Cryptography and Network Security

Sixth Edition

by William Stallings

Chapter 20

IP Security

"If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told."

—The Art of War,

Sun Tzu

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

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
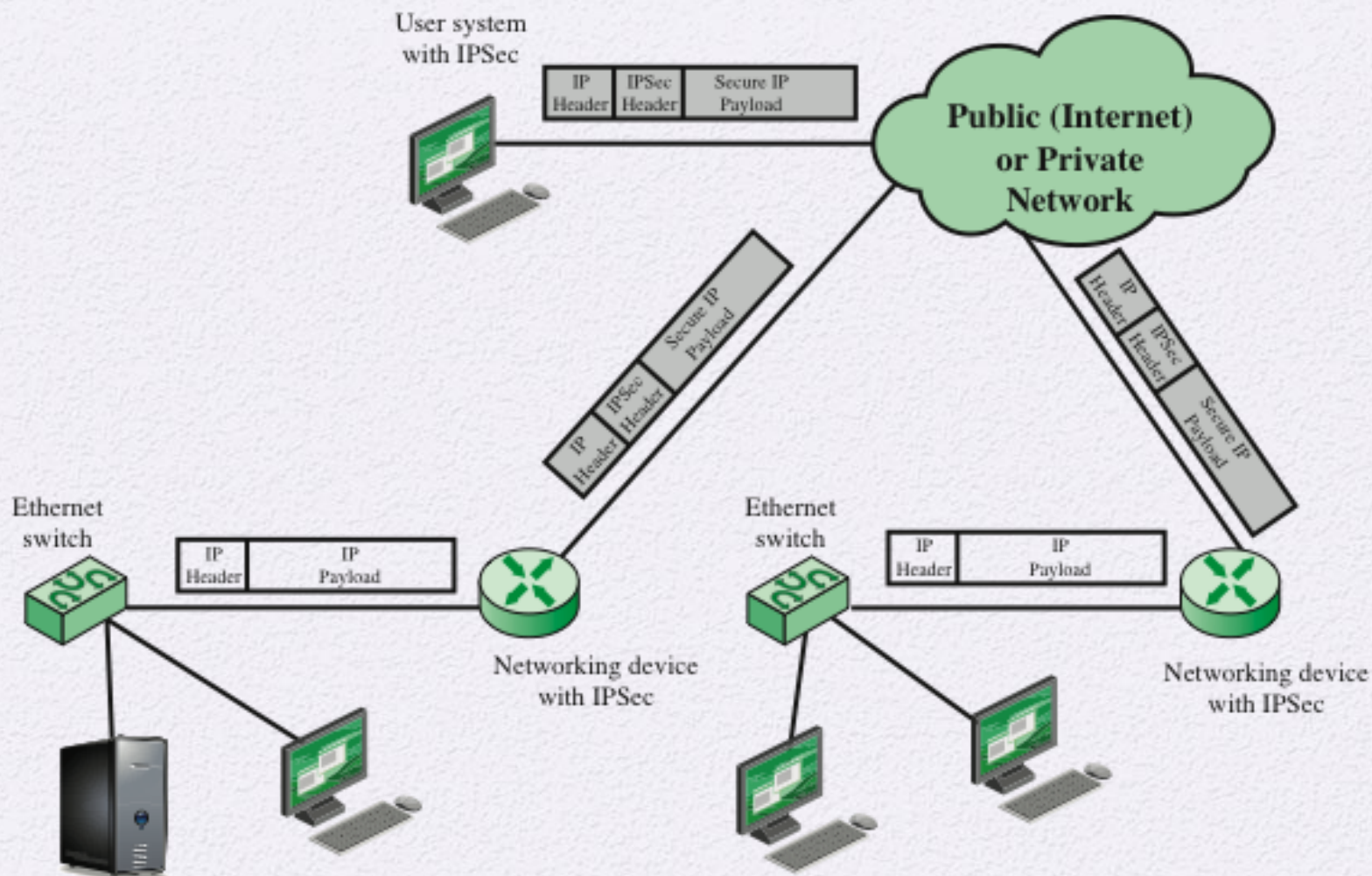
Figure 20.1 An IP Security Scenario

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 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

Encapsulating Security Payload (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)

- A collection of documents describing the key management schemes for use with IPsec
- The main specification is RFC 5996, *Internet Key Exchange (IKEv2) Protocol*, but there are a number of related RFCs

Authentication Header (AH)

- An extension header to provide message authentication
- The current specification is RFC 4302, *IP Authentication Header*

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

IPsec Documents

Architecture

- Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology
- The current specification is RFC4301, *Security Architecture for the Internet Protocol*

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

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 20.1
Tunnel Mode and Transport Mode Functionality

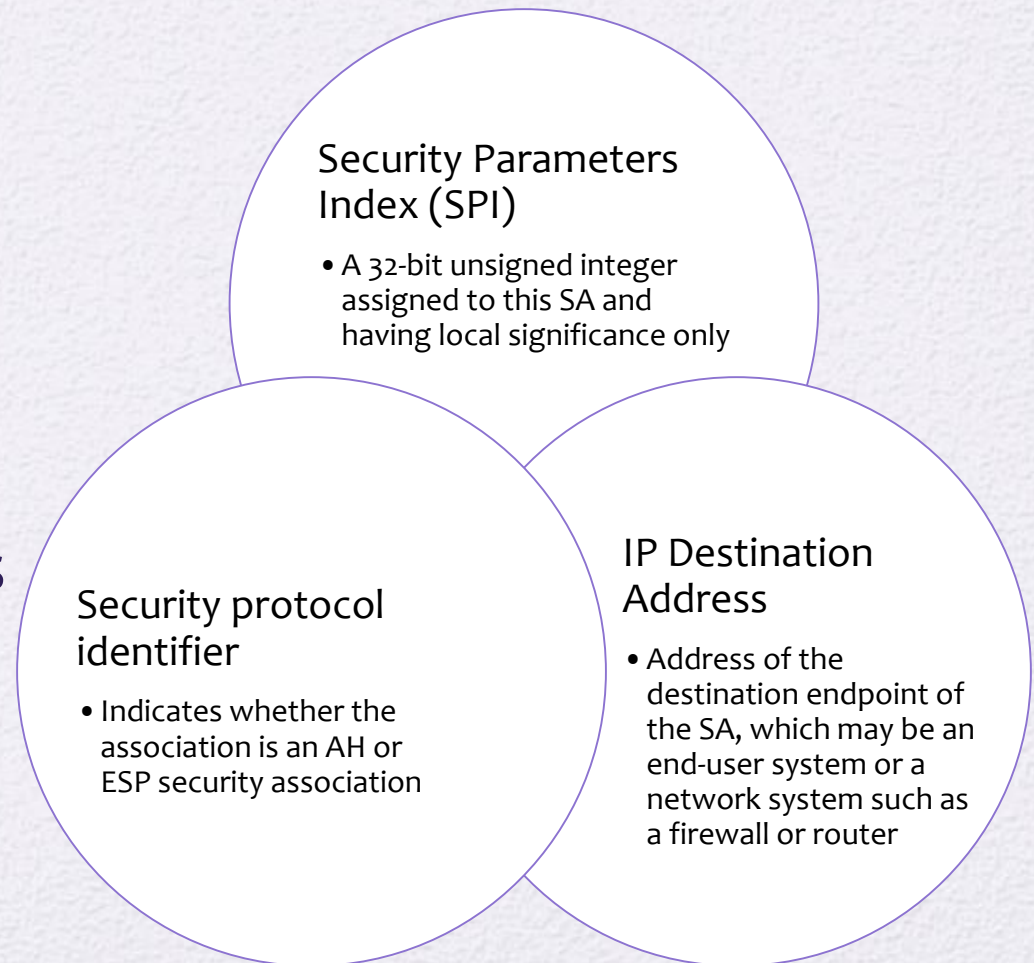|	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any 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.
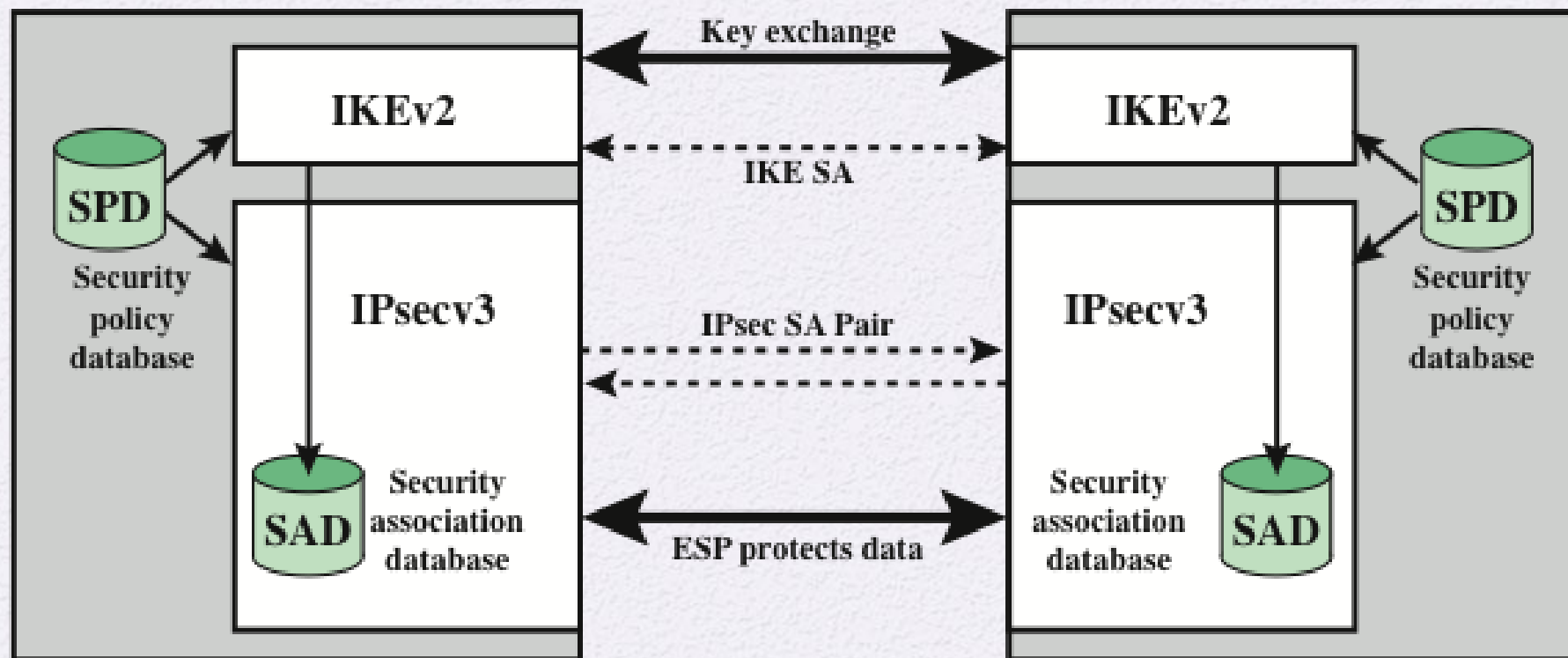
Figure 20.2 IPsec Architecture

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 Parameters Index (SPI)
- A 32-bit unsigned integer assigned to this SA and having local significance only

Security protocol identifier
- Indicates whether the association is an AH or ESP security association

IP Destination Address
- 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 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
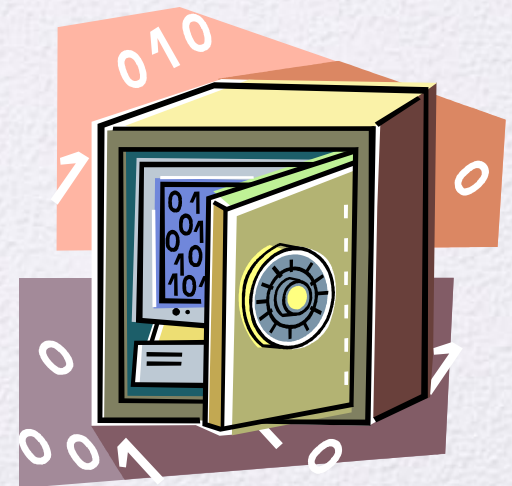
Security Policy Database (SPD)

- 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	Local IP address	Next layer protocol	Name	Local and remote ports
This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address	This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address		A user identifier from the operating system	
The latter two are required to support more than one destination system sharing the same SA	The latter two are required to support more than one source system sharing the same SA	The IP protocol header includes a field that designates the protocol operating over IP	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	These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port

Table 20.2
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
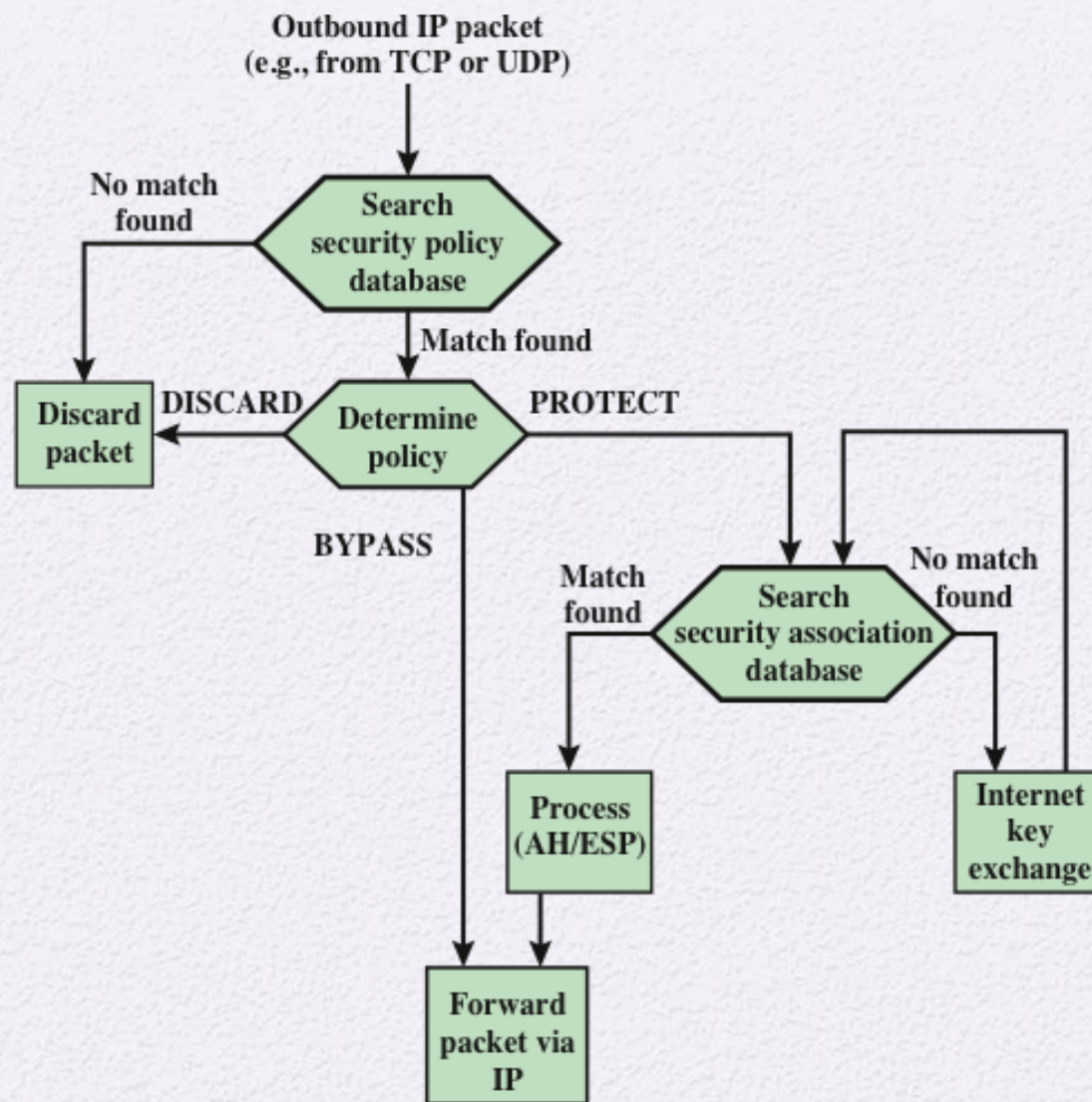
Figure 20.3 Processing Model for Outbound Packets
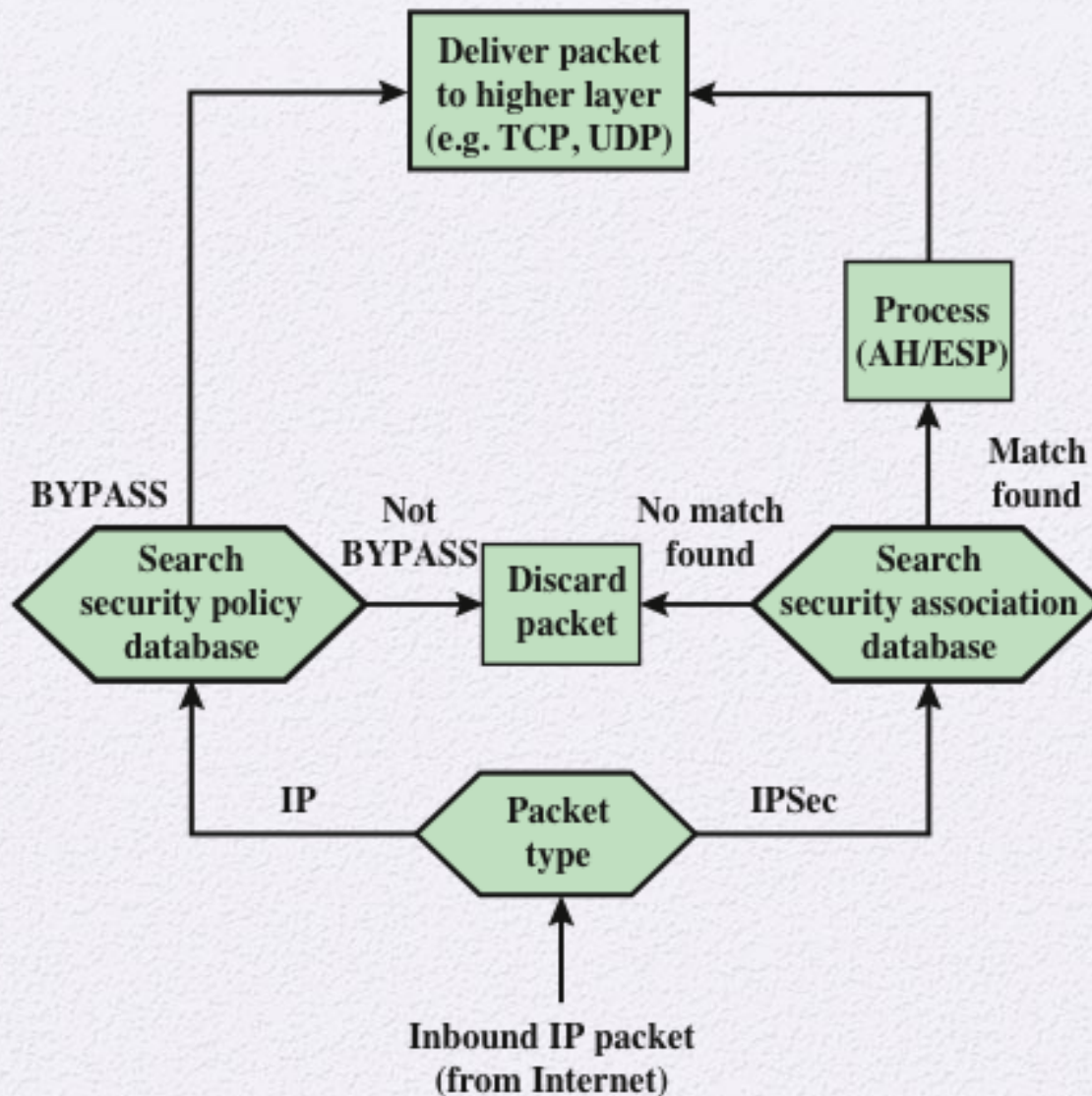
Figure 20.4 Processing Model for Inbound Packets

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**
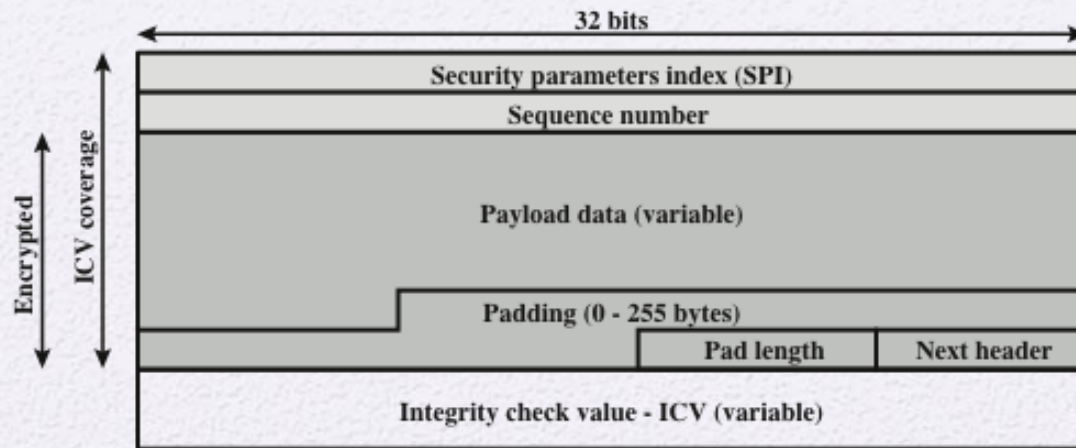
(a) Top-level format of an ESP Packet

| 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**
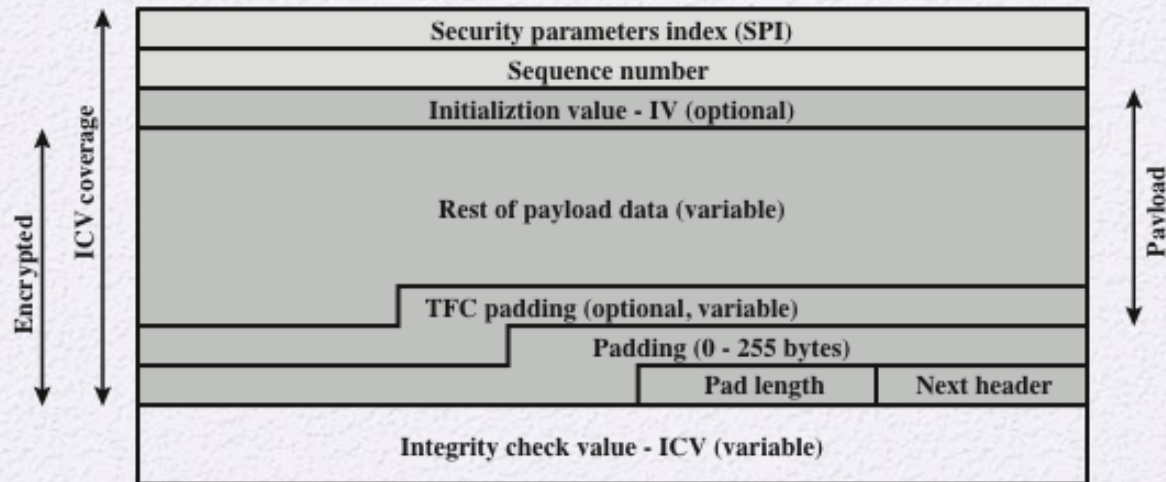
(b) Substructure of payload data

Figure 20.5 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
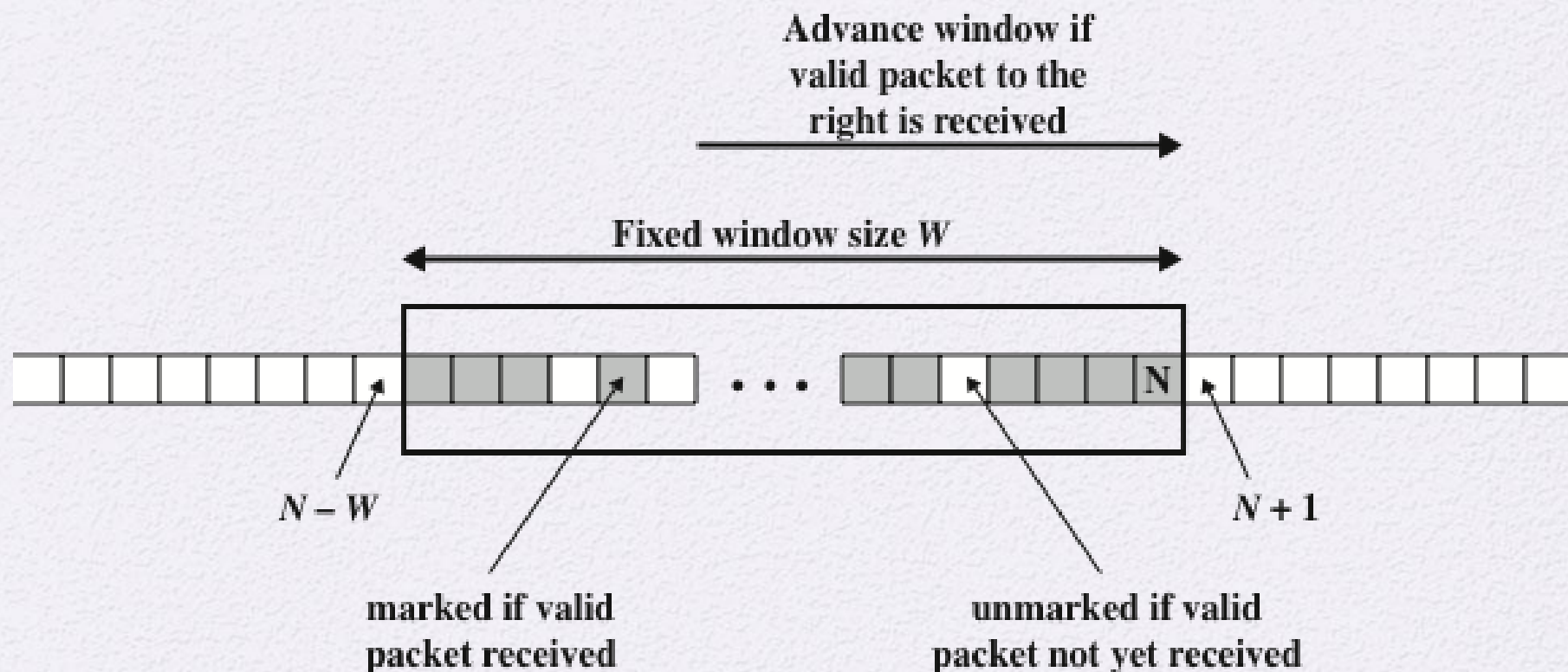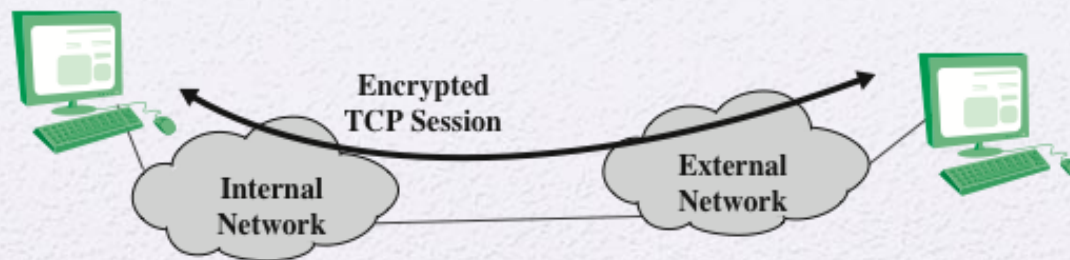
- An optional ICV field is present only if the integrity service is selected and is provided by either a separate integrity algorithm or a combined mode algorithm that uses an ICV
  - ICV is computed after the encryption is performed
  - This order of processing facilitates reducing the impact of DoS 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

Figure 20.6 Anti-Replay Mechanism

Encrypted TCP Session

Internal Network

External Network

(a) Transport-level security

Encrypted tunnels carrying IP traffic

Corporate Network

Corporate Network

Internet

Corporate Network

Corporate Network
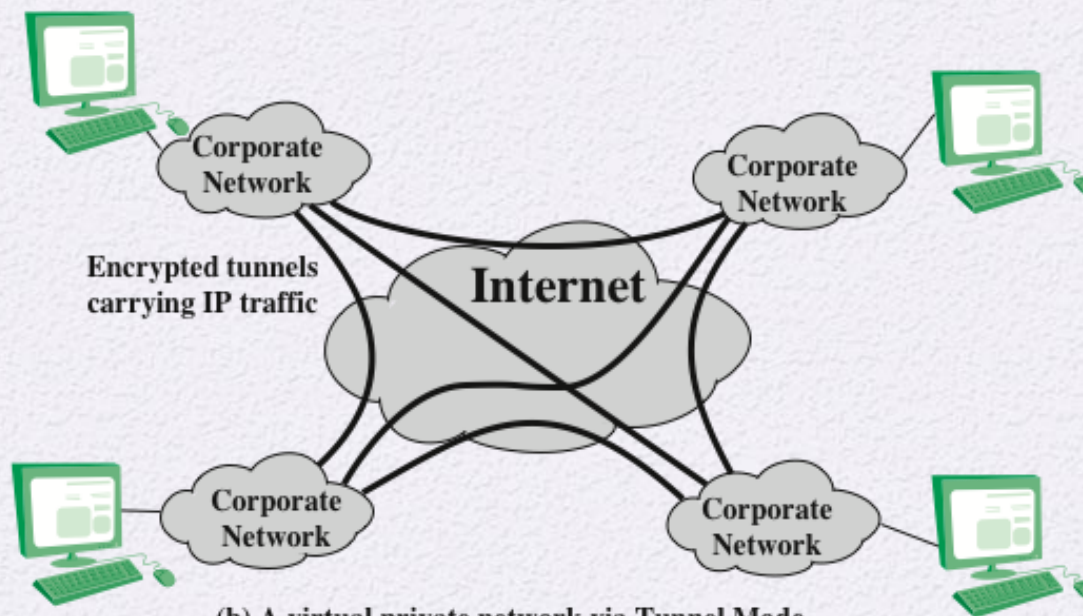
(b) A virtual private network via Tunnel Mode

Figure 20.7 Transport-Mode vs. Tunnel-Mode Encryption

IPv4

orig IP hdr	TCP	Data

IPv6

orig IP hdr	extension headers (if present)	TCP	Data

(a) Before Applying ESP

authenticated

encrypted

IPv4

orig IP hdr	ESP hdr	TCP	Data	ESP trlr	ESP auth

authenticated

encrypted

IPv6

orig IP hdr	hop-by-hop, dest, routing, fragment	ESP hdr	dest	TCP	Data	ESP trlr	ESP auth

(b) Transport Mode

authenticated

encrypted

IPv4

New IP hdr	ESP hdr	orig IP hdr	TCP	Data	ESP trlr	ESP auth

authenticated

encrypted

IPv6

new IP hdr	ext headers	ESP hdr	orig IP hdr	ext headers	TCP	Data	ESP trlr	ESP auth

(c) Tunnel Mode

Figure 20.8 Scope of ESP Encryption and Authentication
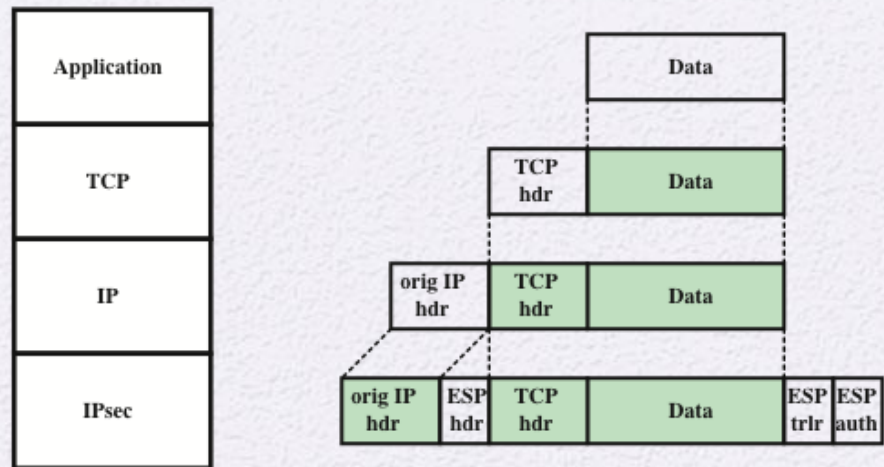
(a) Transport mode
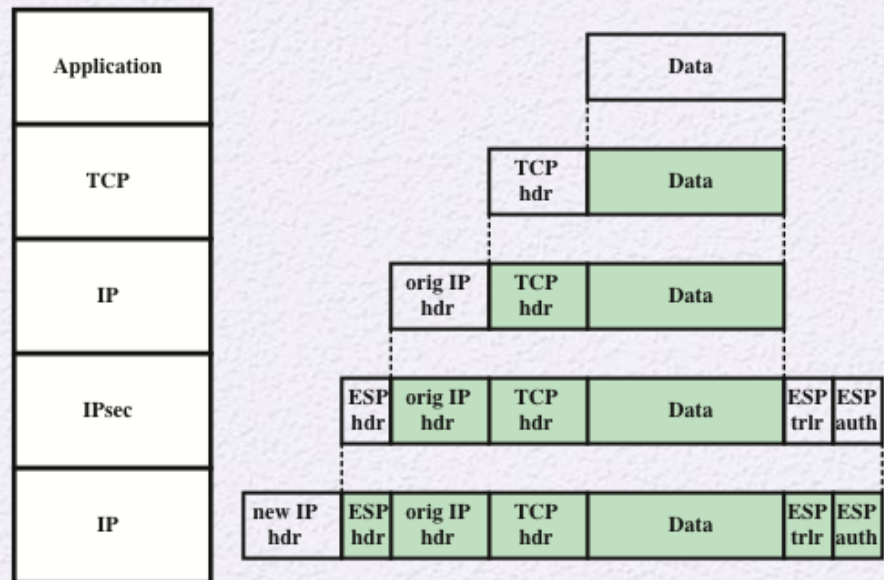
(b) Tunnel mode

Figure 20.9 Protocol Operation for ESP

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

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

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

One or More SAs

Host*

Router

Router

Host*

Local Intranet

Internet

Local Intranet

(a) Case 1

Tunnel SA

One or Two SAs

Host*

Security Gateway*

Security Gateway*

Host*

Local Intranet

Internet

Local Intranet

(c) Case 3

Tunnel SA

Host

Security Gateway*

Security Gateway*

Host

Local Intranet

Internet

Local Intranet

(b) Case 2

Tunnel SA

One or Two SAs

Host*

Security Gateway*

Host*

Internet

Local Intranet
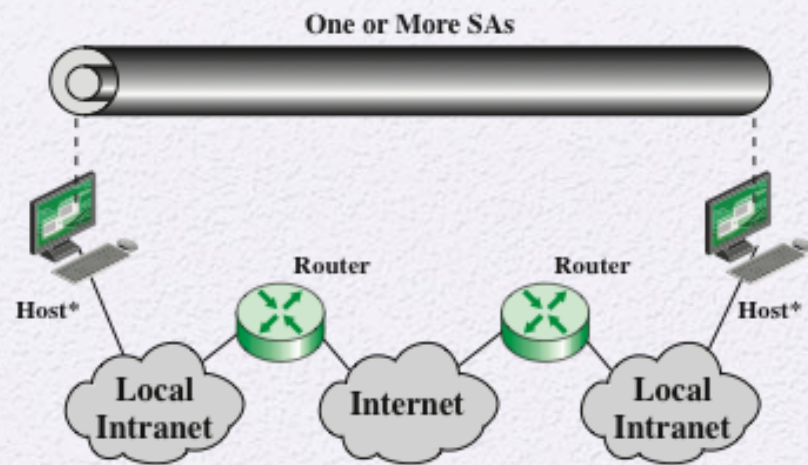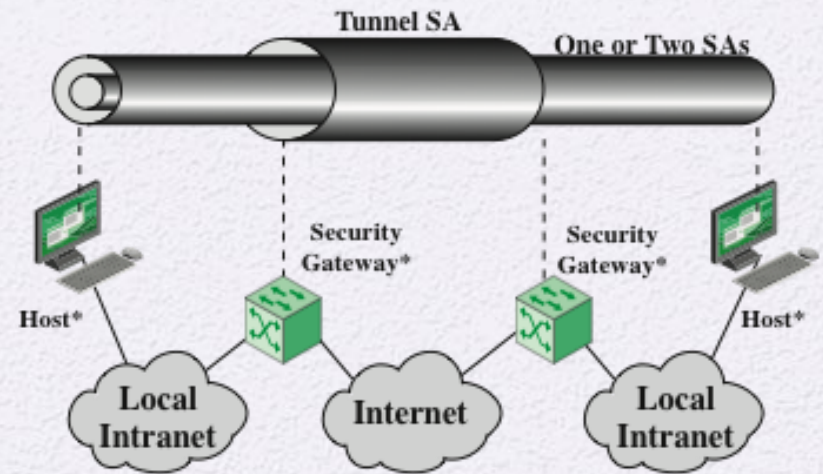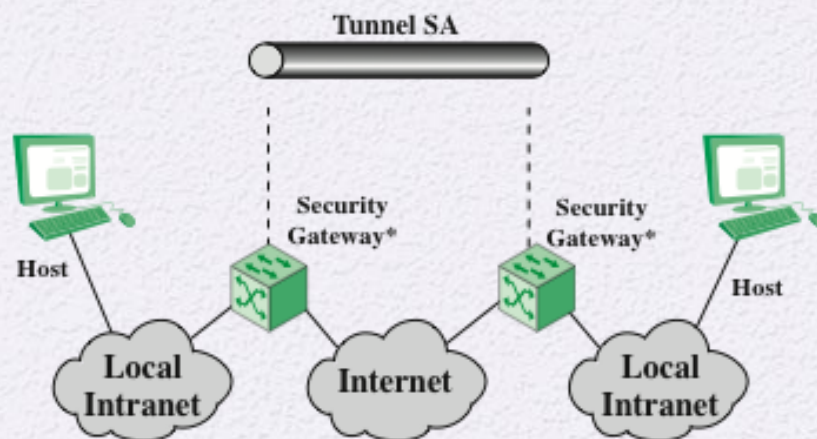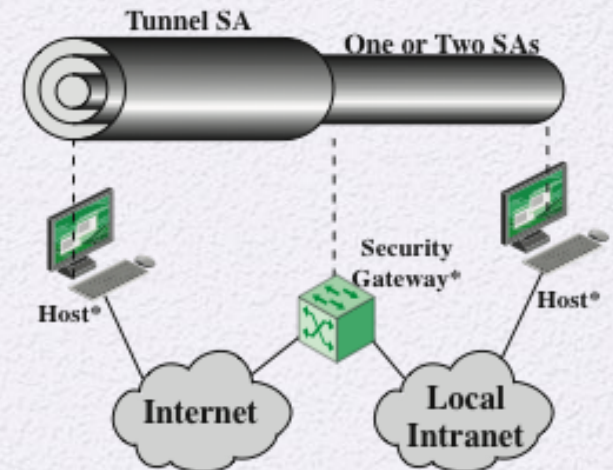
(d) Case 4

* = implements IPsec

Figure 20.10 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
- Enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration
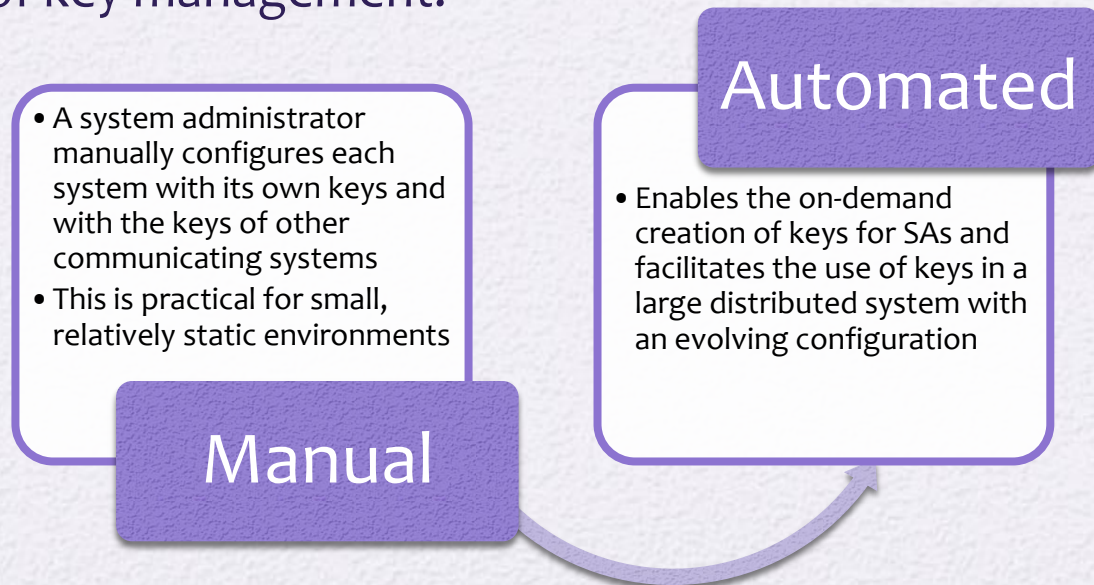
ISAKMP/Oakley

- 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

- Algorithm is characterized by five important features:

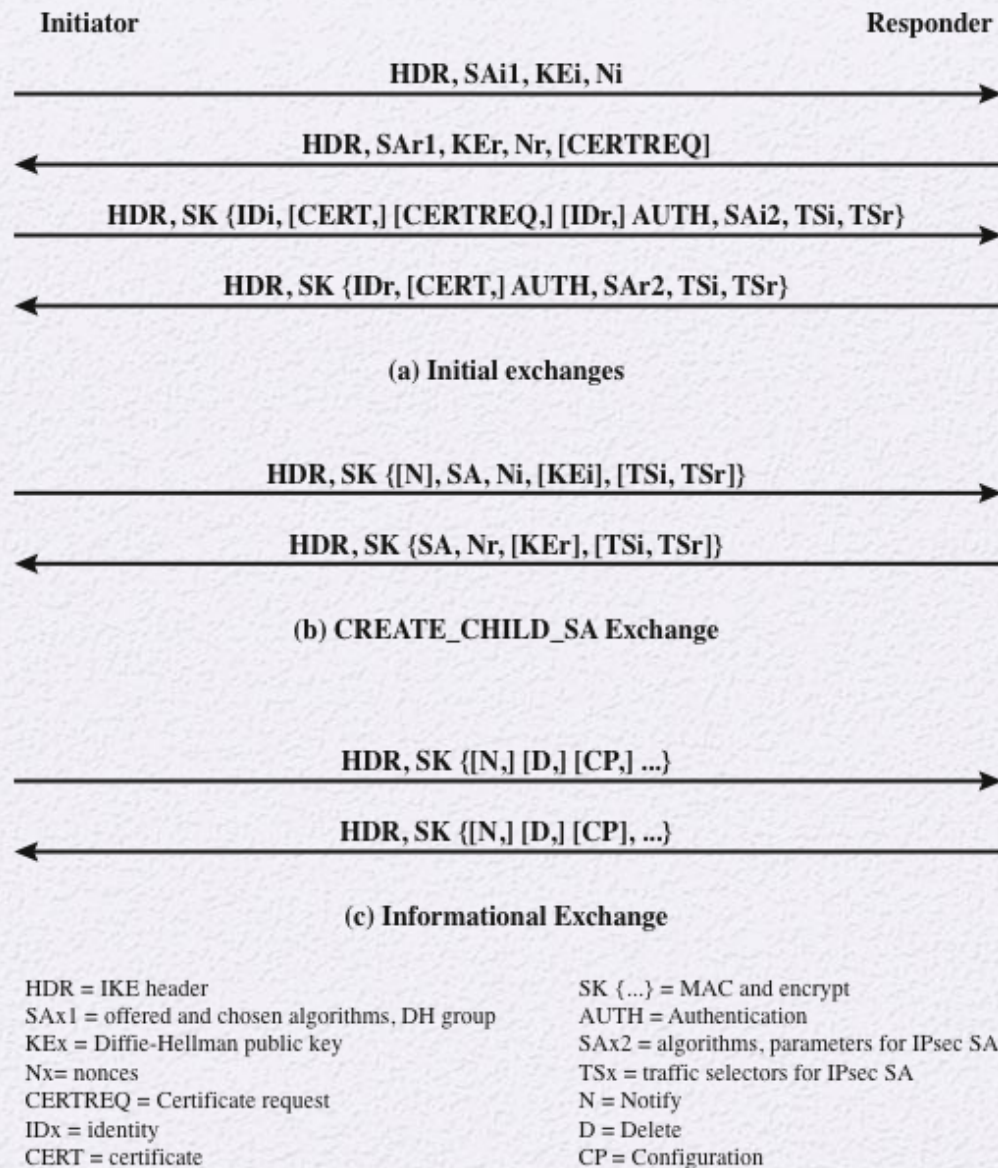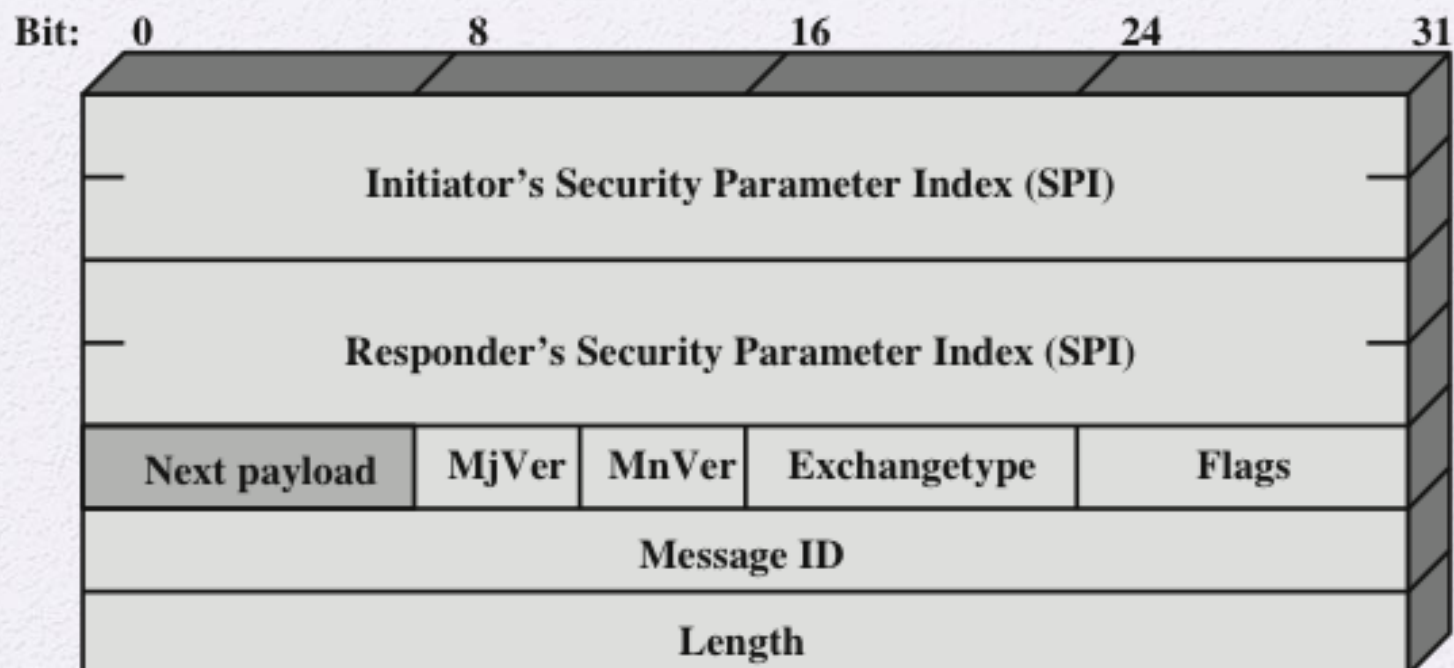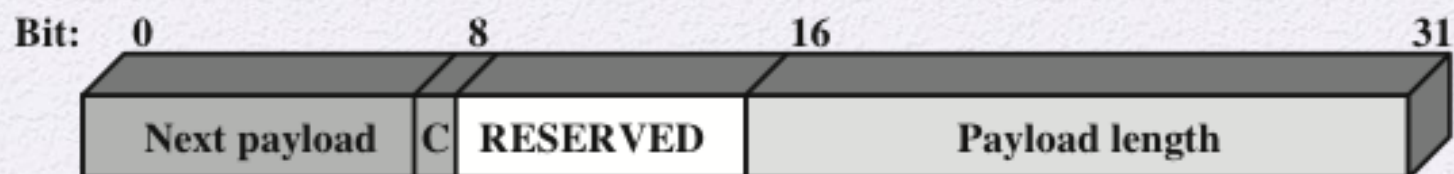|	
1.	• It employs a mechanism known as cookies to thwart clogging attacks
2.	• It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange
3.	• It uses nonces to ensure against replay attacks
4.	• It enables the exchange of Diffie-Hellman 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   SK {...} = MAC and encrypt
SAx1 = offered and chosen algorithms, DH group   AUTH = Authentication
KEx = Diffie-Hellman public key   SAx2 = algorithms, parameters for IPsec SA
Nx= nonces   TSx = traffic selectors for IPsec SA
CERTREQ = Certificate request   N = Notify
IDx = identity   D = Delete
CERT = certificate   CP = Configuration

Figure 20.11 IKEv2 Exchanges

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