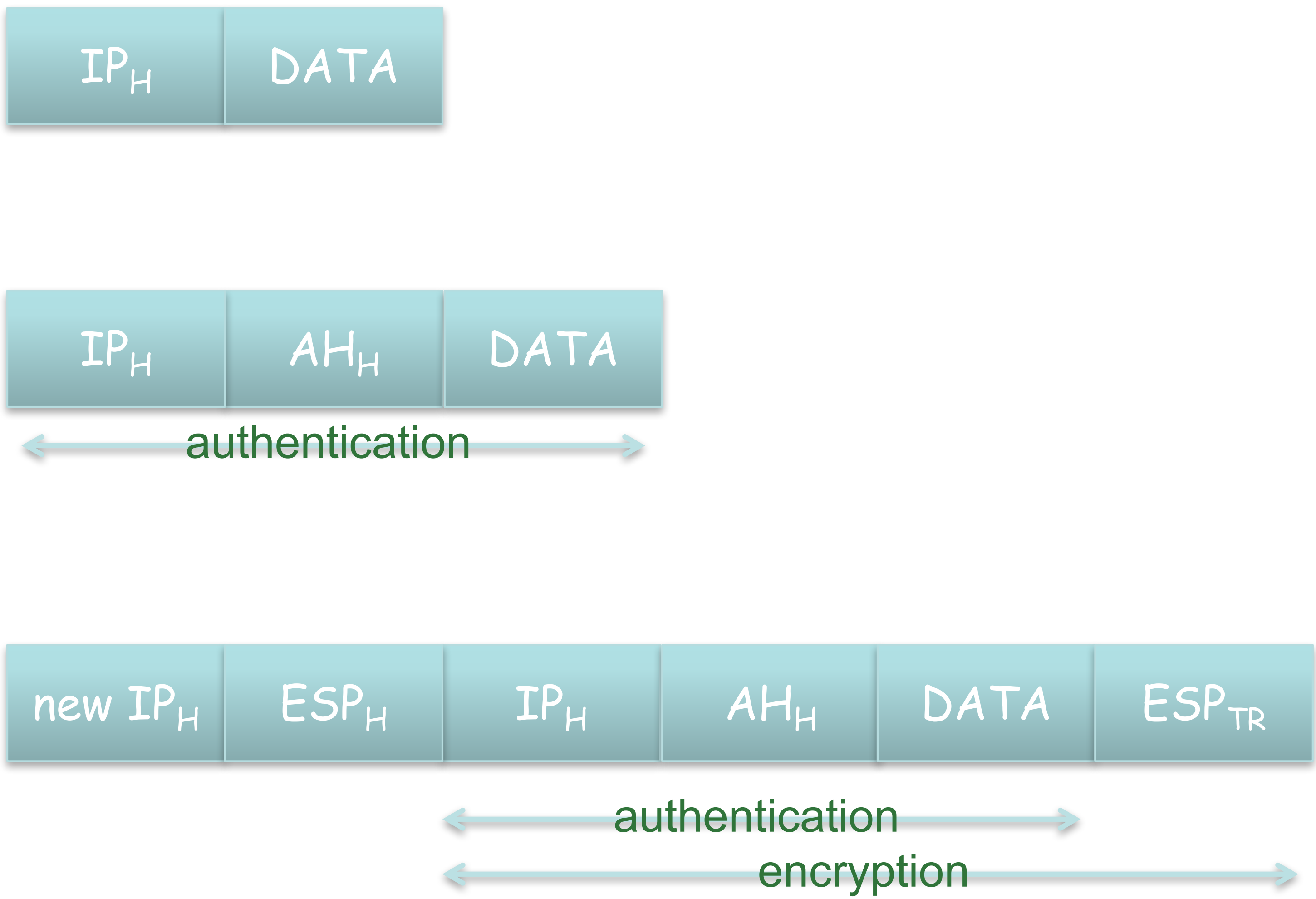
- since authentication data are protected by encryption, it is impossible to alter authentication data without decryption
- if message is stored as plaintext then verifying authentication data requires re-encryption

Transport-tunnel bundle

authentication before encryption between two hosts

- use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
- authentication is applied to IP payload plus the IP header except for mutable fields
- resulting 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

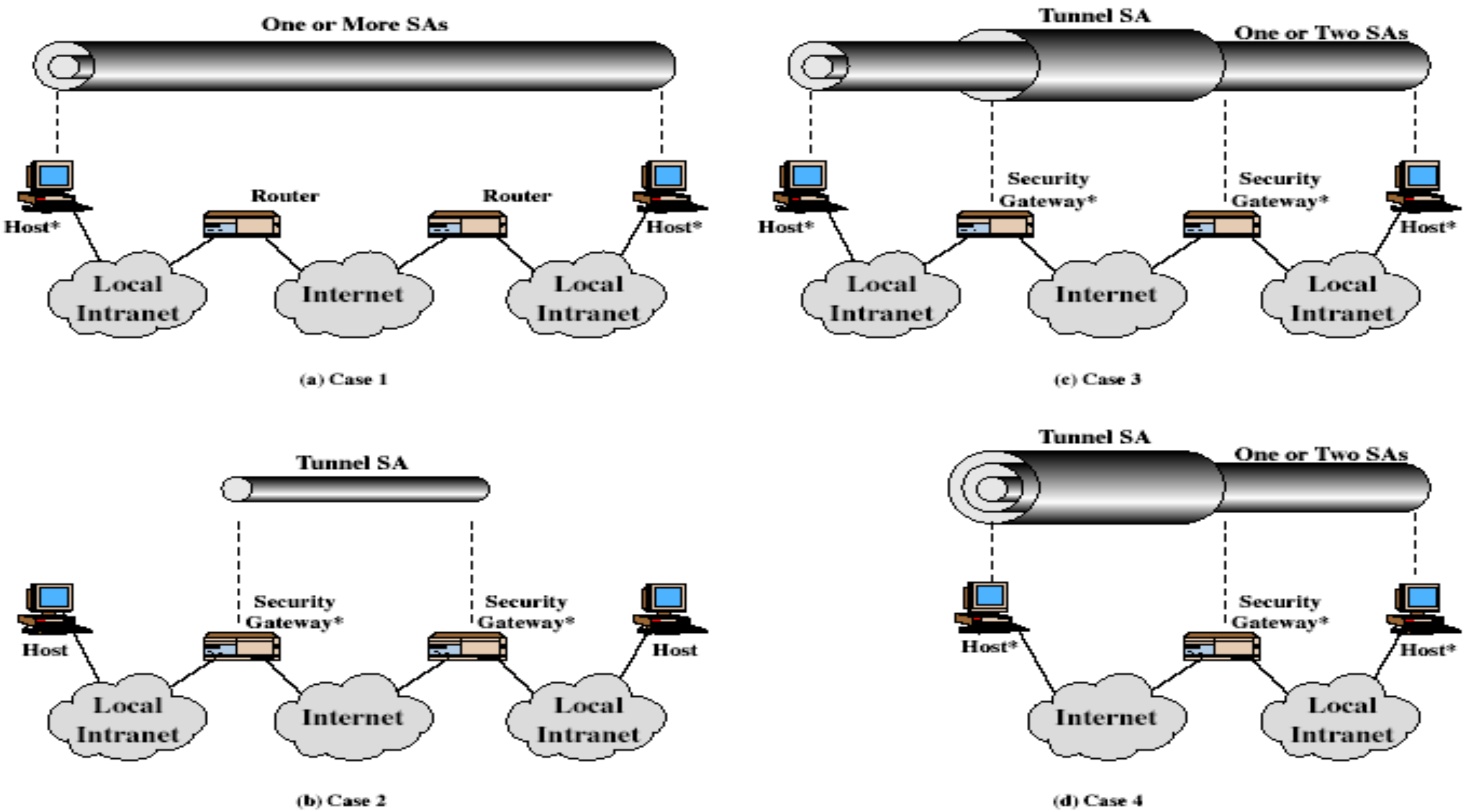
Transport-tunnel bundle



Combining Security Associations

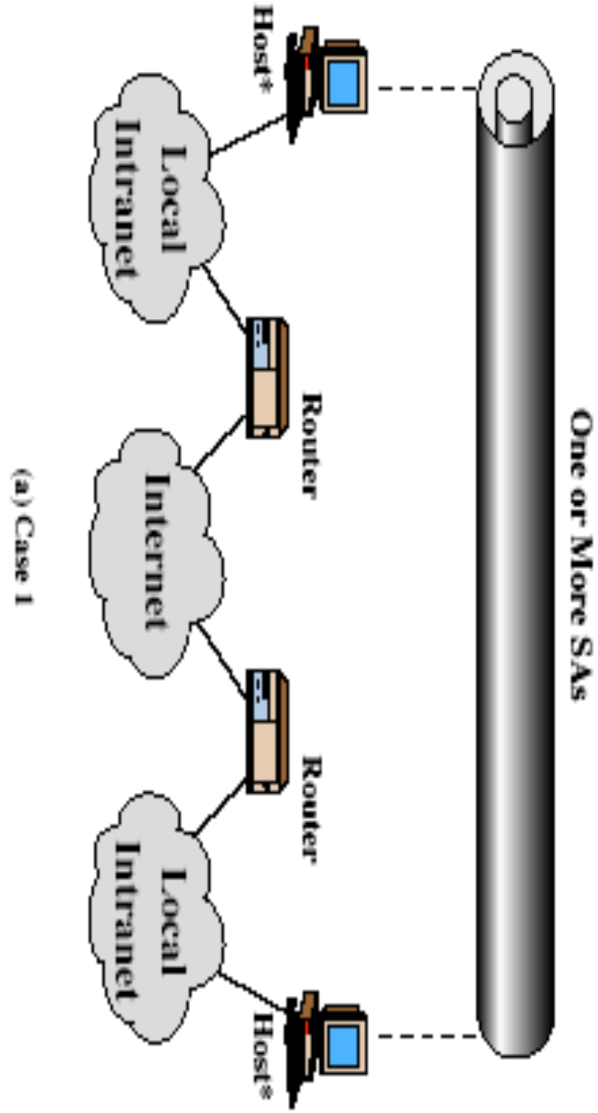
The IPSec Architecture document lists four examples of combinations of SAs that must be supported by compliant IPSec hosts (e.g., workstation, server) or security gateways (e.g. firewall, router)

Combining Security Associations



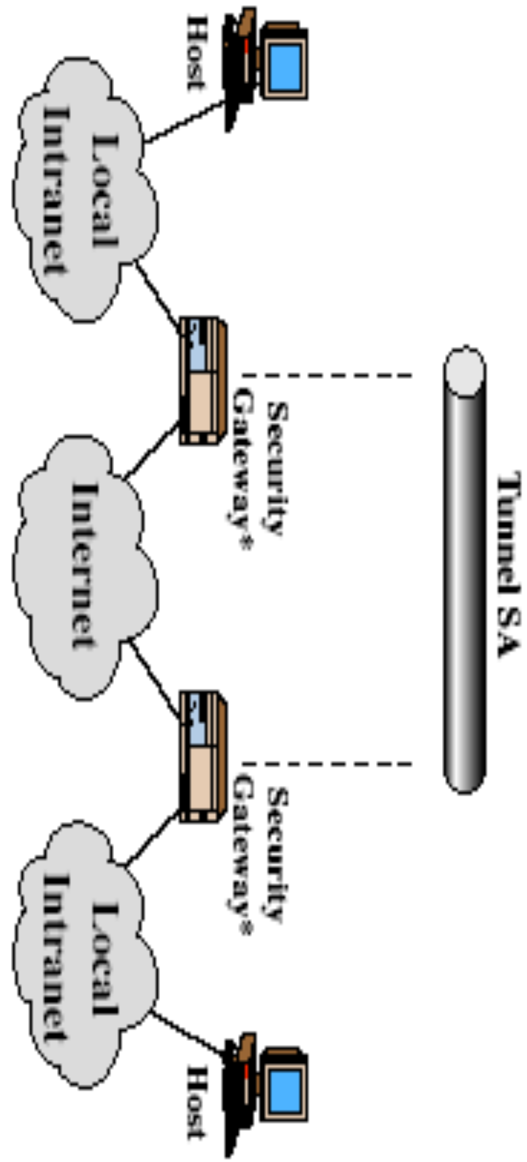
case 1

- All security is provided between end systems that implement IPSec.
- For any two end systems to communicate via an SA, they must share the appropriate secret keys.
- Among the possible combinations:
  - AH in transport mode
  - ESP in transport mode
  - ESP followed by AH in transport mode (an ESP SA inside an AH SA)
  - Any one of the preceding, inside an AH or ESP in tunnel mode
- Support for
  - authentication
  - encryption
  - authentication before encryption
  - authentication after encryption



case 2

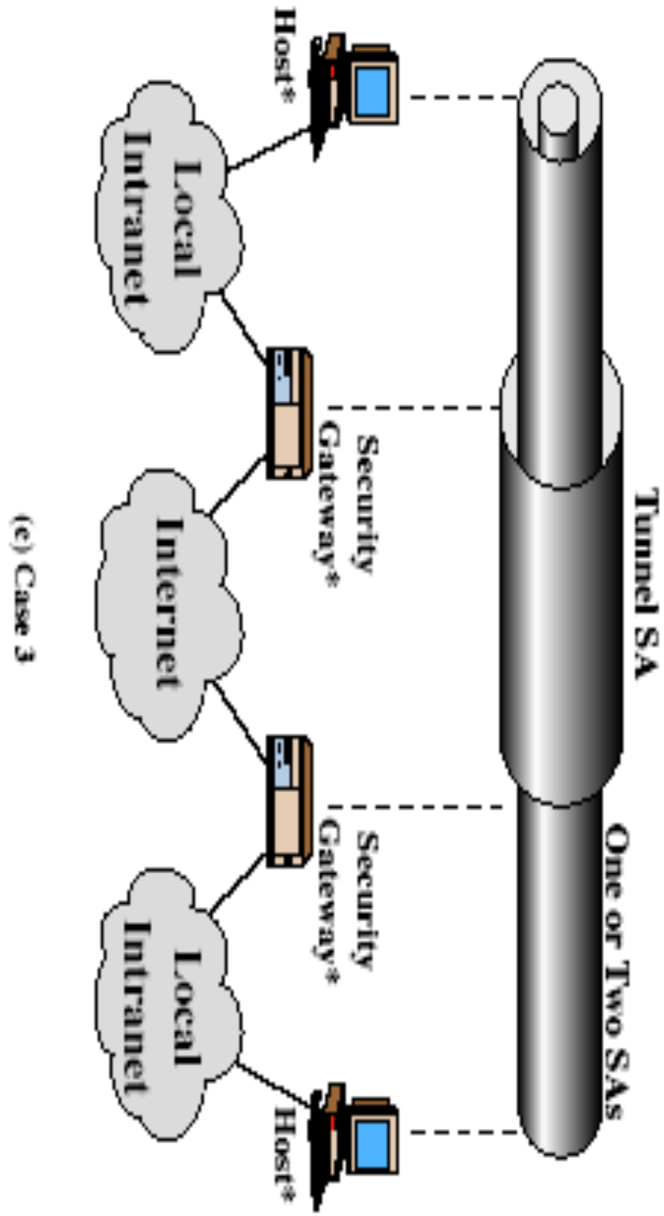
- Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPSec (simple virtual private network support)
- The security architecture document specifies that only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required because the IPSec services apply to the entire inner packet.



(b) Case 2

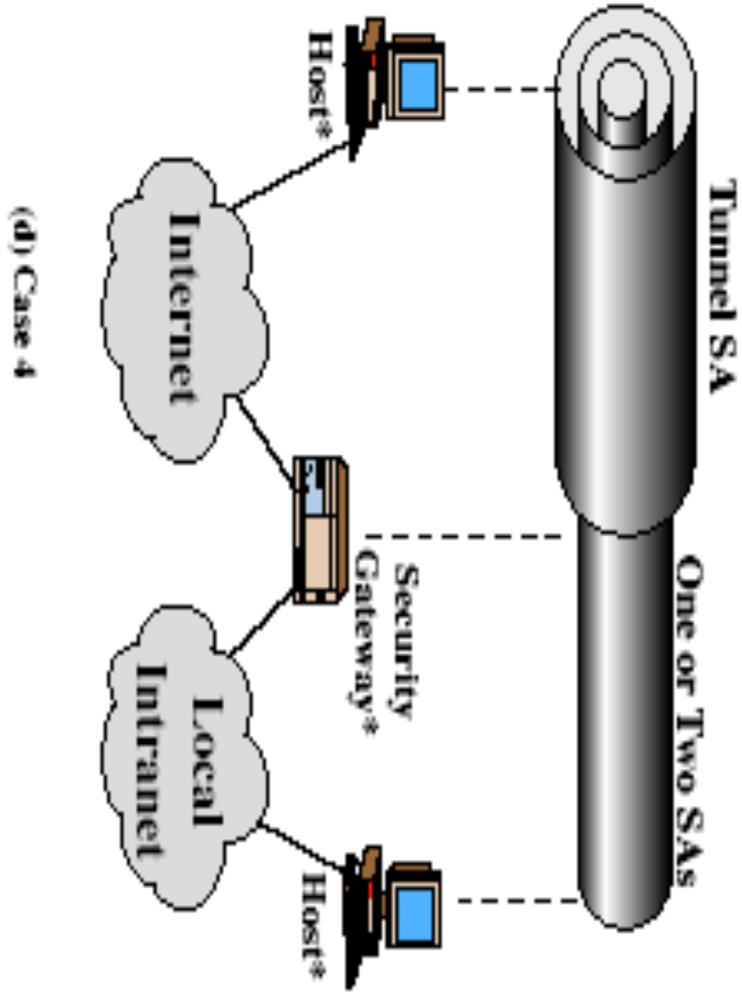
case 3

- Builds on Case 2 by adding end-to-end security. Same combinations discussed for cases 1 and 2 are allowed
- Gateway-to-gateway tunnel provides either authentication or confidentiality or both for all traffic between end systems
- When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality.
- Individual hosts can implement any additional IPSec services required for given applications or given users by means of end-to-end SAs



case 4

- Provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall
- Only tunnel mode is required between the remote host and the firewall. As in Case 1, one or two SAs may be used between the remote host and the local host



Key Management

- IPSEC handles key generation & distribution
- typically needs 2 pairs of keys
  - transmit and receive pair for both AH & ESP
- manual key management (mandatory)
  - system administrator manually configures every system
- automated key management (mandatory)
  - 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
- has Oakley & ISAKMP elements

Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify & delete SAs
- independent of key exchange protocol, encryption alg & authentication method

GDOI

- Group Domain of Interpretation or GDOI is a cryptographic protocol for group key management.
- The GDOI protocol is specified in an IETF Proposed Standard, RFC 3547, and is based on Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, and Internet Key Exchange version 1 (IKE).
- Whereas IKE is run between two peers to establish a "pair-wise security association", GDOI protocol is run between a group member and a "group controller/key server" (controller) and establishes a security association among two or more group members.

Summary

- have considered:
  - IPSec security framework
  - AH
  - ESP
  - key management & Oakley/ISAKMP