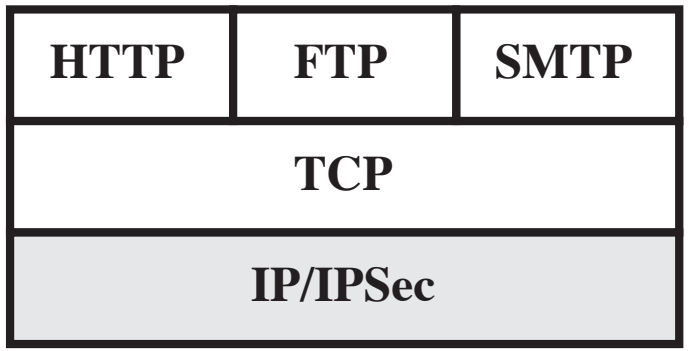
Chapter 20

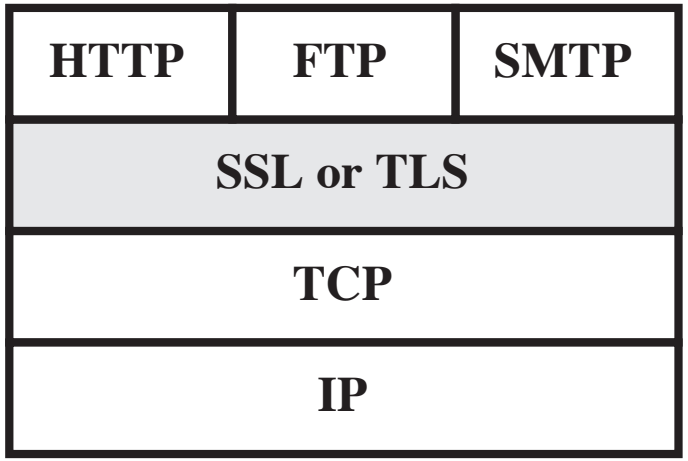
IP Security

IP Security Overview

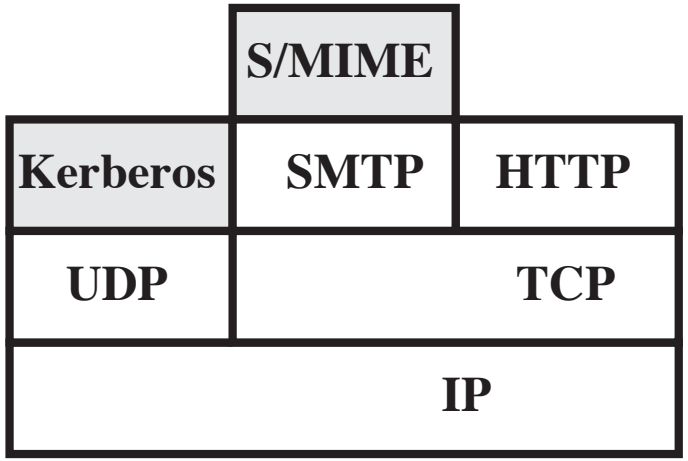
- RFC 1636
  - "Security in the Internet Architecture"
  - Issued in 1994 by the Internet Architecture Board (IAB)
  - Identifies key areas for security mechanisms
    - Need to secure the network infrastructure from unauthorized monitoring and control of network traffic
    - Need to secure end-user-to-end-user traffic using authentication and encryption mechanisms
  - IAB included authentication and encryption as necessary security features in the next generation IP (IPv6)
    - The IPsec specification now exists as a set of Internet standards



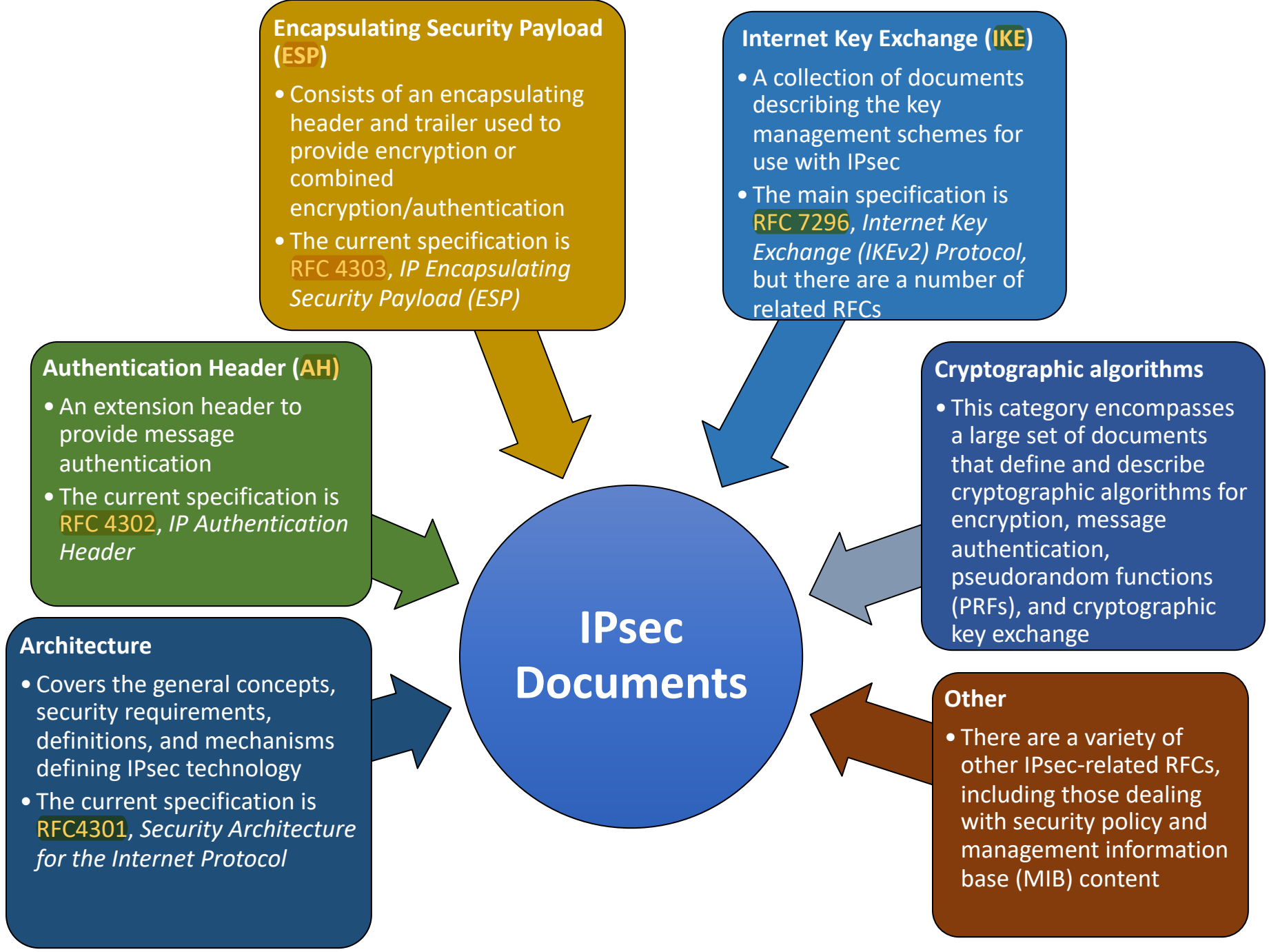
(a) Network Level



(b) Transport Level



(c) Application Level



Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet

Examples include:

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

- Principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level
  - Thus **all** distributed applications (remote logon, client/server, e-mail, file transfer, Web access) can **be secured**

Routing Applications

- IPsec can play a vital role in the routing architecture required for internetworking

IPsec can assure that:

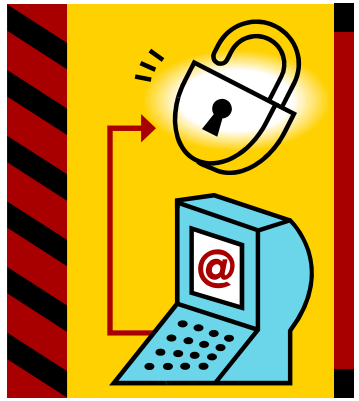
- **A router advertisement comes from an authorized router**
- **A router seeking to establish or maintain a neighbor relationship with a router in another routing domain is an authorized router**
- **A redirect message comes from the router to which the initial IP packet was sent**
- **A routing update is not forged**

Benefits of IPSec

- Some of the 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
    - 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 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

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)
  - Put in place any cryptographic keys required to provide the requested services
- RFC 4301 lists the following services:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality



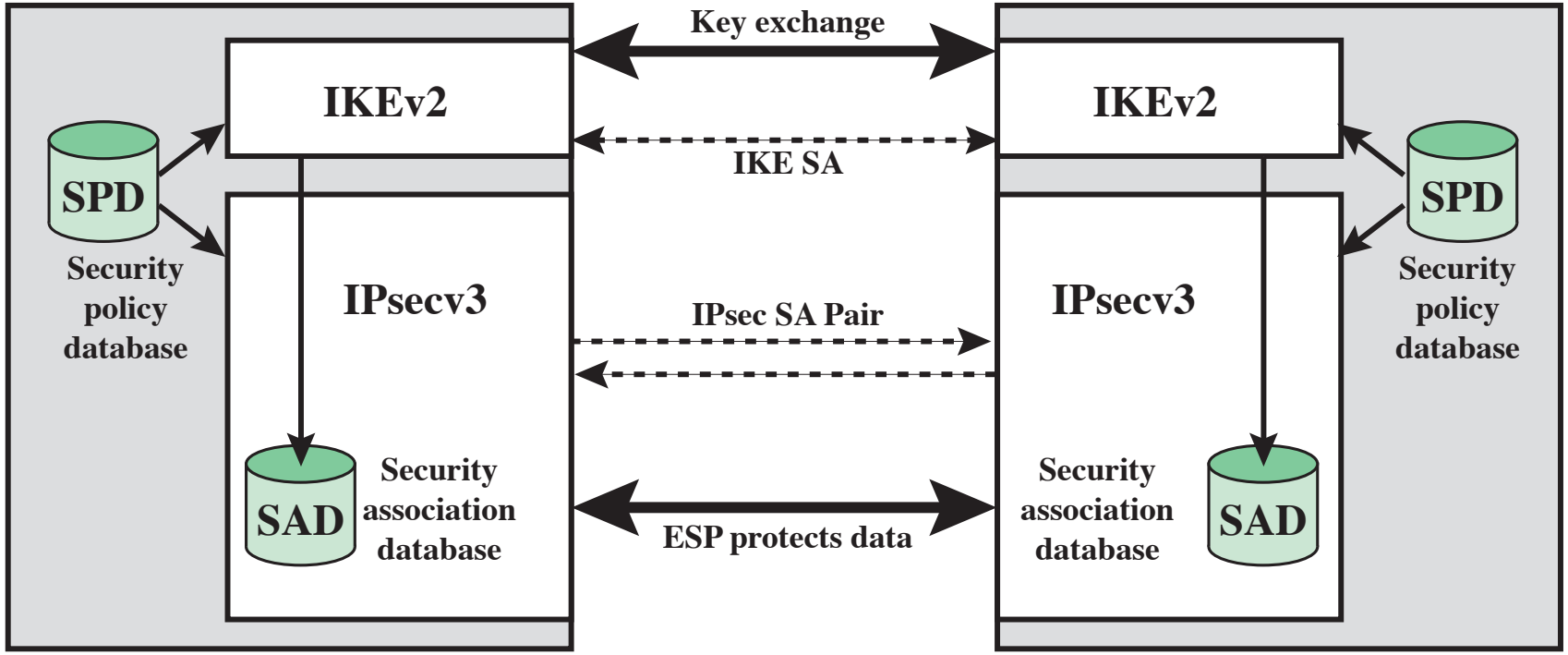
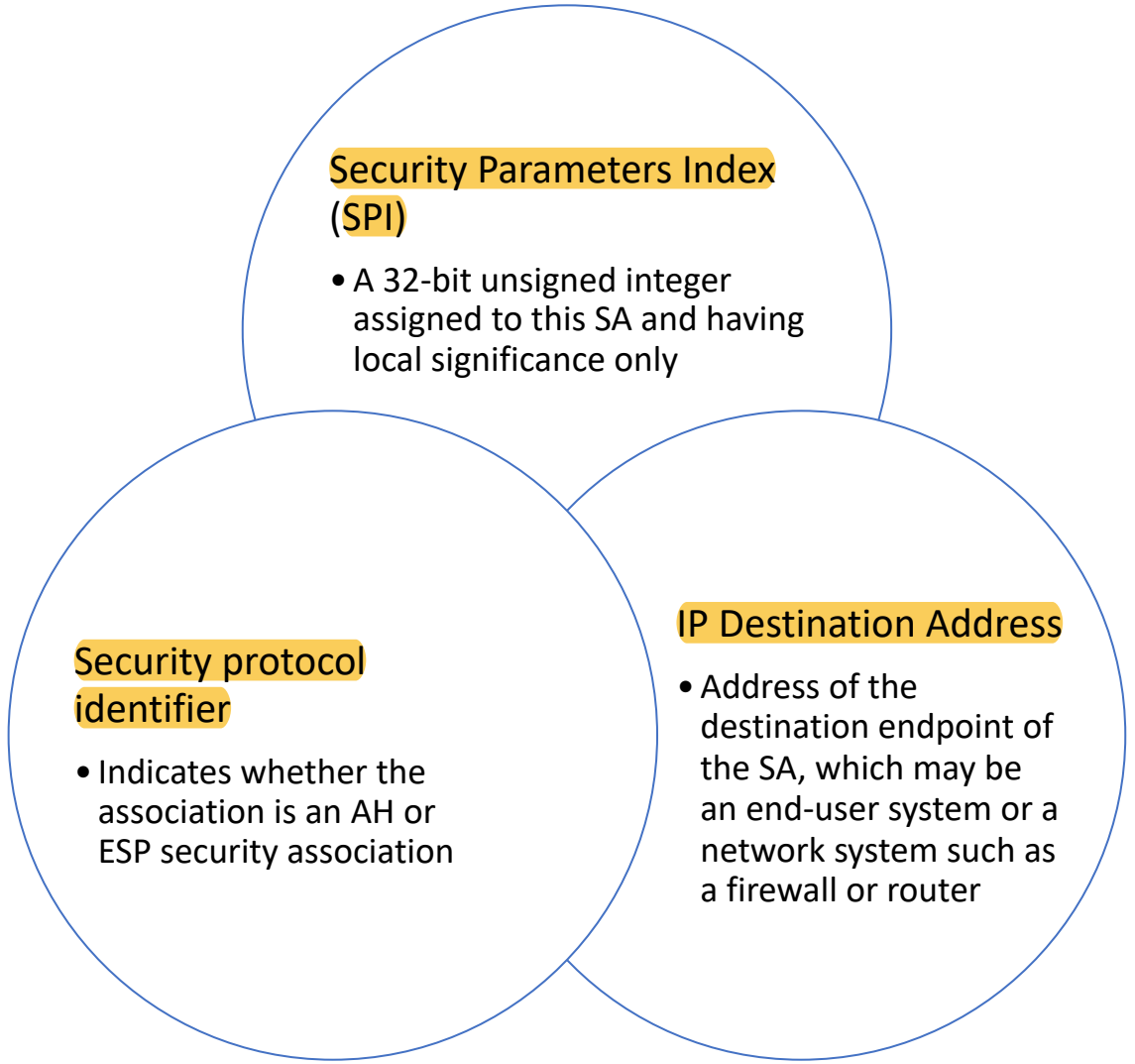


Figure 20.1 IPsec Architecture

Security Association (SA)

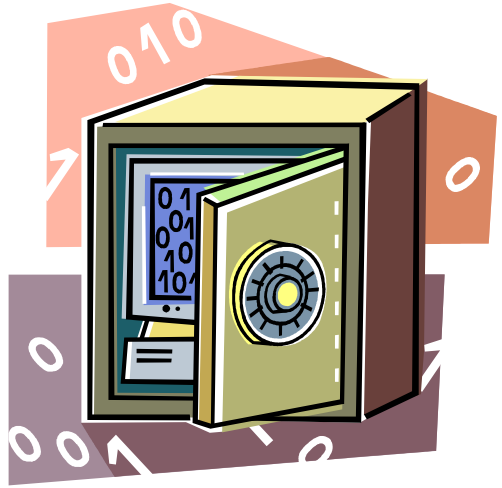
- A one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it
- In any IP packet, the SA is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP)

Uniquely identified by three parameters:



Security Association Database (SAD)

- Defines the parameters associated with each SA
- Normally defined by the following parameters in a SAD entry:
  - Security parameter index
  - Sequence number counter
  - Sequence counter overflow
  - Anti-replay window
  - AH information
  - ESP information
  - Lifetime of this security association
  - IPsec protocol mode
  - Path MTU



Security Policy Database (SPD)

- The means by which IP traffic is related to specific SAs
  - 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
  - Each SPD entry is defined by a set of IP and upper-layer protocol field values called *selectors*
  - These are used to filter outgoing traffic in order to map it into a particular SA

SPD Entries

- The following selectors determine an SPD entry:

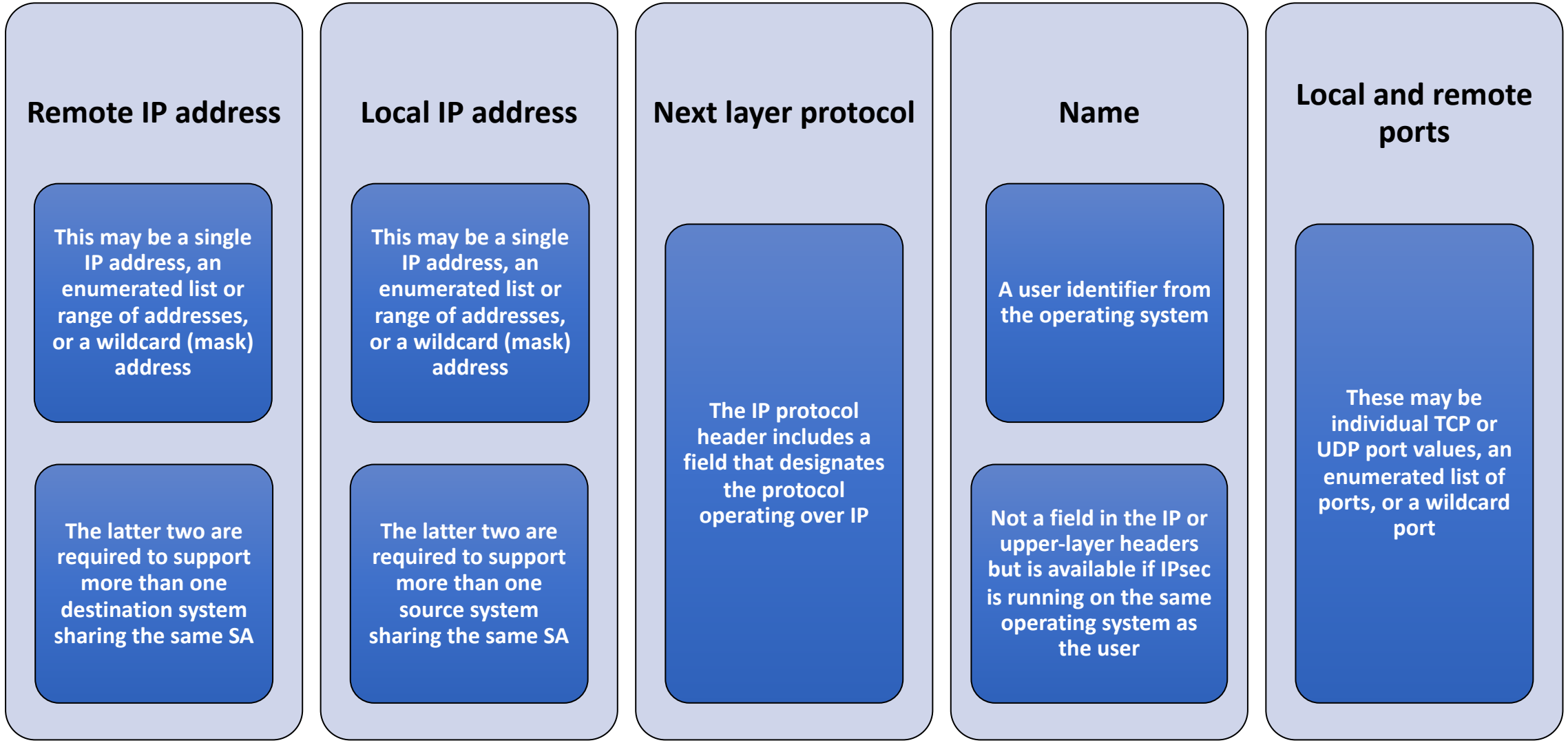


Table 20.1 Host SPD Example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

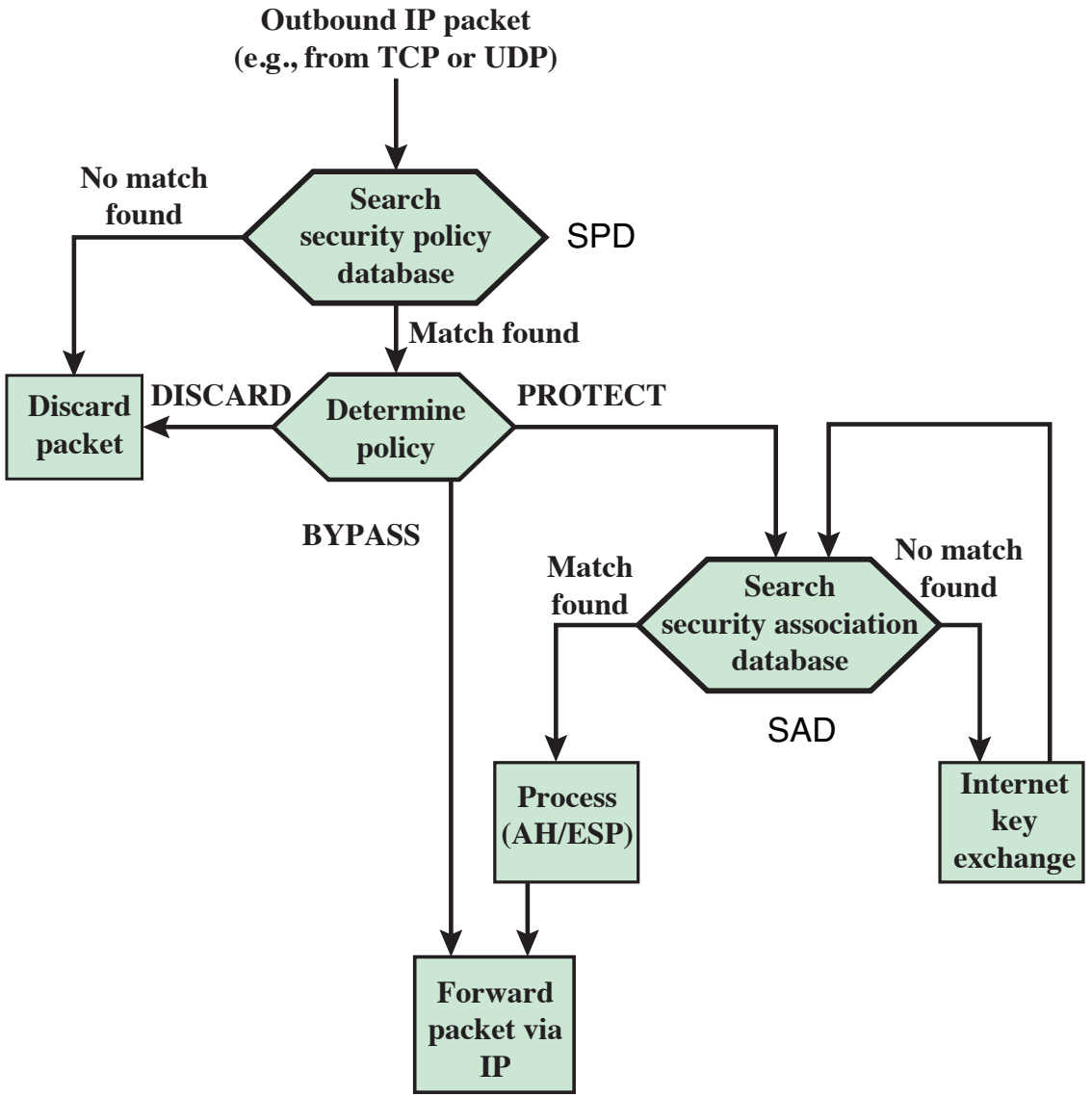


Figure 20.2 Processing Model for Outbound Packets

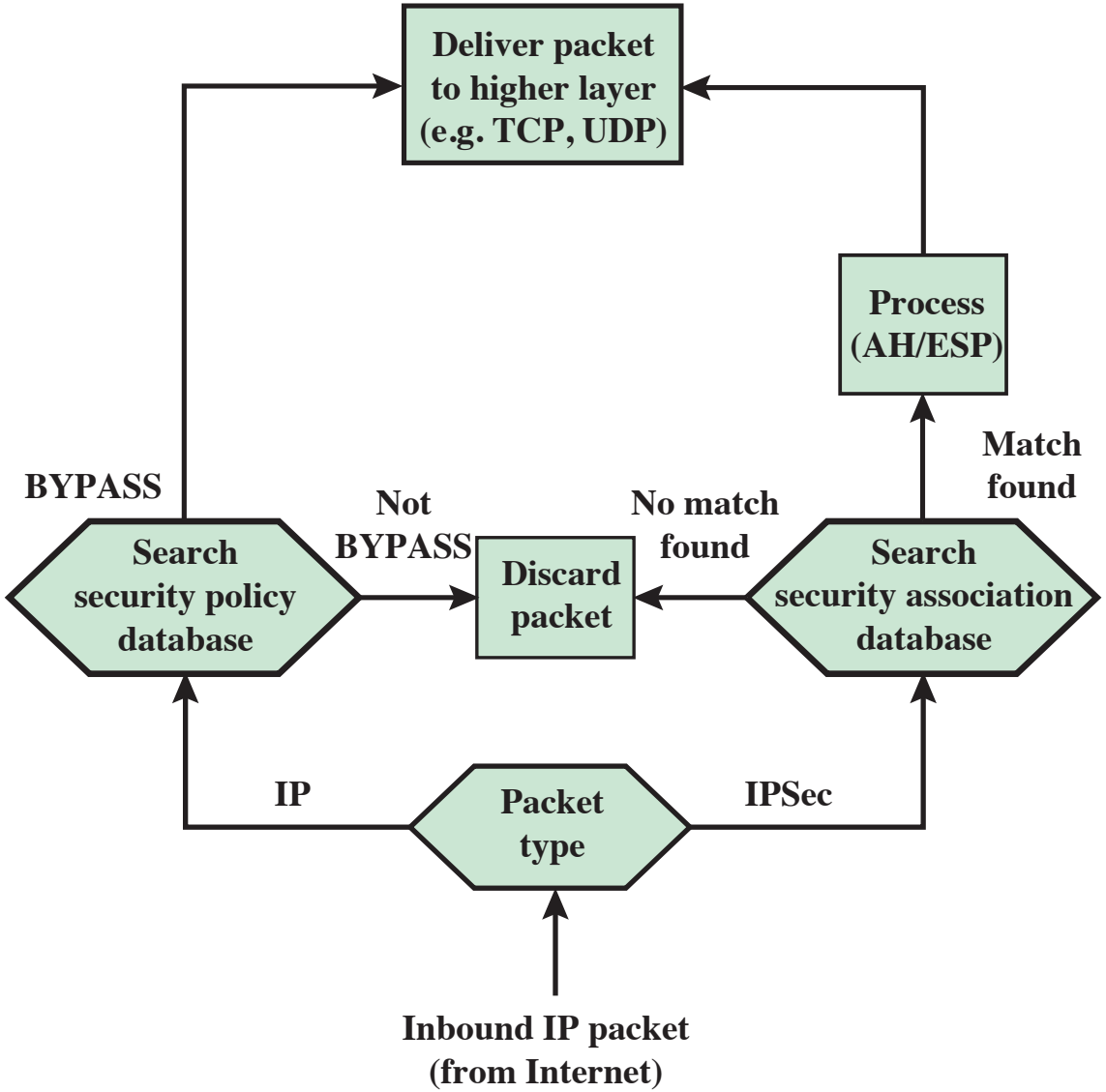
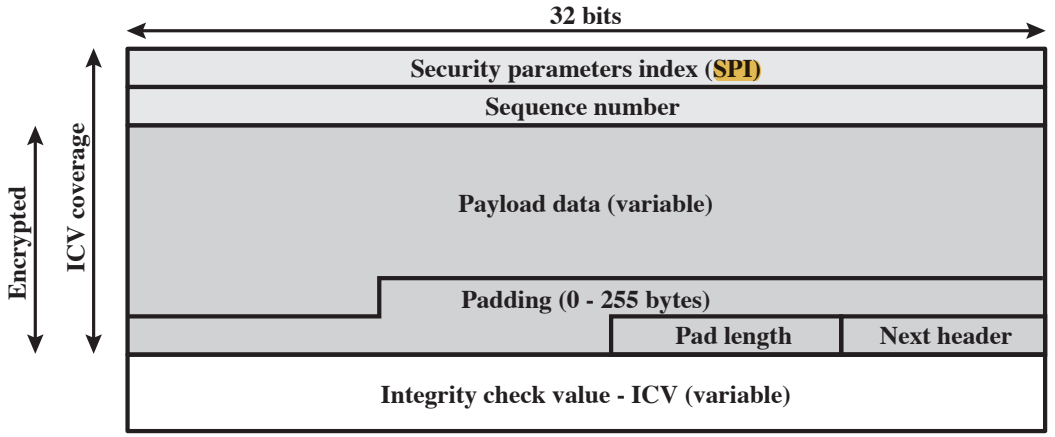
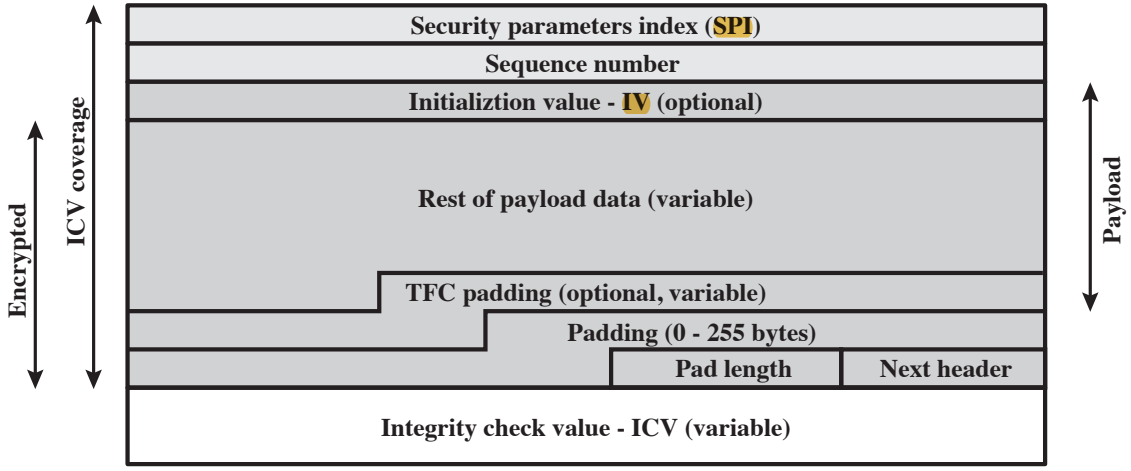


Figure 20.3 Processing Model for Inbound Packets



(a) Top-level format of an ESP Packet



(b) Substructure of payload data

Figure 20.4 ESP Packet Format

Transport and Tunnel Modes

Transport Mode

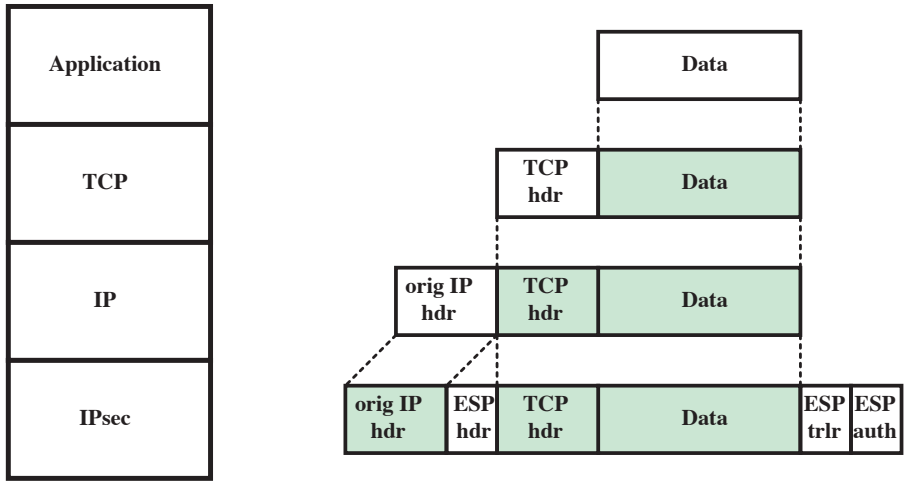
- Provides protection primarily for upper-layer protocols
  - Examples include a TCP or UDP segment or an ICMP packet
- Typically used for end-to-end communication between two hosts
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header
- AH in transport mode authenticates the IP payload and selected portions of the IP header

Tunnel Mode

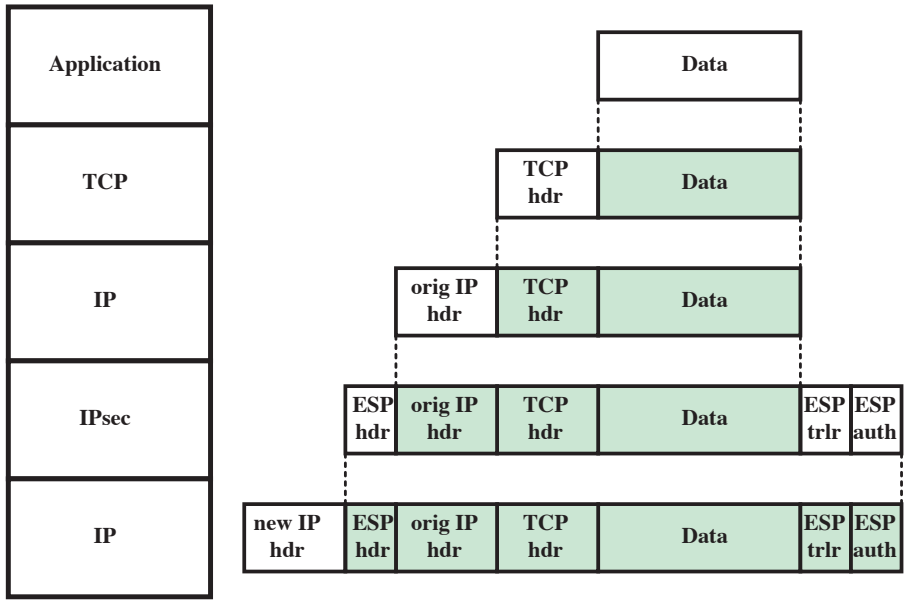
- Provides protection to the entire IP packet
- Used when one or both ends of a security association (SA) are a security gateway
- A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec
- ESP in tunnel mode encrypts and optionally authenticates the 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 20.2 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.



(a) Transport mode



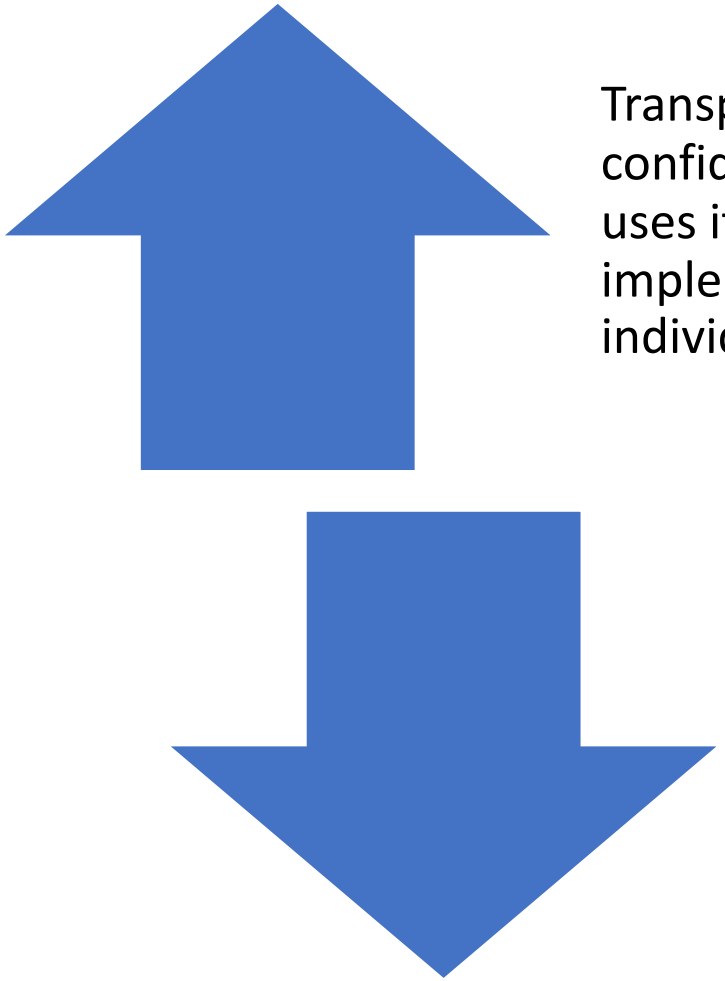
(b) Tunnel mode

Figure 20.9 Protocol Operation for ESP

Transport Mode

- Transport mode operation may be summarized as follows:
  - 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
  - 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
  - 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

Transport Mode



Transport mode operation provides confidentiality for any application that uses it, thus avoiding the 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

Tunnel Mode

- Tunnel mode provides protection to the 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
  - Tunnel mode is used when one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPsec
  - With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec
  - The unprotected packets generated by such hosts are tunneled through external networks by tunnel mode SAs set up by the IPsec software in the firewall or secure router at the boundary of the local network

Tunnel Mode

- 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
- Encryption occurs only between an external host and the security gateway or between two security gateways
    - This relieves hosts on the internal network of the processing burden of encryption and simplifies the key distribution task by reducing the number of needed keys
    - It thwarts traffic analysis based on ultimate destination

Encapsulating Security Payload (ESP)

- Used to encrypt the Payload Data, Padding, Pad Length, and Next Header fields
  - If the algorithm requires cryptographic synchronization data then these data may be carried explicitly at the beginning of the Payload Data field
- An optional ICV field 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
  - ICV is computed after the encryption is performed
  - This order of processing facilitates reducing the impact of DoS attacks
  - Because the ICV is not protected by encryption, a keyed integrity algorithm must be employed to compute the ICV
- 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
  - Used to assure alignment of Pad Length and Next Header fields
  - Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload

ESP with Authentication Option

- In this approach, the first user applies ESP to the data to be protected and then appends the authentication data field

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 and authentication is performed at that destination
- The 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

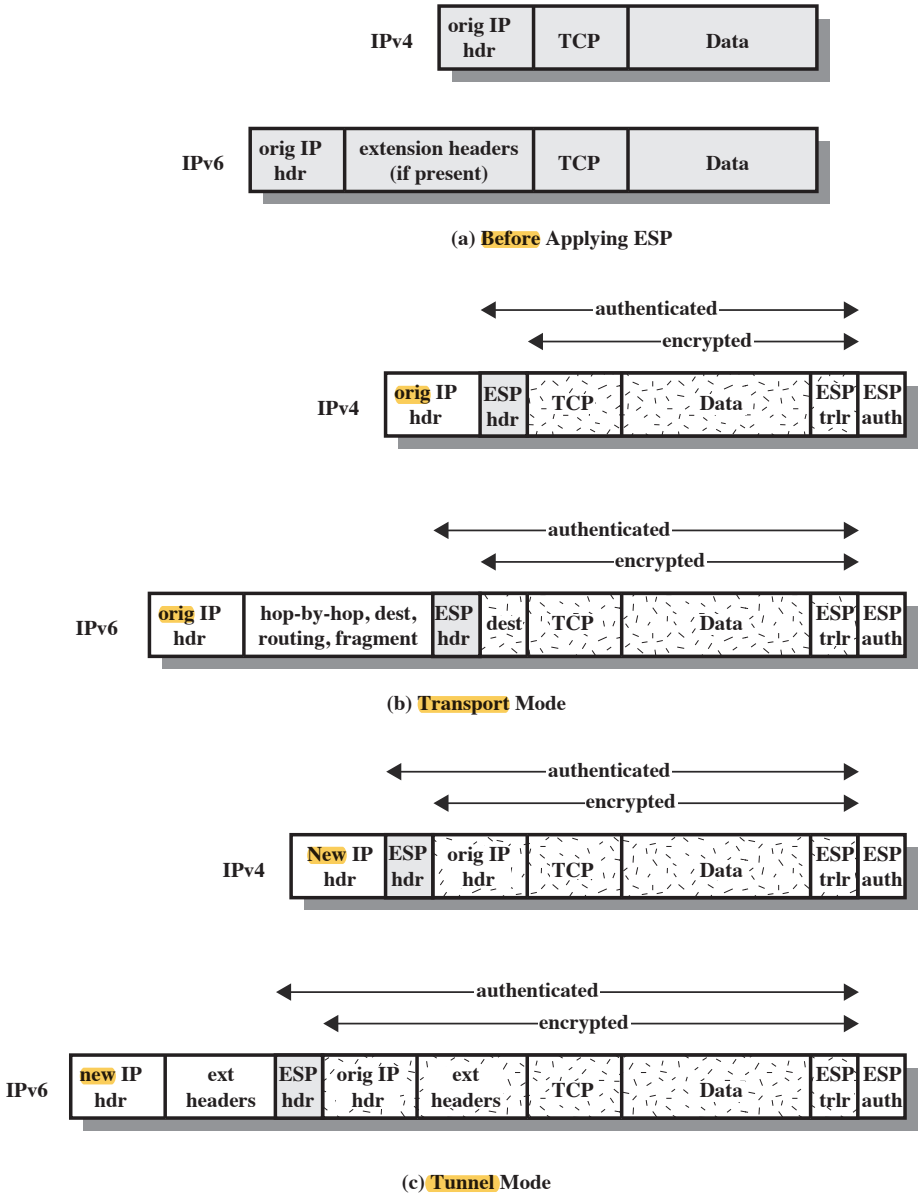


Figure 20.6 Scope of ESP Encryption and Authentication

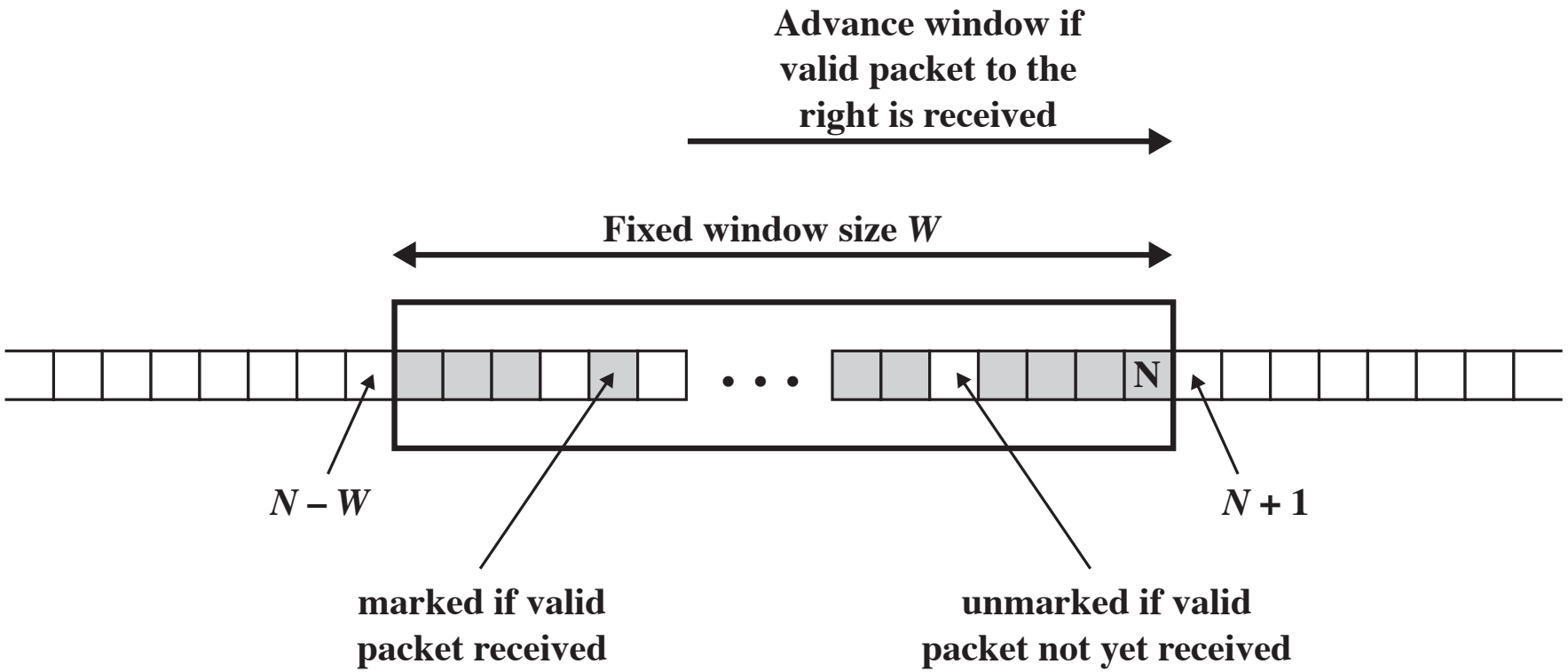


Figure 20.5 Anti-Replay Mechanism

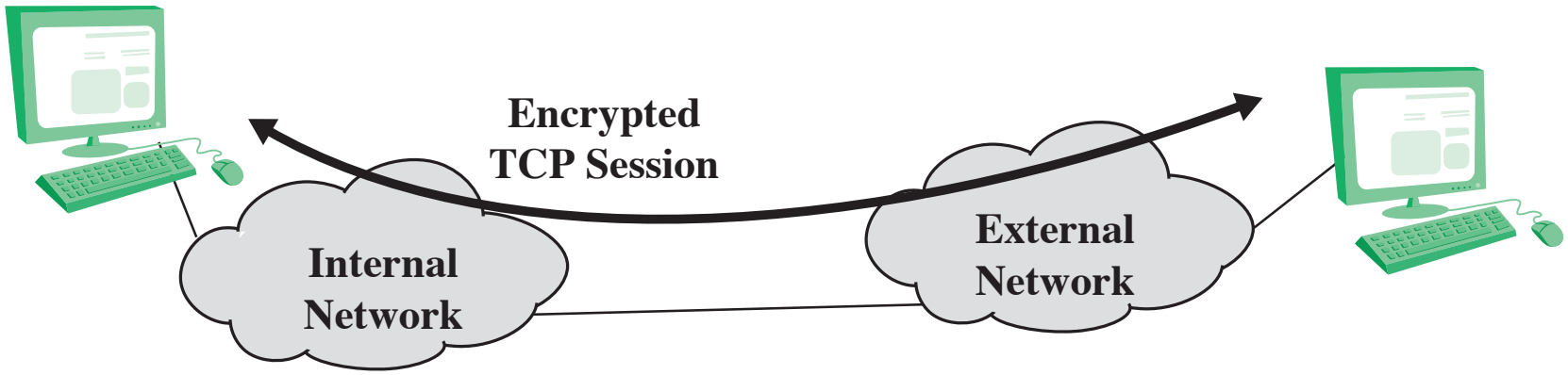


Figure 20.7 End-to-end IPsec Transport-Mode Encryption

VPN

Tunnel mode can be used to implement a secure virtual private network

A *virtual private network (VPN)* is a private network that is configured within a public network in order to take advantage of the economies of scale and management facilities of large networks

VPNs are widely used by enterprises to create wide area networks that span large geographic areas, to provide site-to-site connections to branch offices, and to allow mobile users to dial up their company LANs

The pubic network facility is shared by many customers, with the traffic of each customer segregated from other traffic

Traffic designated as VPN traffic can only go from a VPN source to a destination in the same VPN

It is often the case that encryption and authentication facilities are provided for the VPN

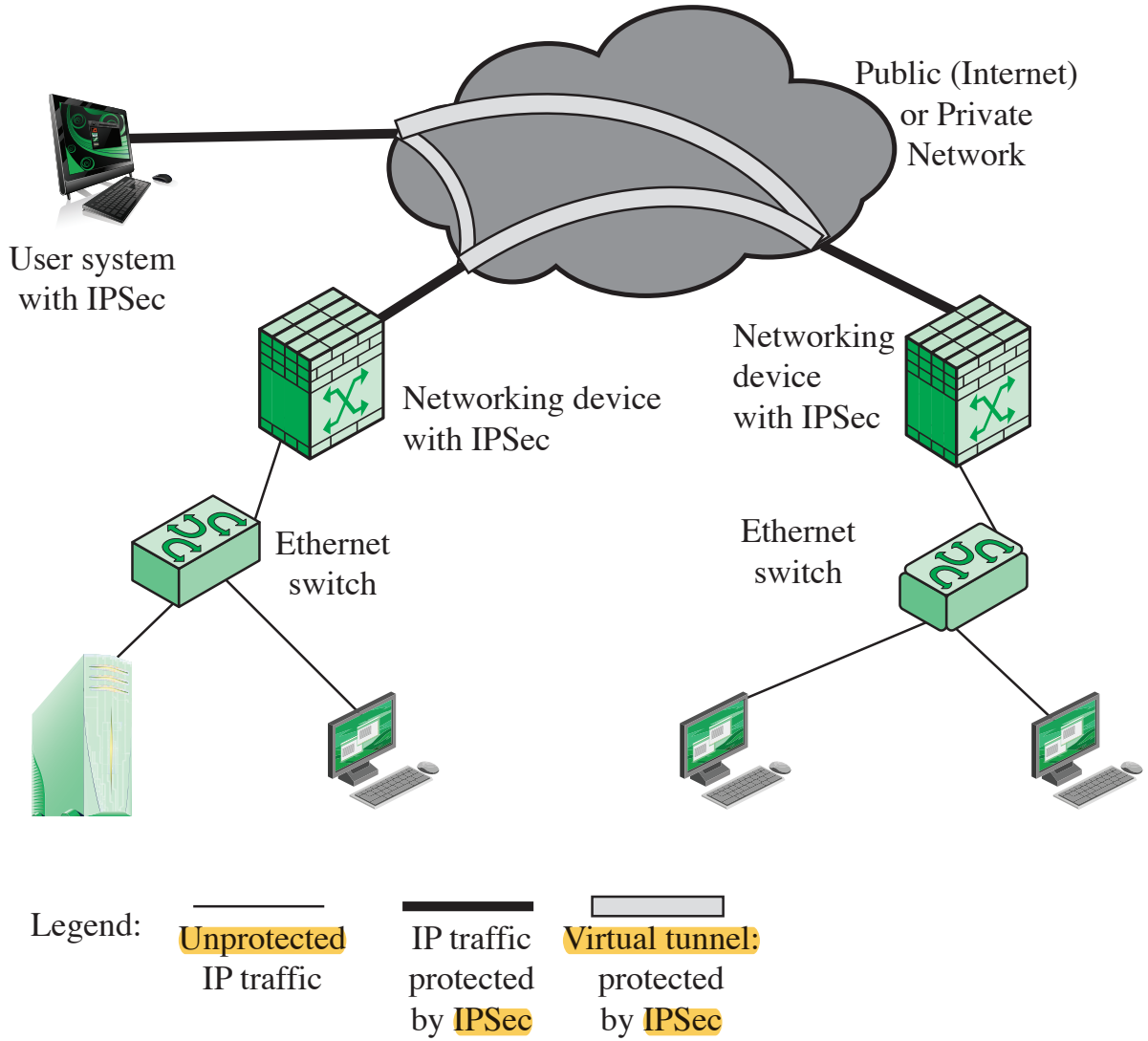


Figure 20.8 Example of Virtual Private Network Implemented with IPsec Tunnel Mode

Combining Security Associations

- An individual SA can implement either the AH or ESP protocol but not both
- *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 endpoint
- 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
- This approach allows for only one level of combination

Iterated tunneling

- Refers to the application of multiple layers of security protocols effected through IP tunneling
- This approach allows for multiple levels of nesting

Combining Security Associations

- Issue of authentication & encryption order
- authentication + confidentiality
  - ESP with authentication option
  - transport adjacency: $AH_{transport}(ESP_{transport})$
  - transport-tunnel bundle: $ESP_{tunnel}(AH_{transport})$
- have 4 cases (see next)

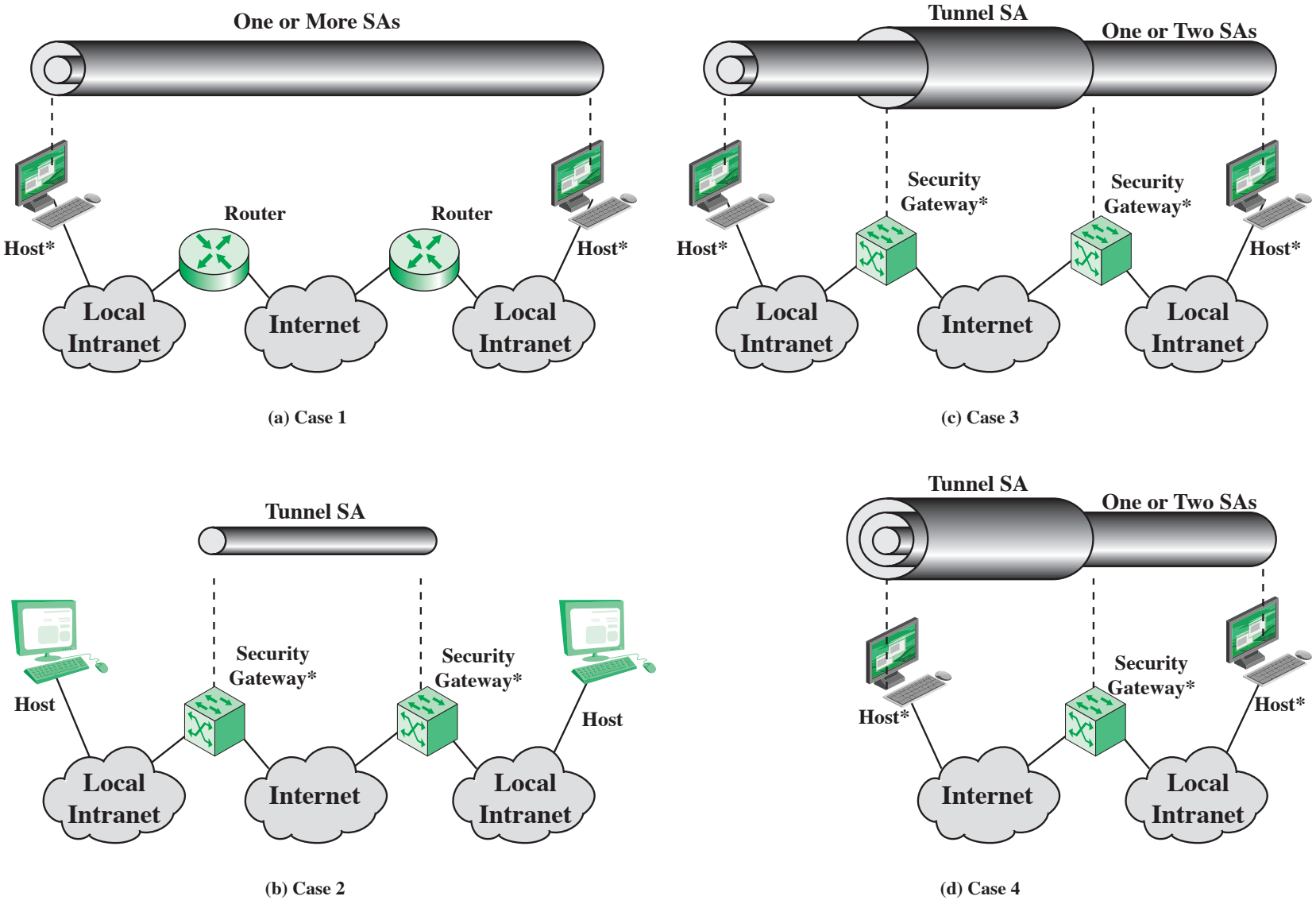


Figure 20.10 Basic Combinations of Security Associations

Transport Adjacency

- $AH_{transport}(ESP_{transport})$
- 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
  - Encryption is applied to the IP payload
  - AH is then applied in transport mode
  - Advantage of this approach is that the authentication covers more fields
  - Disadvantage is the overhead of two SAs versus one SA

Transport-Tunnel Bundle

- The use of authentication prior to encryption might be preferable for several reasons:
  - It is impossible for anyone to intercept the message and alter the authentication data without detection
  - It may be desirable to store the authentication information with the message at the destination for later reference
- One approach is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
  - $ESP_{tunnel}(AH_{transport})$
  - Authentication is applied to the IP payload plus the IP header
  - The resulting IP 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

Internet Key Exchange (IKE)

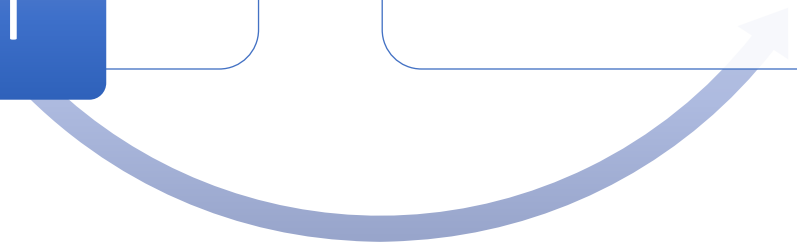
- The key management portion of IPsec involves the determination and distribution of secret keys
  - A typical requirement is four keys for communication between two applications
    - Transmit and receive pairs for both integrity and confidentiality
- The IPsec Architecture document mandates support 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
- This is practical for small, relatively static environments

Automated

- Enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration



ISAKMP/Oakley

- The default automated key management protocol of IPsec
- Consists of:
  - **Oakley Key Determination Protocol**
    - A key exchange protocol based on the Diffie-Hellman algorithm but providing added security
    - Generic in that it does not dictate specific formats
  - **Internet Security Association and Key Management Protocol (ISAKMP)**
    - Provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes
    - Consists of a set of message types that enable the use of a variety of key exchange algorithms

Clogging Attacks on DH key exchanges

Problem:

- Opponent forges the source address of a legitimate user and sends a public Diffie–Hellman key to the victim
- The victim then performs a modular exponentiation to compute the secret key
- Repeated messages of this type can *clog* the victim's system with useless work

Counter measure - **cookie exchange**

- Each side is required to send a pseudorandom number, the cookie, in the initial message, which the other side acknowledges. This acknowledgment must be repeated in the first message of the Diffie–Hellman key exchange.
- If the source address was forged, the opponent gets no answer. Thus, an opponent can only force a user to generate acknowledgments and not to perform the Diffie–Hellman calculation.

Features of IKE Key Determination

- Algorithm is characterized by five important features:

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

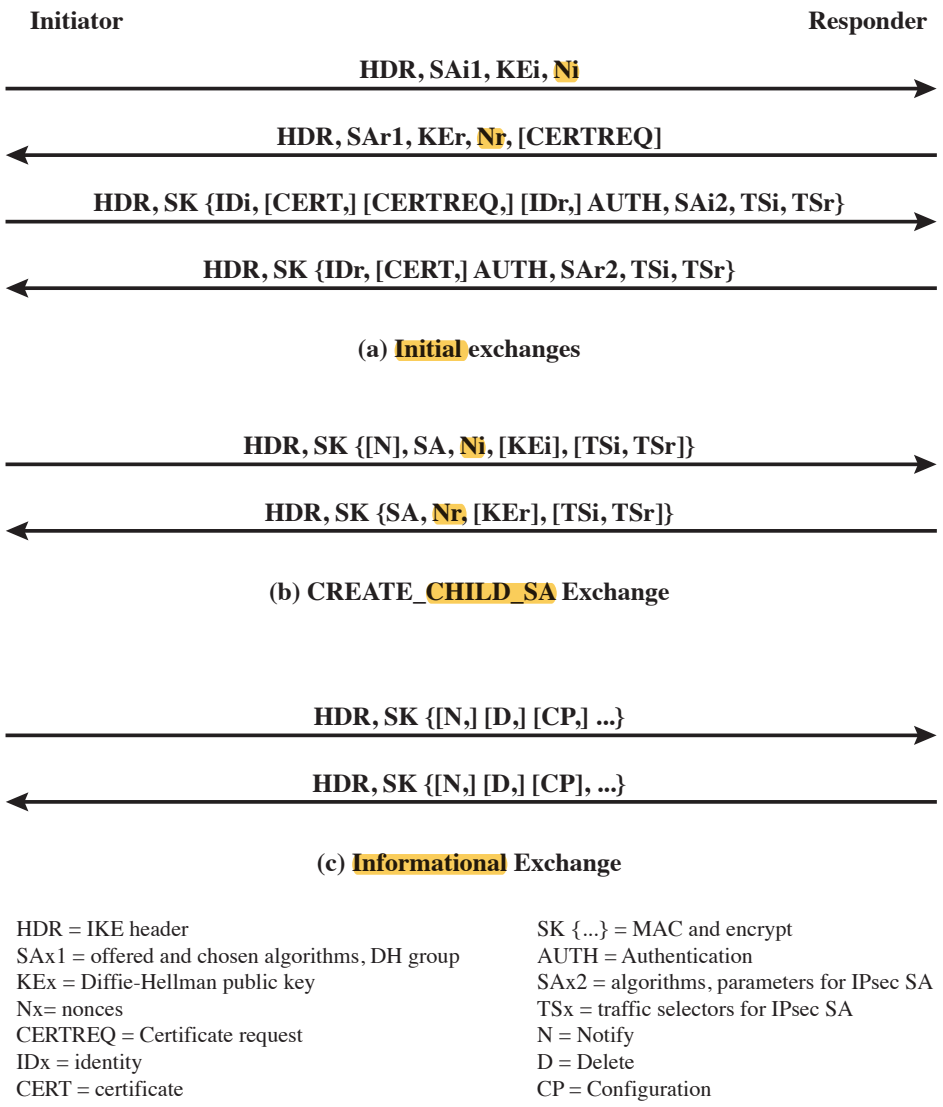


Figure 20.11 IKEv2 Exchanges

Groups for DH key exchange:

- Modular exponentiation with a 768-bit modulus

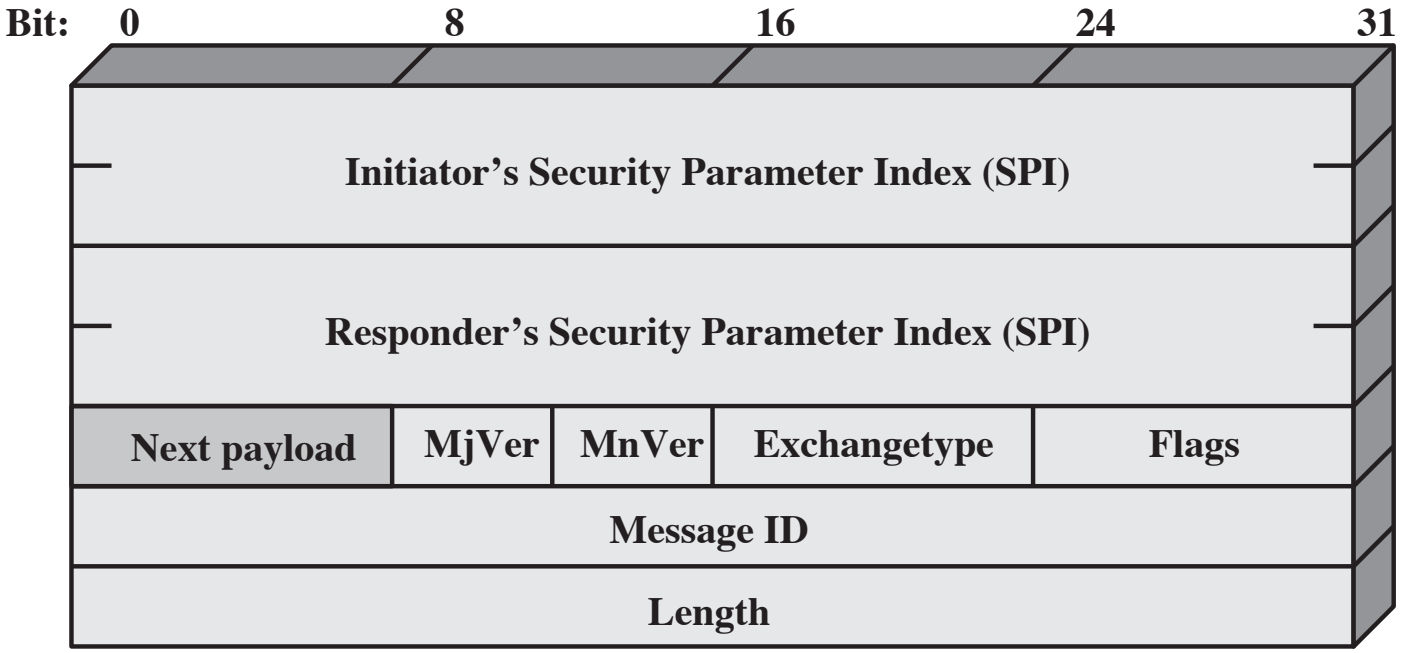
$$q = 2^{768} - 2^{704} - 1 + 2^{64} \times (\lfloor 2^{638} \times \pi \rfloor + 149686)$$
$$\alpha = 2$$

- Modular exponentiation with a 1024-bit modulus

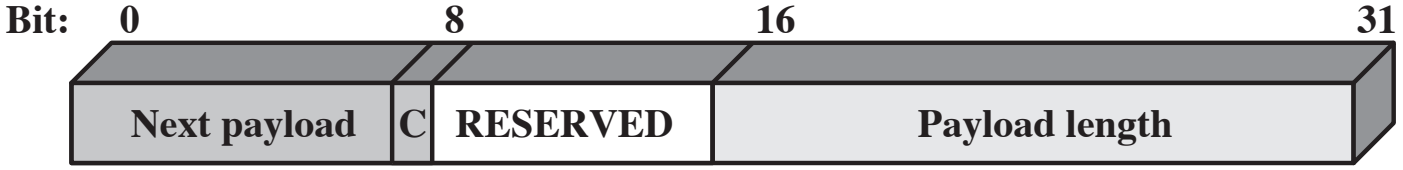
$$q = 2^{1024} - 2^{960} - 1 + 2^{64} \times (\lfloor 2^{894} \times \pi \rfloor + 129093)$$
$$\alpha = 2$$

- 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

The (pseudorandom number) cookie is created by hash over the IP Source and Destination addresses, the UDP Source and Destination ports, and a locally generated secret value.



(a) IKE Header



(b) Generic Payload Header

Figure 20.12 IKE Formats

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

Table 20.4 Cryptographic Suites for IPsec

(a) Virtual private networks (RFC 4308)

	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

(b) NSA Suite B (RFC 4869)

	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

Summary

- IP security overview
  - Applications of IPsec
  - Benefits of IPsec
  - Routing applications
  - IPsec documents
  - IPsec services
  - Transport and tunnel modes
- IP security policy
  - Security associations
  - Security association database
  - Security policy database
  - IP traffic processing
- Cryptographic suites

- Encapsulating security payload
  - ESP format
  - Encryption and authentication algorithms
  - Padding
  - Anti-replay service
  - Transport and tunnel modes
- Combining security associations
  - Authentication plus confidentiality
  - Basic combinations of security associations
- Internet key exchange
  - Key determination protocol
  - Header and payload formats