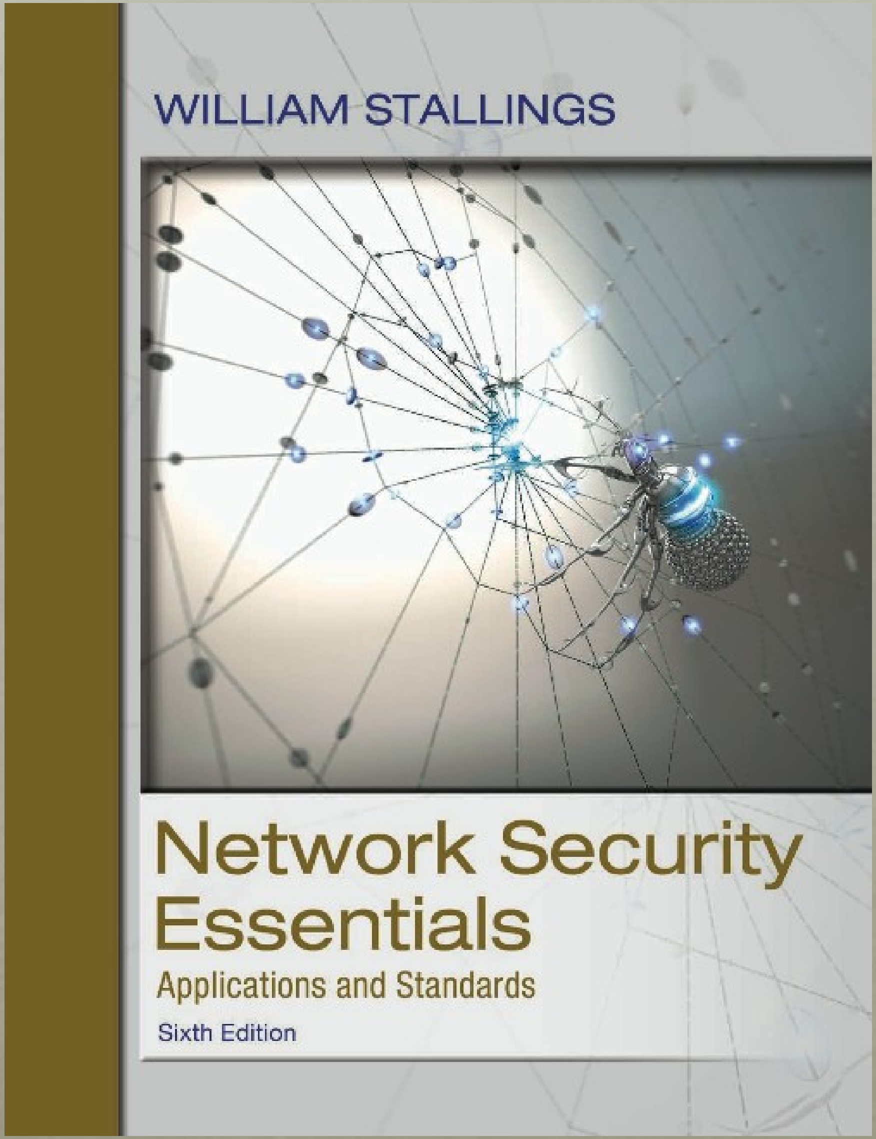
Network Security Essentials

Sixth Edition

by William Stallings



Chapter 9

IP Security

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:

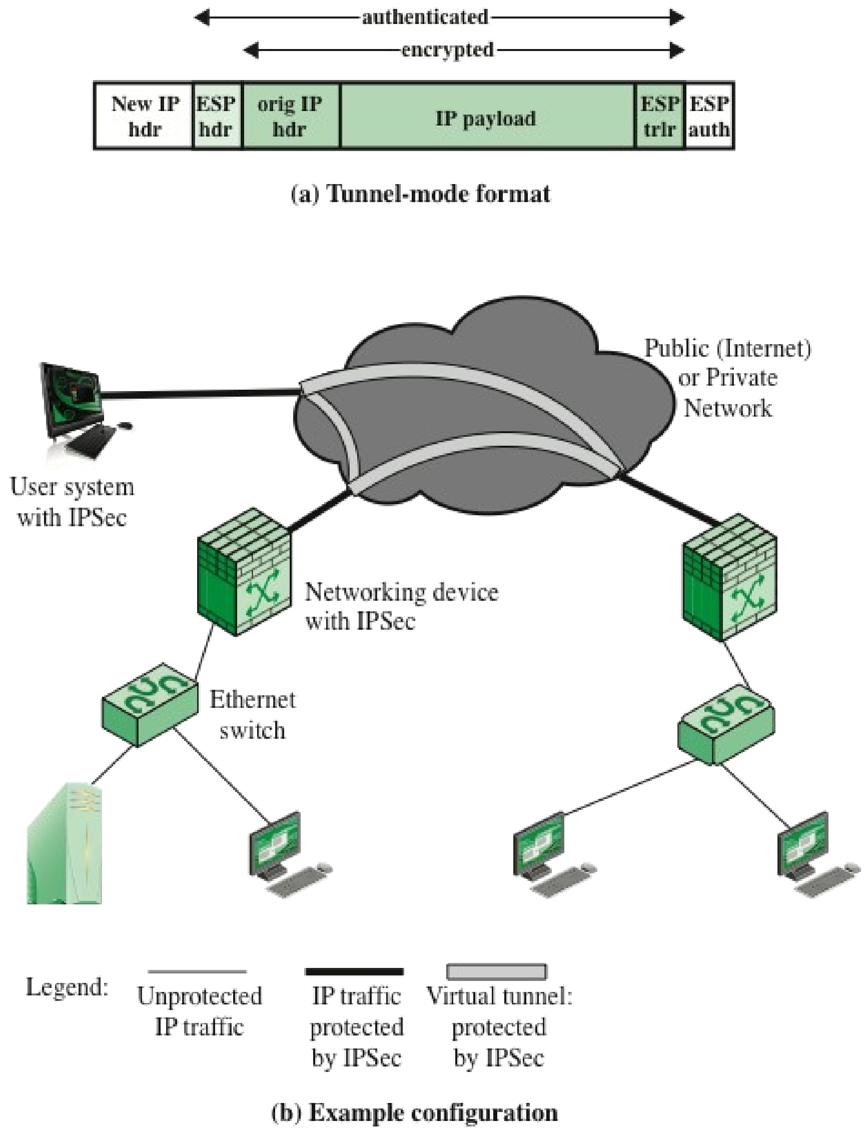
- Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

- 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. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

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, and so on) can be secured.



(a) Tunnel-mode format

(b) Example configuration

Figure 9.1 An IPSec VPN Scenario

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

Routing Applications

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 IP packet was sent.

- A routing update is not forged.

Without such security measures, an opponent can disrupt communications or divert some traffic. Routing protocols such as Open Shortest Path First (OSPF) should be run on top of security associations between routers that are defined by IPsec.

IPsec encompasses three functional areas: authentication, confidentiality, and key management.

The totality of the IPsec specification is scattered across dozens of RFCs and draft IETF documents, making this the most complex and difficult to grasp of all IETF specifications. The best way to grasp the scope of IPsec is to consult the latest version of the IPsec document roadmap, which as of this writing is RFC 6071 [IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, February 2011].

The documents can be categorized into the following groups:

- **Architecture**: Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology. The current specification is RFC 4301, *Security Architecture for the Internet Protocol .*
- **Authentication Header (AH)**: AH is an extension header to provide message authentication. The current specification is RFC 4302, IP Authentication Header . Because message authentication is provided by ESP, the use of AH is deprecated. It is included in IPsecv3 for backward compatibility but should not be used in new applications. We do not discuss AH in this chapter.
- **Encapsulating Security Payload (ESP)**: ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication. The current specification is RFC 4303, IP Encapsulating Security Payload (ESP) .
- **Internet Key Exchange (IKE)**: This is a collection of documents describing the key management schemes for use with IPsec. The main specification is RFC 7296, Internet Key Exchange (IKEv2) Protocol , but there are a number of related RFCs.
- **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)
  - 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

Transport and Tunnel Modes

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

The operation of these two modes is best understood in the context of a description of ESP, which is covered in Section 9.3.

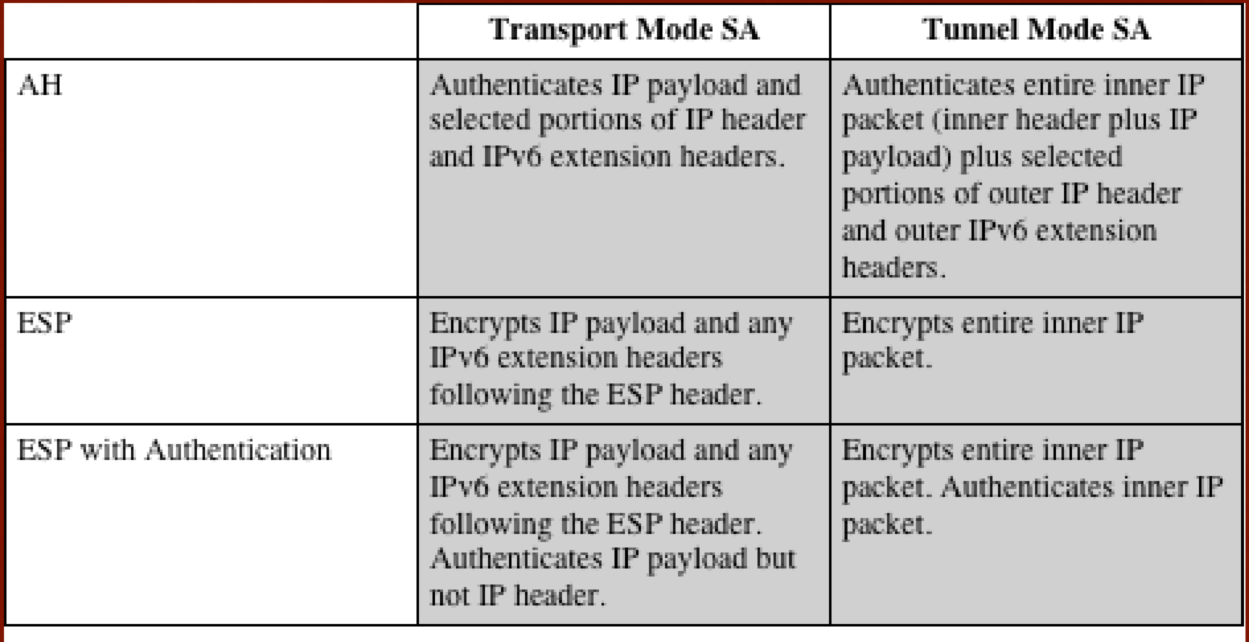
Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Examples include a TCP or UDP segment or an ICMP packet, all of which operate directly above IP in a host protocol stack. Typically, transport mode is used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

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 9.1
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.

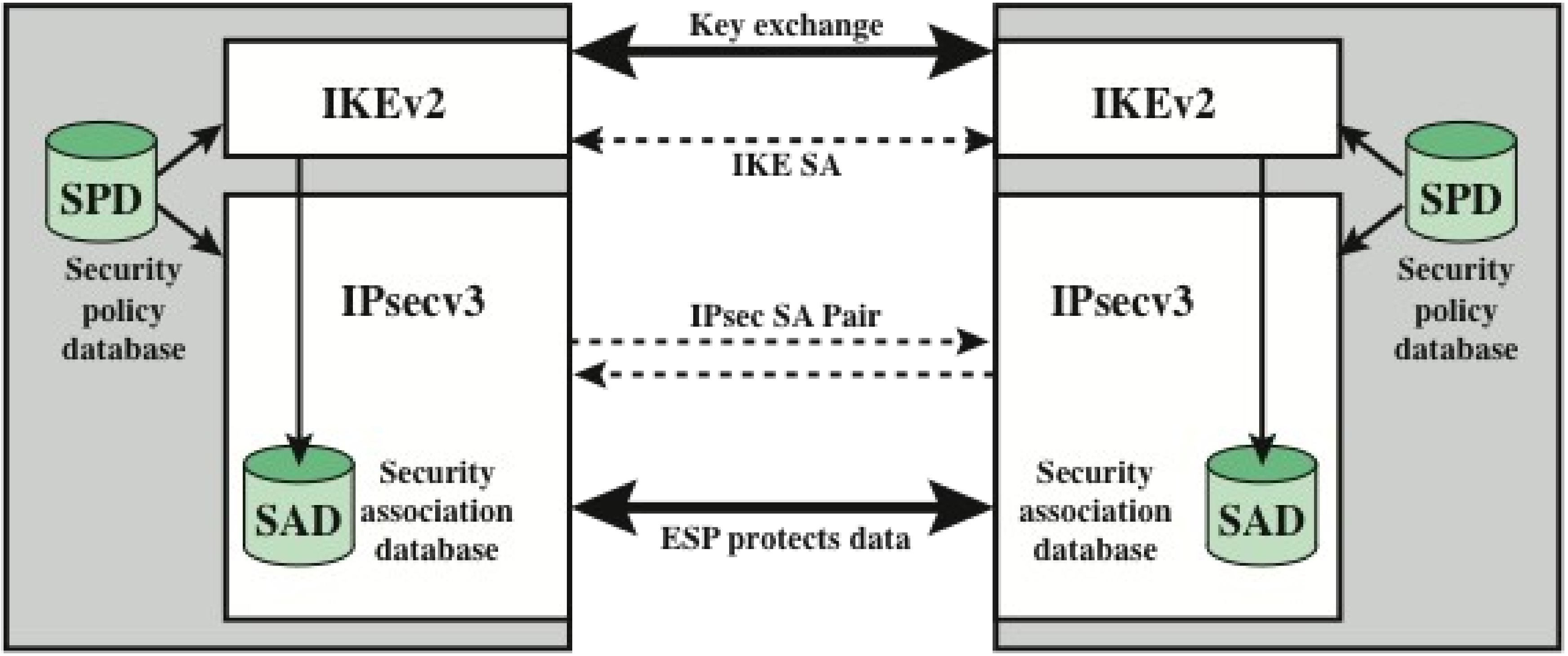


Figure 9.2 IPsec Architecture

Security Association (SA)

A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). 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.

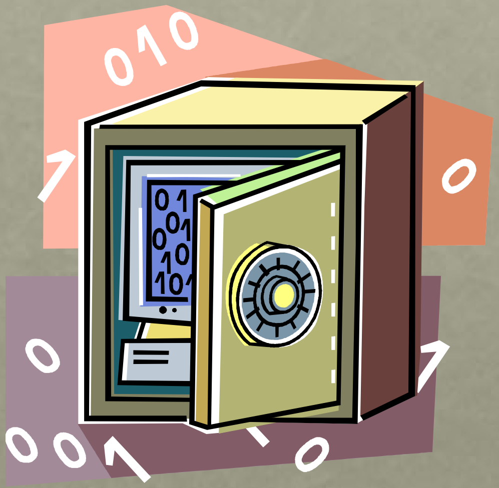
- **IP Destination Address**: This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.

- **Security Protocol Identifier**: This field from the outer IP header indicates whether the association is an AH or ESP security association.

Hence, in any IP packet, the security association is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP).

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:

- **Remote IP Address**: This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one destination system sharing the same SA (e.g., behind a firewall).

- **Local IP Address**: This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one source system sharing the same SA (e.g., behind a firewall).

- **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. This is an individual protocol number, ANY, or for IPv6 only, OPAQUE. If AH or ESP is used, then this IP protocol header immediately precedes the AH or ESP header in the packet.

- **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.

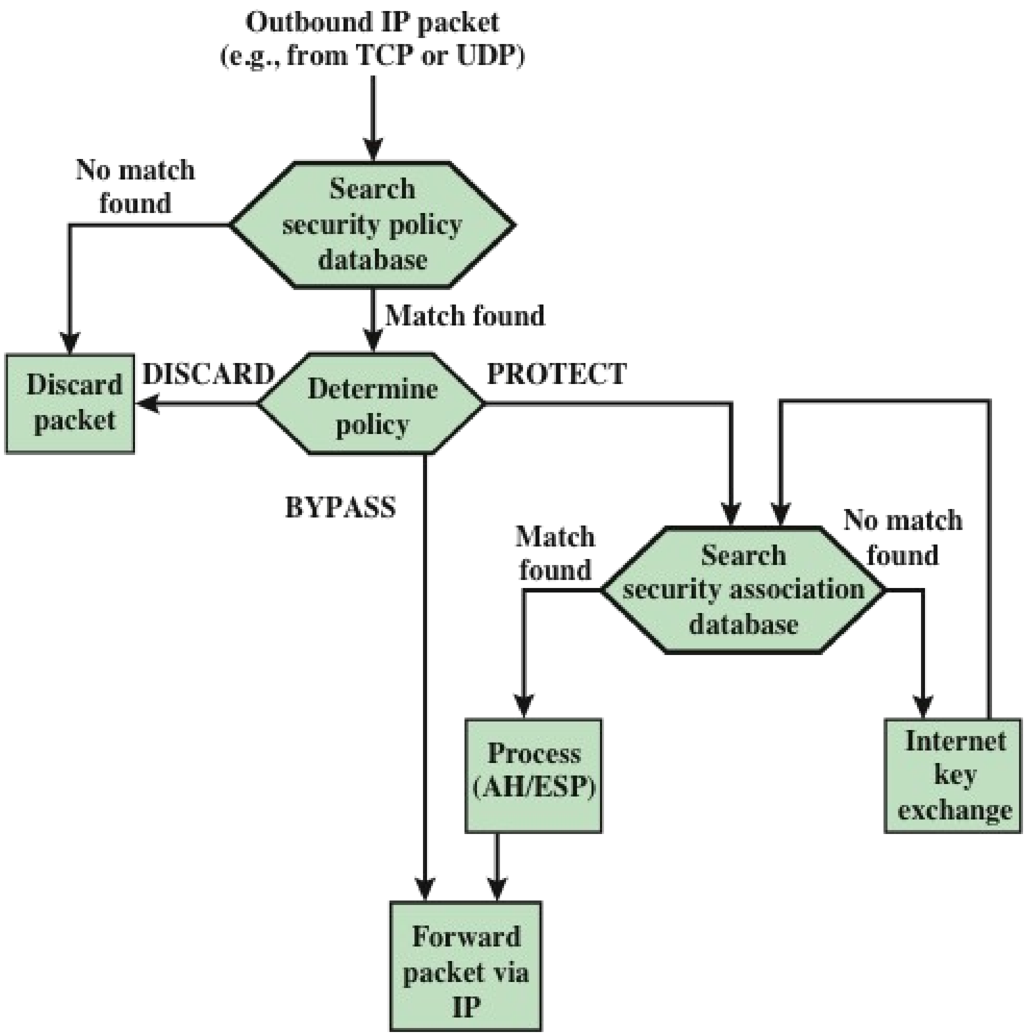


Figure 9.3 Processing Model for Outbound Packets

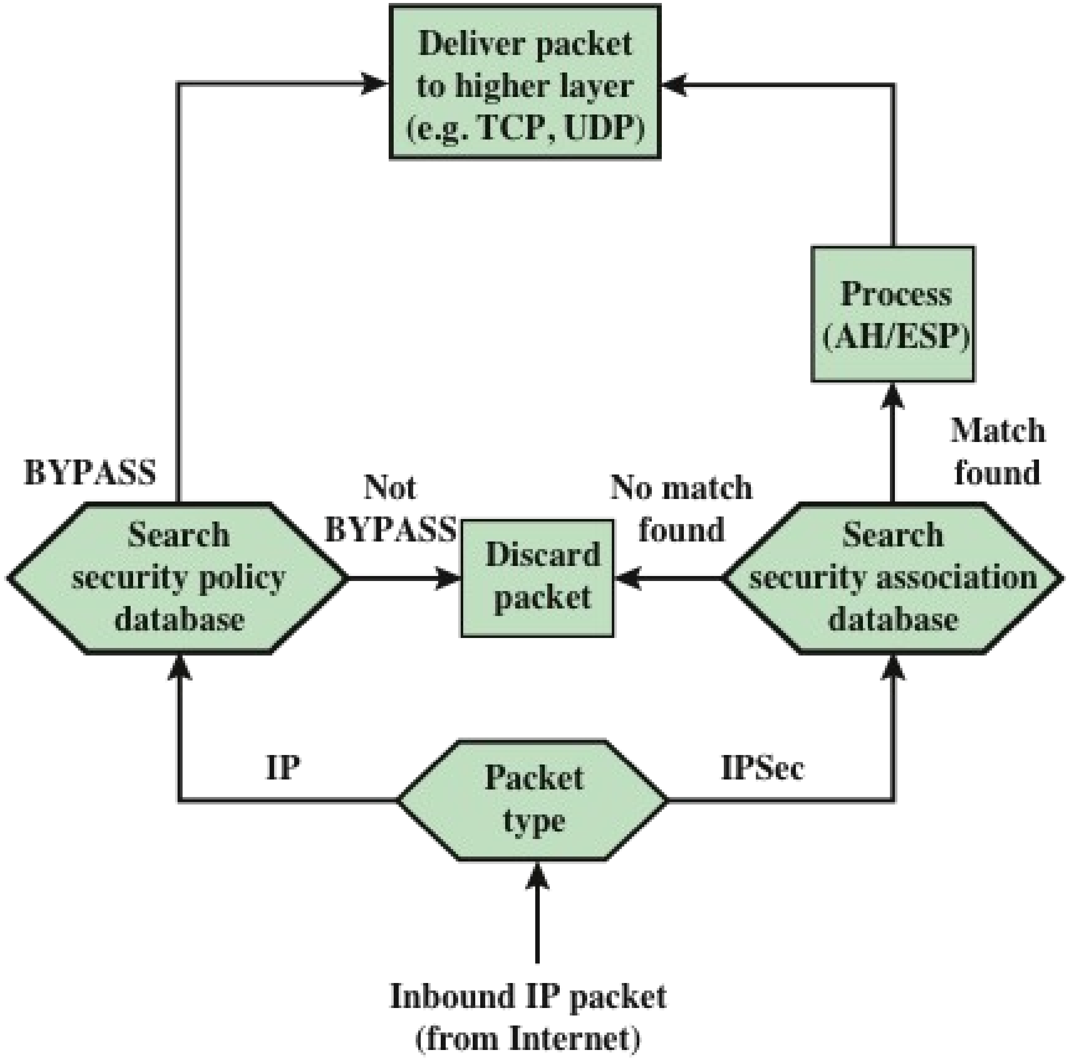
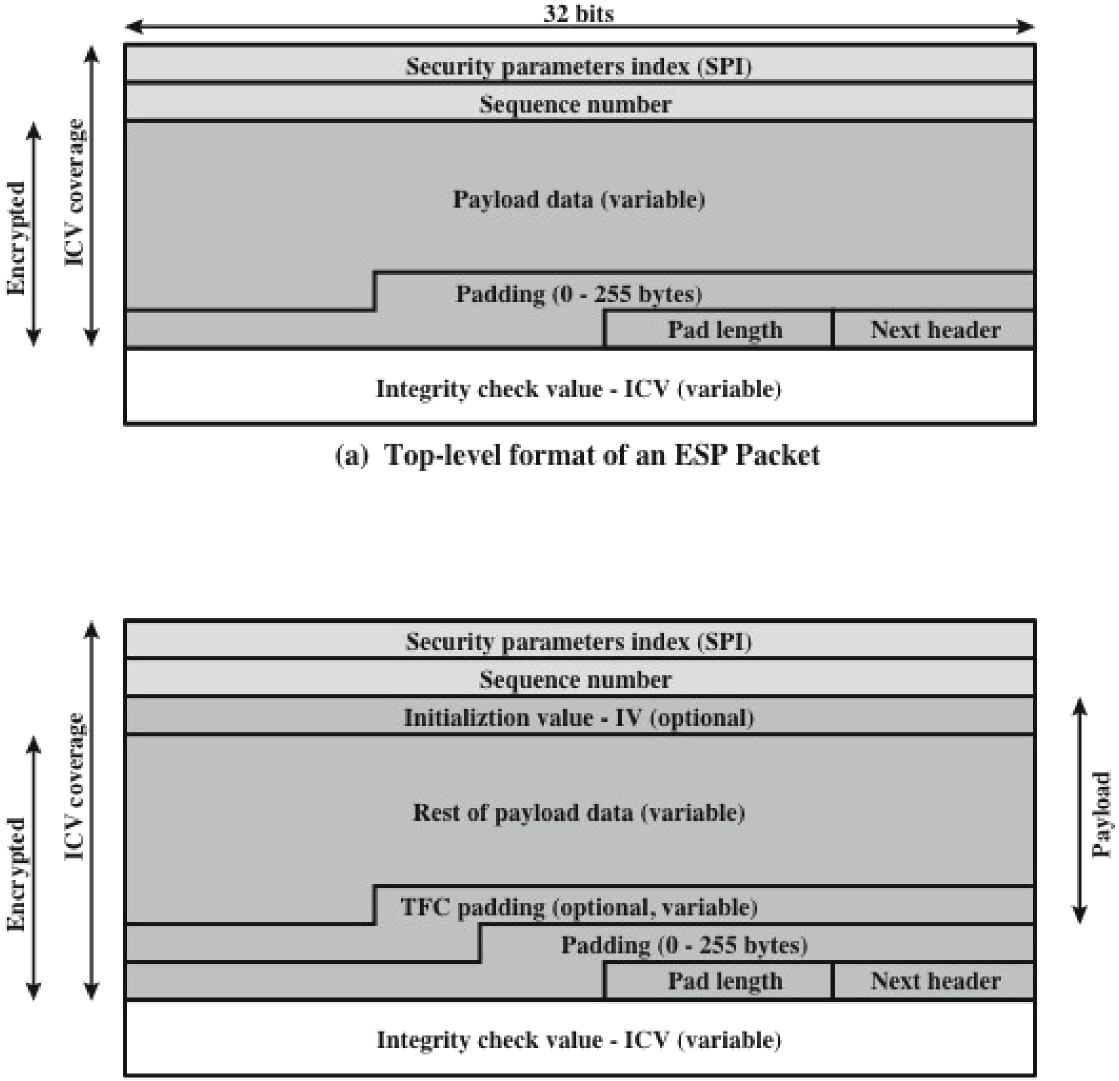


Figure 9.4 Processing Model for Inbound Packets


32 bits
Security parameters index (SPI)
Sequence number
Payload data (variable)
Padding (0 - 255 bytes)
Pad length
Next header
Integrity check value - ICV (variable)
Encrypted
ICV coverage
Security parameters index (SPI)
Sequence number
Initializtion value - IV (optional)
Rest of payload data (variable)
TFC padding (optional, variable)
Padding (0 - 255 bytes)
Pad length
Next header
Integrity check value - ICV (variable)
Encrypted
ICV coverage
Payload

(a) Top-level format of an ESP Packet

(b) Substructure of payload data

Figure 9.5 ESP Packet Format

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

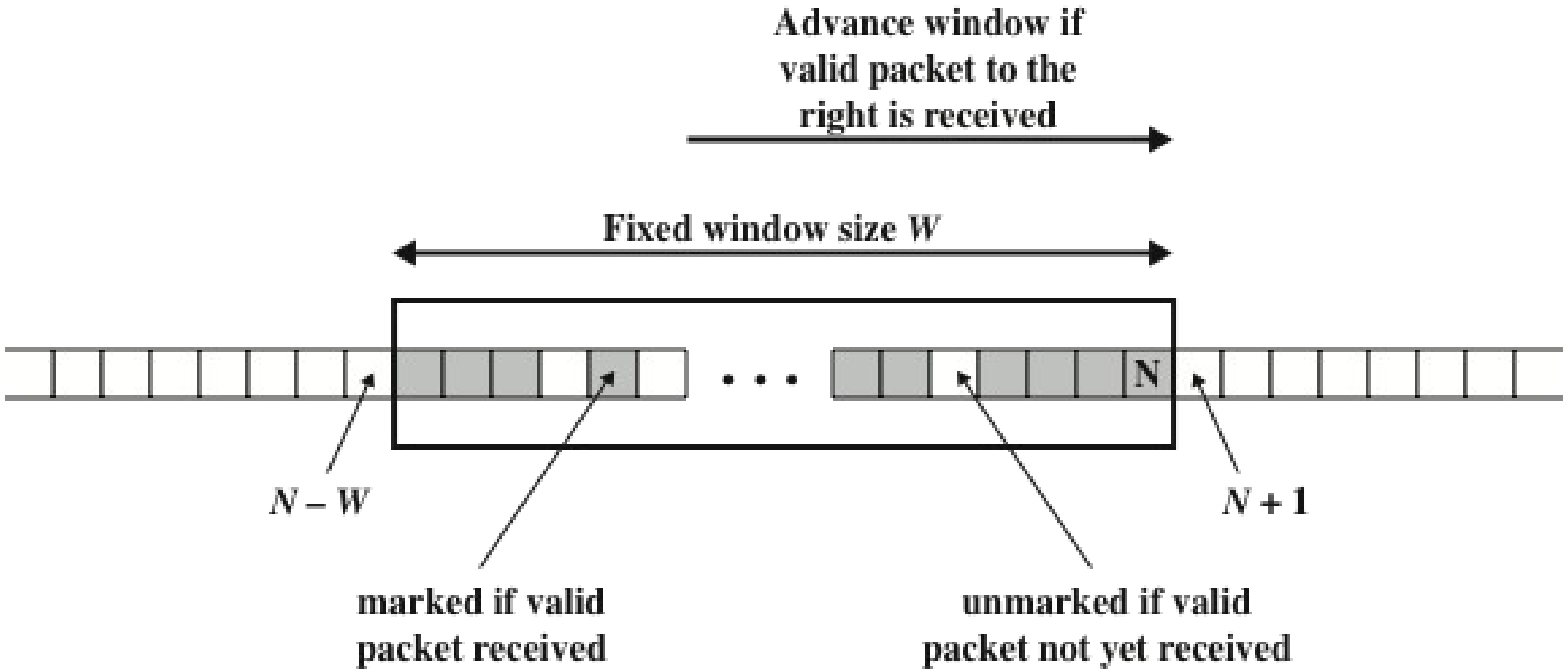

Advance window if valid packet to the right is received
Fixed window size *W*
N
• • •
N – *W*
N + 1
marked if valid packet received
unmarked if valid packet not yet received

Figure 9.6 Anti-Replay Mechanism

Replay Attack

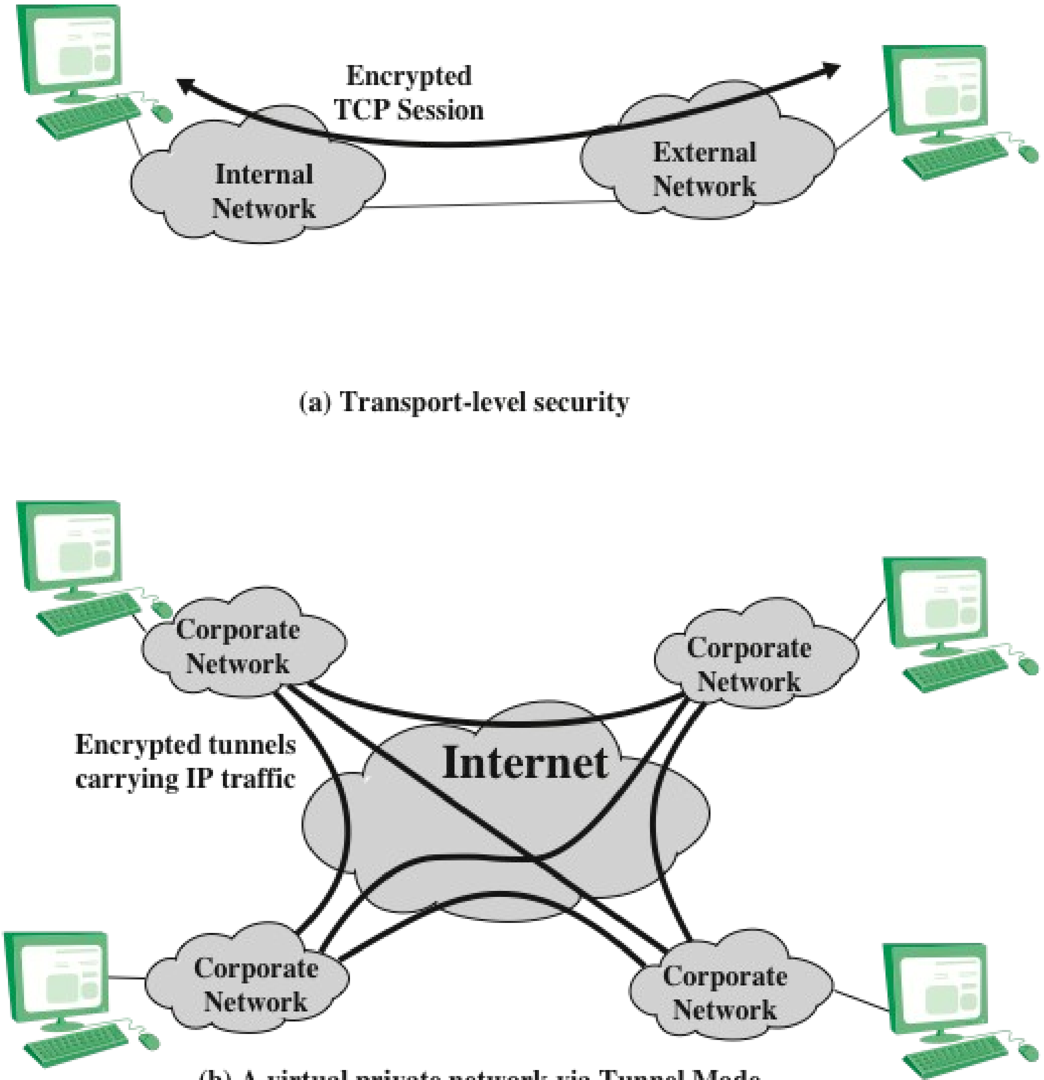
A **replay attack** is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The Sequence Number field is designed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

First, we discuss sequence number generation by the sender, and then we look at how it is processed by the recipient.

When a new SA is established, the sender initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field. Thus, the first value to be used is 1. If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past 2^{32} - 1 back to zero. Otherwise, there would be multiple valid packets with the same sequence number. If the limit of 2^{32} -1 is reached, the sender should terminate this SA and negotiate a new SA with a new key.

Because IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered. Therefore, the IPsec authentication document dictates that the receiver should implement a window of size W , with a default of W = 64. The right edge of the window represents the highest sequence number, N , so far received for a valid packet. For any packet with a sequence number in the range from N - W + 1 to N that has been correctly received (i.e., properly authenticated), thecorresponding slot in the window is marked (Figure 9.6). 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.



(a) Transport-level security

(b) A virtual private network via Tunnel Mode

Figure 9.7 Transport-Mode vs. Tunnel-Mode Encryption

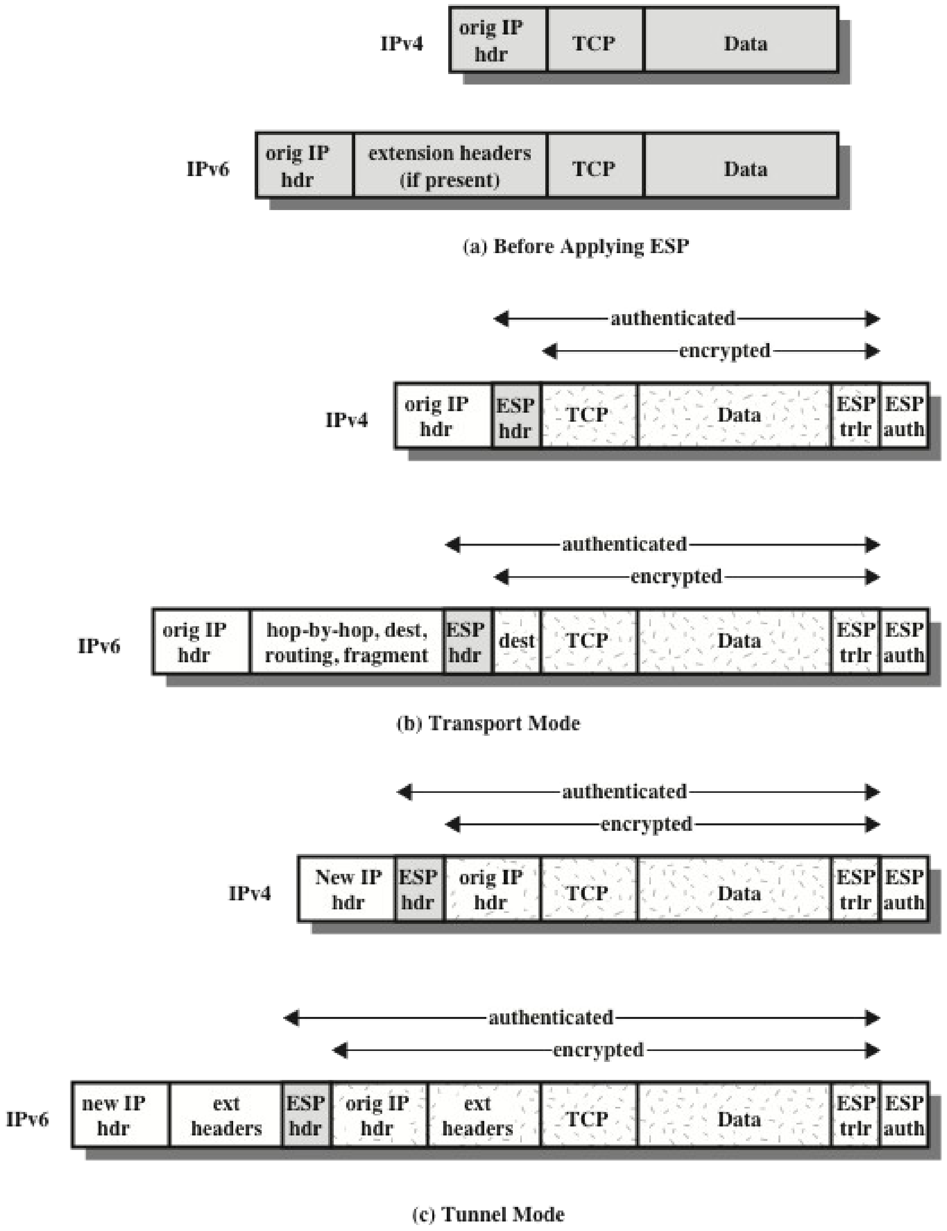


Figure 9.8 Scope of ESP Encryption and Authentication

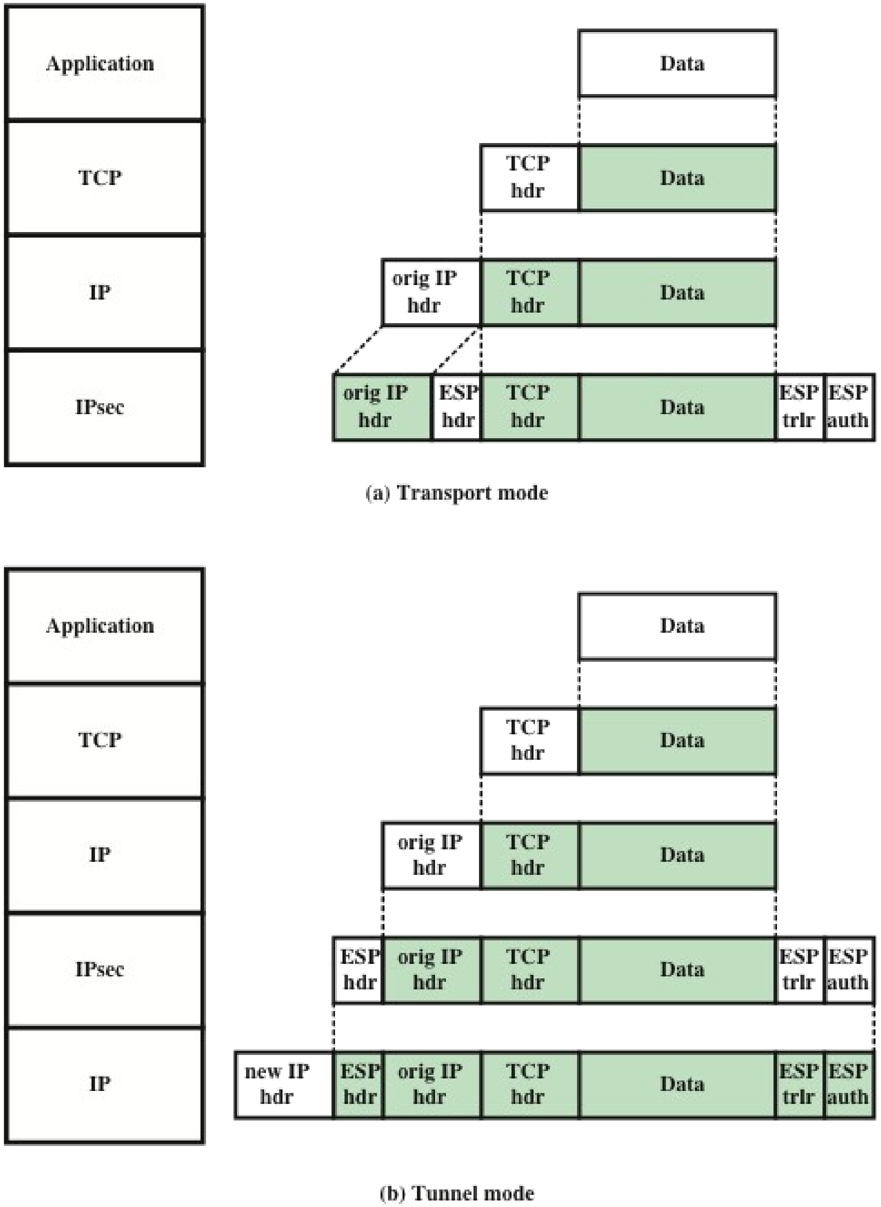


Figure 9.9 Protocol Operation for ESP

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 endpointsor at the same endpoints.

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. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPsec instance: the (ultimate) destination.

- **Iterated tunneling**: Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPsec site along the path.

The two approaches can be combined, for example, by having a transport SA between hosts travel part of the way through a tunnel SA between security gateways.

One interesting issue that arises when considering SA bundles is the order in which authentication and encryption may be applied between a given pair of endpoints and the ways of doing so.

ESP with Authentication Option

Encryption and authentication can be combined in order to transmit an IP packet that has both confidentiality and authentication between hosts. We look at several approaches.

In this approach, the user first applies ESP to the data to be protected and then appends the authentication data field. There are actually two subcases:

- **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. 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.

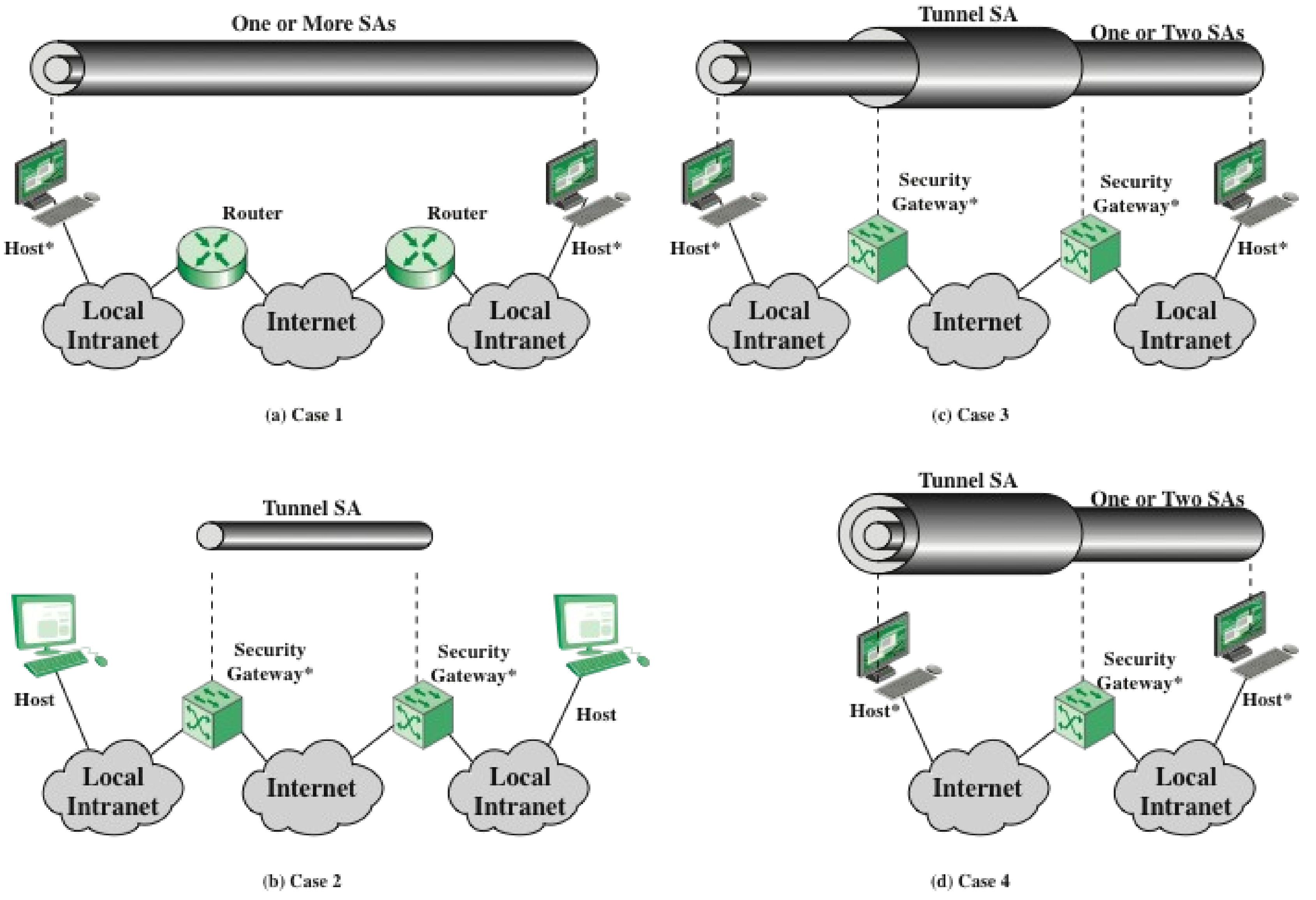
Transport Adjacency

- 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
  - 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
  - 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



* = implements IPsec

Figure 9.10 Basic Combinations of Security Associations

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. This is practical for small, relatively static environments.

- **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.

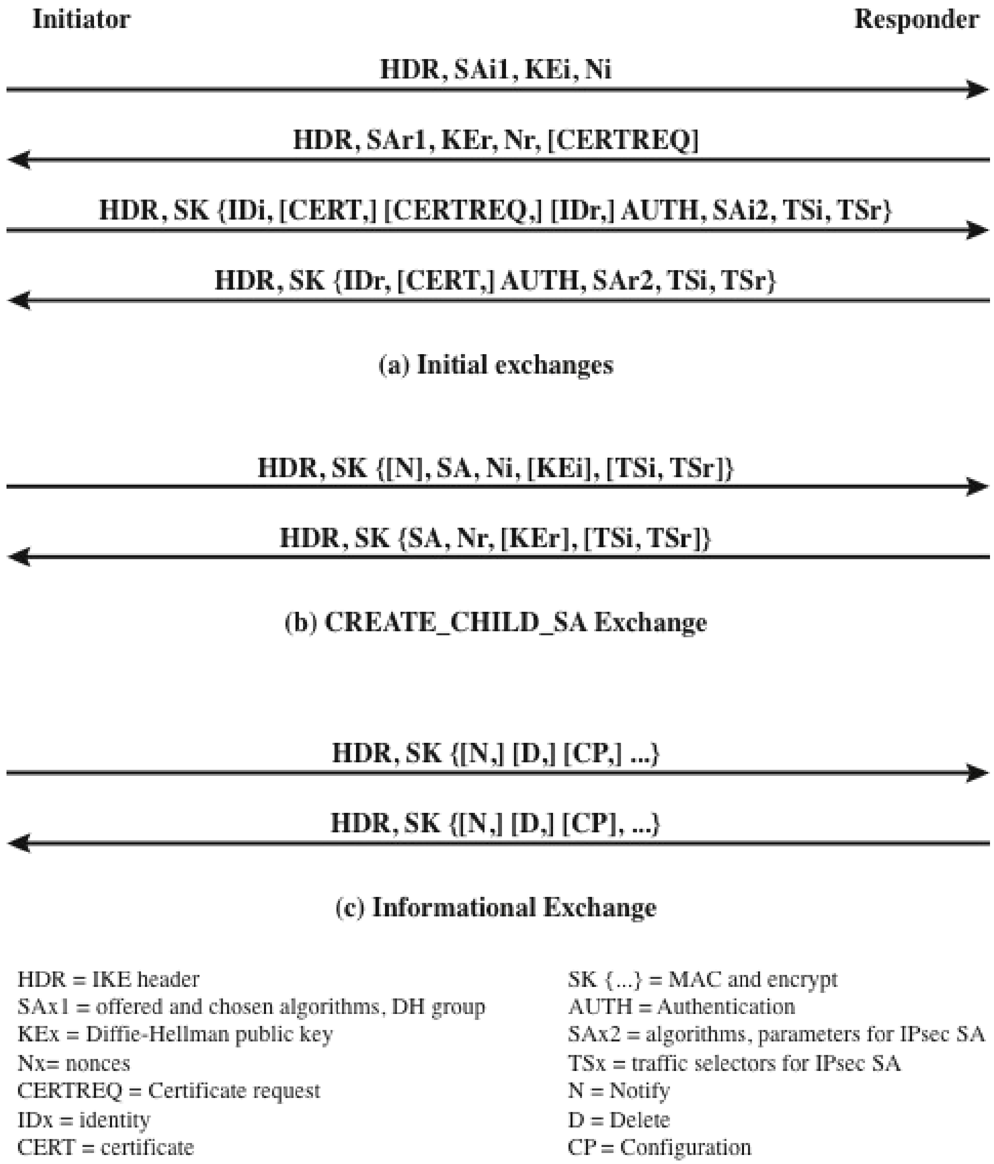
ISAKMP/Oakley

- 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

Features of IKE Key Determination

The 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.



Initiator

Responder

HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}

HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

(a) Initial exchanges

HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]}

HDR, SK {SA, Nr, [KEr], [TSi, TSr]}

(b) CREATE_CHILD_SA Exchange

HDR, SK {[N,] [D,] [CP,] ...}

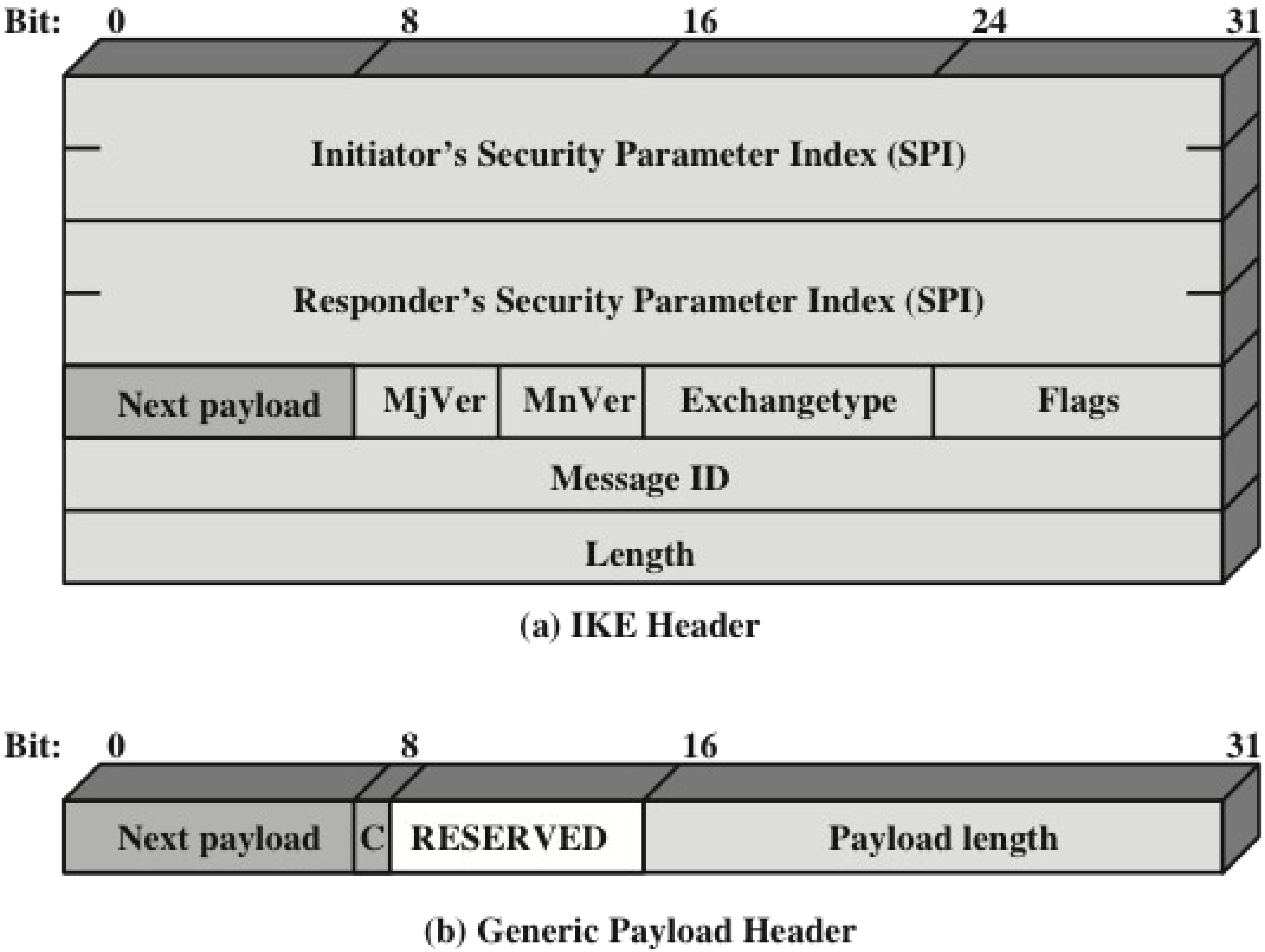
HDR, SK {[N,] [D,] [CP], ...}

(c) Informational Exchange

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 9.11 IKEv2 Exchanges

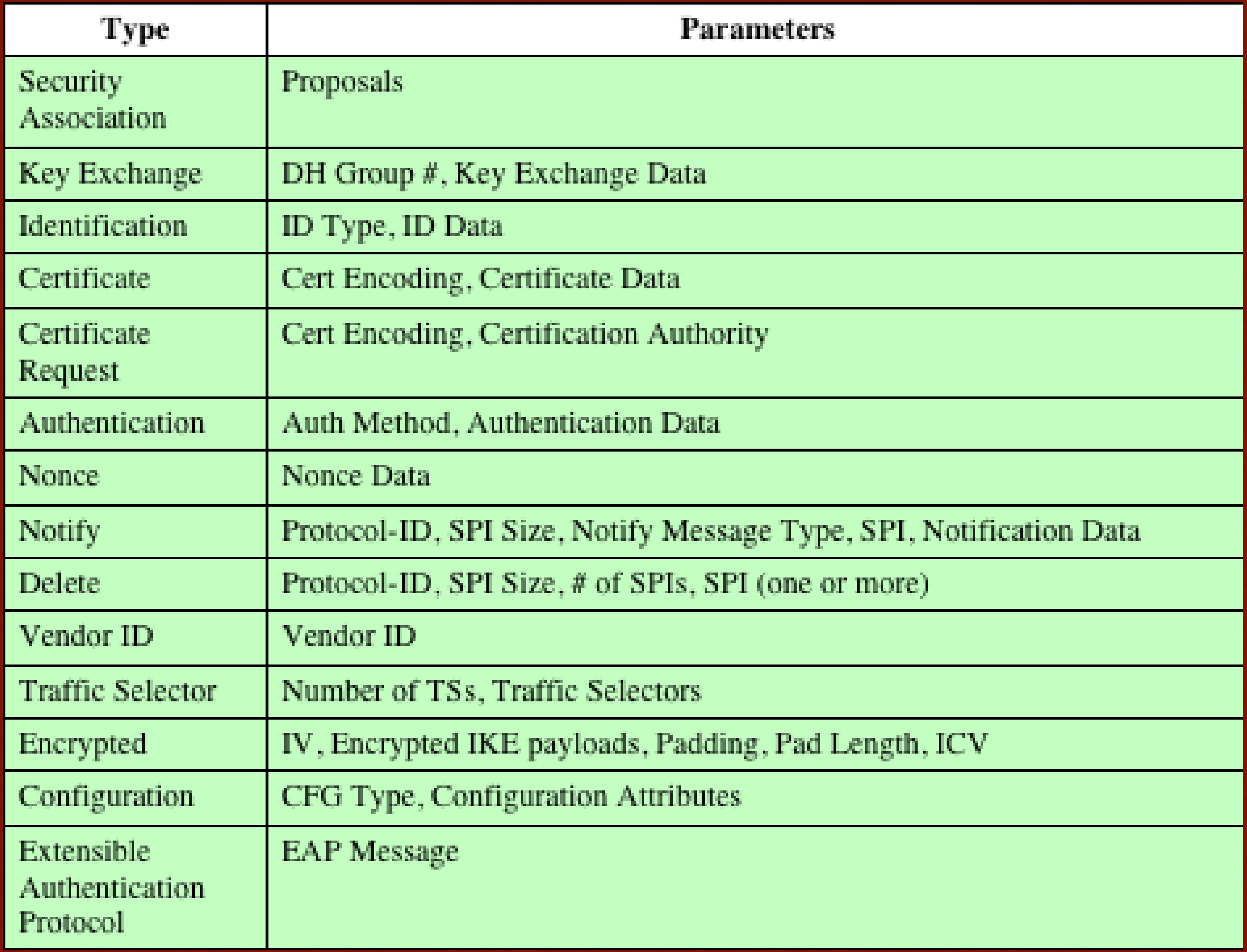


(a) IKE Header

(b) Generic Payload Header

Figure 9.12 IKE Formats

Table 9.3
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

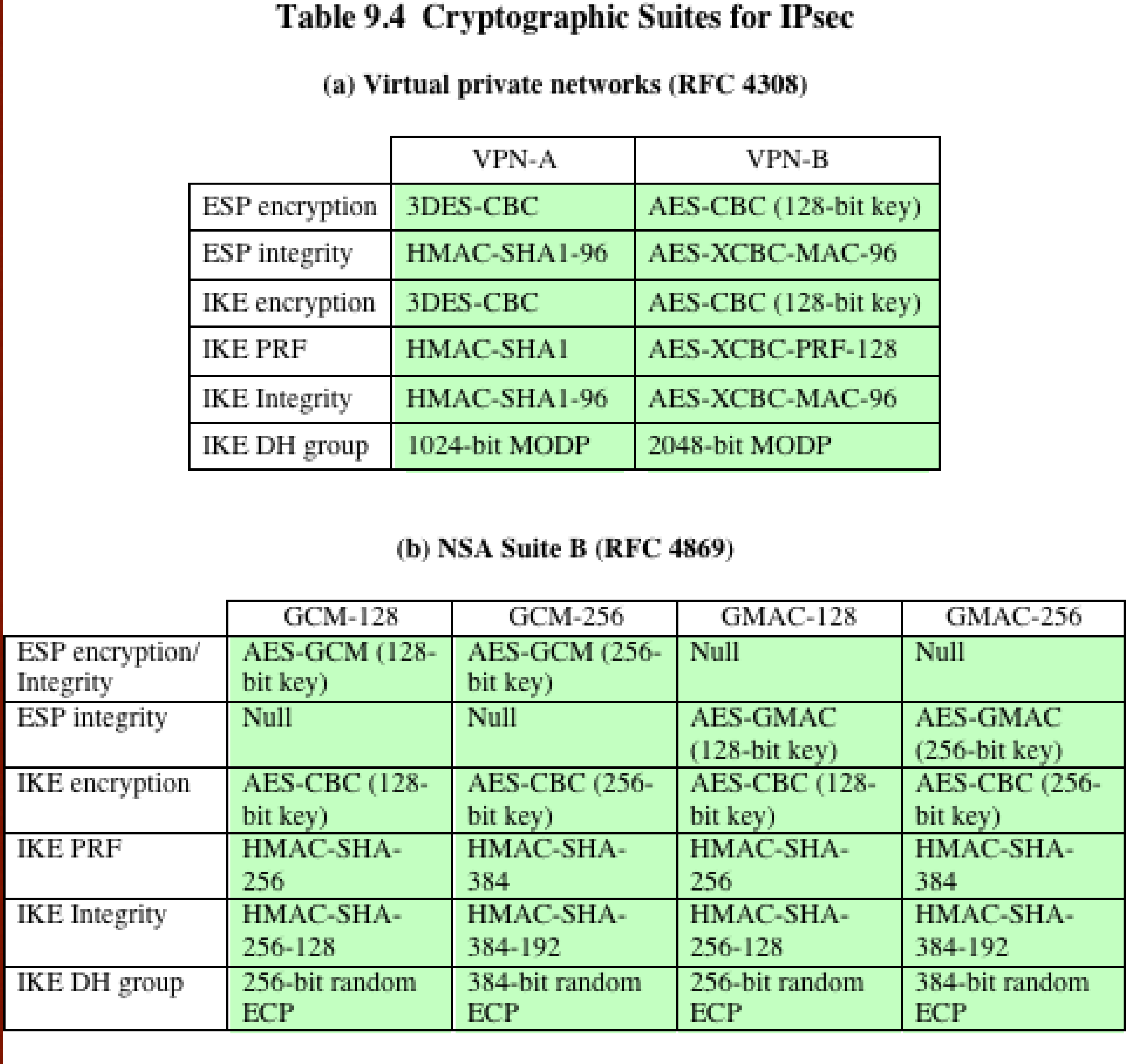


Table 9.4 Cryptographic Suites for IPsec

(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

(Table 9.4 can be found on page 318 in the textbook)

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

Table 9.2
Host SPD Example

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