

Network Security

(6CCS3NSE – 7CCSMNSE)

Diego Sempredoni

Department of Informatics
King's College London, UK

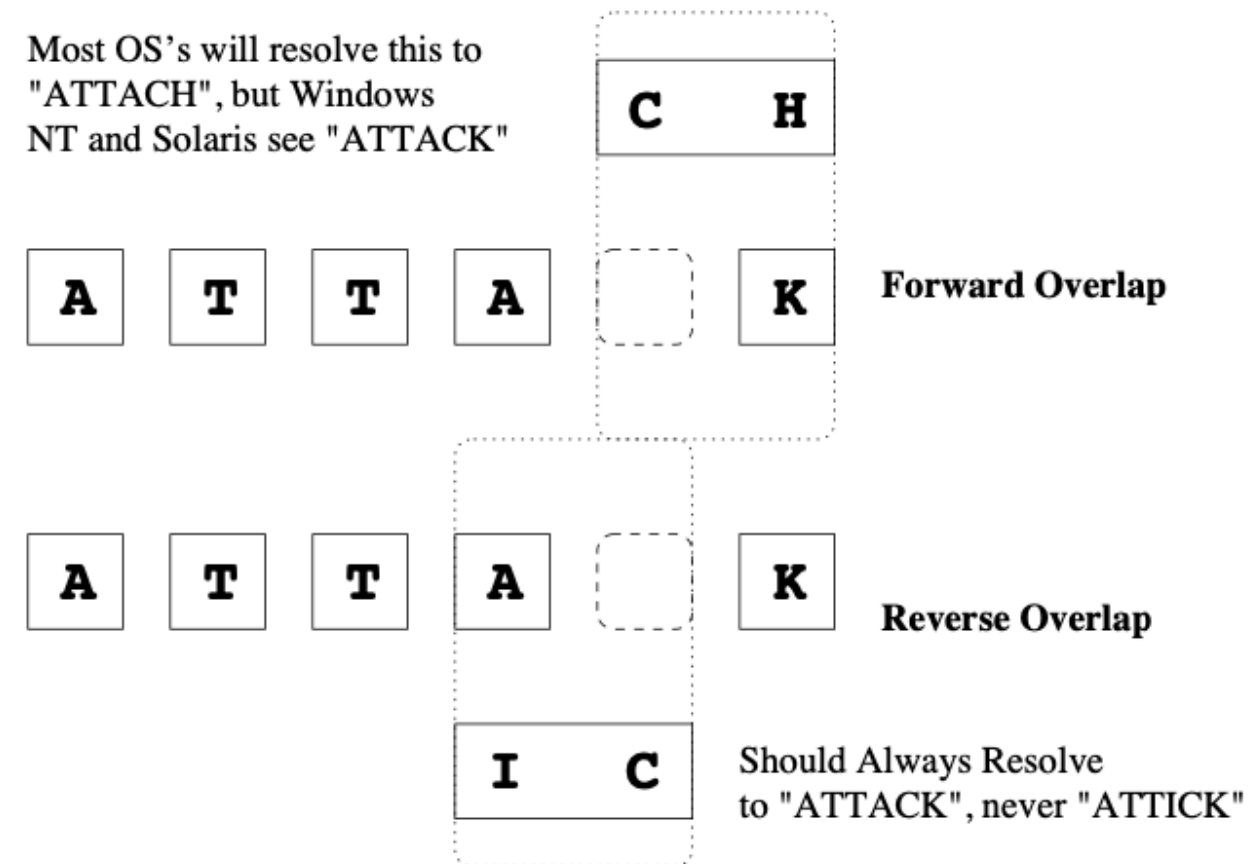
Second term 2019/20
Lecture 7-8

Previously on Network Security

- What does “The way packets are handled by the IDS and the end host might be different” mean?
- An IDS can be evaded by obfuscating or encoding the attack payload in a way that the target computer will reverse but the IDS will not. In this way, an attacker can exploit the end-host without alerting the IDS.
- Examples?...

Previously on Network Security

- Evasion: de-fragmenting behaviour
 - Windows prefers **OLD** data
- The IDS has to process all of the packets, not knowing how they will be reconstructed in the host, so there might be a situation in which the host at the end discard the OLD (e.g., like Linux which prefers the NEW) but others instead will discard the NEW preferring the OLD (e.g., like Windows).



Operating System	Overlap Behavior
Windows NT 4.0	Always Favors Old Data
4.4BSD	Favors New Data for Forward Overlap
Linux	Favors New Data for Forward Overlap
Solaris 2.6	Always Favors Old Data
HP-UX 9.01	Favors New Data for Forward Overlap
Irix 5.3	Favors New Data for Forward Overlap

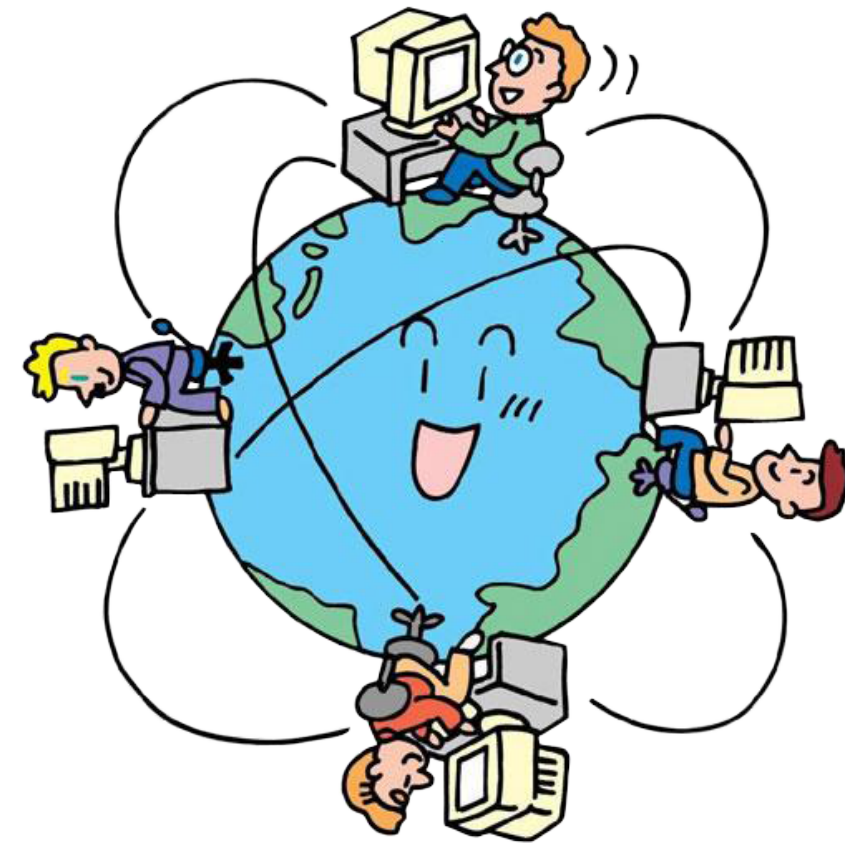
Objectives and learning outcomes

- Examine some popular protocols, used in securing systems.
 - Protocol concepts more important than details of latest release.
- Consider supporting infrastructure, use, risks, and related issues.
 - Need some (minimal) networking background for this

“A step back”: computer networks

- Physically: a collection of “segment” that transmit bit streams.

Examples: wire between two nodes or multi-access links like a LAN (e.g., Ethernet, token rings, packet radio networks).



- Logically: a communication medium between principals.
Example: client communicates to server
- A secure channel is yet another abstraction. Other abstractions may concern **availability, privacy** of communication partners, etc.

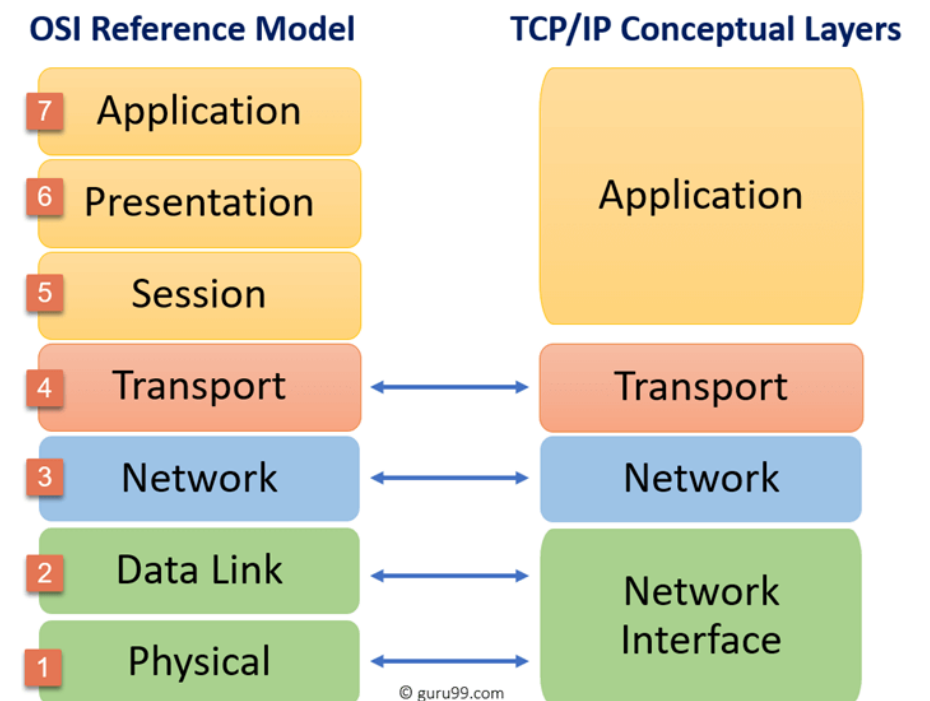
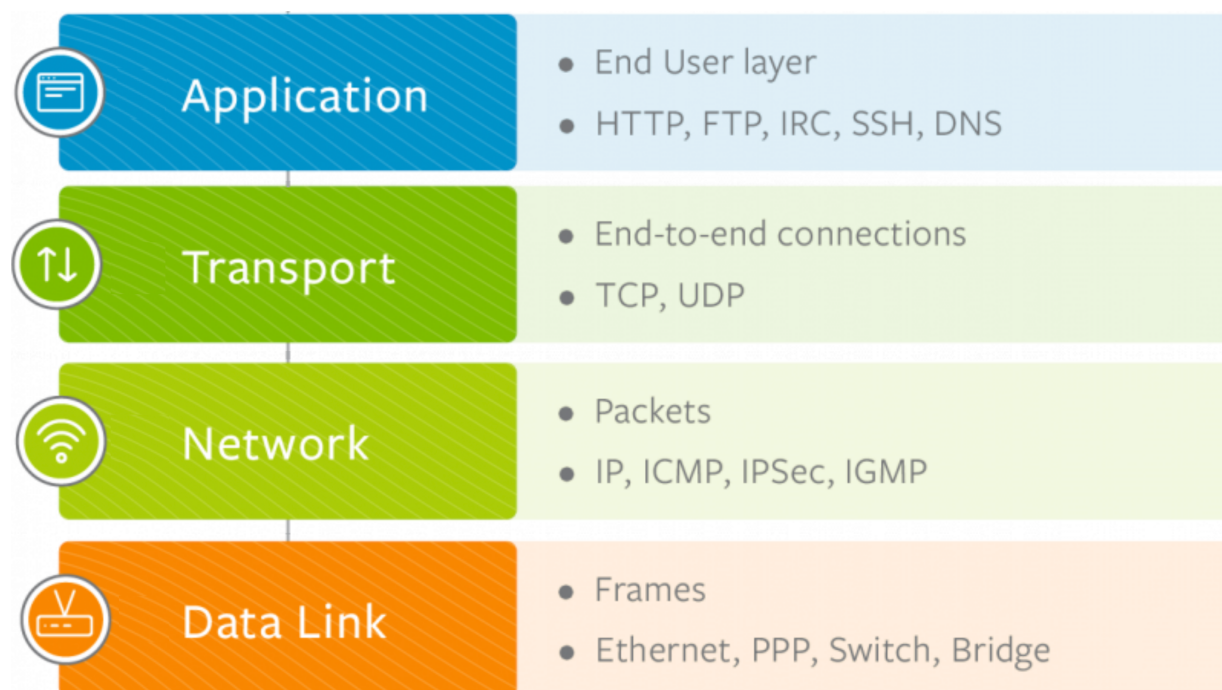
Layered communication in networks

- Logical functionality built in layered way.
 - Application communication
 - Reliable transport between nodes
 - Unreliable transport across links and switches
 - Packet transportation across single links

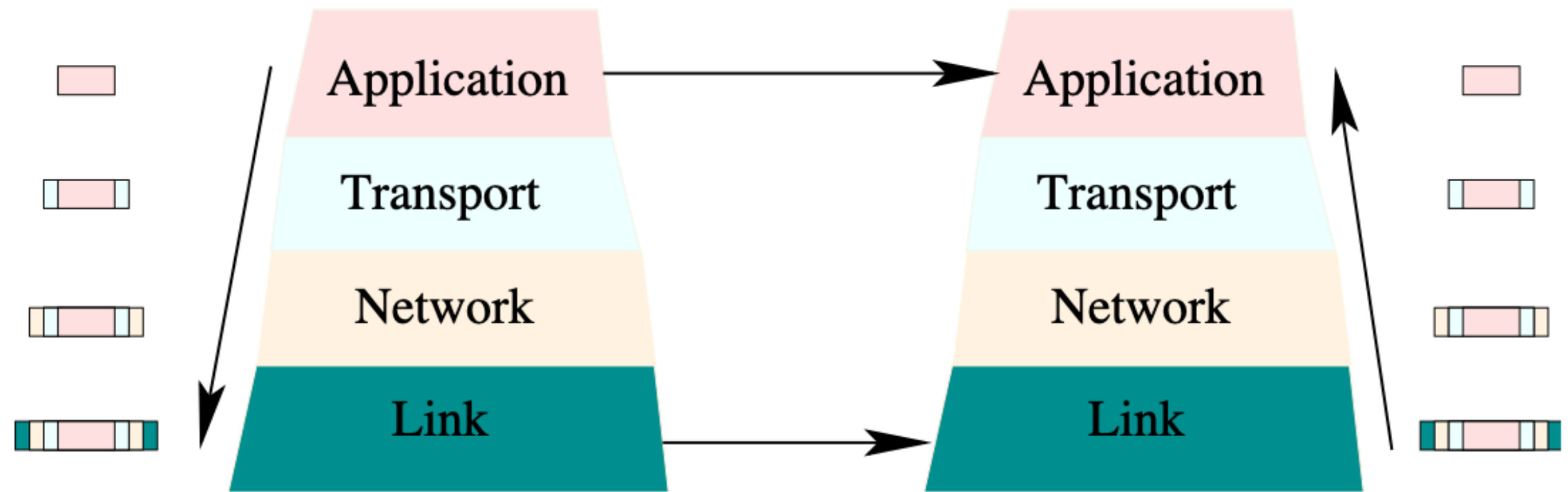
builds upon
builds upon
builds upon



- TCP/IP protocol reference model (simplified):



Layered communication in networks



- i^{th} layer of one node communicates with i^{th} layer of different node, each using services provided by their lower layers.
- Headers/trailers added to (or stripped from) packets as they traverse the protocol stack.
- Layers are an abstraction. Reality is usually rather different

Layered communication in networks

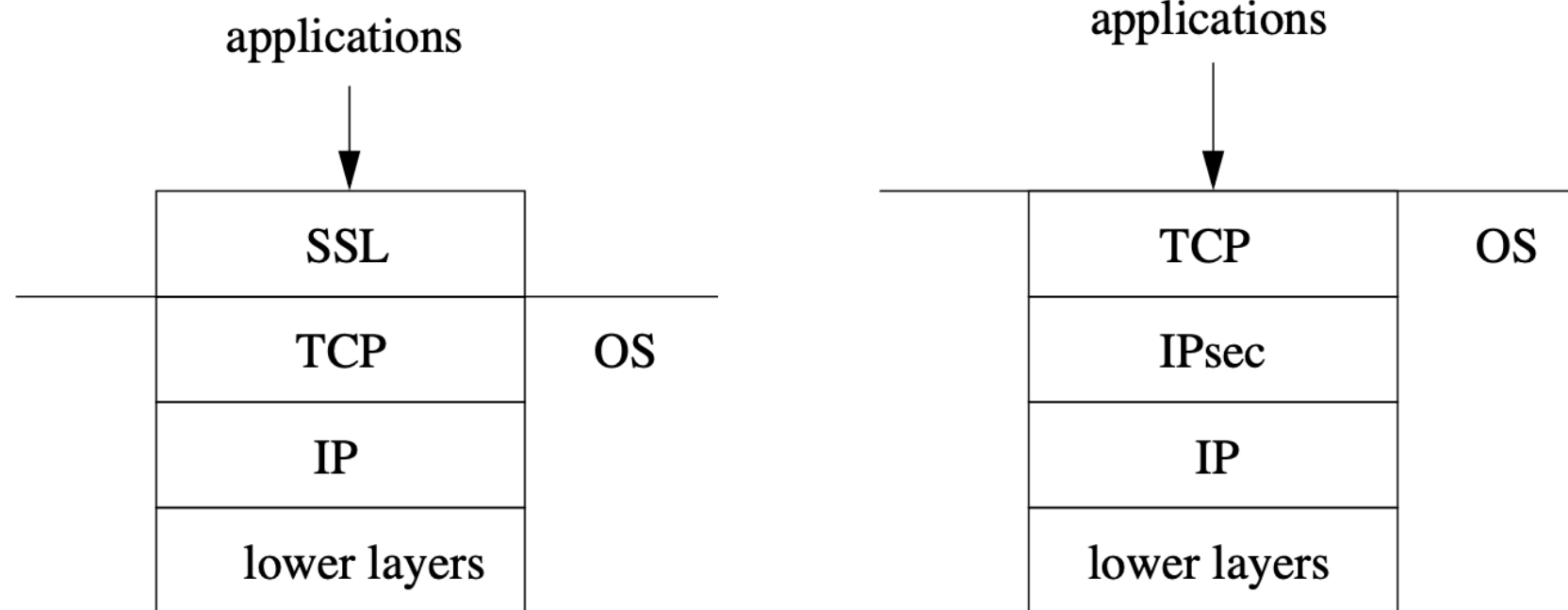
- Internet: confederation of networks using TCP/IP protocols.
- No global domain of trust.
 - Different subnetworks may (or may not) be trustworthy
 - 15+ hops for a packet from source to destination is common.
- Problem: how do we secure communication/applications?
- One possibility: secure applications over insecure channels.
 - Example: Use of PGP to encrypt/sign mail
 - Example: Kerberos is typically implemented and supported by different applications. Requires “kerberized” applications.
 - Solutions involved also other protocols: SSH, SSL/TLS, IPSEC,...
- We will consider underlying ideas and a few example protocols.
- **Note that securing other layers is also possible.**

What layer? – TCP/IP

- Internet Protocol (IP): deliver data across a network.
 - Packet headers specify source and destination addresses.
 - Protocol computes path and forwards packets over multiple links from source to destination.
 - Current version is IPv4 (transition to IPv6 under way).
- Transmission Control Protocol (TCP): establishes *reliable* communication between systems across a network.
Reliable: either all data delivered without loss, duplication, or reordering, or the connection is terminated.
- Neither provide security: no authentication or confidentiality.
 - Addresses can be faked.
 - Payload can be read and modified.

What layer? – (cont.)




- For most implementations of IP stacks:
 - Transport layer and below implemented in operating system.
 - Above transport layer implemented in user process.
- Two representative examples:





- **SSL (or TLS/SSH):** OS doesn't change, applications do. SSL API is a superset of “sockets” API to TCP.
- **IPsec:** OS changes. Applications and (TCP) API unchanged.

What layer? – (cont.)




- **Application (end-to-end):**

- No assumptions needed about security of protocols used, routers, etc... 
- Security decision can be based on user-ID, data, etc. 
- Applications must be designed “security aware”. 

- **Between application layer and transport layer, e.g., SSL:**

- No modification to OS. Minimal changes to applications. 
- Problems interacting with TCP. SSL may reject data that TCP accepts. SSL must then drop connection ⇒ easy DOS attack. 

- **IPsec:**

- Transport layer security without modifying applications. 
- Only authenticates IP addresses, no user authentication. 
- More is possible, but it requires changing API and applications. 

IPsec

IP security (IPsec) in a nutshell

- IP security (IPsec): A capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.
- There are application-specific security mechanisms for a number of application areas, including
 - electronic mail (S/MIME, PGP),
 - client/server (Kerberos),
 - Web access (Secure Sockets Layer), ...
- By implementing security at the IP level, an organisation can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications.

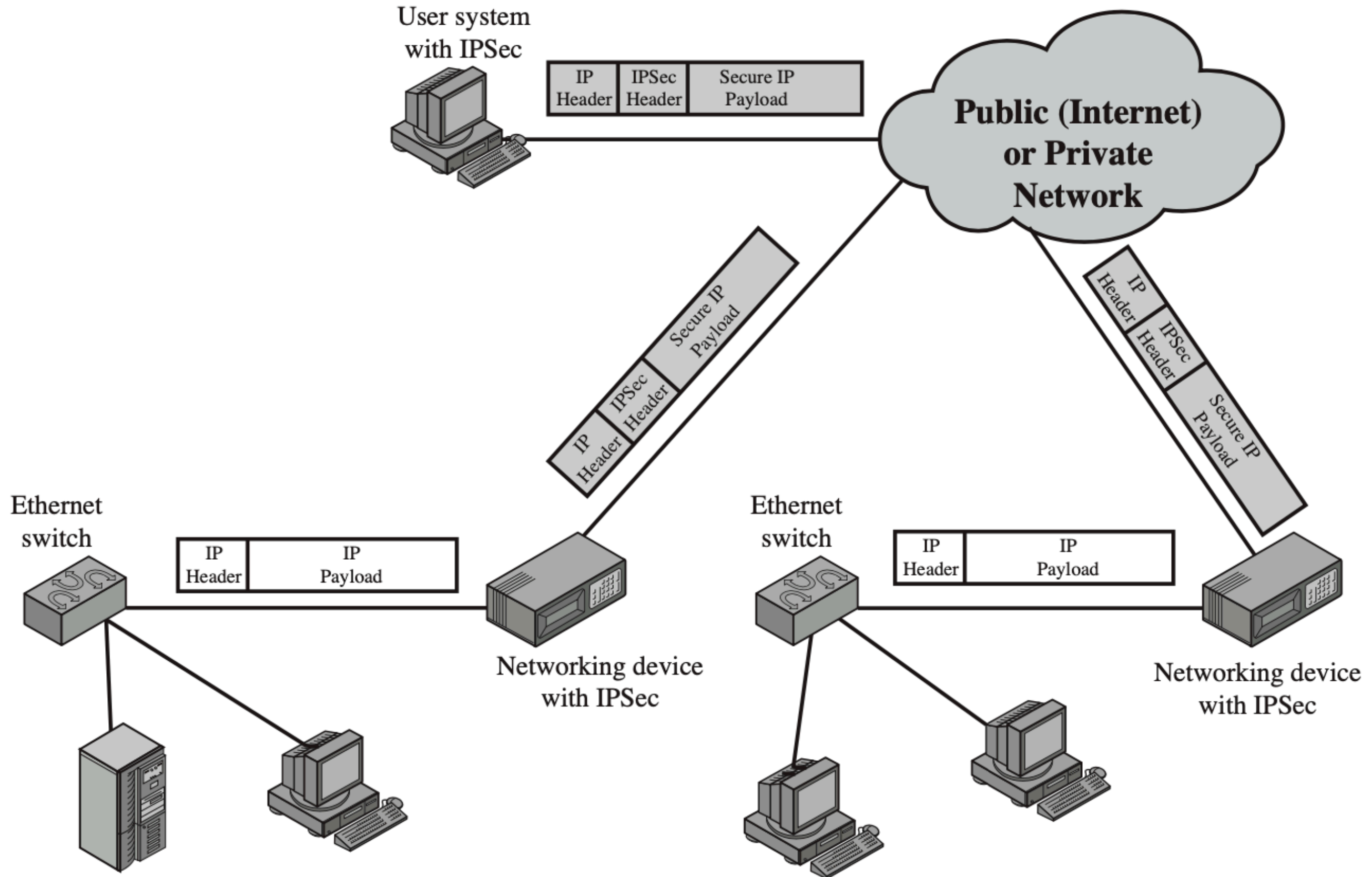
IP security (IPsec) in a nutshell

- IP-level security encompasses three functional areas:
 - **Authentication:** assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header, and that the packet has not been altered in transit.
 - **Confidentiality:** enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
 - **Key management:** concerned with secure exchange of keys.
- Ability to do filtering, based on a policy database. Just as if there were a firewall between the two ends.
- Installed in:
 - Operating systems: for end-to-end security;
 - Security gateways: firewalls or routers.
- Latter used for implementing Virtual Private Networks (VPNs).

Application of IPsec

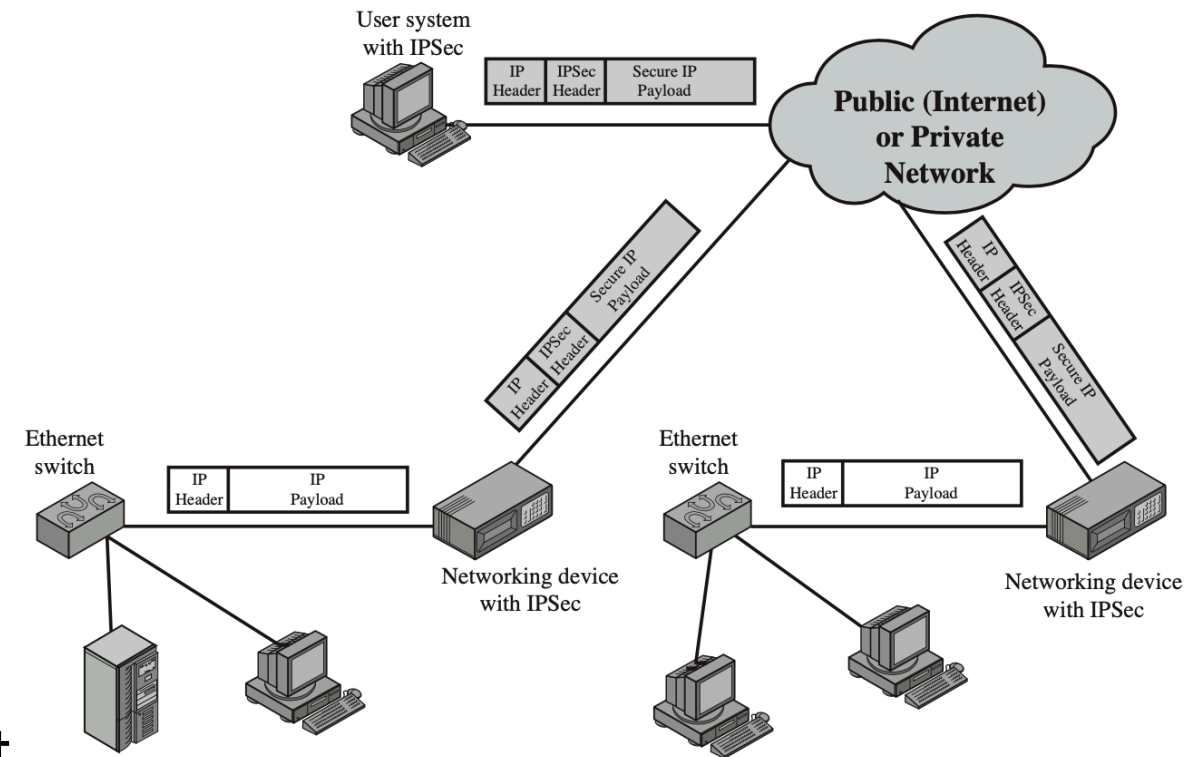
- Application of IPsec:
 - Secure branch office connectivity over the Internet.
 - Secure remote access over the Internet.
 - Establishing extranet and intranet connectivity with partners.
 - Enhancing e-commerce security.
- The principal feature of IPsec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level.
- Thus, all distributed applications (including remote logon, client/server, e-mail, file transfer, Web access, ...) can be secured.

An IPsec scenario



An IPsec scenario

- An organisation maintains LANs at dispersed locations.
- Nonsecure IP traffic is conducted on each LAN.
- For traffic offsite, through some sort of private or public WAN, IPsec protocols are used which operate in networking devices, such as a router or firewall, that connect each LAN to the outside world.
- The IPsec networking device will typically encrypt and compress all traffic going into the WAN and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN.
- Secure transmission is also possible with individual users who connect to the WAN. Such user workstations must implement the IPsec protocols to provide security.



Benefits of IPsec

- When implemented in a firewall or router, IPsec provides strong security that can be applied to all traffic crossing the perimeter.
 - Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPsec in a firewall is resistant to bypass if all traffic from outside must use IP and firewall is only entrance from Internet into organization.
- IPsec is below transport layer (TCP, UDP) and so is transparent to applications.
 - There is no need to change software on a user or server system when IPsec is implemented in the firewall or router.
 - Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

Benefits of IPsec

- IPsec can be transparent to end-users.
 - There is no need to train users on security mechanisms, issue keying material on a peruser basis, or revoke keying material when users leave the organisation.
- IPsec can provide security for individual users if needed.
 - This is useful for offsite workers and for setting up a secure virtual subnetwork within an organisation for sensitive applications.

The IPsec standard

- There are two ways to design a system. One is to make it so simple there are obviously no deficiencies. The other is to make it so complex there are no obvious deficiencies.

- C.A.R Hoare

- IPsec is an IETF Standard. Complex specification covering protocols for a variety of purposes:
 - **Authentication Header (AH)**: protects the integrity and the authenticity of IP datagrams (but not their confidentiality).
 - **Encapsulating Security Payload (ESP)**: protects confidentiality and optionally also integrity.
 - **Internet Key Exchange Protocol (IKE)**: Key Management.

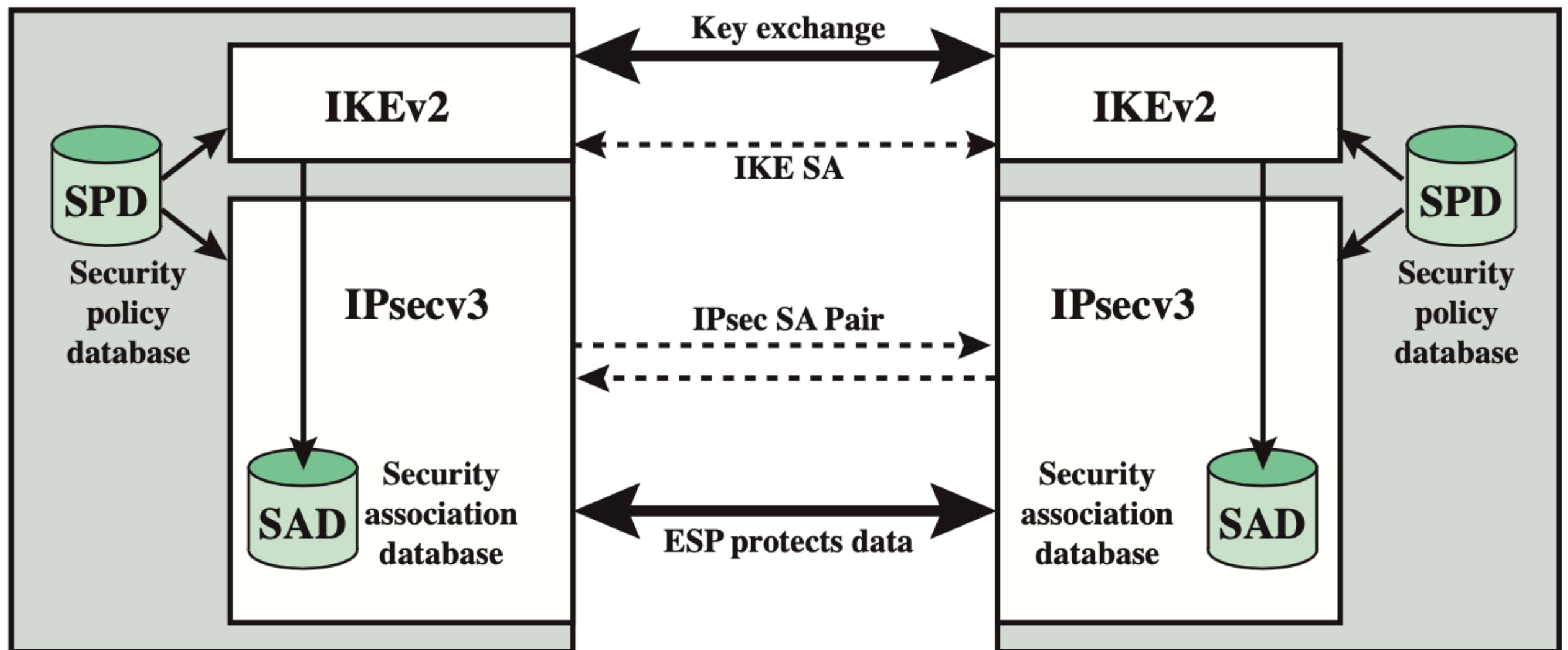
IPsec Services

- IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

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

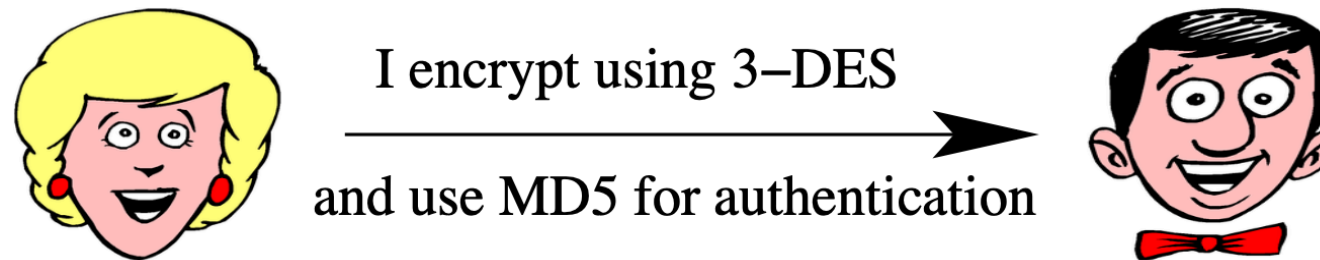
IP security policy

- Fundamental to the operation of IPsec is the concept of a **security policy** applied to each IP packet that transits from a source to a destination.
- Policy is determined primarily by the interaction of two databases:
 - the security association database (SAD) and
 - the security policy database (SPD).



Security Association Database

- A security association (SA) is a one-way relationship between sender and receiver defining security services.



- SA specifies things like: authentication algorithm (AH), encryption algorithm (ESP), keys, key lifetimes, lifetime of security association, protocol mode (tunnel or transport), ...
- SA is uniquely identified by three parameters:
 - **Security Parameters Index (SPI):** a bit string assigned to this SA and having local significance only.
SPI is carried in AH and ESP headers to enable receiving system to select SA under which a received packet will be processed.
 - **IP Destination Address:** address of destination endpoint of SA (may be an end-user system or a network system such as a firewall or router).
 - **Security Protocol Identifier:** a field from the outer IP header that indicates whether SA is an AH or ESP SA.

Security Policy Database (SPD)

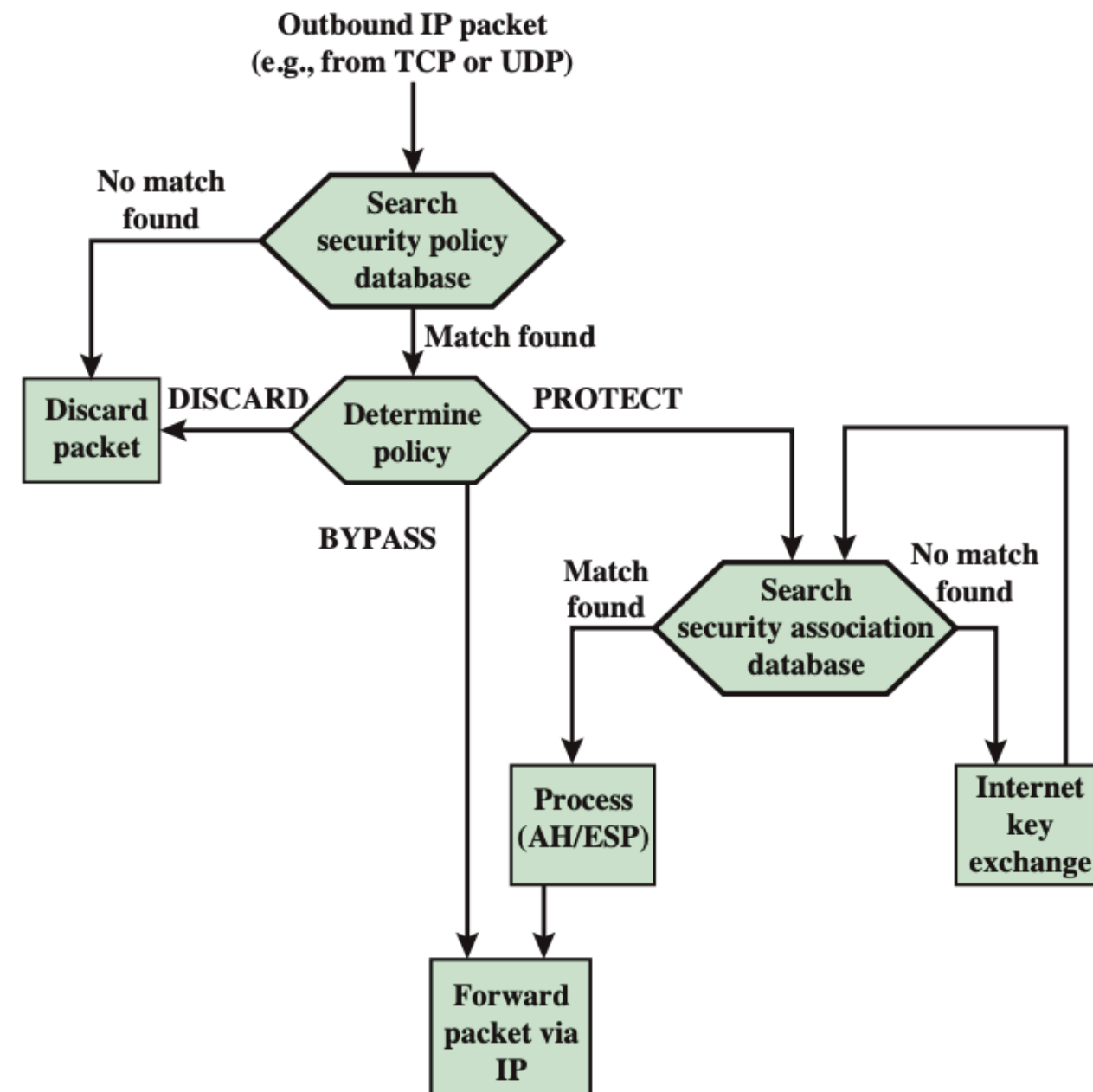
- Security Policy Database (SPD): means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec).
- In its simplest form, an SPD contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic.
- In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry.

IP traffic processing

- IPsec is executed on a packet-by-packet basis.
- When IPsec is implemented,
 - each outbound IP packet is processed by the IPsec logic before transmission, and
 - each inbound packet is processed by the IPsec logic after reception and before passing the packet contents on to the next higher layer (e.g., TCP or UDP).

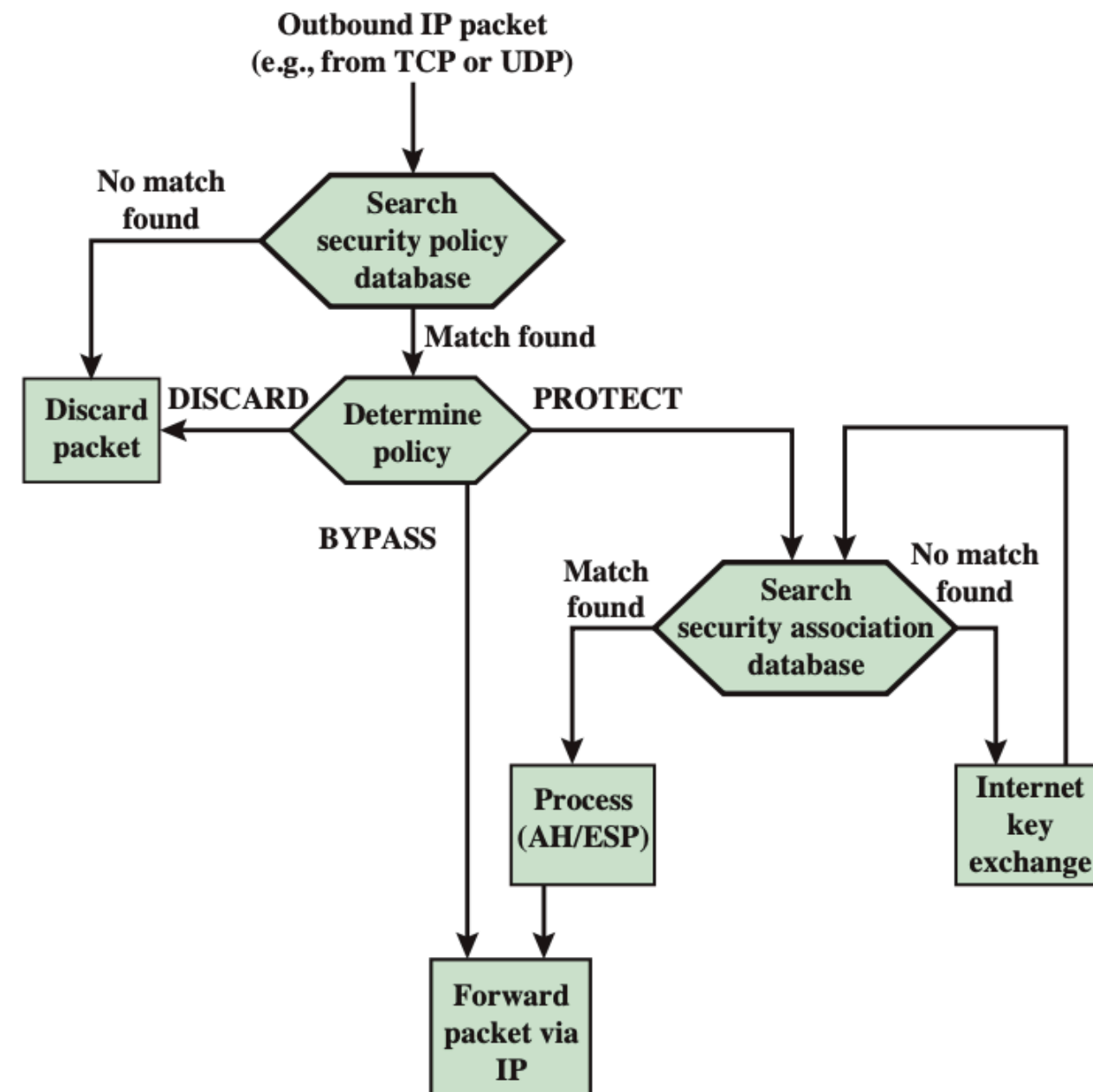
IP traffic processing: outbound

- A block of data from a higher layer (e.g., TCP), is passed down to IP layer and an IP packet is formed, consisting of an IP header and an IP body.
- Then the following steps occur:
 - IPsec searches SPD for a match to this packet.
 - If no match is found, packet is discarded and an error message is generated.
 - If a match is found, further processing is determined by the first matching entry in the SPD: ...



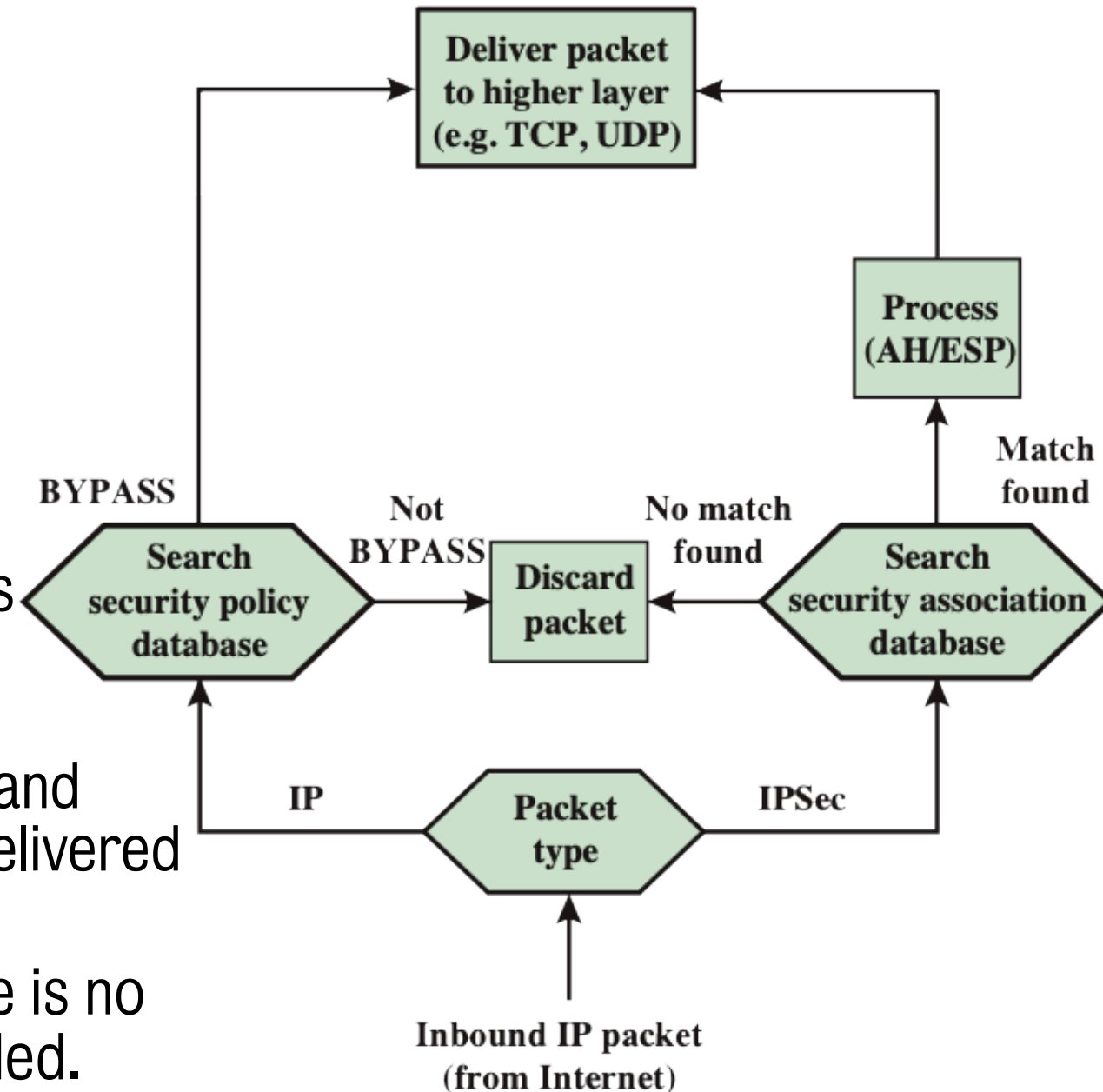
IP traffic processing: outbound

- If a match is found, further processing is determined by the first matching entry in the SPD: if the policy for this packet is
 - DISCARD, then the packet is discarded;
 - BYPASS, then there is no further IPsec processing (the packet is forwarded to the network for transmission);
 - PROTECT, then SAD is searched for a matching entry.
- If no entry is found, IKE is invoked to create an SA with the appropriate keys and an entry is made in the SAD.
- Matching entry in SAD determines processing for this packet.
 - Either encryption, authentication, or both can be performed, and either transport or tunnel mode can be used.
 - The packet is then forwarded to the network for transmission.



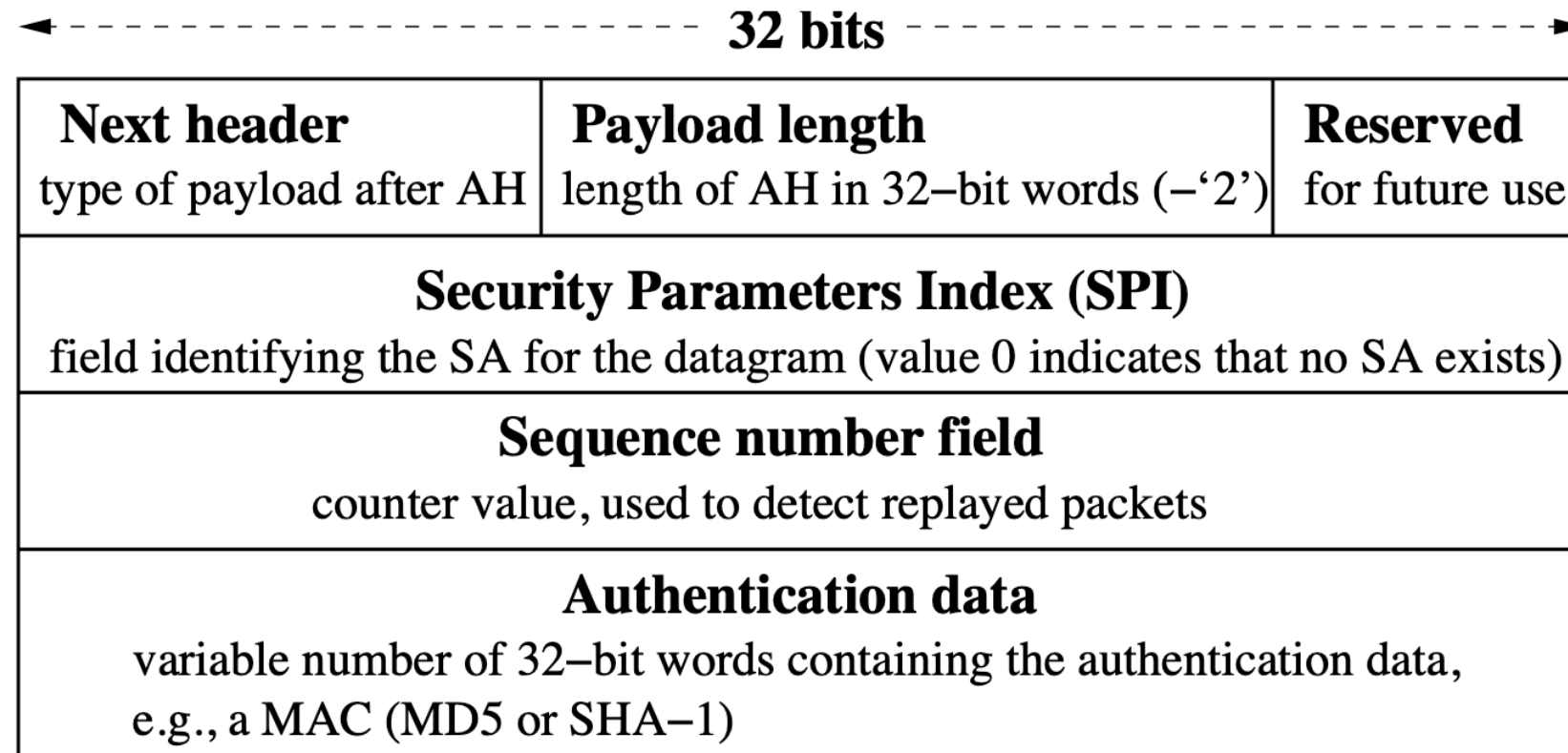
IP traffic processing: inbound

- Incoming IP packet triggers IPsec processing:
- 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).
- If packet is unsecured, IPsec searches SPD for a match to this packet. If the first matching entry has a policy of
 - BYPASS, IP header is processed and stripped off and packet body is delivered to next higher layer, such as TCP;
 - PROTECT or DISCARD, or if there is no matching entry, packet is discarded.
- For a secured packet, IPsec searches the SAD.
 - If no match is found, then packet is discarded.
 - Else IPsec applies appropriate ESP or AH processing, and then IP header is processed and stripped off and packet body is delivered to next higher layer, such as TCP.

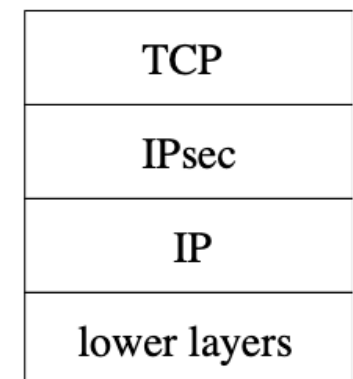


IPsec: Authentication Header

Authentication Header (AH)



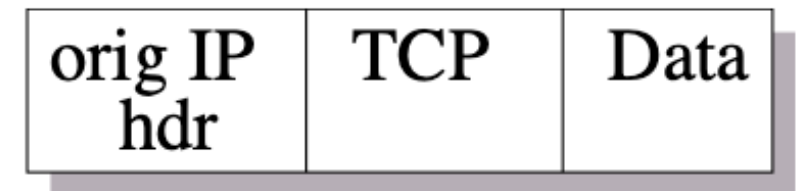
- Extra header between layers 3 and 4 (IP and TCP) providing destination enough information to identify SA.
- AH guarantees integrity only, but also protects part of IP header.



Sequence number is initialised to zero and incremented by sender for each packet. Receiver stores incoming packets in a sliding window (default size 64) to order and sort out duplicates. (IP does not guarantee delivery or order.)

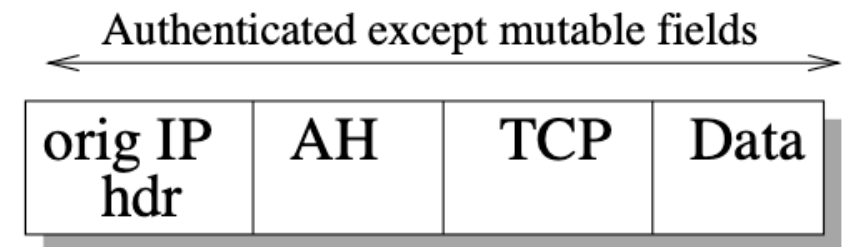
AH modes

- **Original Datagram (here for TCP):**



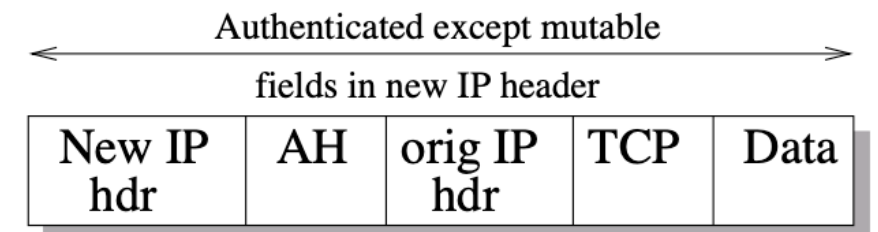
- **Transport mode:**

- AH inserted after IP header, before IP payload.
- MAC taken of entire packet (except for mutable fields).
- Provides end-to-end protection between IPsec-enabled systems.



- **Tunnel mode:**

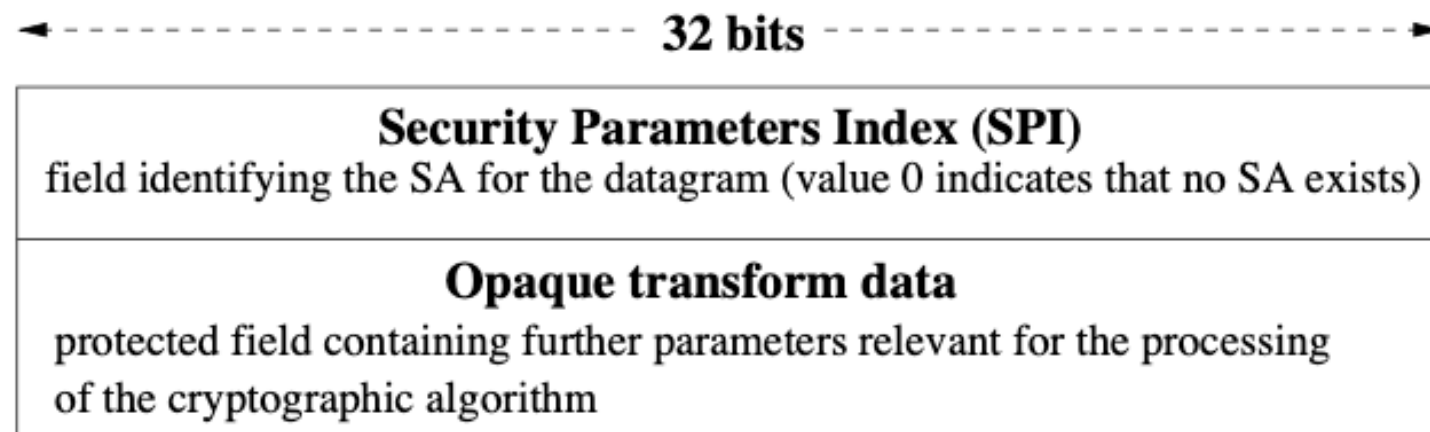
- Entire original packet authenticated; new outer IP header.
- Inner header carries ultimate source/destination address.
- New outer header also protected (except mutable fields) and may contain different IP addresses, e.g., firewalls or security gateways.



IPsec: Encapsulating Security Payload

Encapsulating Security Payload (ESP)

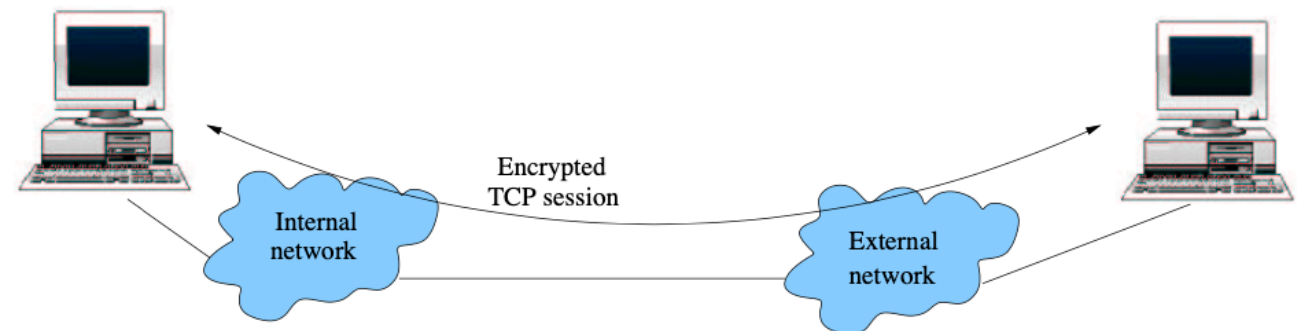
- Can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and (limited) traffic flow confidentiality.
- Set of services provided depends on options selected at the time of establishment of the SA and on the location of the implementation in a network topology.
- Header specifies encryption and optional authentication



- Two ways in which the IPsec ESP service can be used:
 - transport mode,
 - tunnel mode.

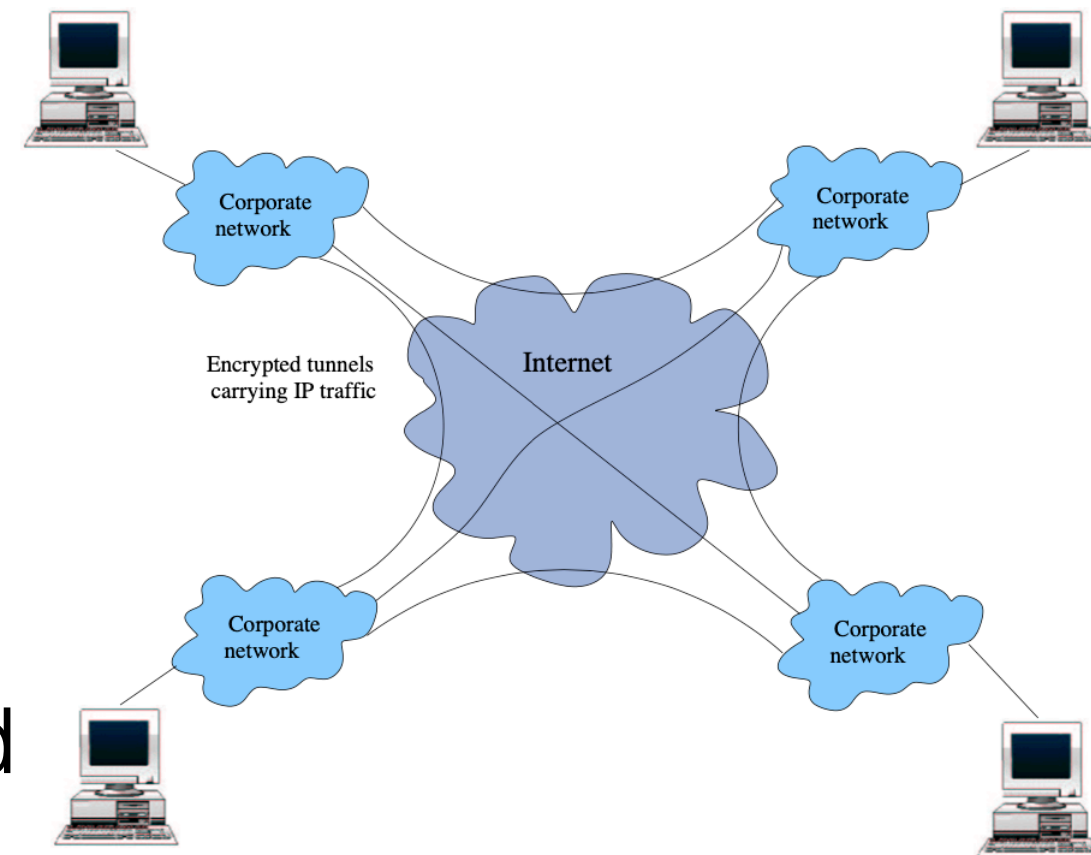
ESP applications

- **Transport mode:** provides end-to-end encryption between hosts supporting IPsec.



- **Tunnel mode:** can be used to set up a VPN.
Example:

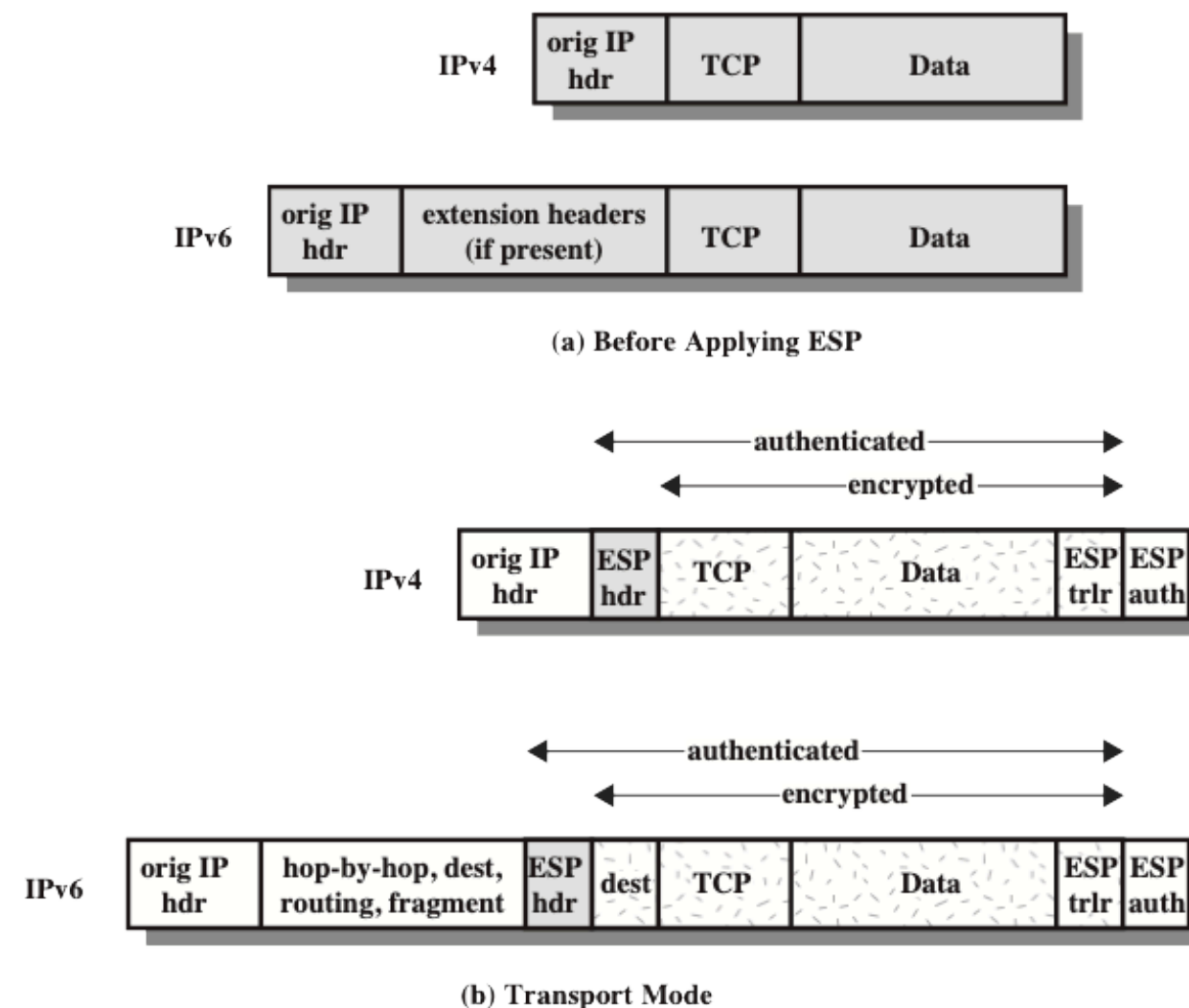
- Hosts on internal networks use Internet for transport of data but do not interact with other Internet-based hosts.
- By terminating tunnels at security gateway to each internal network, configuration allows hosts to avoid implementing security capability.



- Former technique is supported by a transport mode SA, while latter technique uses a tunnel mode SA.

ESP applications: Transport mode

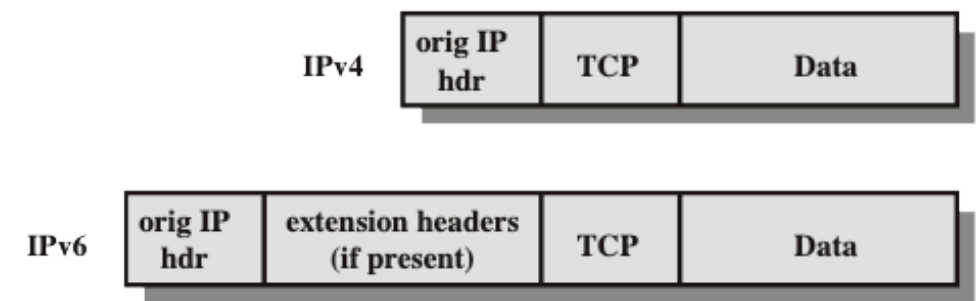
- Encrypts only the data portion (**payload**) of each packet, but leaves the header untouched.
- For this mode using IPv4, ESP header is inserted into IP packet immediately prior to transport-layer header (e.g., TCP, UDP, ICMP), and an ESP trailer (Padding, Pad Length, and Next Header fields) is placed after IP packet.



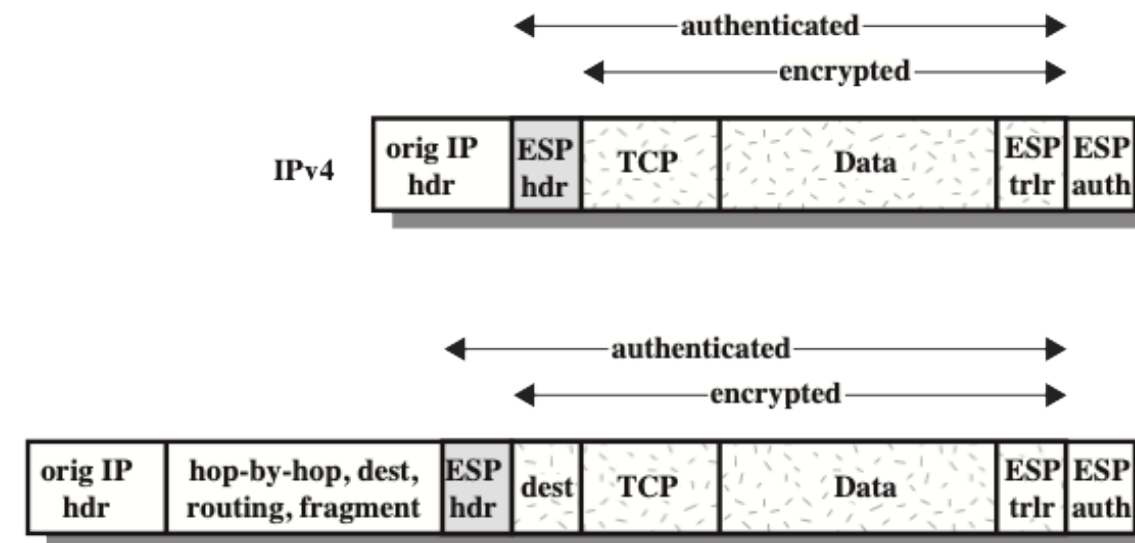
- If authentication is selected, ESP Authentication Data field is added after ESP trailer.
- Entire transport-level segment plus ESP trailer are encrypted.
- Authentication covers all of ciphertext plus ESP header.

ESP applications: Transport mode

- IPv6: ESP is viewed as an end-to-end payload (i.e., it is not examined or processed by intermediate routers).
 - Thus, ESP header appears after IPv6 base header and hop-by-hop, routing, and fragment extension headers.
 - Destination options extension header could appear before or after ESP header, depending on semantics desired.
 - For IPv6, encryption covers entire transport-level segment plus ESP trailer plus destination options extension header if it occurs after ESP header.
 - Again, authentication covers ciphertext plus ESP header.



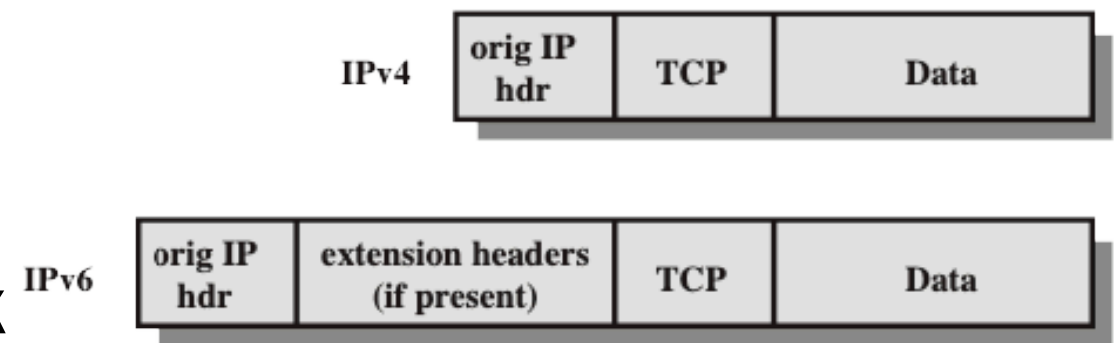
(a) Before Applying ESP



(b) Transport Mode

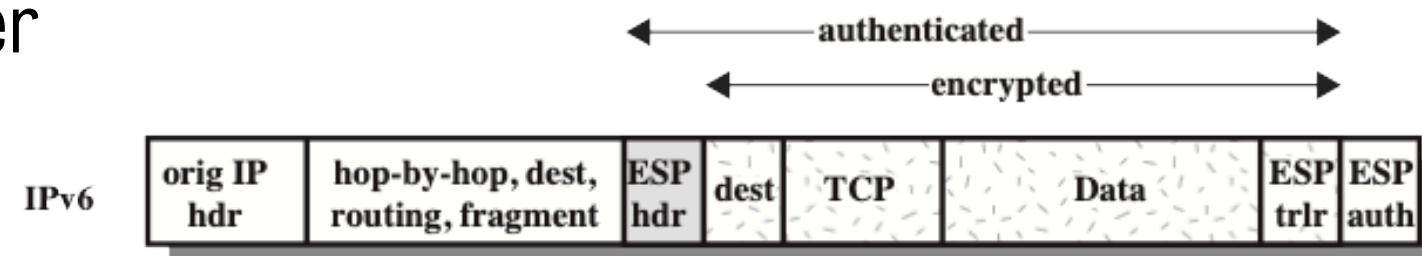
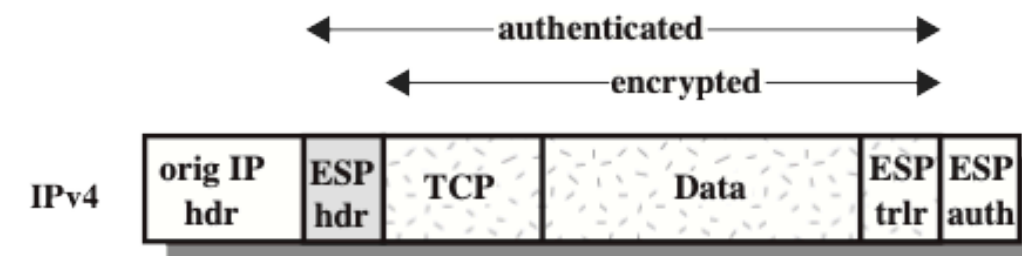
Transport mode summary

1. At the source, block of data consisting of ESP trailer plus entire transport-layer segment is encrypted and plaintext of this block is replaced with its ciphertext to form IP packet for transmission. Authentication is added if this option is selected.



(a) Before Applying ESP

2. Packet is then routed to destination. Each intermediate router needs to examine and process IP header plus any plaintext IP extension headers but does not need to examine ciphertext.



(b) Transport Mode

3. Destination node examines and processes IP header plus any plaintext IP extension headers. Then, on basis of SPI in ESP header, destination node decrypts remainder of packet to recover plaintext transport-layer segment.

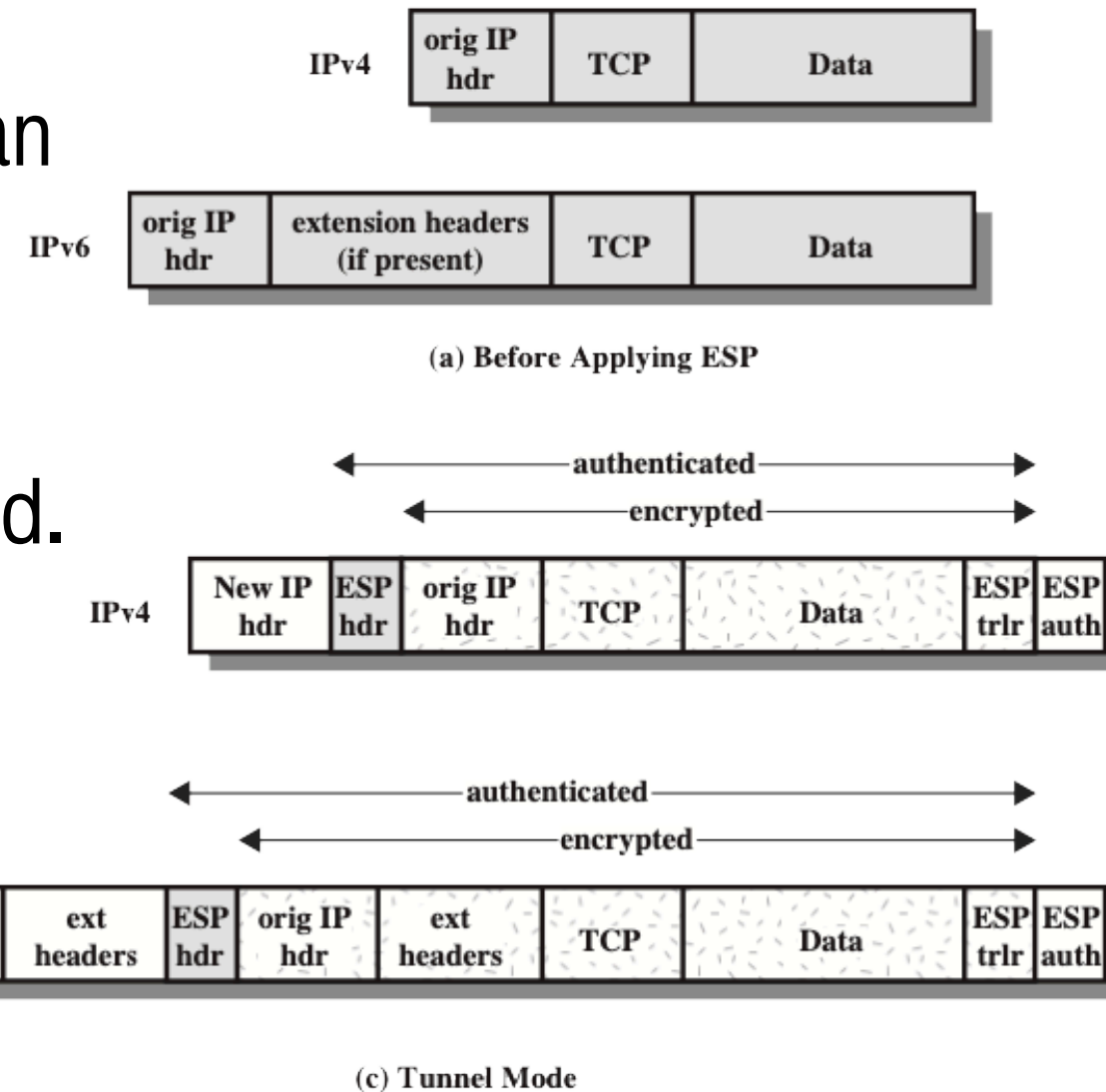
Transport mode operation provides confidentiality for any application that uses it, thus avoiding need to implement confidentiality in every individual application. One drawback to this mode is that it is possible to do traffic analysis on the transmitted packets.

ESP applications: Tunnel mode

- Tunnel mode ESP is used to encrypt an entire IP packet.
- ESP header is prefixed to packet,
- packet plus ESP trailer is encrypted.

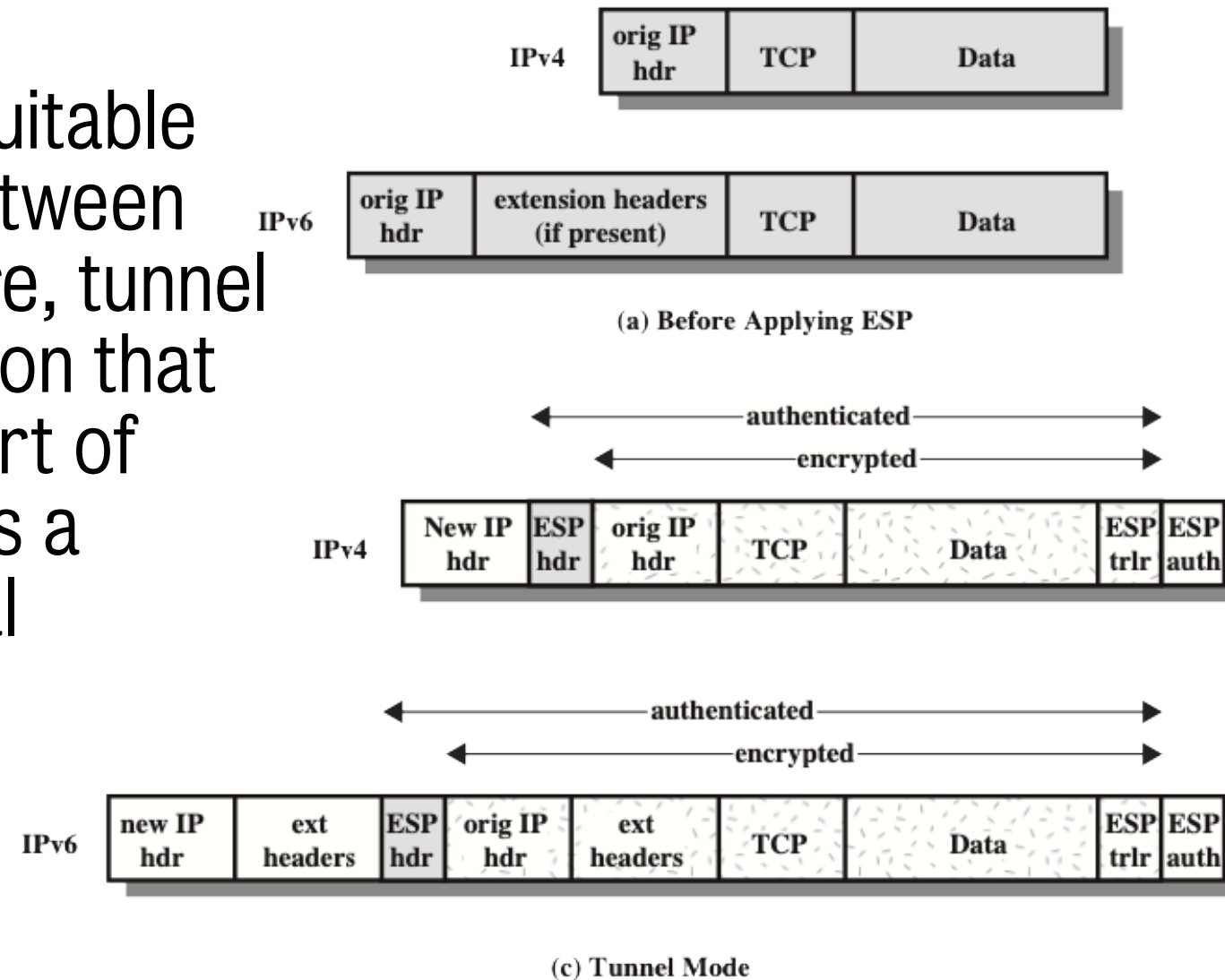
This method can be used to counter traffic analysis.

- As IP header contains destination address and possibly source routing directives and hop-by-hop option information, it is not possible simply to transmit encrypted IP packet prefixed by ESP header.
- Intermediate routers would be unable to process such a packet.
- Thus: encapsulate entire block (ESP header plus ciphertext plus Authentication Data, if present) with a new IP header that will contain sufficient information for routing but not for traffic analysis.



ESP applications: Tunnel mode

- Whereas transport mode is suitable for protecting connections between hosts that support ESP feature, tunnel mode is useful in a configuration that includes a firewall or other sort of security gateway that protects a trusted network from external networks.
- In this latter case, encryption occurs only between an external host and security gateway or between two security gateways.
- This relieves hosts on internal network of processing burden of encryption and simplifies key distribution task by reducing number of needed keys.
- Further, it prevents traffic analysis based on ultimate destination.



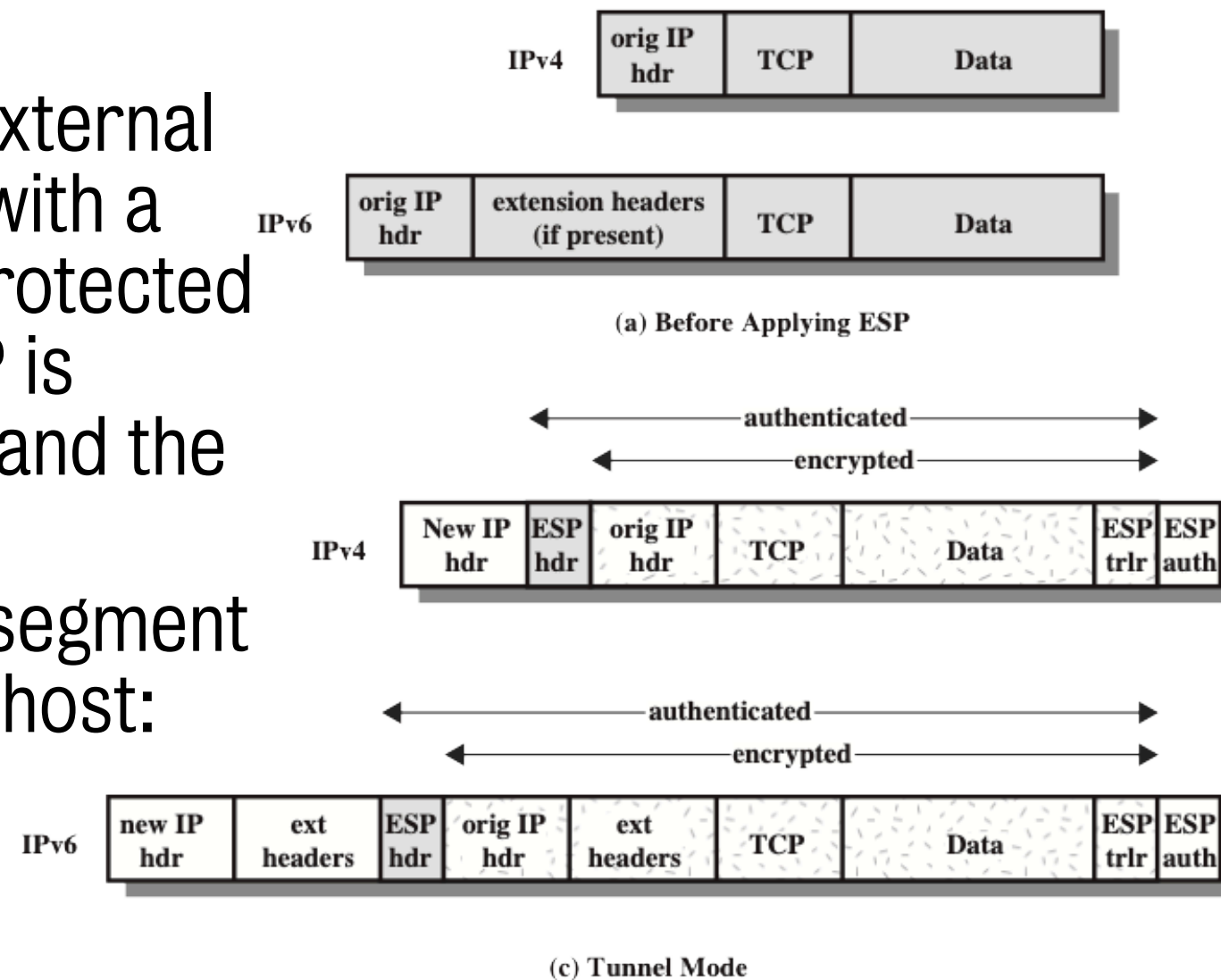
ESP applications: Tunnel mode

- Consider a case in which an external host wishes to communicate with a host on an internal network protected by a firewall, and in which ESP is implemented in external host and the firewalls.

- Transfer of a transport-layer segment from external host to internal host:

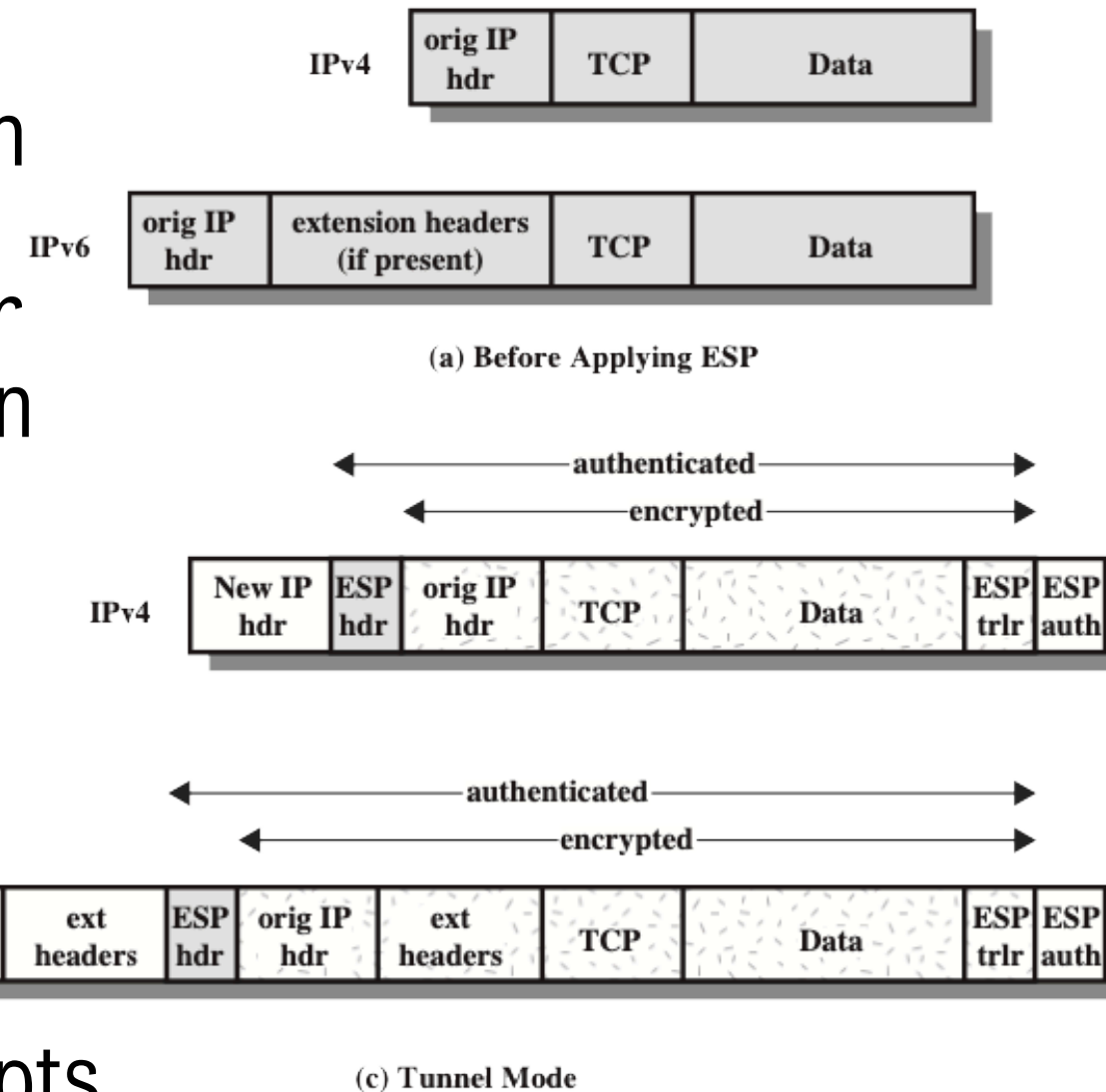
- Source prepares an inner IP packet with a destination address of the target internal host.

- This packet is prefixed by an ESP header; then packet and ESP trailer are encrypted and Authentication Data may be added.
- Outer IP packet: resulting block is encapsulated with a new IP header (base header plus optional extensions such as routing and hop-by-hop options for IPv6) whose destination address is the firewall.

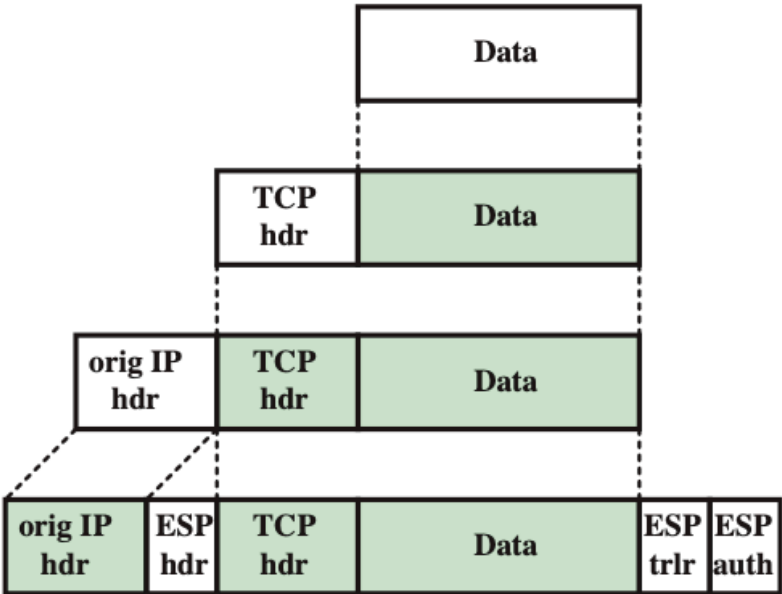
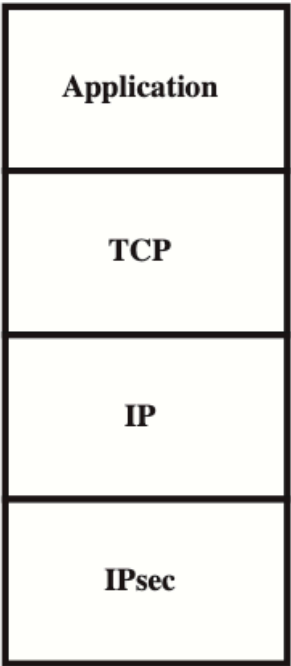


ESP applications: Tunnel mode

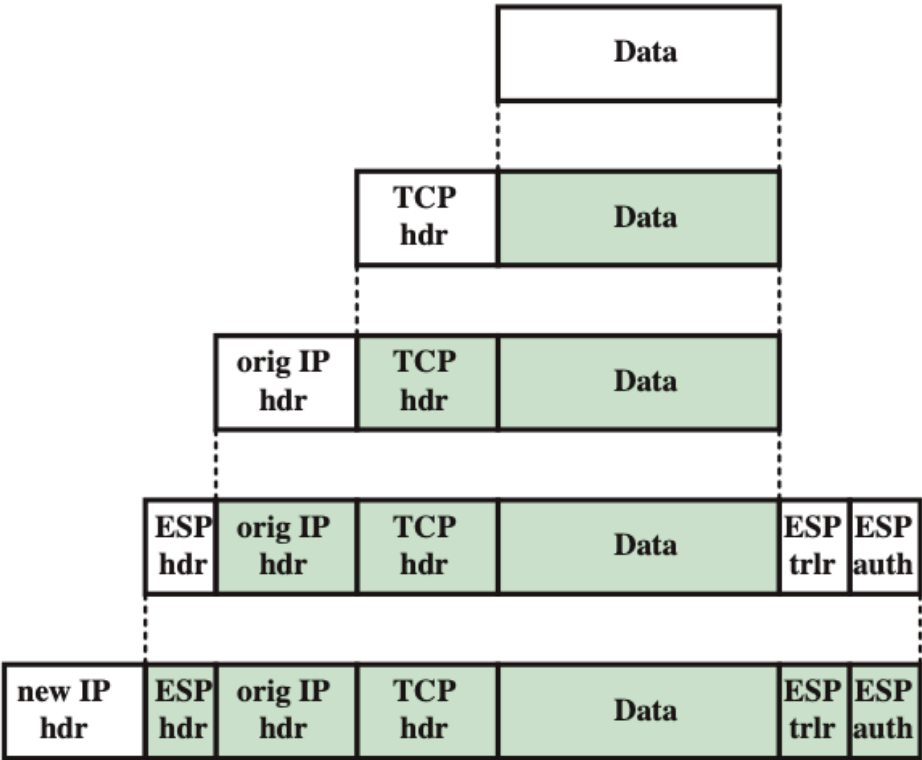
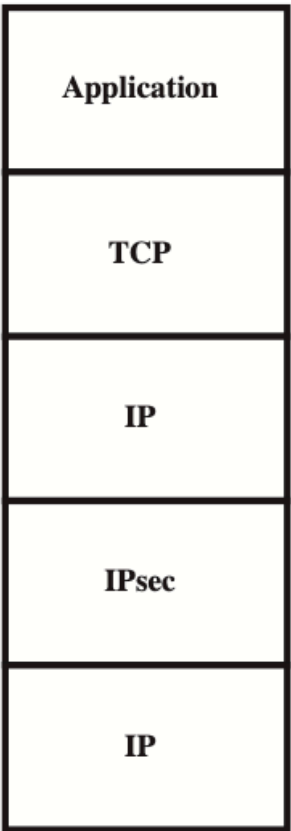
- Outer packet is routed to destination firewall. Each intermediate router needs to examine and process outer IP header plus any outer IP extension headers but does not need to examine ciphertext.
- Destination firewall examines and processes outer IP header plus any outer IP extension headers. Then, on basis of the SPI in ESP header, destination node decrypts the remainder of packet to recover the plaintext inner IP packet. This packet is then transmitted in internal network.
- Inner packet is routed through zero or more routers in internal network to destination host.



ESP: protocol operation



(a) Transport mode



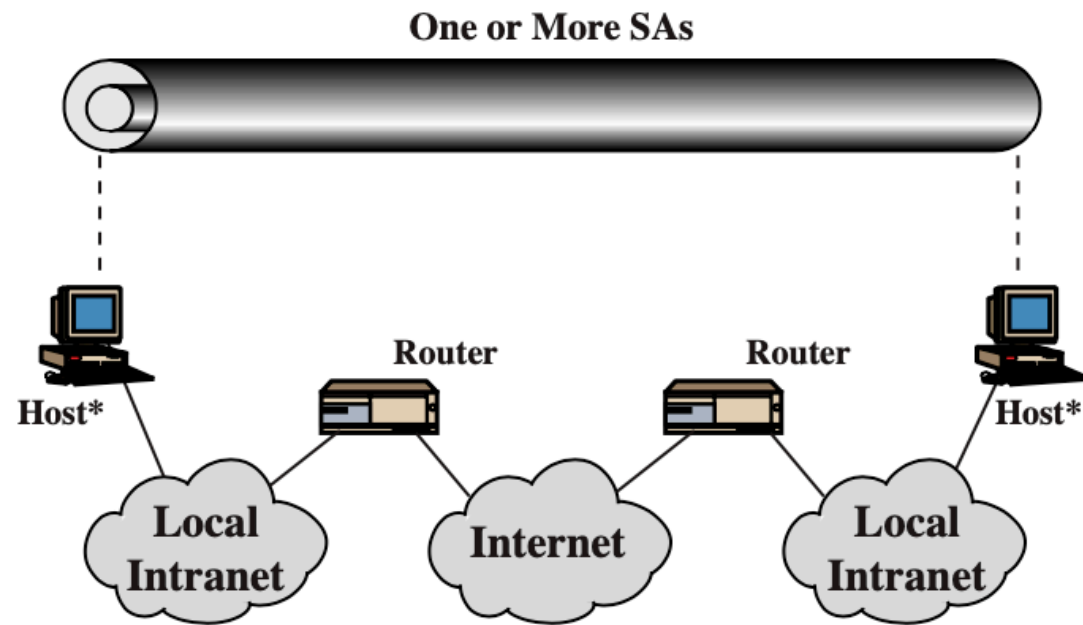
(b) Tunnel mode

IPsec: Combining Security Associations

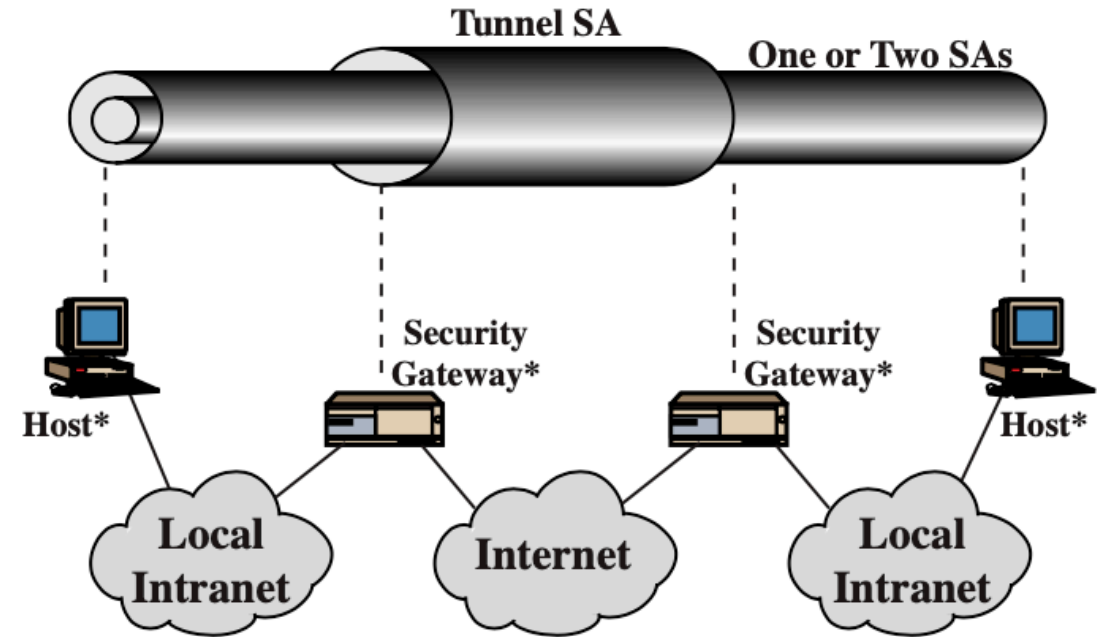
Combining Security Associations

- An individual SA can implement either the AH or ESP protocol but not both.
- Sometimes a particular traffic flow will call for the services provided by both AH and ESP.
Further, a particular traffic flow may require IPsec services between hosts and, for that same flow, separate services between security gateways, such as firewalls.
- In all of these cases, multiple SAs must be employed for the same traffic flow to achieve the desired IPsec services.
- The term **security association bundle** refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPsec services.
- The SAs in a bundle may terminate at different endpoints or at the same endpoints.

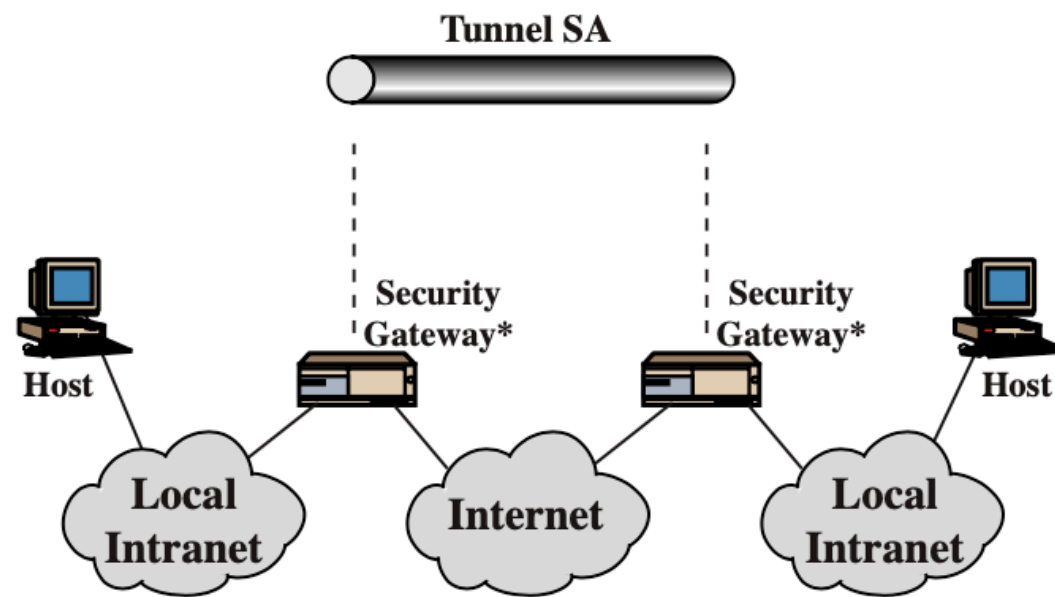
Combining Security Associations: 4 examples



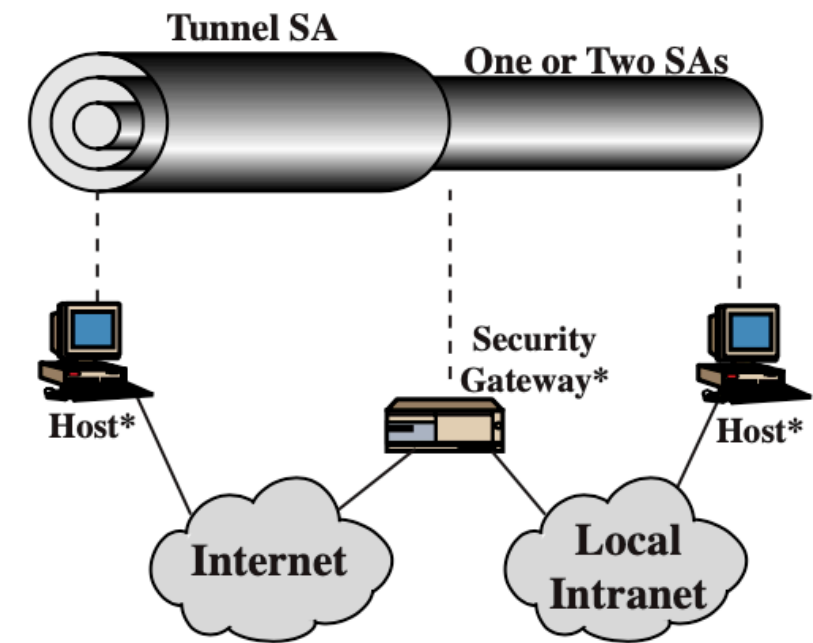
(a) Case 1



(c) Case 3



(b) Case 2

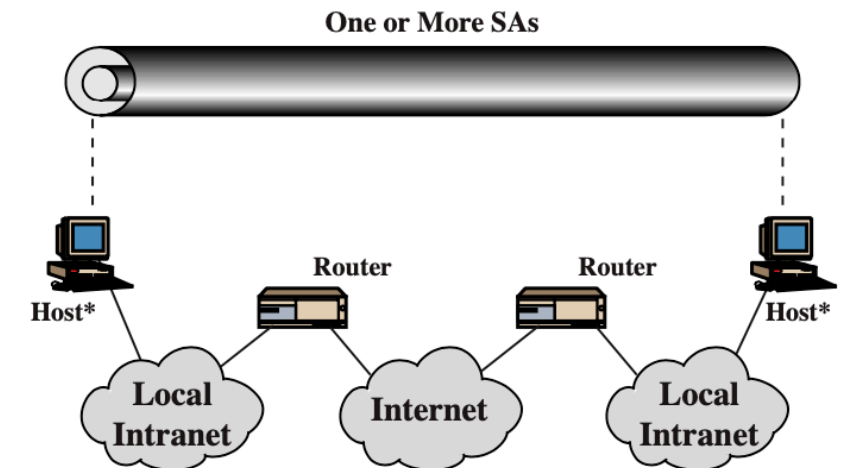


(d) Case 4

* = implements IPSec

Combining Security Associations: 4 examples

- Lower part of each case represents physical connectivity of elements.
- Upper part represents logical connectivity via one or more nested SAs.
- Each SA can be either AH or ESP.
- For host-to-host SAs, mode may be either transport or tunnel; otherwise it must be tunnel mode.



(a) Case 1

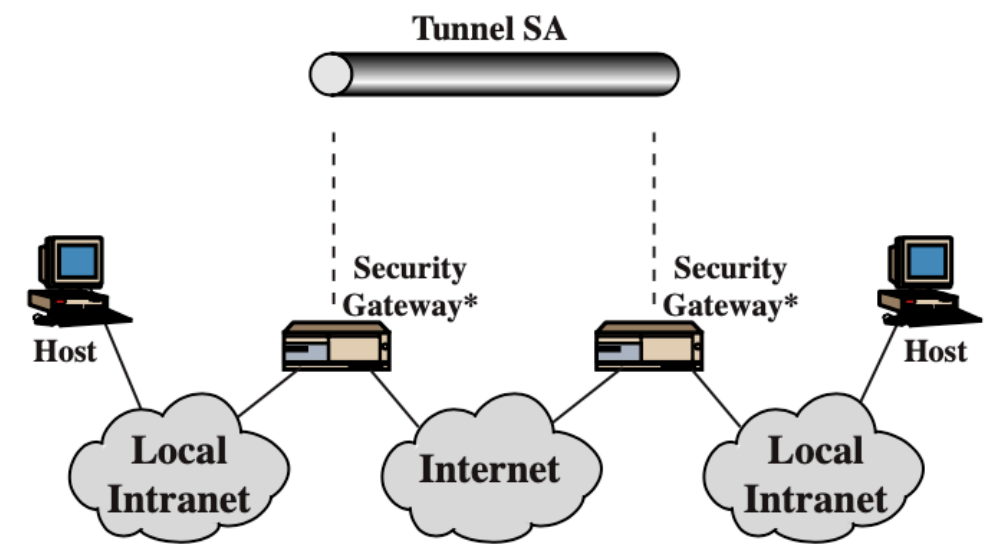
1. All security is provided between end systems that implement IPsec. For any two end systems to communicate via an SA, they must share appropriate secret keys.

Among the possible combinations are

- I. AH in transport mode.
 - II. ESP in transport mode.
 - III. ESP followed by AH in transport mode (an ESPSA inside an AHSA)
 - IV. Any one of (i), (ii) or (iii) inside an AH or ESP in tunnel mode.
- As we have discussed, these various combinations can be used to support authentication, encryption, authentication before encryption, and authentication after encryption.

Combining Security Associations: 4 examples

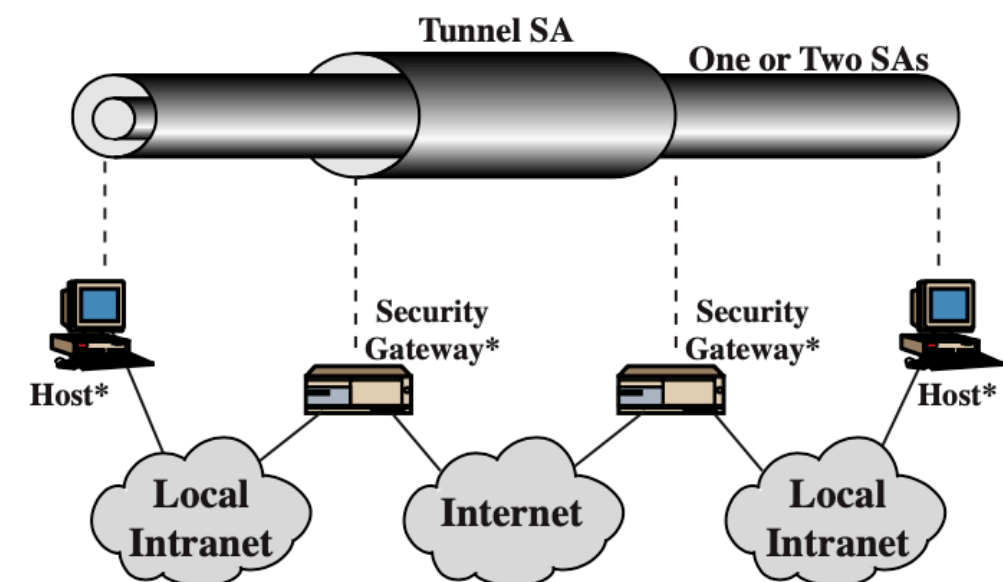
2. Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec.
- This case illustrates simple virtual private network support.
 - The security architecture document specifies that only a single tunnel SA is needed for this case.
 - Tunnel could support AH, ESP,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



(b) Case 2

Combining Security Associations: 4 examples

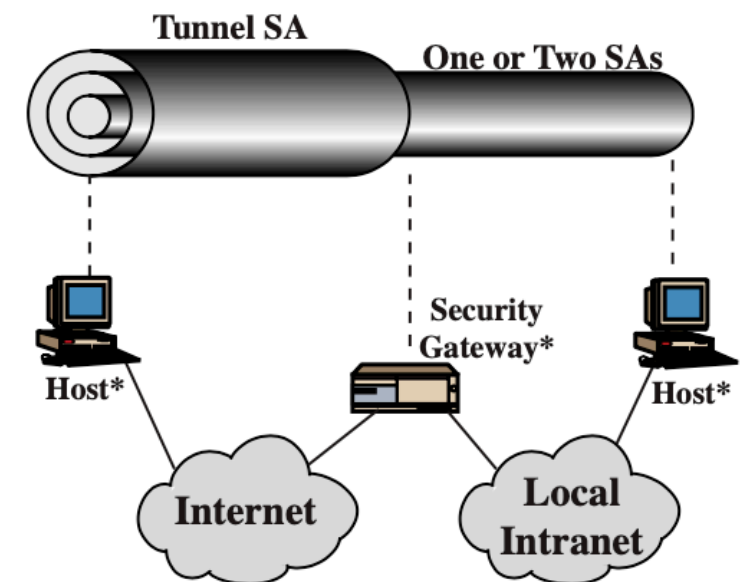
3. Security is provided only between gateways (routers, firewalls, etc.) and both hosts implement IPsec.
- Builds on case 2 by adding end-to-end security.
 - Same combinations as for cases 1 and 2.
 - The gateway-to-gateway tunnel provides either authentication, confidentiality, or both for all traffic 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



(c) Case 3

Combining Security Associations: 4 examples

4. This provides support for a remote host that uses 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 remote host and firewall.
 - As in case 1, one or two SAs may be used between remote host and local host



(d) Case 4

LAB time (EPISODE 6)

- nmap
 - enumeration of a targeted host
 - e.g., **nmap** -p 1-65535 -sV -sS -T4 target
- iptables
 - IPTables is a popular tool used to filter network packets in Linux systems.
 - e.g., iptables -A INPUT -i eth0 -p tcp --d port 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --s port 80 -m state --state ESTABLISHED -j ACCEPT