Internet Security

Prof. A. A. Daptardar
HIT, Nidasoshi

IP Security Overview:

- IP security (IPSec) is a capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.
- Users have security concerns that cut across protocol layers.
- For example, an enterprise can run a secure, private IP network by disallowing links to untrusted sites, encrypting packets that leave the premises, and authenticating packets that enter the premises.

- By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications.
- IP - level security encompasses three functional areas: authentication, confidentiality, and key management.

Applications of IPSec:

- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- Examples of its use include the following:
  - **Secure branch office connectivity over the Internet:** A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

- **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. This reduces the cost of toll charges for traveling employees and telecommuters.
- **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.

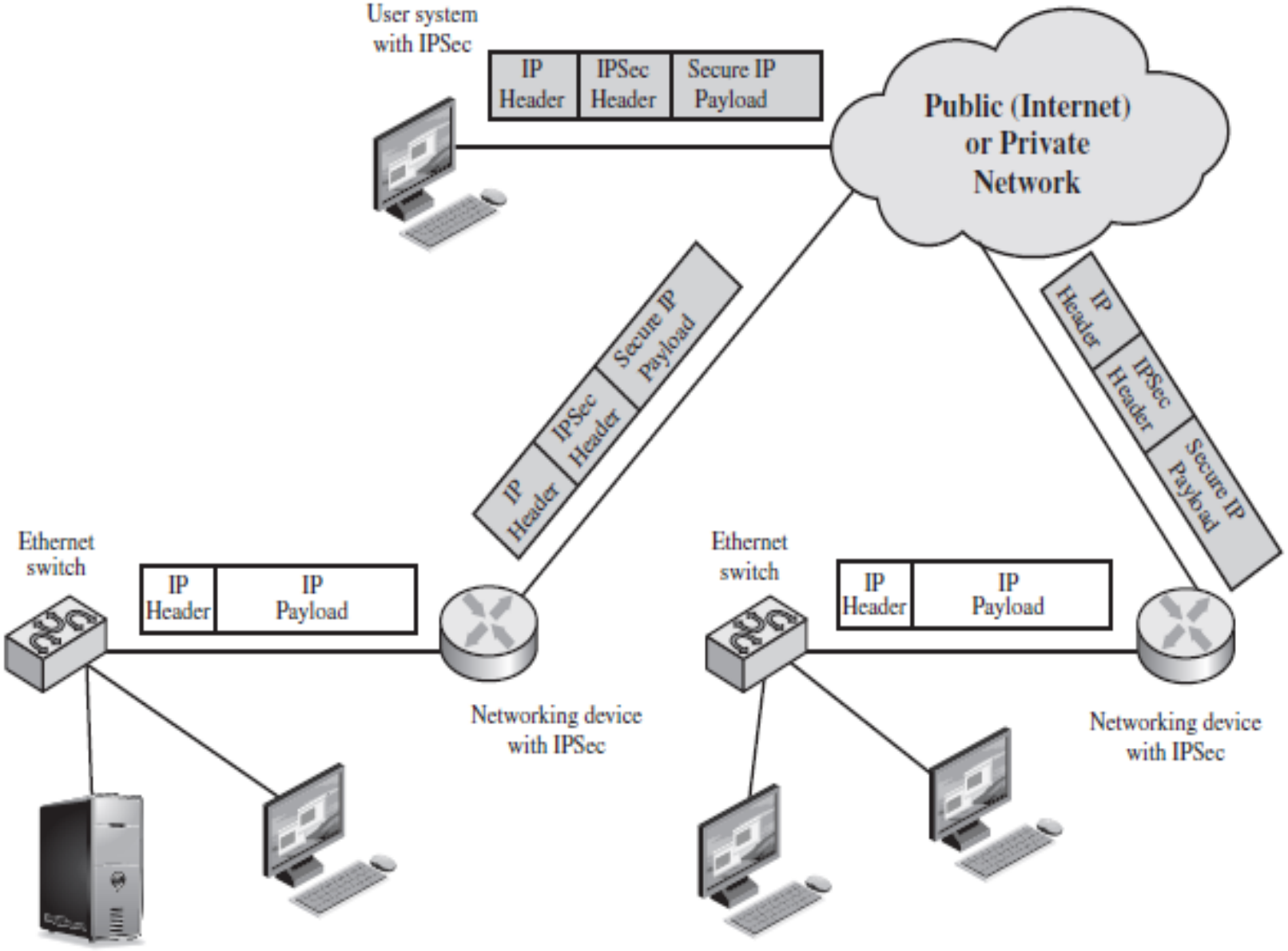


Figure 20.1 An IP Security Scenario

Benefits of IPSec:

- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- IPSec is below the 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.

- IPSec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- 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 organization for sensitive applications.

Routing Applications:

- In addition to supporting end users and protecting premises systems and networks, IPSec can play a vital role in the routing architecture required for internetworking. IPSec can assure that:
  - A router advertisement (a new router advertises its presence) comes from an authorized router.
  - A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router.
  - A redirect message comes from the router to which the initial packet was sent.
  - A routing update is not forged.

IPSec Documents:

- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.
- **Authentication Header (AH):** AH is an extension header to provide message authentication.
- **Encapsulating Security Payload (ESP):** ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
- **Internet Key Exchange (IKE):** This is a collection of documents describing the key management schemes for use with IPsec.

- **Cryptographic algorithms:** This category encompasses a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange.
- **Other:** There are a variety of other IPsec-related RFCs, including those dealing with security policy and management information base (MIB) content.

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.
- Two protocols are used to provide security:
  - an authentication protocol designated by the header of the protocol, Authentication Header (AH);
  - a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).

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

Transport & Tunnel Modes:

- Both AH and ESP support two modes of use:
  - transport mode
  - tunnel mode

Transport Mode

- Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet.
- Examples include a TCP or UDP segment or an ICMP packet, all of which operate directly above IP in a host protocol stack.
- Typically, transport mode is used for end-to-end communication between two hosts.

- When a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header.
- For IPv6, the payload is the data that normally follow both the IP header and any IPv6 extensions headers that are present, with the possible exception of the destination options header, which may be included in the protection.
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
- AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel Mode

- Tunnel mode provides protection to the entire IP packet.
- To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new outer IP packet with a new outer IP header.
- The entire original, inner, packet travels through a tunnel from one point of an IP network to another.

- No routers along the way are able to examine the inner IP header.
- Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security.
- With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec.
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Table 20.1 Tunnel Mode and 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.

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.
- IPsec policy is determined primarily by the interaction of two databases, the **security association database (SAD) and the security policy database (SPD).**

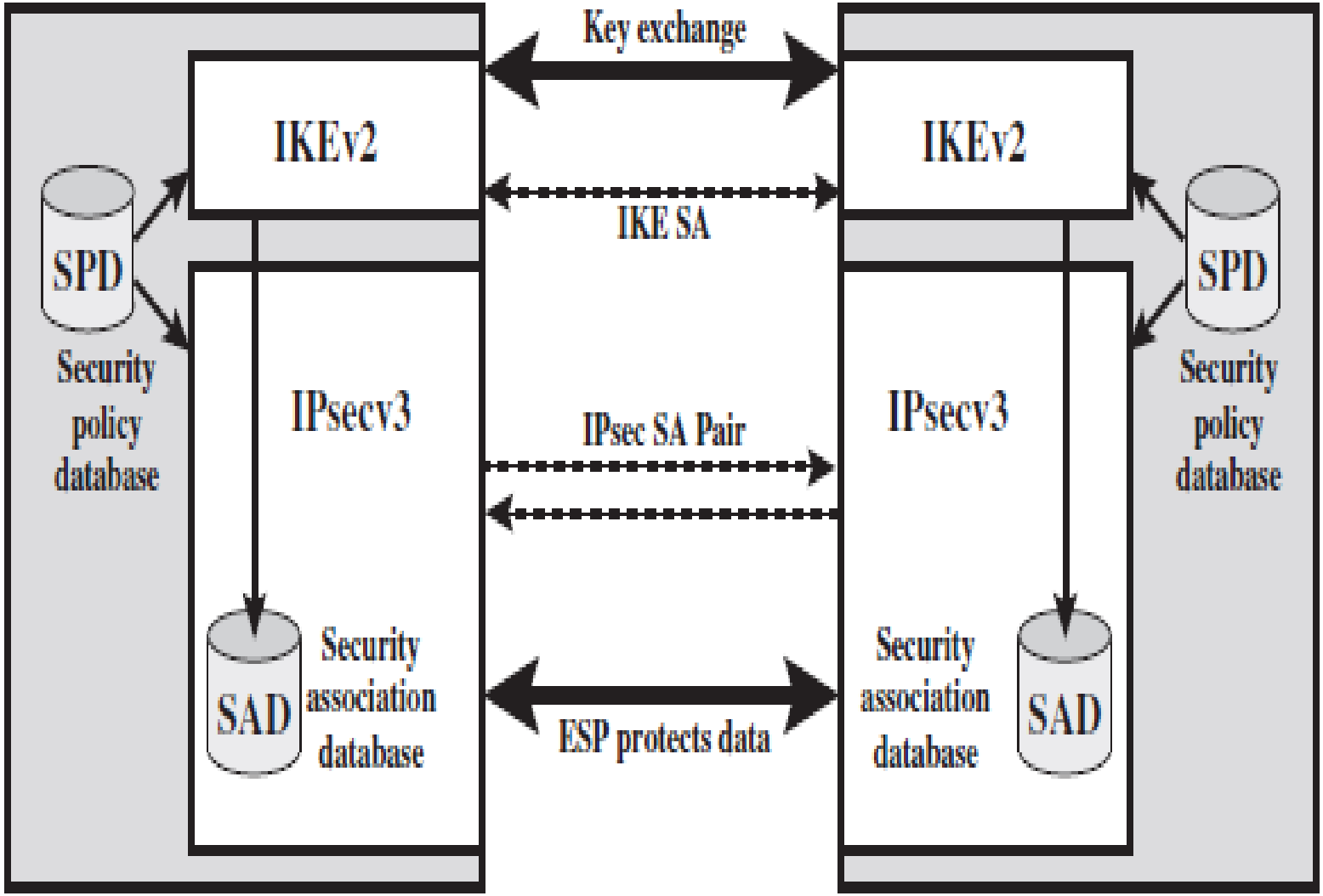


Figure 20.2 IPsec Architecture

Security Associations

- An association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.
- If a peer relationship is needed for two-way secure exchange, then two security associations are required.

- A security association is uniquely identified by three parameters.
  - **Security Parameters Index (SPI):** A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
  - **IP Destination Address:** This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
  - **Security Protocol Identifier:** This field from the outer IP header indicates whether the association is an AH or ESP security association.

Security Association Database

- In each IPsec implementation, there is a nominal Security Association Database that defines the parameters associated with each SA.
- A security association is normally defined by the following parameters in an SAD entry.

- **Security Parameter Index:** A 32-bit value selected by the receiving end of an SA to uniquely identify the SA.
- **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers
- **Sequence Counter Overflow:** A 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
- **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
- **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 (required for all implementations).

Security Policy Database

- The means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec) is the nominal Security Policy Database (SPD).
- Each SPD entry is defined by a set of IP and upper-layer protocol field values, called selectors.
- In effect, these selectors are used to filter outgoing 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).

- The following selectors determine an SPD entry:
  - **Remote IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
  - **Local IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
  - **Next Layer Protocol:** The IP protocol header (IPv4, IPv6, or IPv6 Extension) includes a field (Protocol for IPv4, Next Header for IPv6 or IPv6 Extension) that designates the protocol operating over IP.
  - **Name:** A user identifier from the operating system. This is 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.
  - **Local and Remote Ports:** These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port.

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).

Outbound Packets

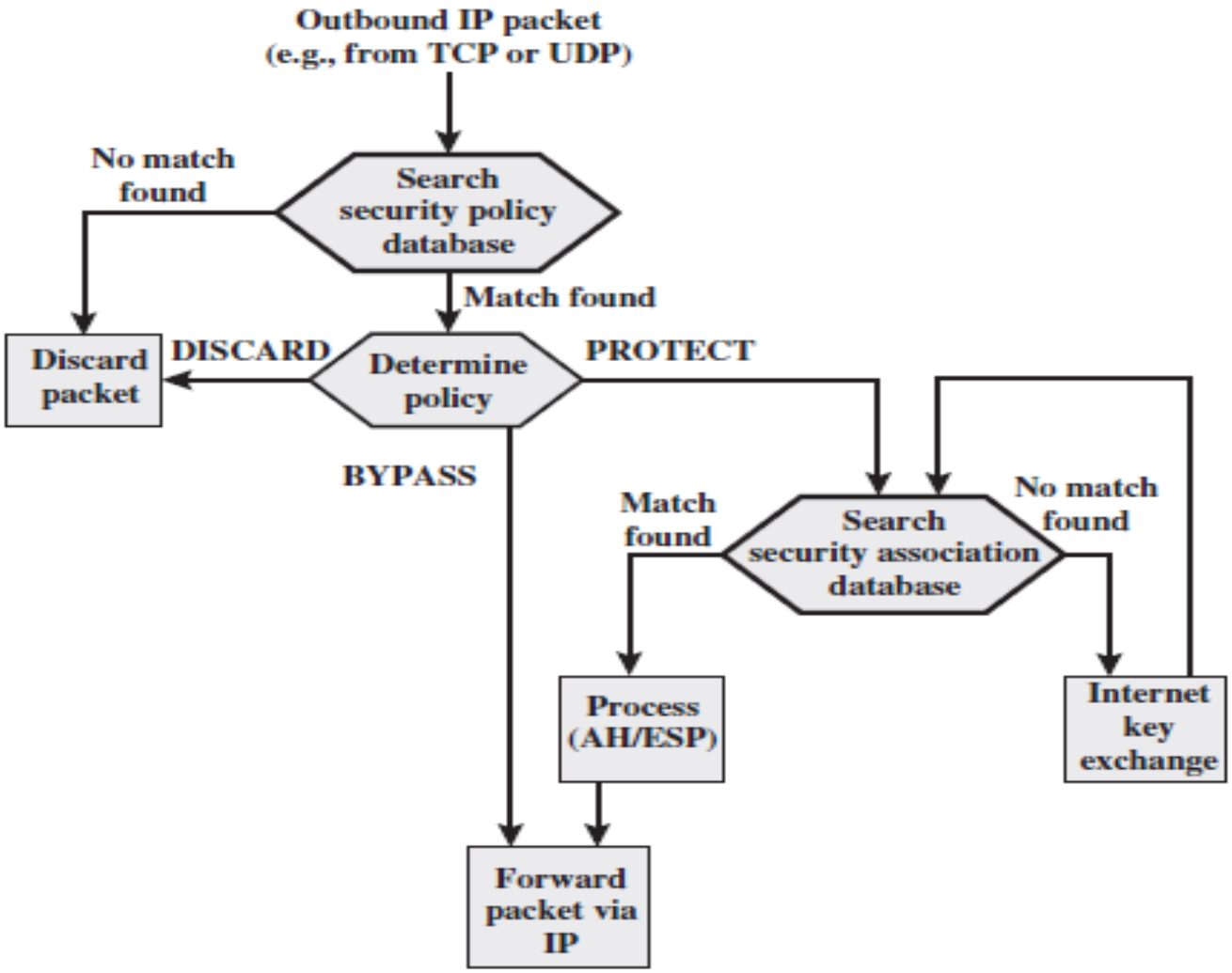


Figure 20.3 Processing Model for Outbound Packets

- A block of data from a higher layer, such as TCP, is passed down to the IP layer and an IP packet is formed, consisting of an IP header and an IP body. Then the following steps occur:
  - **1.** IPsec searches the SPD for a match to this packet.
  - **2.** If no match is found, then the packet is discarded and an error message is generated.
  - **3.** 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. If the policy is BYPASS, then there is no further IPsec processing; the packet is forwarded to the network for transmission.
  - **4**. If the policy is PROTECT, then a search is made of the SAD for a matching entry. If no entry is found, then IKE is invoked to create an SA with the appropriate keys and an entry is made in the SA.
  - **5.** The matching entry in the SAD determines the 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.

Inbound Packets

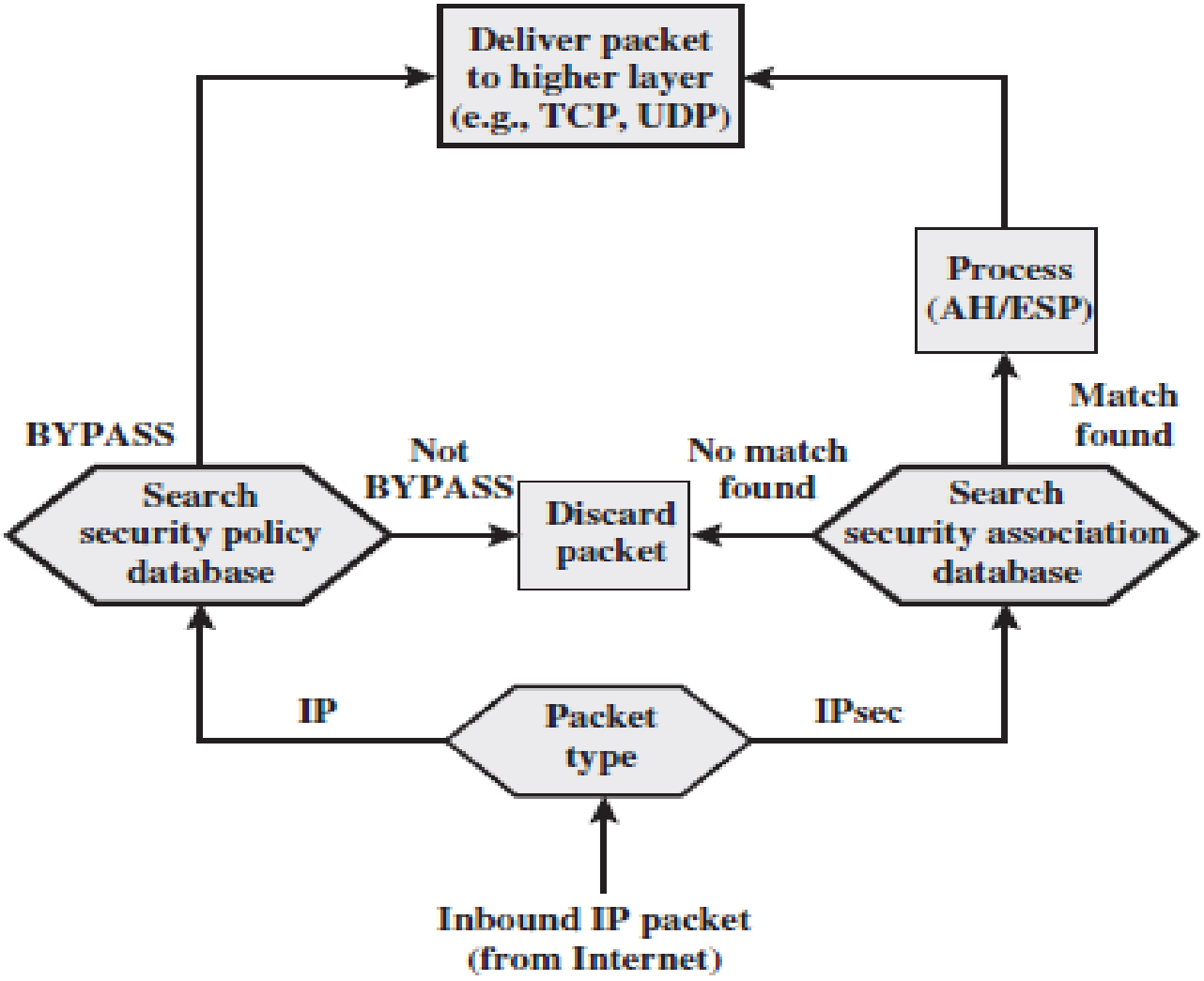


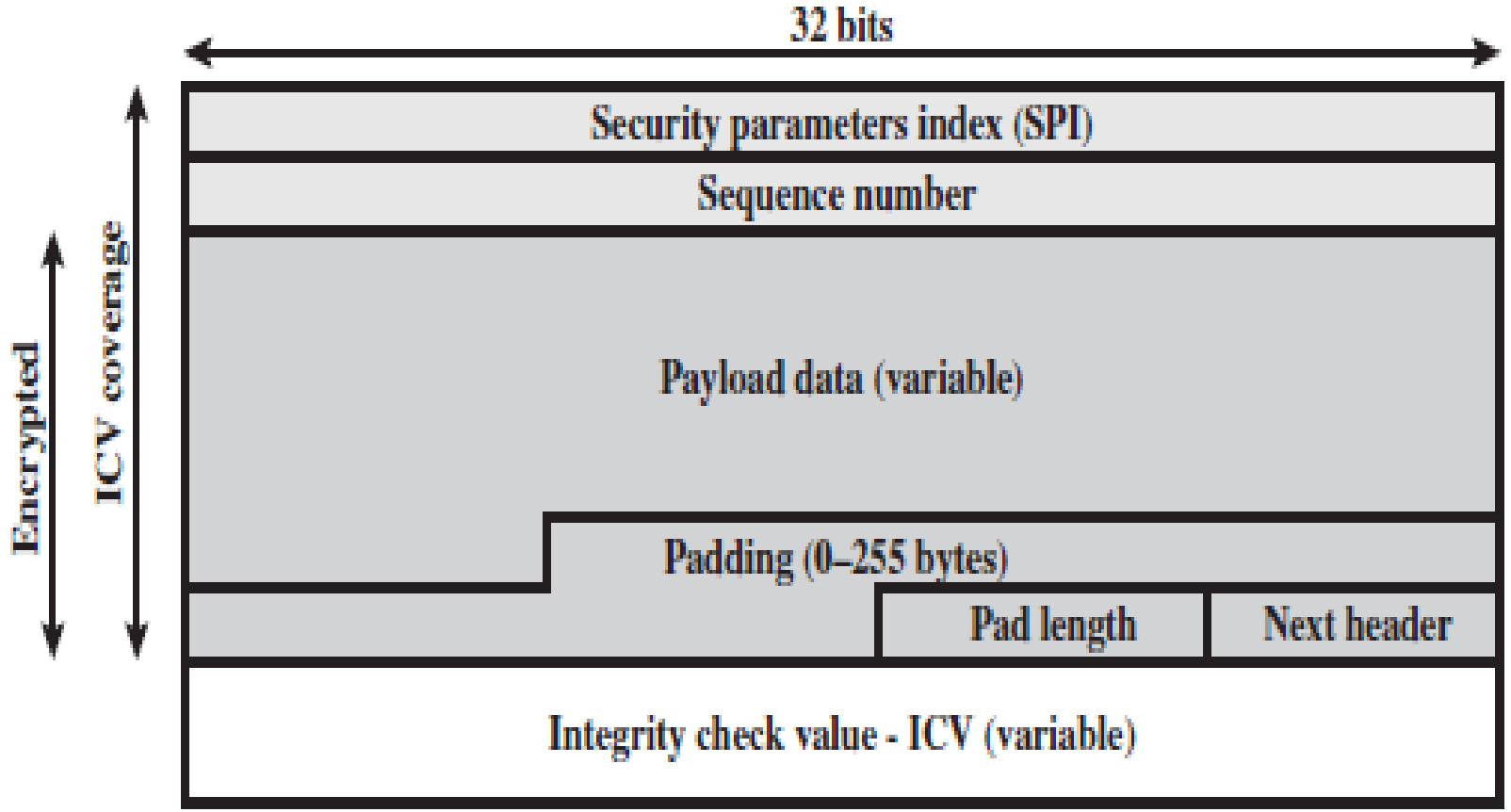
Figure 20.4 Processing Model for Inbound Packets

- An incoming IP packet triggers the IPsec processing. The following steps occur:
  - **1.** 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).
  - **2.** If the packet is unsecured, IPsec searches the SPD for a match to this packet. If the first matching entry has a policy of BYPASS, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP. If the first matching entry has a policy of PROTECT or DISCARD, or if there is no matching entry, the packet is discarded.
  - **3.** For a secured packet, IPsec searches the SAD. If no match is found, the packet is discarded. Otherwise, IPsec applies the appropriate ESP or AH processing. Then, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP.

ENCAPSULATING SECURITY PAYLOAD

- ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.
- The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.

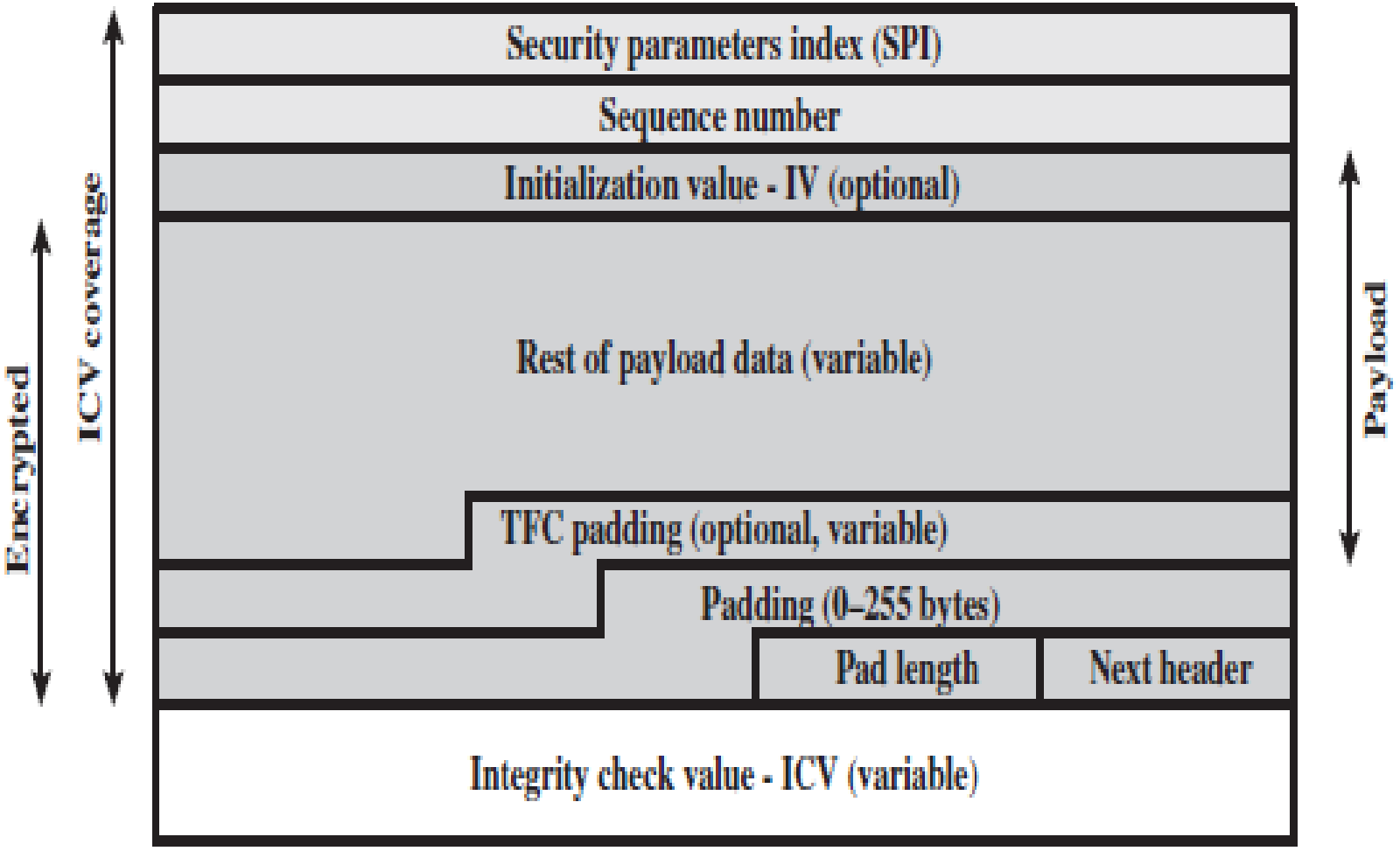
IPSec ESP Format



(a) Top-level format of an ESP Packet

- **Security Parameters Index (32 bits):** Identifies a security association.
- **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0–255 bytes):** The purpose of this field is discussed later.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.

- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (e.g., an extension header in IPv6, or an upper-layer protocol such as TCP).
- **Integrity Check Value (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.



(b) Substructure of payload data

- Two additional fields may be present in the payload (Figure 20.5b).
  - An **initialization value (IV), or nonce,** is present if this is required by the encryption or authenticated encryption algorithm used for ESP.
  - If tunnel mode is being used, then the IPsec implementation may add **traffic flow confidentiality (TFC)** padding after the Payload Data and before the Padding field, as explained subsequently.

Encryption Algorithms

- The Payload data, Padding, pad length & Next header fields are encrypted by ESP service.
- If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an initialization vector (IV), then these data may be carried explicitly at the beginning of the Payload Data field.
- If included, an IV is usually not encrypted, although it is often referred to as being part of the ciphertext.

- The ICV field is optional. It is present only if the integrity service is selected and is provided by either a separate integrity algorithm or a combined mode algorithm that uses an ICV.
- The ICV is computed after the encryption is performed.
- This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver prior to decrypting the packet, hence potentially reducing the impact of denial of service (DoS) attacks..

Padding

- The Padding field serves several purposes:
  - If an encryption algorithm requires the plaintext to be a multiple of some number of bytes the Padding field is used to expand the plaintext to the required length.
  - The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word.
  - Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.

Anti-Replay Service

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
- The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.
- The Sequence Number field is designed to thwart such attacks.

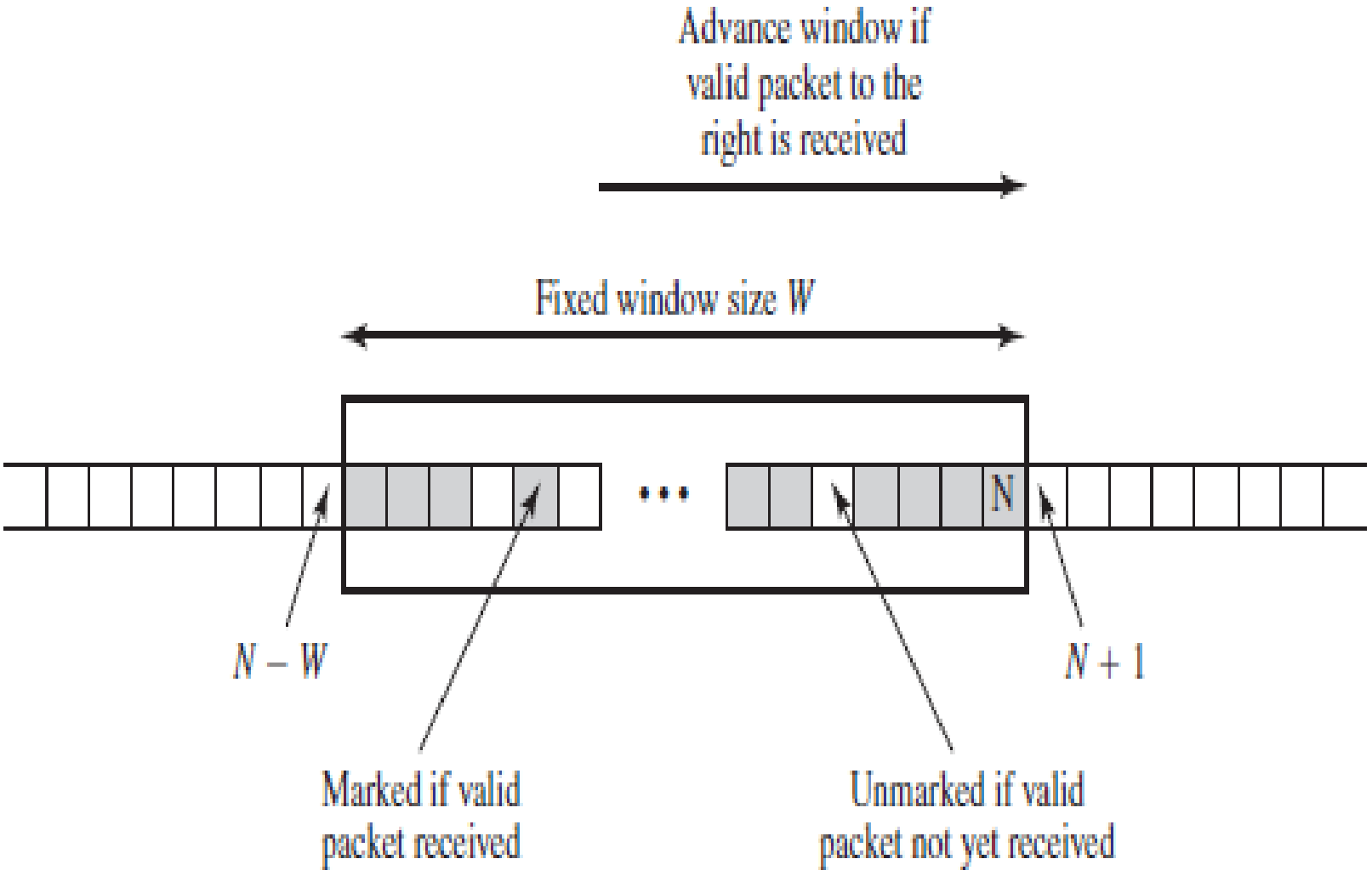
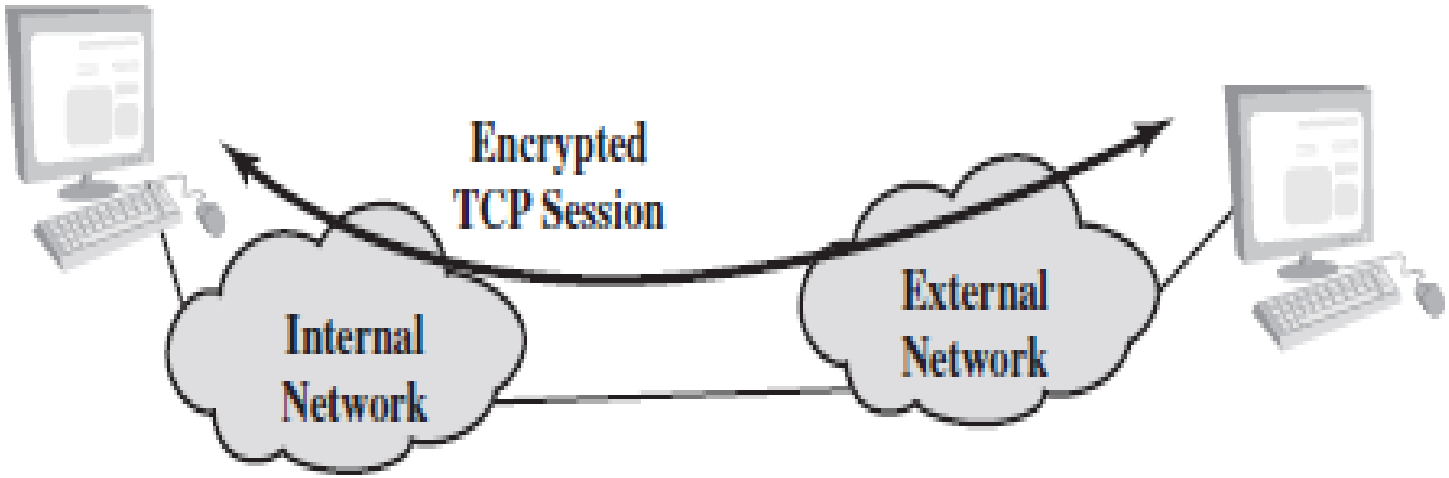


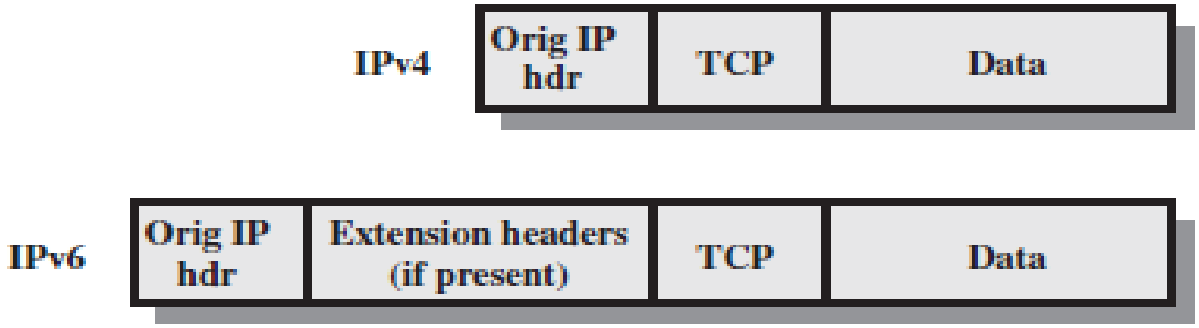
Figure 20.6 Anti-replay Mechanism

- Inbound processing proceeds as follows when a packet is received:
  - 1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
  - 2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
  - 3. If the received packet is to the left of the window or if authentication fails, the packet is discarded; this is an auditable event.

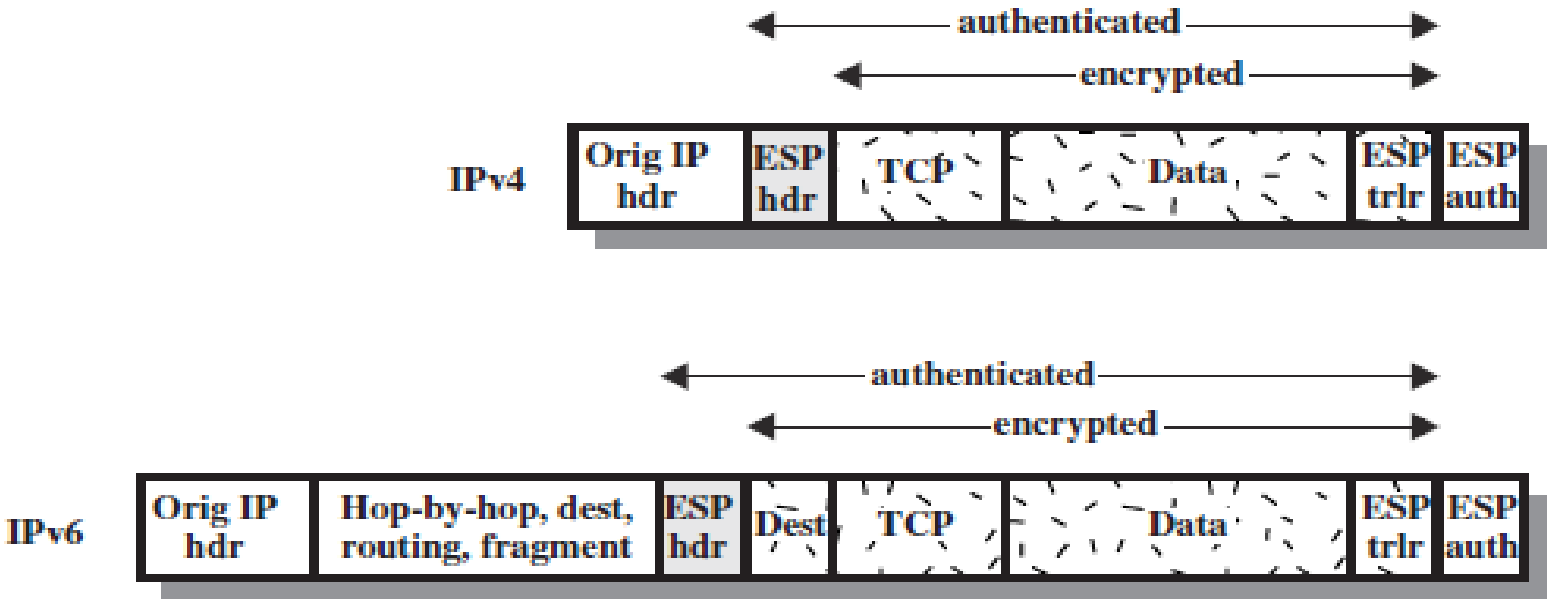
Transport Mode



(a) Transport-level security

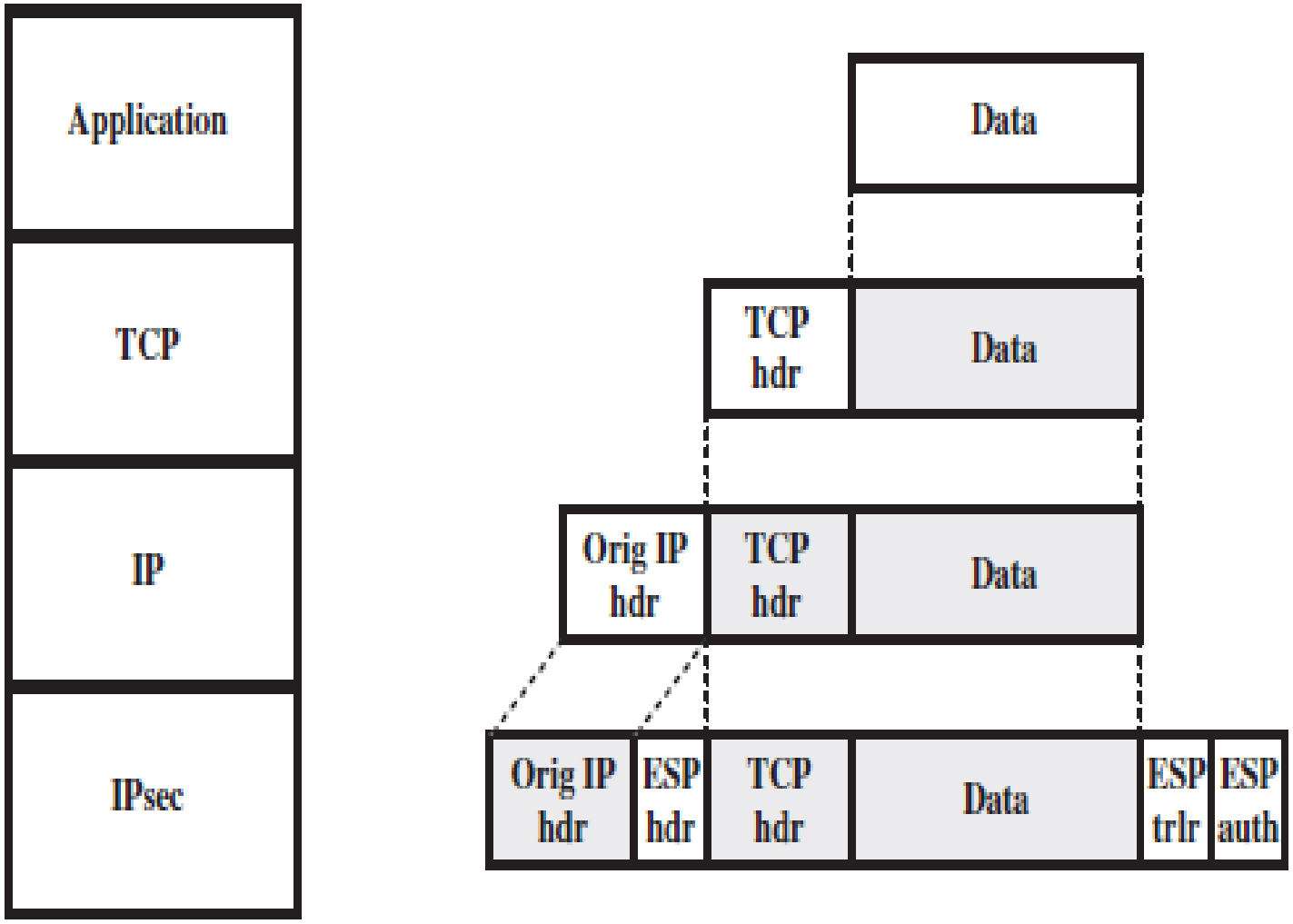


(a) Before Applying ESP



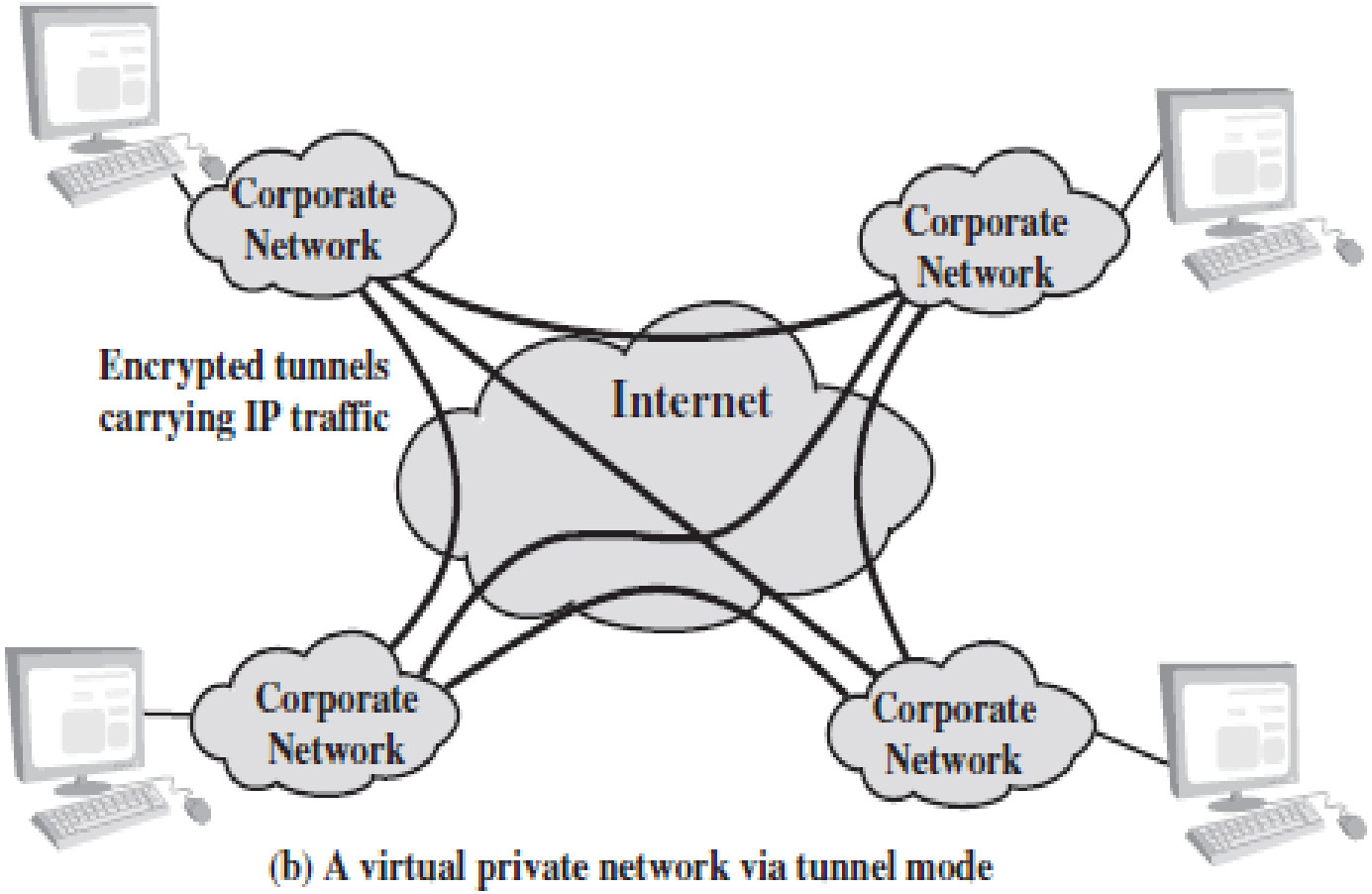
(b) Transport Mode

- Transport mode operation may be summarized as follows.
  - 1. At the source, the block of data consisting of the ESP trailer plus the entire transport-layer segment is encrypted and the plaintext of this block is replaced with its ciphertext to form the IP packet for transmission. Authentication is added if this option is selected.
  - 2. The packet is then routed to the destination. Each intermediate router needs to examine and process the IP header plus any plaintext IP extension headers but does not need to examine the ciphertext.
  - 3. The destination node examines and processes the IP header plus any plaintext IP extension headers. Then, on the basis of the SPI in the ESP header, the destination node decrypts the remainder of the packet to recover the plaintext transport-layer segment.

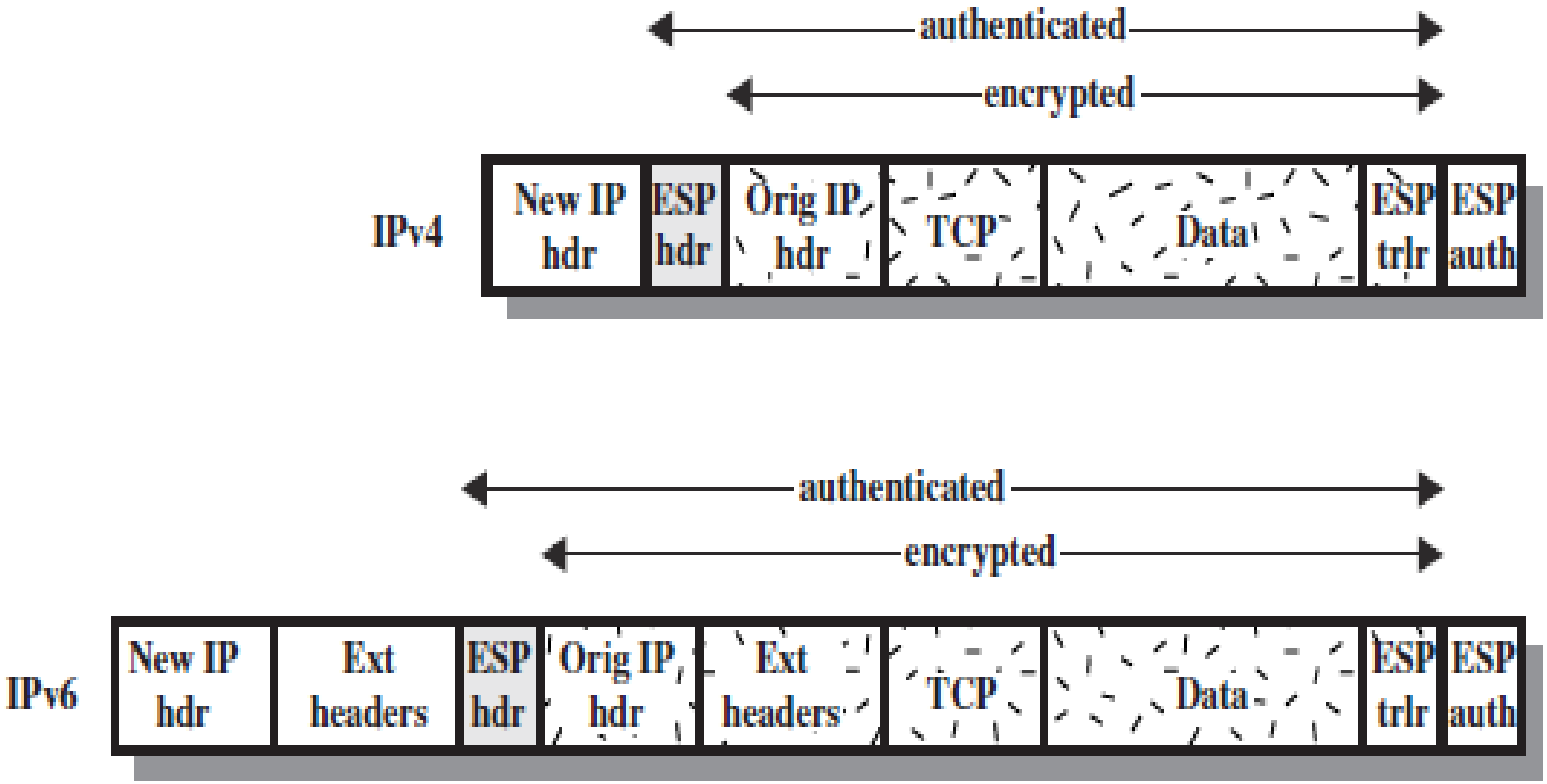


(a) Transport mode

Tunnel Mode



(b) A virtual private network via tunnel mode

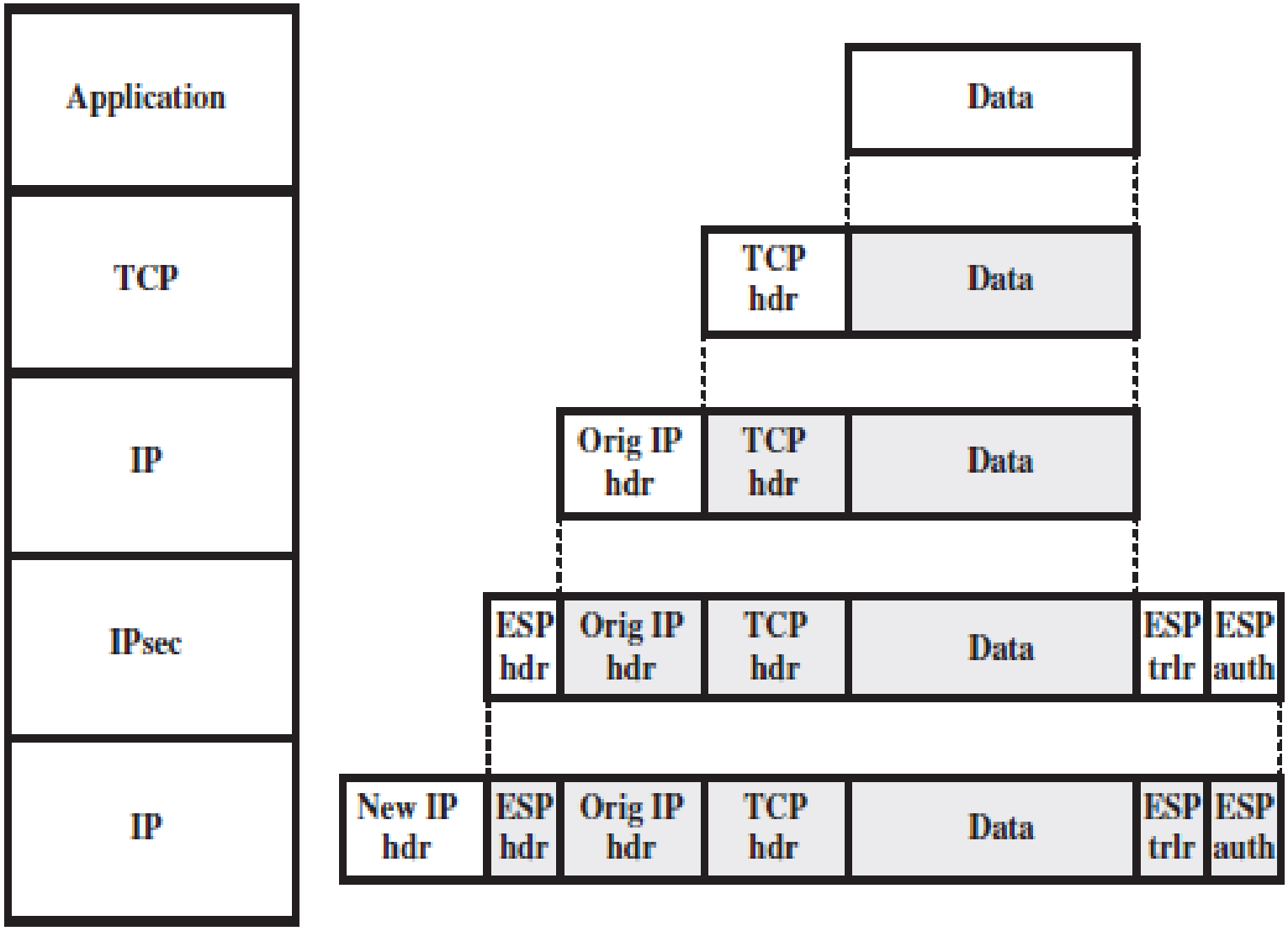


(c) Tunnel Mode

Tunnel Mode Operation

- The source prepares an inner IP packet with a destination address of the target internal host. This packet is prefixed by an ESP header; then the packet and ESP trailer are encrypted and Authentication Data may be added. The resulting block is encapsulated with a new IP header whose destination address is the firewall; this forms the outer IP packet.
- The outer packet is routed to the destination firewall. Each intermediate router needs to examine and process the outer IP header plus any outer IP extension headers but does not need to examine the ciphertext.

- The destination firewall examines and processes the outer IP header plus any outer IP extension headers. Then, on the basis of the SPI in the ESP header, the destination node decrypts the remainder of the packet to recover the plaintext inner IP packet. This packet is then transmitted in the internal network.
- The inner packet is routed through zero or more routers in the internal network to the destination host.



(b) Tunnel mode

COMBINING SECURITY ASSOCIATIONS

- 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.
- Security associations may be combined into bundles in two ways:
  - Transport adjacency: Refers to applying more than one security protocol to the same IP packet without invoking tunneling.
  - Iterated tunneling: Refers to the application of multiple layers of security protocols effected through IP tunneling.

Authentication Plus Encryption

- ESP WITH AUTHENTICATION OPTION
- TRANSPORT ADJACENCY
- TRANSPORT-TUNNEL BUNDLE

ESP WITH AUTHENTICATION OPTION

- **Transport mode ESP**: Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected.
- **Tunnel mode ESP**: Authentication applies to the entire IP packet delivered to the outer IP destination address (e.g., a firewall), and authentication is performed at that destination.

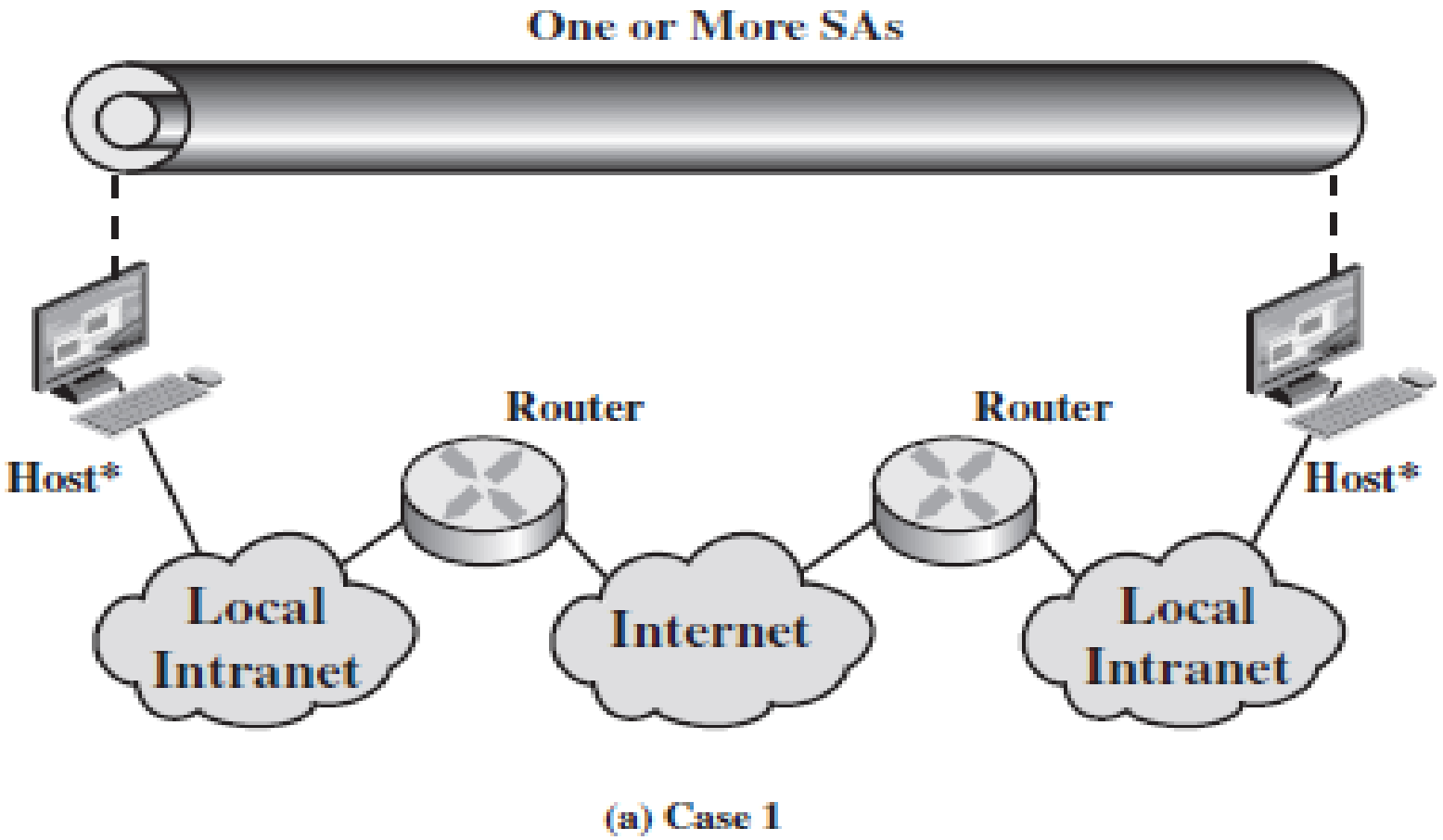
TRANSPORT ADJACENCY

- Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA.
- In this case, ESP is used without its authentication option.
- ***Advantage :*** ***A***uthentication covers more fields, including the source and destination IP addresses.
- Disadvantage is the overhead of two SAs versus one SA.

TRANSPORT-TUNNEL BUNDLE

- Authentication data needs to be protected.
- May be desirable to store the authentication data with the message at the destination for later reference.
- One approach to applying authentication before encryption between two hosts is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA.

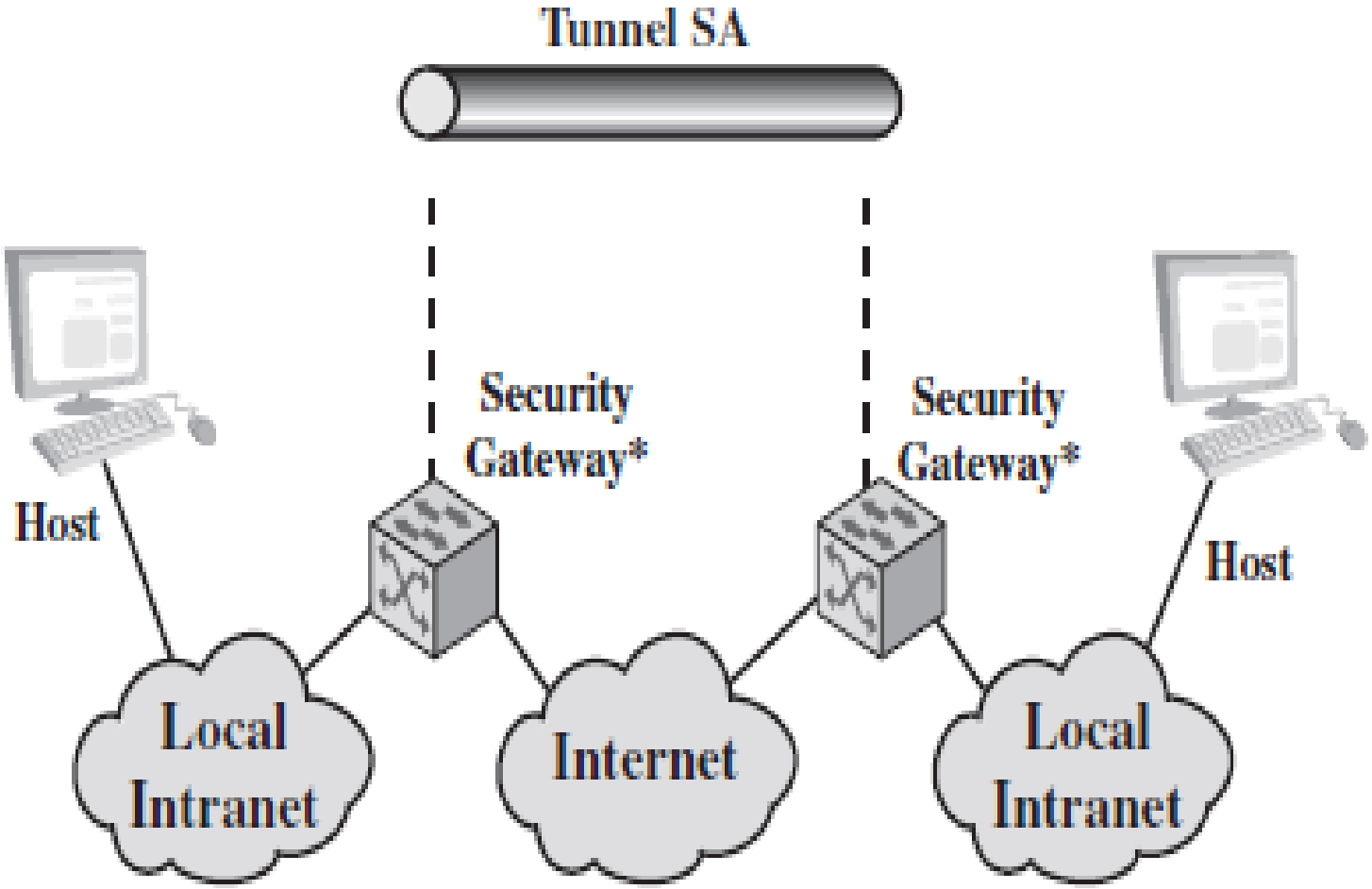
Basic Combinations of SAs



(a) Case 1

Case 1

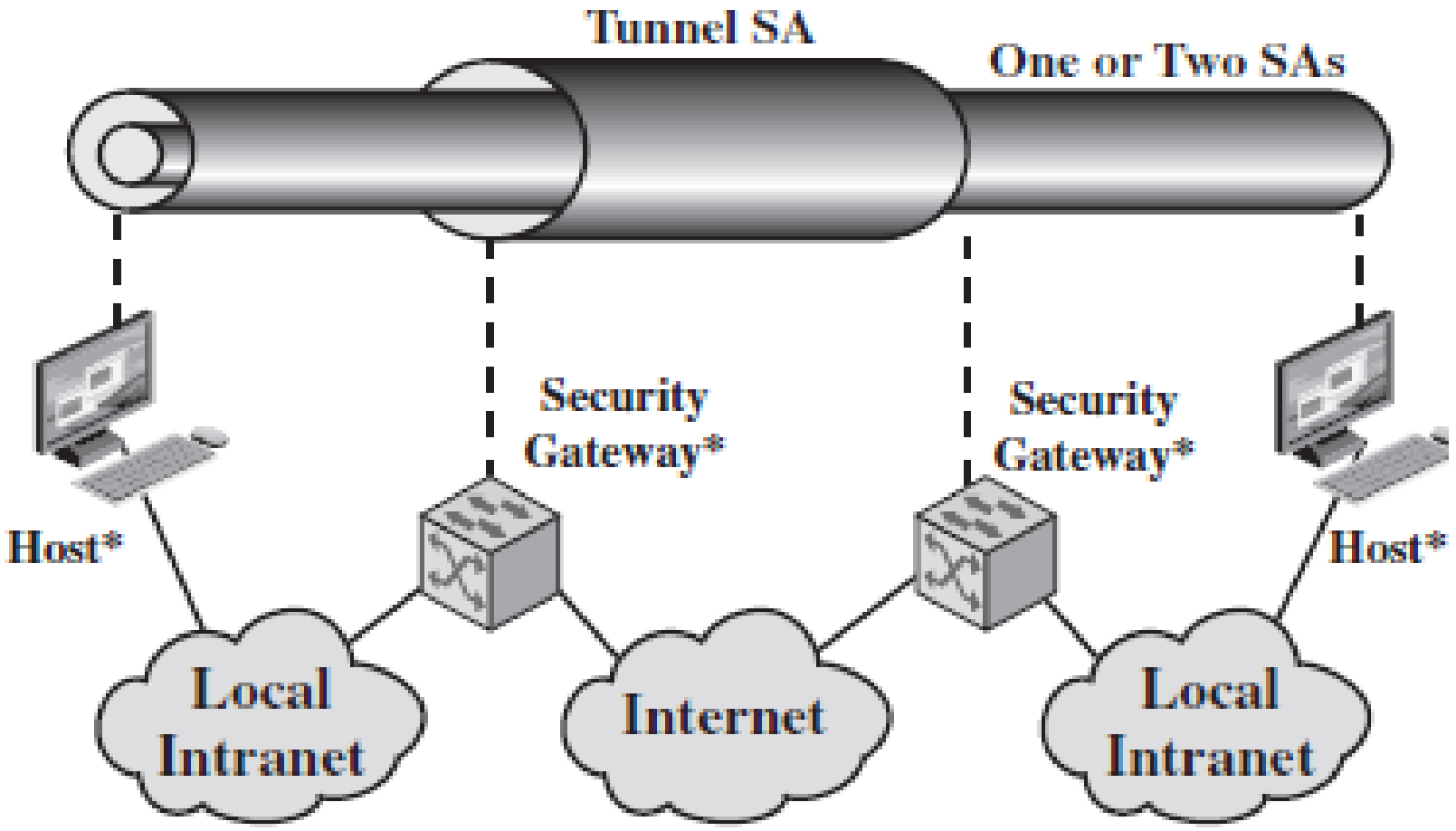
- All security is provided between end systems that implement IPsec.
- For any two end systems to communicate via an SA, they must share the appropriate secret keys.
- Among the possible combinations are
  - a. AH in transport mode
  - b. ESP in transport mode
  - c. ESP followed by AH in transport mode (an ESP SA inside an AH SA)
  - d. Any one of a, b, or c inside an AH or ESP in tunnel mode


Tunnel SA
Security Gateway*
Security Gateway*
Host
Host
Local Intranet
Internet
Local Intranet

(b) Case 2

Case 2

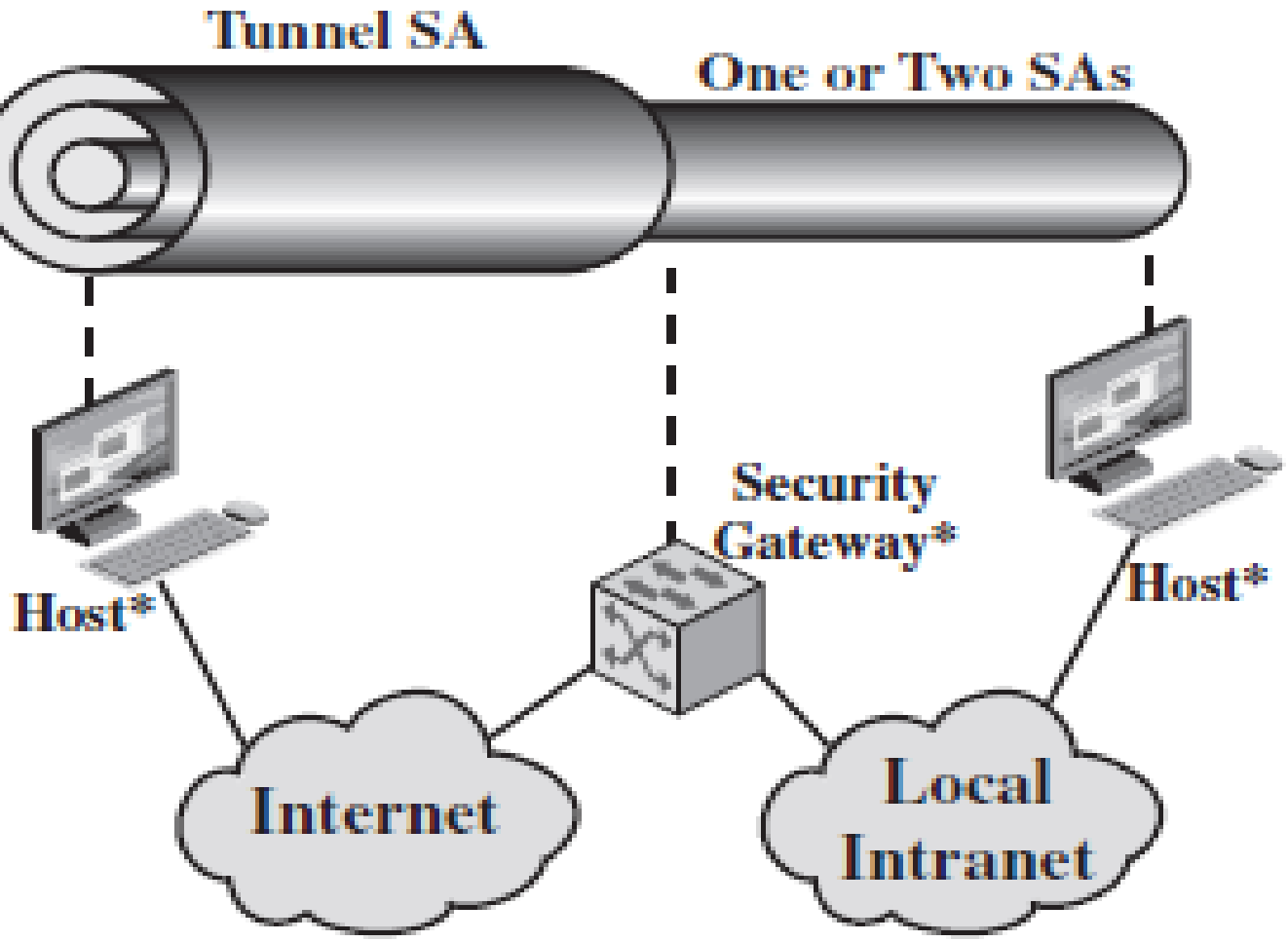
- Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec.
- This case illustrates simple virtual private network support.
- The security architecture document specifies that only a single tunnel SA is needed for this case.
- The tunnel could support AH, ESP,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


Tunnel SA
One or Two SAs
Security Gateway*
Security Gateway*
Host*
Host*
Local Intranet
Internet
Local Intranet

(c) Case 3

Case 3

- 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.


Tunnel SA
One or Two SAs
Security
Gateway*
Host*
Host*
Internet
Local
Intranet

(d) Case 4

Case 4

- This 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.

Internet Key Exchange

- The key management portion of IPsec involves the determination and distribution of secret keys.
- A typical requirement is four keys for communication between two applications: transmit and receive pairs for both integrity and confidentiality.

- The IPsec Architecture document mandates support for two types of key management:
  - **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems.
  - **Automated:** An 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.

- The default automated key management protocol for IPsec
  - **Oakley Key Determination Protocol:** Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.
  - **Internet Security Association and Key Management Protocol (ISAKMP):** ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

Key Determination Protocol

- The Diffie-Hellman algorithm has two attractive features:
  - Secret keys are created only when needed. There is no need to store secret keys for a long period of time, exposing them to increased vulnerability.
  - The exchange requires no pre-existing infrastructure other than an agreement on the global parameters.

Weaknesses of Diffie-Hellman

- It does not provide any information about the identities of the parties.
- It is subject to a man-in-the-middle attack, in which a third party C impersonates B while communicating with A and impersonates A while communicating with B. Both A and B end up negotiating a key with C, which can then listen to and pass on traffic.
- It is computationally intensive. As a result, it is vulnerable to a clogging attack, in which an opponent requests a high number of keys. The victim spends considerable computing resources doing useless modular exponentiation rather than real work.

Features of IKE key determination

- It employs a mechanism known as cookies to thwart clogging attacks.
- It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange.
- It uses nonces to ensure against replay attacks.
- It enables the exchange of Diffie-Hellman public key values.
- It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

- IKE mandates that cookie generation satisfy three basic requirements:
  - 1. The cookie must depend on the specific parties. This prevents an attacker from obtaining a cookie using a real IP address and UDP port and then using it to swamp the victim with requests from randomly chosen IP addresses or ports.
  - 2. It must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity.
  - 3. The cookie generation and verification methods must be fast to thwart attacks intended to sabotage processor resources.

- IKE key determination supports the use of different **groups for the Diffie-** Hellman key exchange. Each group includes the definition of the two global parameters and the identity of the algorithm.
- The current specification includes the following groups.
- Modular exponentiation with a 768-bit modulus

$$q = 2^{768} - 2^{704} - 1 + 2^{64} \times (\lfloor 2^{638} \times \pi \rfloor + 149686)$$
$$\alpha = 2$$

- Modular exponentiation with a 1024-bit modulus

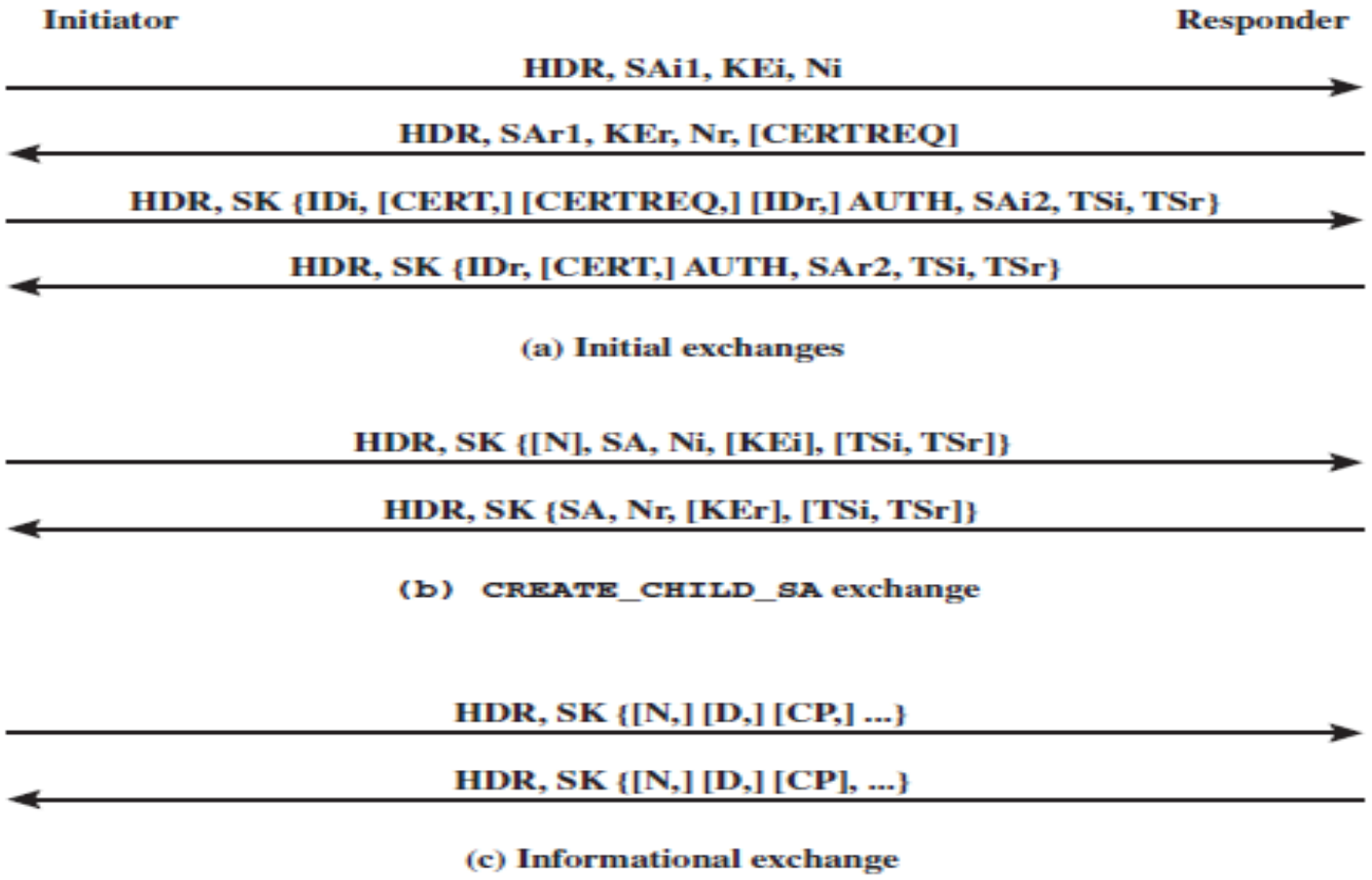
$$q = 2^{1024} - 2^{960} - 1 + 2^{64} \times (\lfloor 2^{894} \times \pi \rfloor + 129093)$$
$$\alpha = 2$$

- Modular exponentiation with a 1536-bit modulus
  - Parameters to be determined
- Elliptic curve group over 2^{155}
  - Generator (hexadecimal): X = 7B, Y = 1C8
  - Elliptic curve parameters (hexadecimal): A = 0, Y = 7338F
- Elliptic curve group over 2^{185}
  - Generator (hexadecimal): X = 18, Y = D
  - Elliptic curve parameters (hexadecimal): A = 0, Y = 1EE9

- IKE key determination employs nonces to ensure against replay attacks.
- Each nonce is a locally generated pseudorandom number.
- Nonces appear in responses and are encrypted during certain portions of the exchange to secure their use.

- Three different authentication methods can be used with IKE key determination:
  - Digital signatures: The exchange is authenticated by signing a mutually obtainable hash; each party encrypts the hash with its private key. The hash is generated over important parameters, such as user IDs and nonces.
  - Public-key encryption: The exchange is authenticated by encrypting parameters such as IDs and nonces with the sender's private key.
  - Symmetric-key encryption: A key derived by some out-of-band mechanism can be used to authenticate the exchange by symmetric encryption of exchange parameters.

IKE v2 Exchanges



HDR = IKE header
SAx1 = offered and chosen algorithms, DH group
KEx = Diffie-Hellman public key
Nx= nonces
CERTREQ = Certificate request
IDx = identity
CERT = certificate

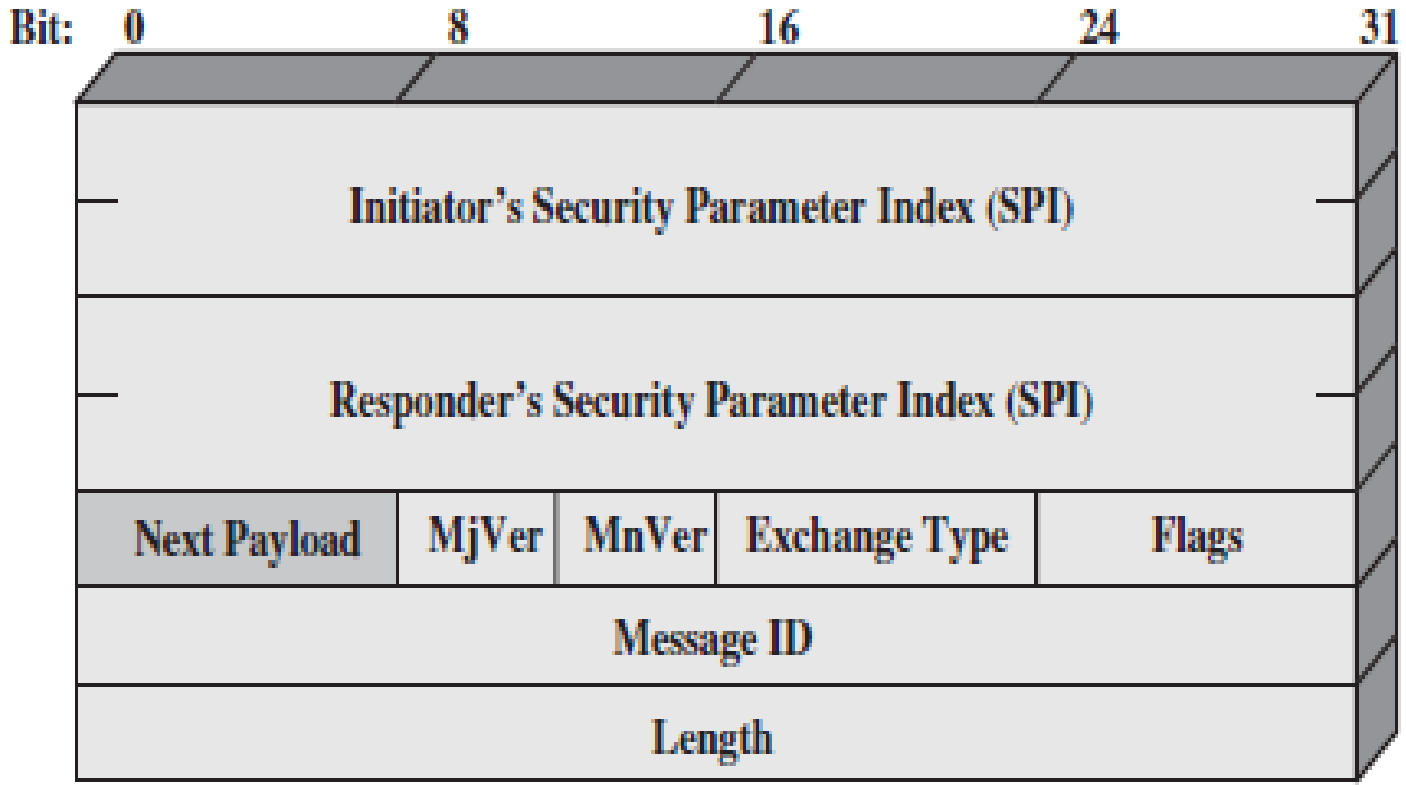
SK {...} = MAC and encrypt
AUTH = Authentication
SAx2 = algorithms, parameters for IPsec SA
TSx = traffic selectors for IPsec SA
N = Notify
D = Delete
CP = Configuration

Figure 20.11 IKEv2 Exchanges

Header and Payload Formats

- IKE defines procedures and packet formats to establish, negotiate, modify, and delete security associations. As part of SA establishment, IKE defines payloads for exchanging key generation and authentication data.
- These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm, and authentication mechanism.

IKE Header Format



(a) IKE header

- **Initiator SPI (64 bits):** A value chosen by the initiator to identify a unique IKE security association (SA).
- **Responder SPI (64 bits):** A value chosen by the responder to identify a unique IKE SA.
- **Next Payload (8 bits):** Indicates the type of the first payload in the message;
- **Major Version (4 bits):** Indicates major version of IKE in use.
- **Minor Version (4 bits):** Indicates minor version in use.
- **Exchange Type (8 bits):** Indicates the type of exchange;

- **Flags (8 bits):** Indicates specific options set for this IKE exchange. Three bits are defined so far. The initiator bit indicates whether this packet is sent by the SA initiator. The version bit indicates whether the transmitter is capable of using a higher major version number than the one currently indicated. The response bit indicates whether this is a response to a message containing the same message ID.
- **Message ID (32 bits):** Used to control retransmission of lost packets and matching of requests and responses.
- **Length (32 bits):** Length of total message (header plus all payloads) in octets.

IKE Payload Types

Table 20.3 IKE Payload Types

Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message

SA payload

- The **SA payload is used to begin the** establishment of an SA.
- The payload has a complex, hierarchical structure.
- The payload may contain multiple proposals.
- Each proposal may contain multiple protocols.
- Each protocol may contain multiple transforms.
- And each transform may contain multiple attributes.

- These elements are formatted as substructures within the payload as follows.
  - **Proposal:** This substructure includes a proposal number, a protocol ID (AH, ESP, or IKE), an indicator of the number of transforms, and then a transform substructure.
  - **Transform:** Different protocols support different transform types. The transforms are used primarily to define cryptographic algorithms to be used with a particular protocol.
  - **Attribute:** Each transform may include attributes that modify or complete the specification of the transform. An example is key length.

Key Exchange payload

- The Key Exchange payload can be used for a variety of key exchange techniques, including Oakley, Diffie-Hellman, and the RSA-based key exchange used by PGP.
- The Key Exchange data field contains the data required to generate a session key and is dependent on the key exchange algorithm used.

Identification payload

- The Identification payload is used to determine the identity of communicating peers and may be used for determining authenticity of information.
- Typically the ID Data field will contain an IPv4 or IPv6 address.

Certificate payload

- The Certificate payload transfers a public-key certificate.
- The Certificate Encoding field indicates the type of certificate or certificate-related information, which may include the following:
  - PKCS #7 wrapped X.509 certificate
  - PGP certificate
  - DNS signed key
  - X.509 certificate—signature
  - X.509 certificate—key exchange
  - Kerberos tokens
  - Certificate Revocation List (CRL)
  - Authority Revocation List (ARL)
  - SPKI certificate

Certificate Request payload

- At any point in an IKE exchange, the sender may include a Certificate Request payload to request the certificate of the other communicating entity.
- The payload may list more than one certificate type that is acceptable and more than one certificate authority that is acceptable.

Authentication payload

- The Authentication payload contains data used for message authentication purposes.
- The authentication method types so far defined are RSA digital signature, shared-key message integrity code, and DSS digital signature.

Nonce payload

- The Nonce payload contains random data used to guarantee liveness during an exchange and to protect against replay attacks.

Notify payload

- The Notify payload contains either error or status information associated with this SA or this SA negotiation. The following table lists the IKE notify messages.

Error Messages	Status Messages
Unsupported Critical Payload	Initial Contact
Invalid IKE SPI	Set Window Size
Invalid Major Version	Additional TS Possible
Invalid Syntax	IPCOMP Supported
Invalid Payload Type	NAT Detection Source IP
Invalid Message ID	NAT Detection Destination IP
Invalid SPI	Cookie
	Use Transport Mode

Error Messages	Status Messages
No Proposal Chosen	HTTP Cert Lookup Supported
Invalid KE Payload	Rekey SA
Authentication Failed	ESP TFC Padding Not Supported
Single Pair Required	Non First Fragments Also
No Additional SAS	
Internal Address Failure	
Failed CP Required	
TS Unacceptable	
Invalid Selectors	

Delete payload

- The Delete payload indicates one or more SAs that the sender has deleted from its database and that therefore are no longer valid.

Vendor ID payload

- The Vendor ID payload contains a vendor-defined constant.
- The constant is used by vendors to identify and recognize remote instances of their implementations.
- This mechanism allows a vendor to experiment with new features while maintaining backward compatibility.

Traffic Selector payload

- The Traffic Selector payload allows peers to identify packet flows for processing by IPsec services.

Encrypted payload

- The Encrypted payload contains other payloads in encrypted form.
- The encrypted payload format is similar to that of ESP.
- It may include an IV if the encryption algorithm requires it and an ICV if authentication is selected.

Configuration payload

- The Configuration payload is used to exchange configuration information between IKE peers.

Extensible Authentication Protocol (EAP) payload

- The Extensible Authentication Protocol (EAP) payload allows IKE SAs to be authenticated using EAP.

Cryptographic Suites

- The IPsecv3 and IKEv3 protocols rely on a variety of types of cryptographic algorithms.
- RFC 4308 defines two cryptographic suites for establishing virtual private networks.
    - Suite VPN-A matches the commonly used corporate VPN security used in older IKEv1 implementations at the time of the issuance of IKEv2 in 2005.
    - Suite VPN-B provides stronger security and is recommended for new VPNs that implement IPsecv3 and IKEv2.

Table 20.4 Cryptographic Suites for IPsec

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

(a) Virtual private networks (RFC 4308)

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/ Integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP

(b) NSA Suite B (RFC 4869)