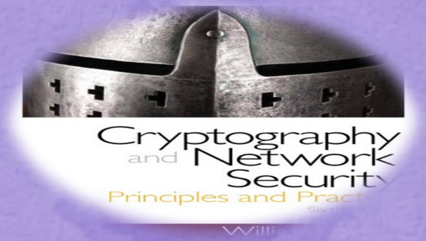
Cryptography and Network Security

Eighth Edition

by William Stallings

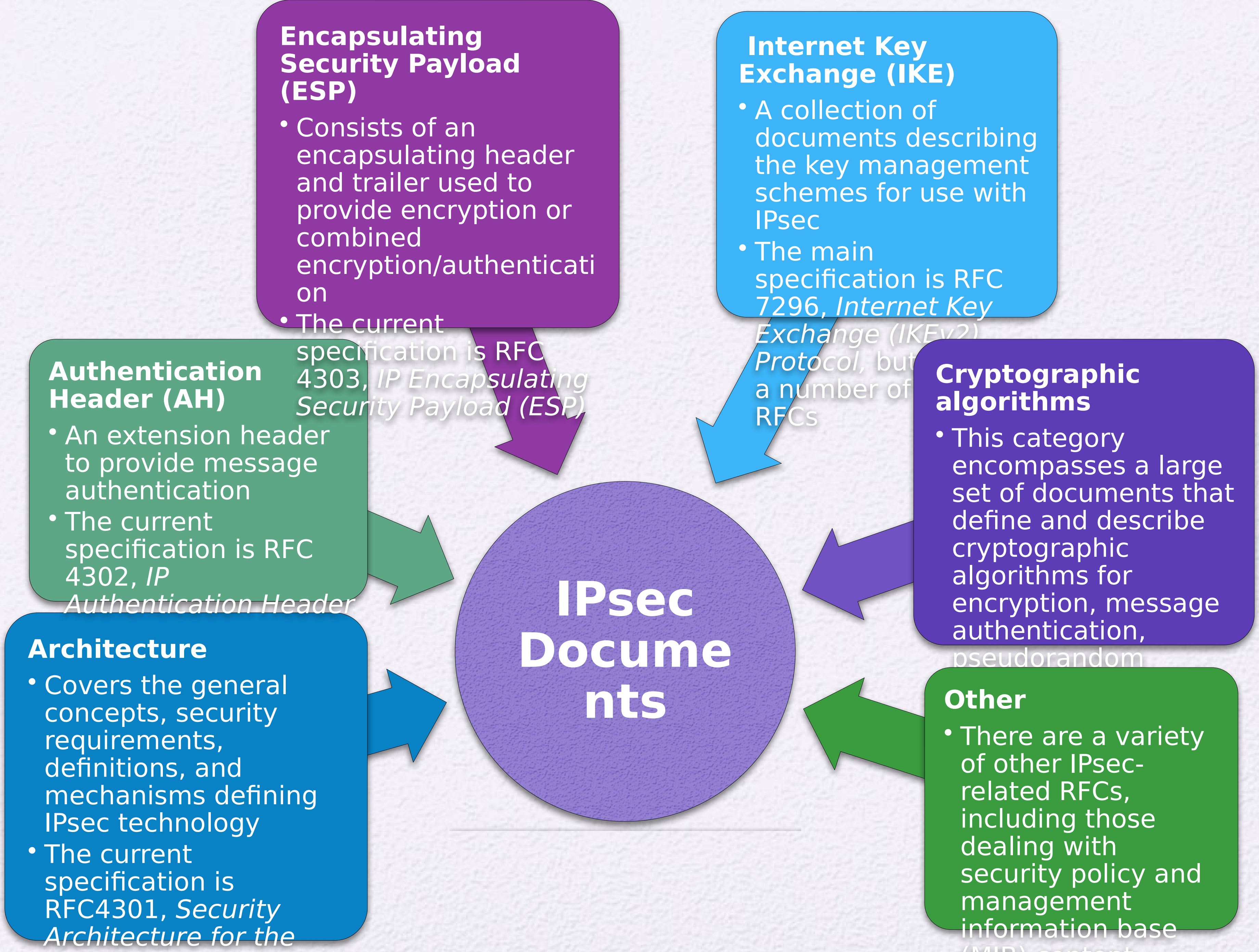


Chapter 20

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



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*

Authentication Header (AH)

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

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 7296, *Internet Key Exchange (IKEv2) Protocol*, but a number of RFCs

Cryptographic algorithms

- This category encompasses a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom

Other

- There are a variety of other IPsec-related RFCs, including those dealing with security policy and management information base (MIB) content

Applications of IPsec

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

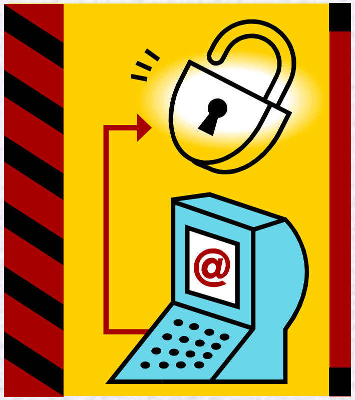
Examples include:

- 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

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



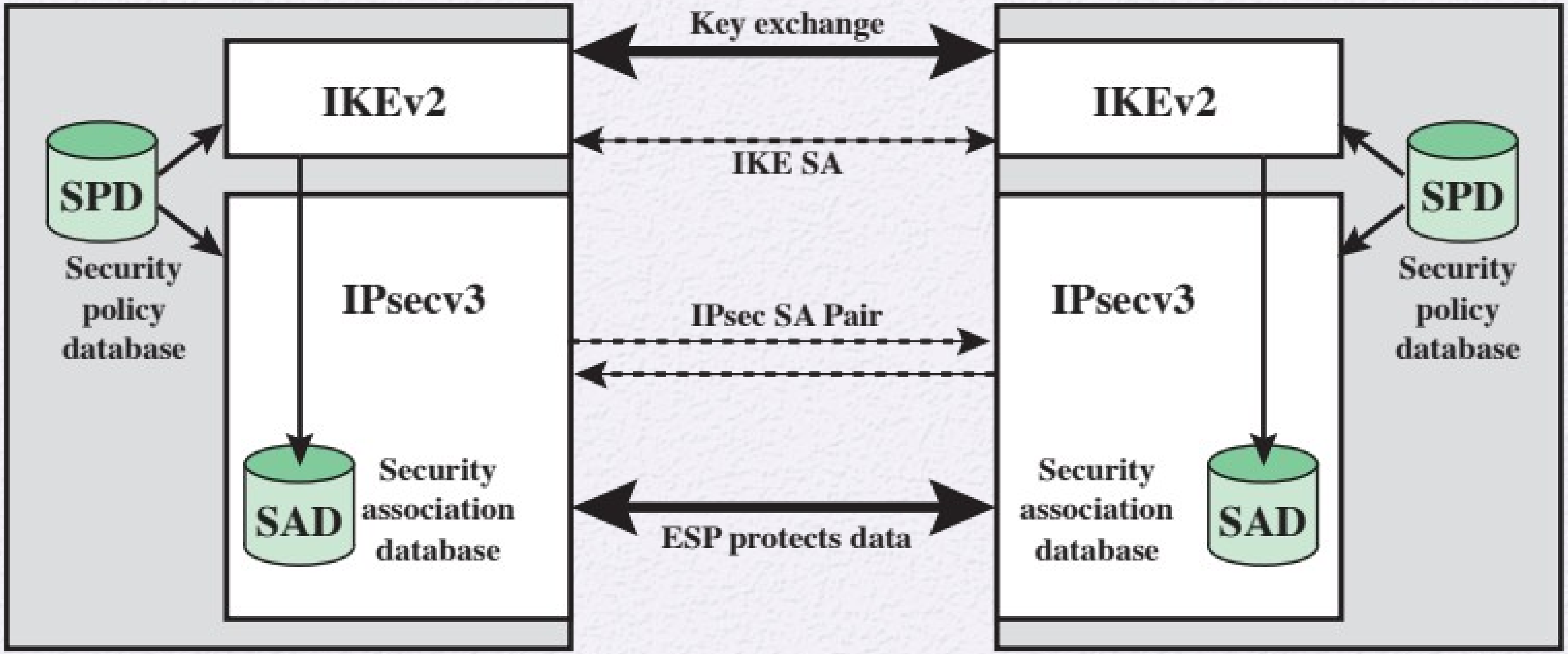
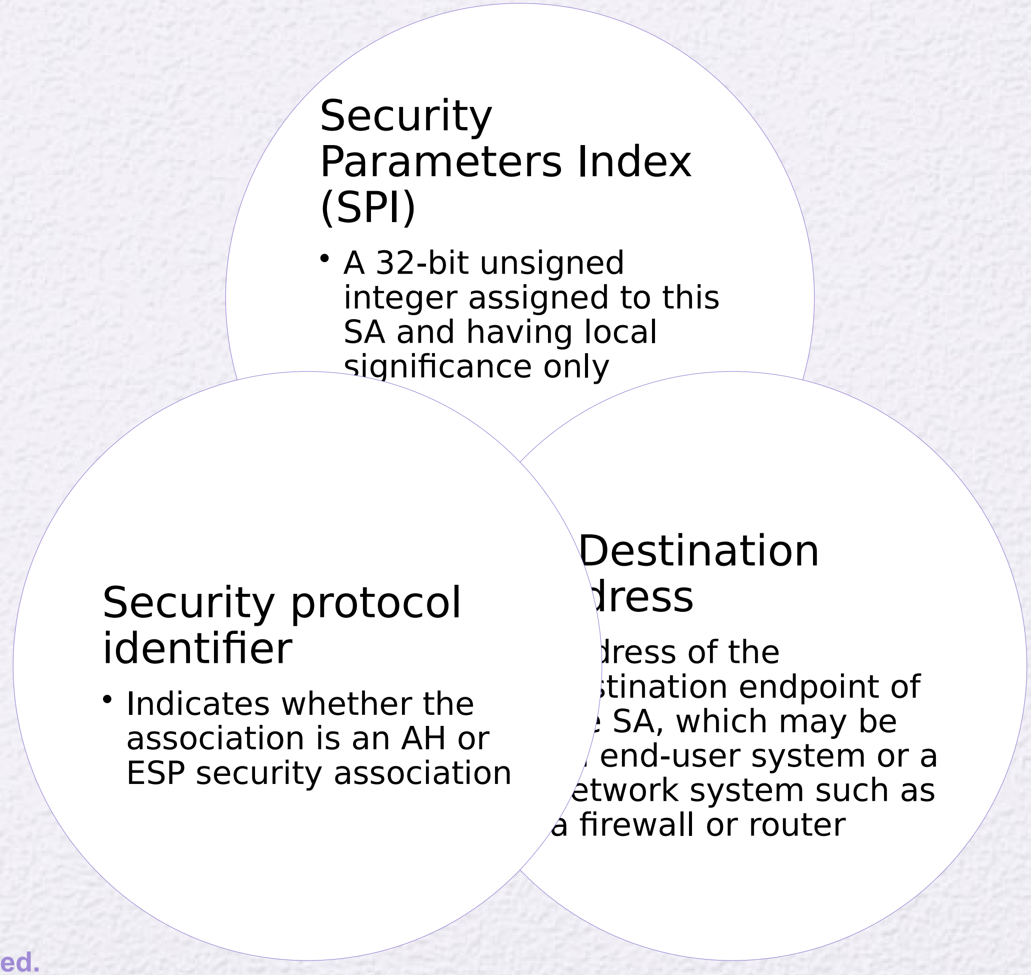


Figure 20.1 IPsec Architecture

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 Parameters Index (SPI)

- A 32-bit unsigned integer assigned to this SA and having local significance only

Security protocol identifier

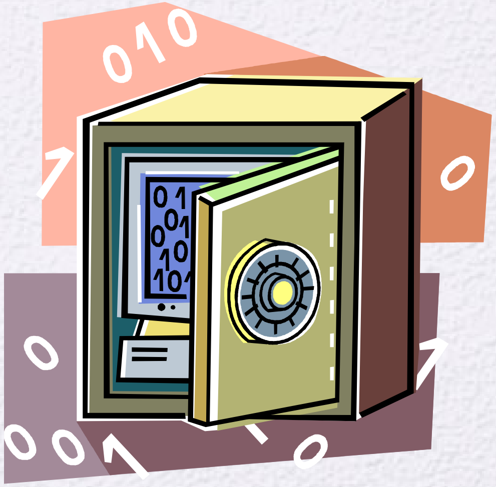
- Indicates whether the association is an AH or ESP security association

Destination
dress

dress of the
stination endpoint of
SA, which may be
end-user system or a
etwork 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

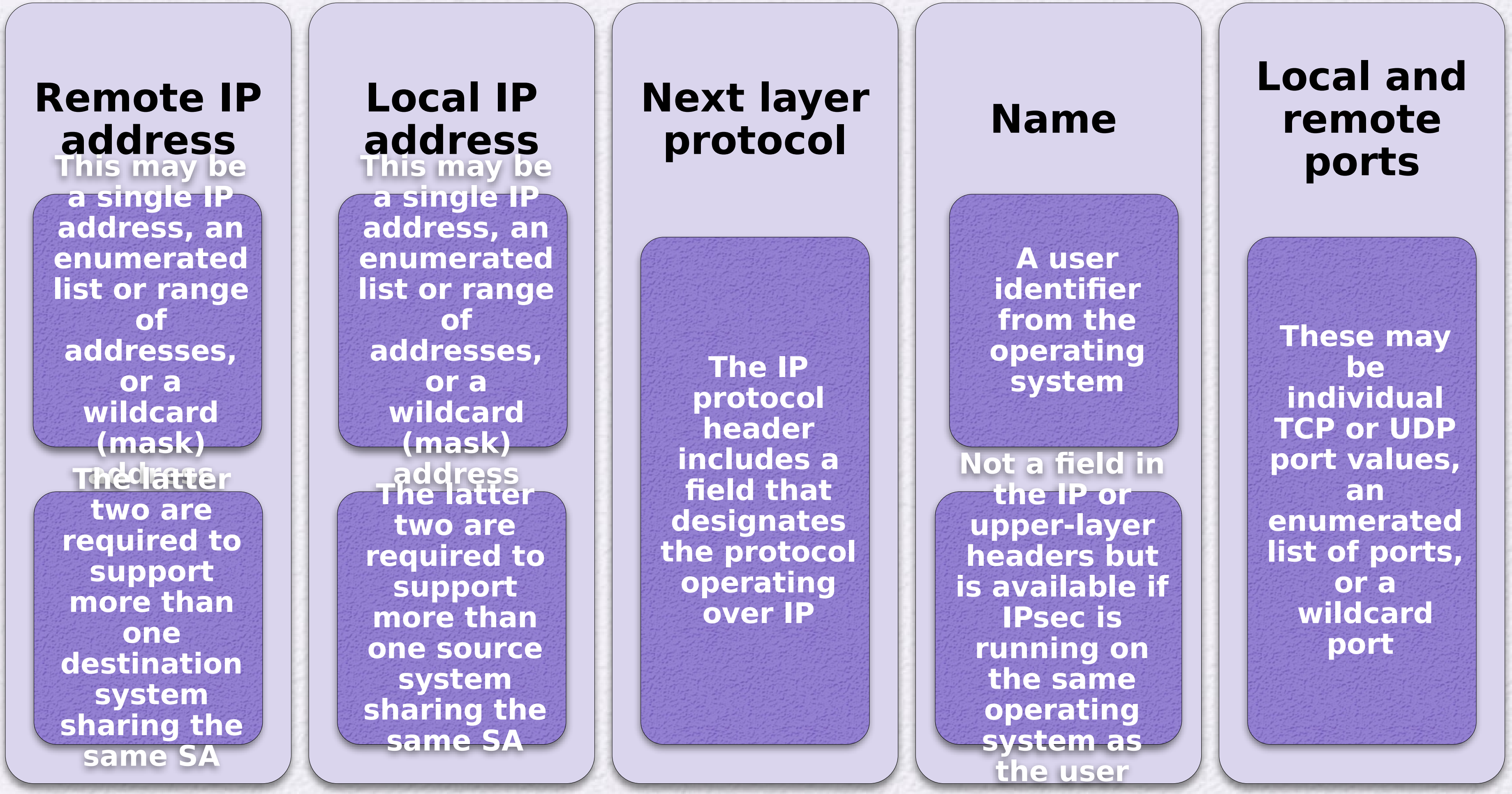


Security Policy Database (SPD)

- 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

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

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

Next layer protocol

The IP protocol header includes a field that designates the protocol operating over IP

Name

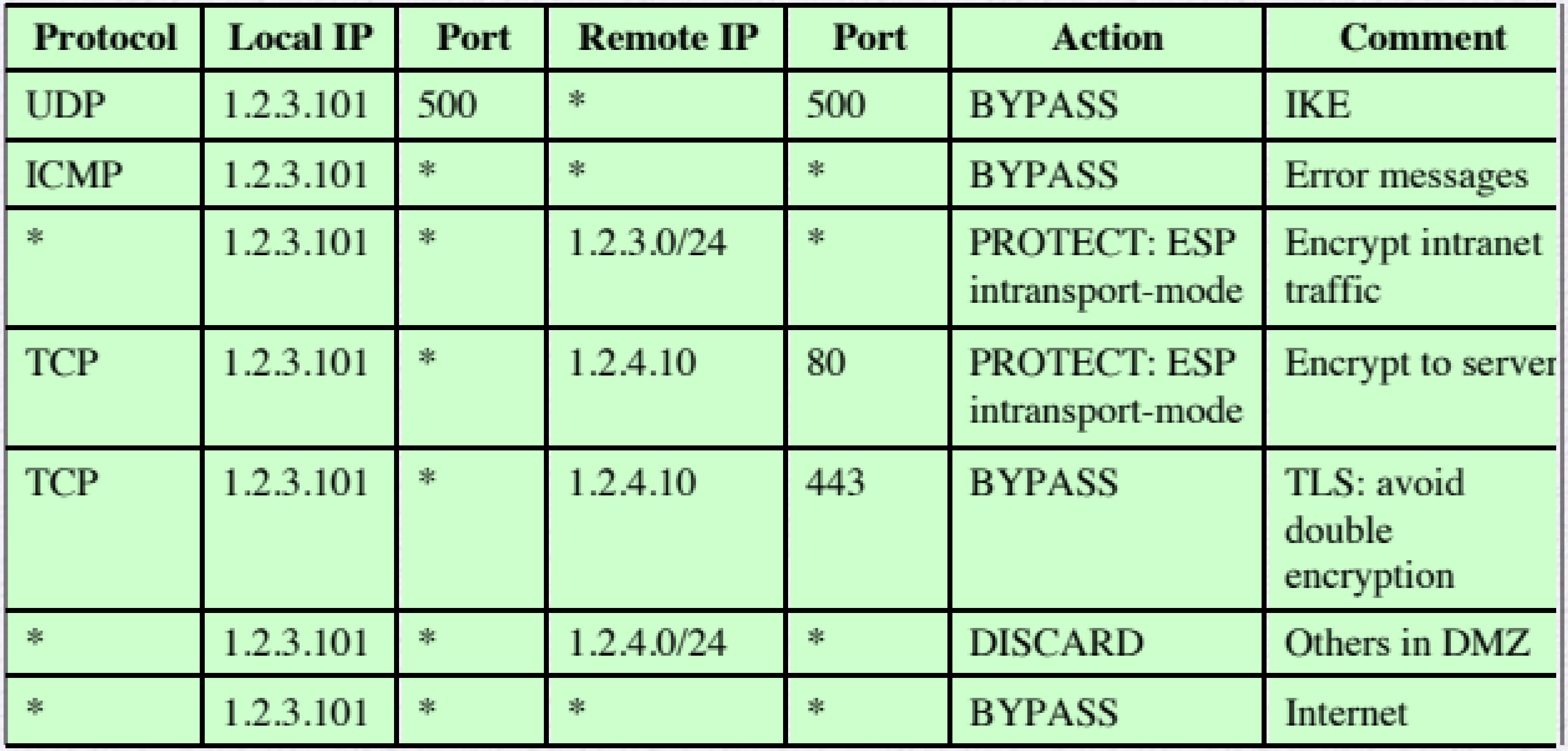
A user identifier from the operating system

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

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

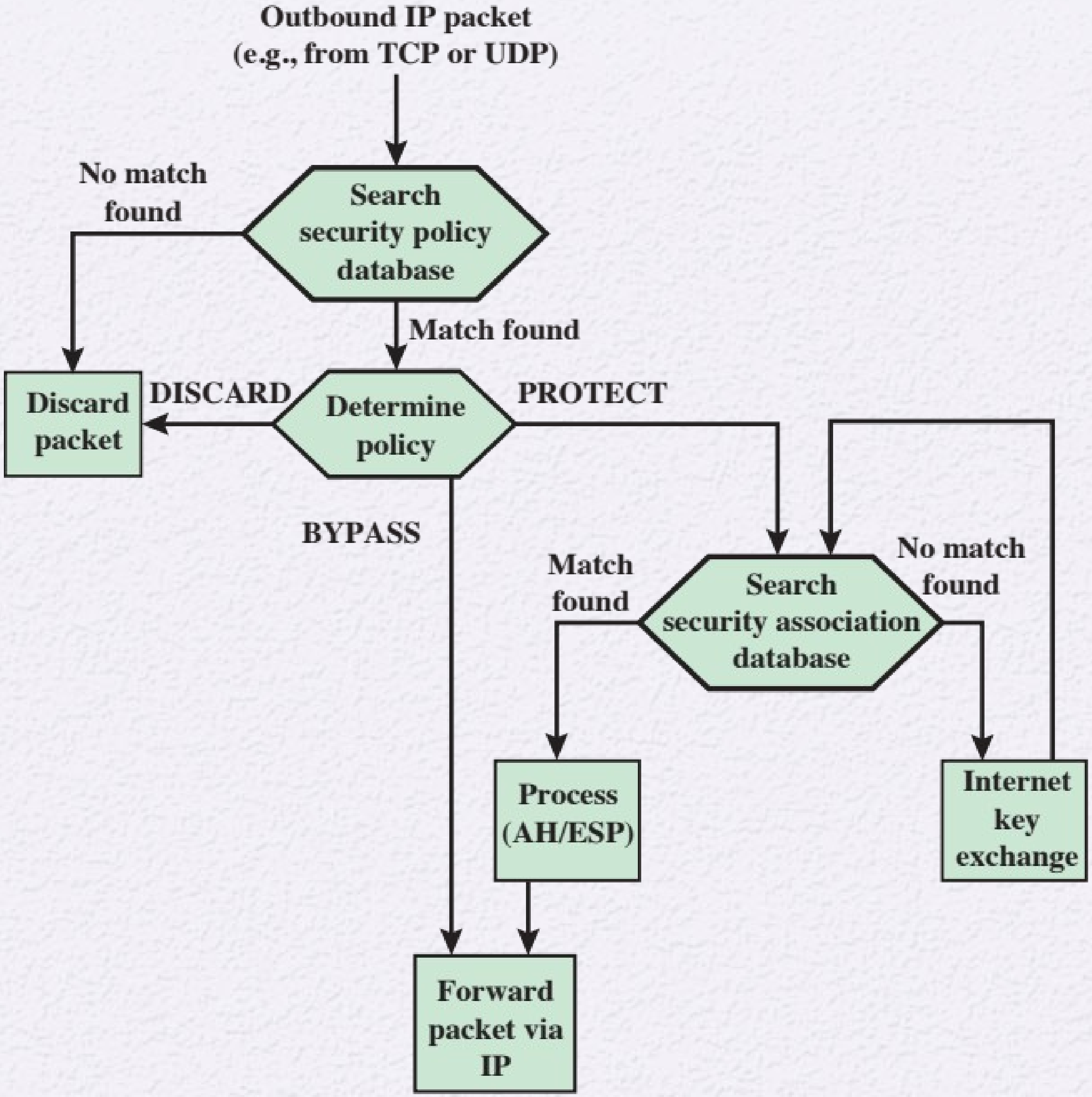


Figure 20.2 Processing Model for Outbound Packets

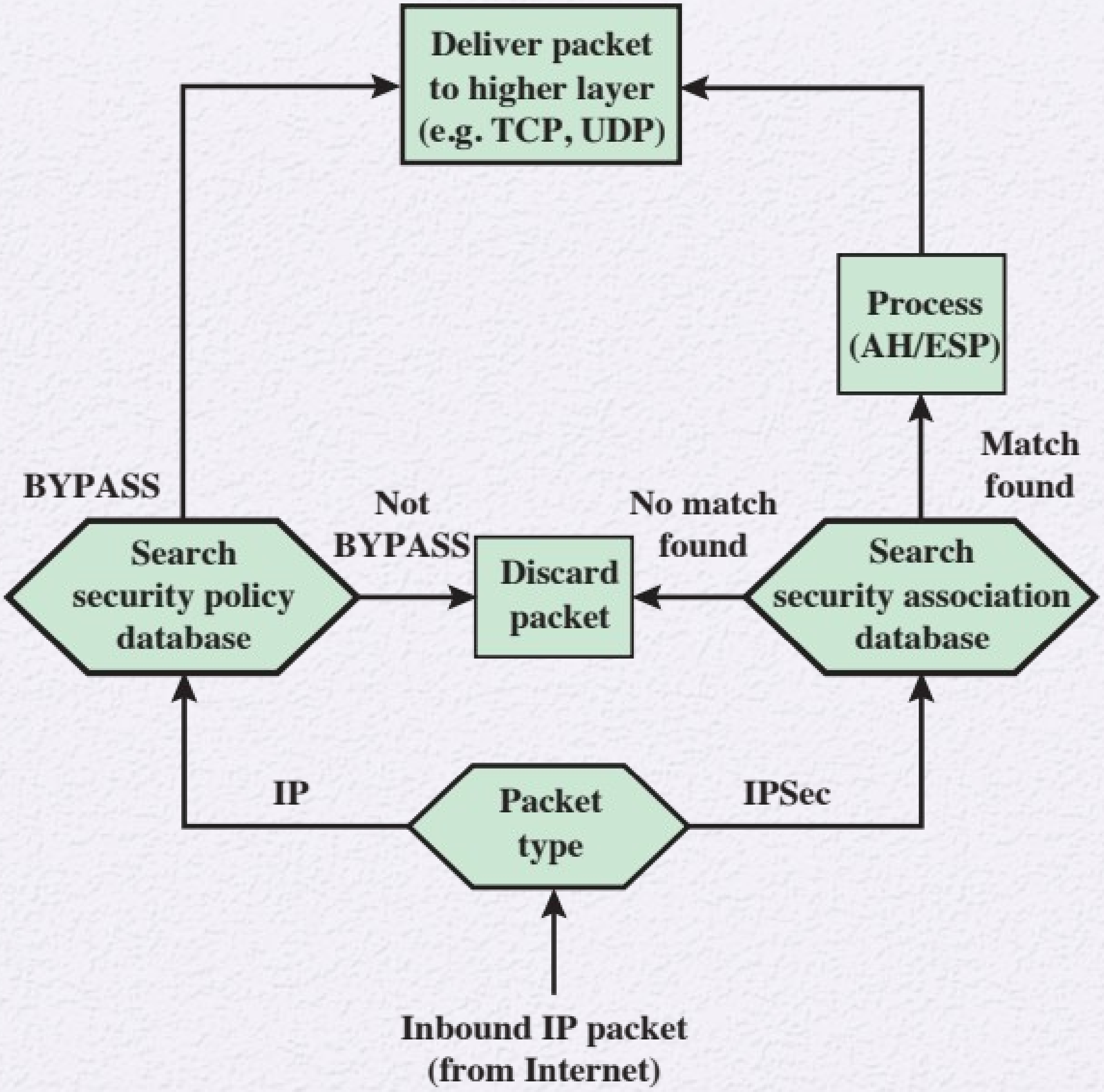
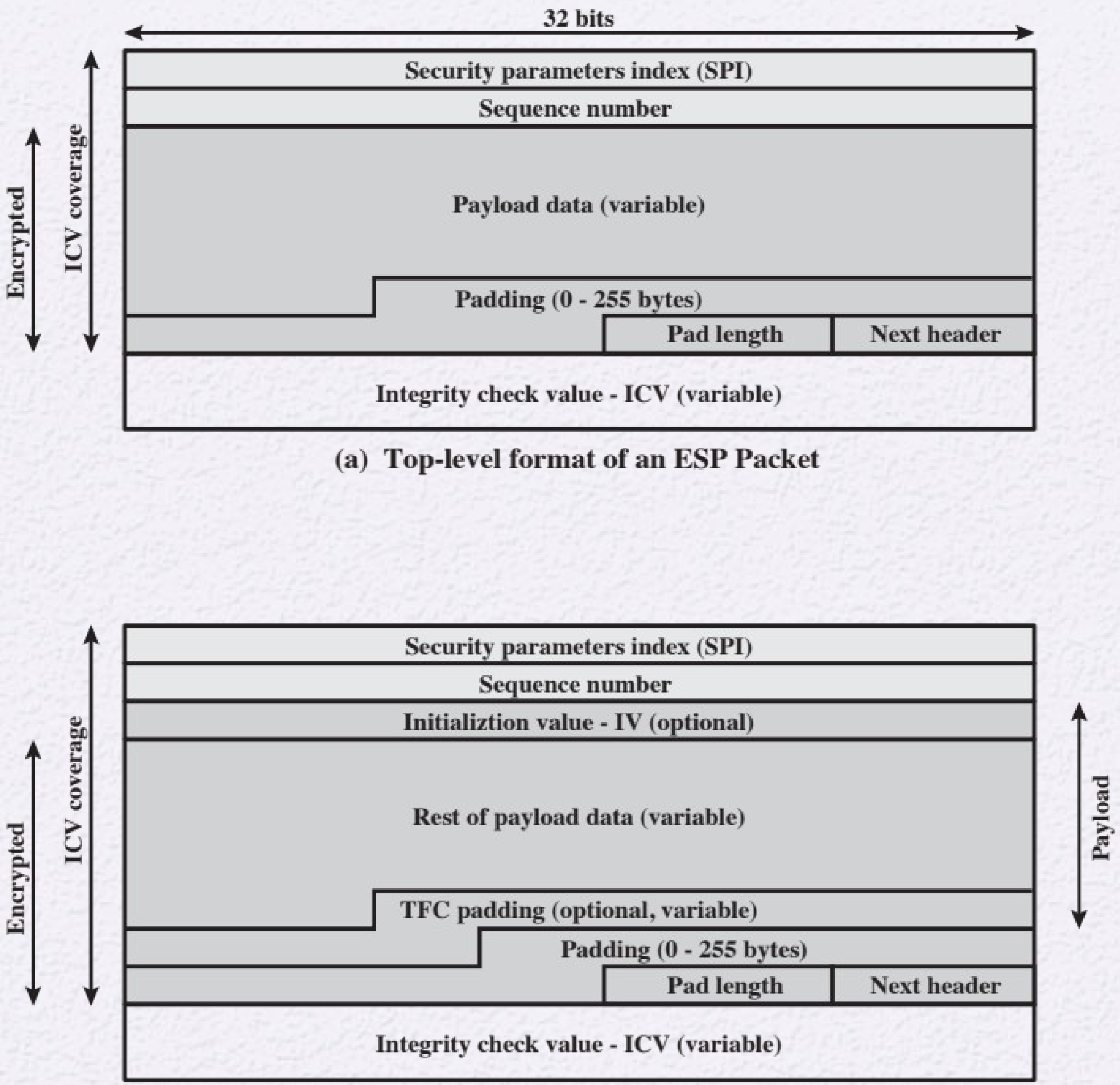

Deliver packet to higher layer (e.g. TCP, UDP)
BYPASS
Process (AH/ESP)
Match found
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
Packet type
IPSec
Inbound IP packet (from Internet)

Figure 20.3 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 20.4 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

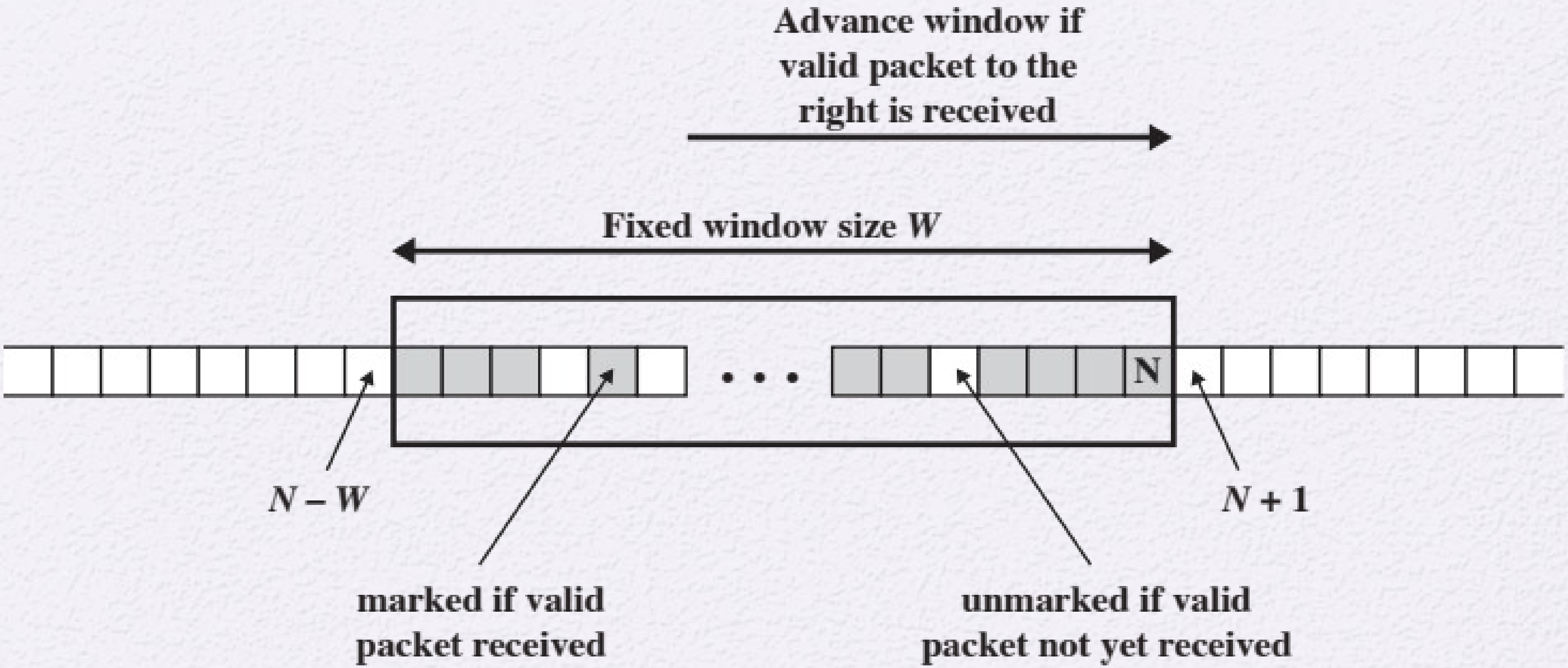
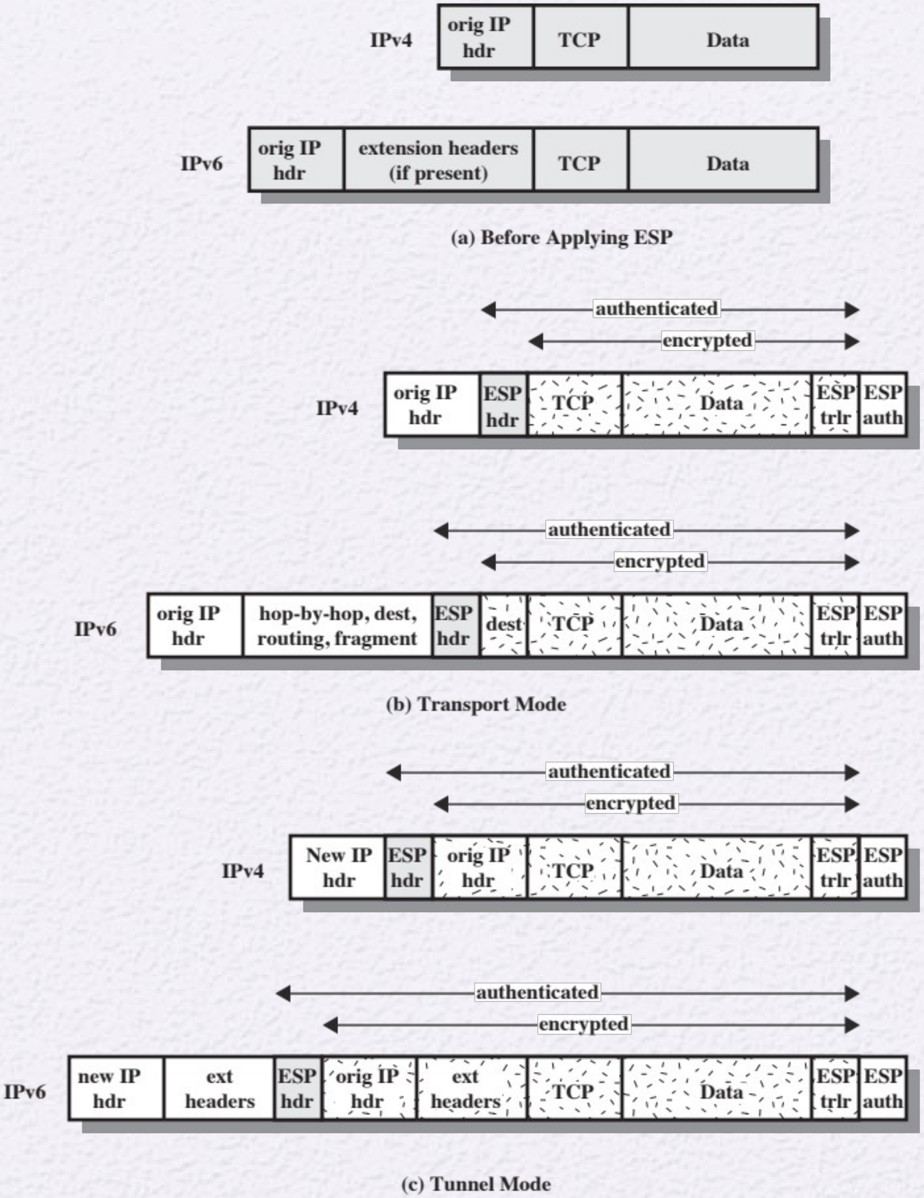

Advance window if valid packet to the right is received
Fixed window size W
N
N – W
marked if valid packet received
unmarked if valid packet not yet received
N + 1

Figure 20.5 Anti-Replay Mechanism



(a) Before Applying ESP

(b) Transport Mode

(c) Tunnel Mode

Figure 20.6 Scope of ESP Encryption and Authentication

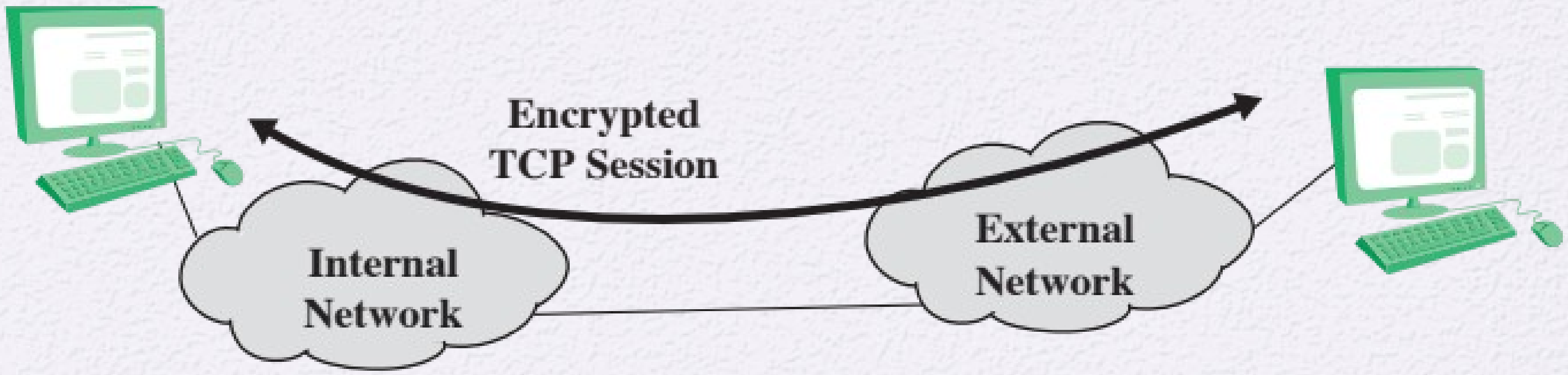
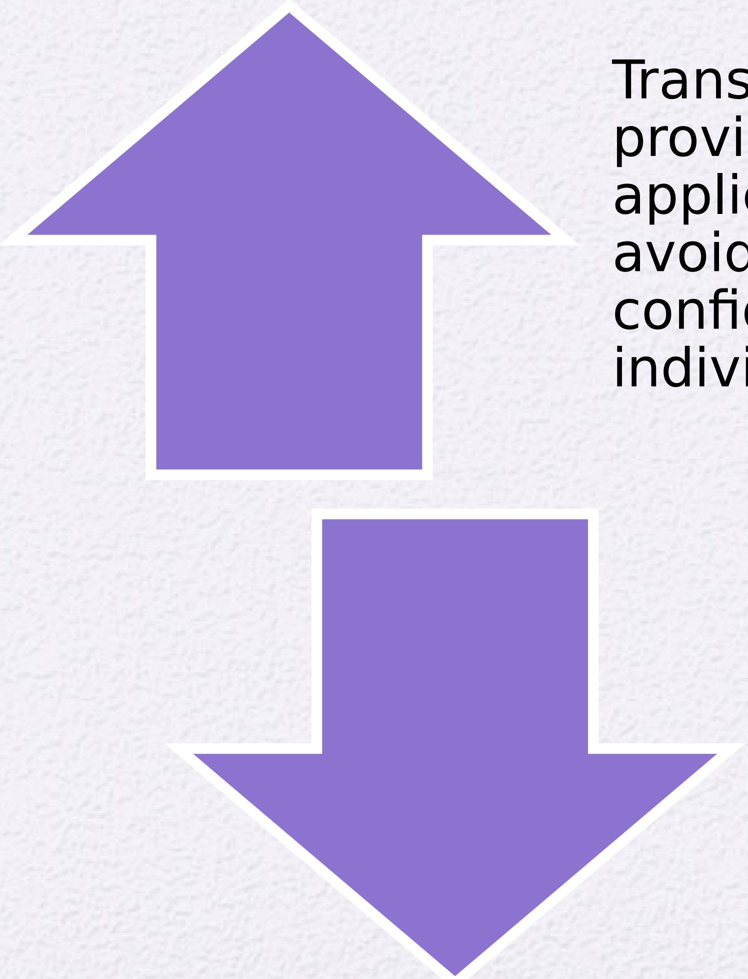


Figure 20.7 End-to-end IPsec Transport-Mode Encryption

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

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

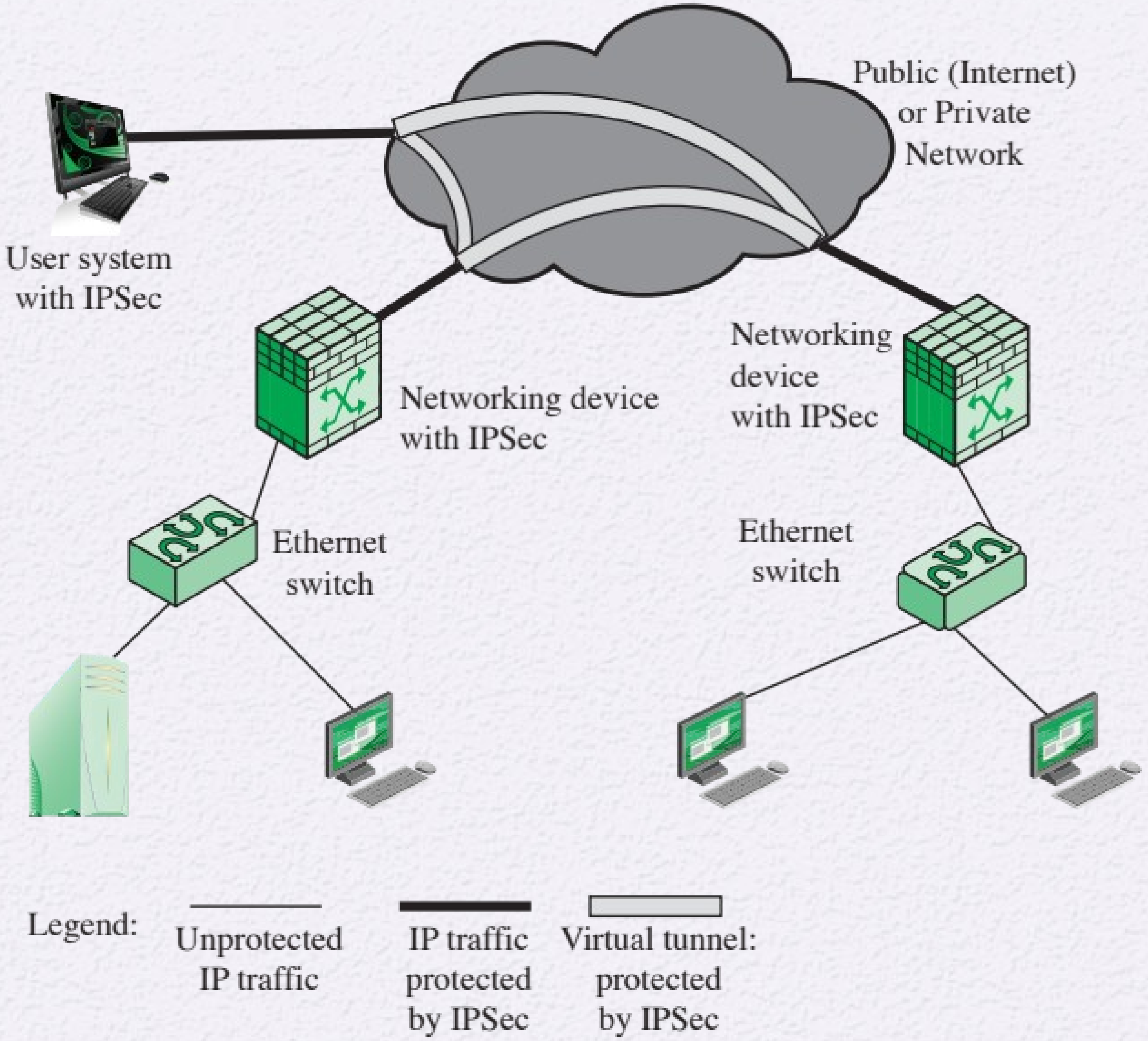
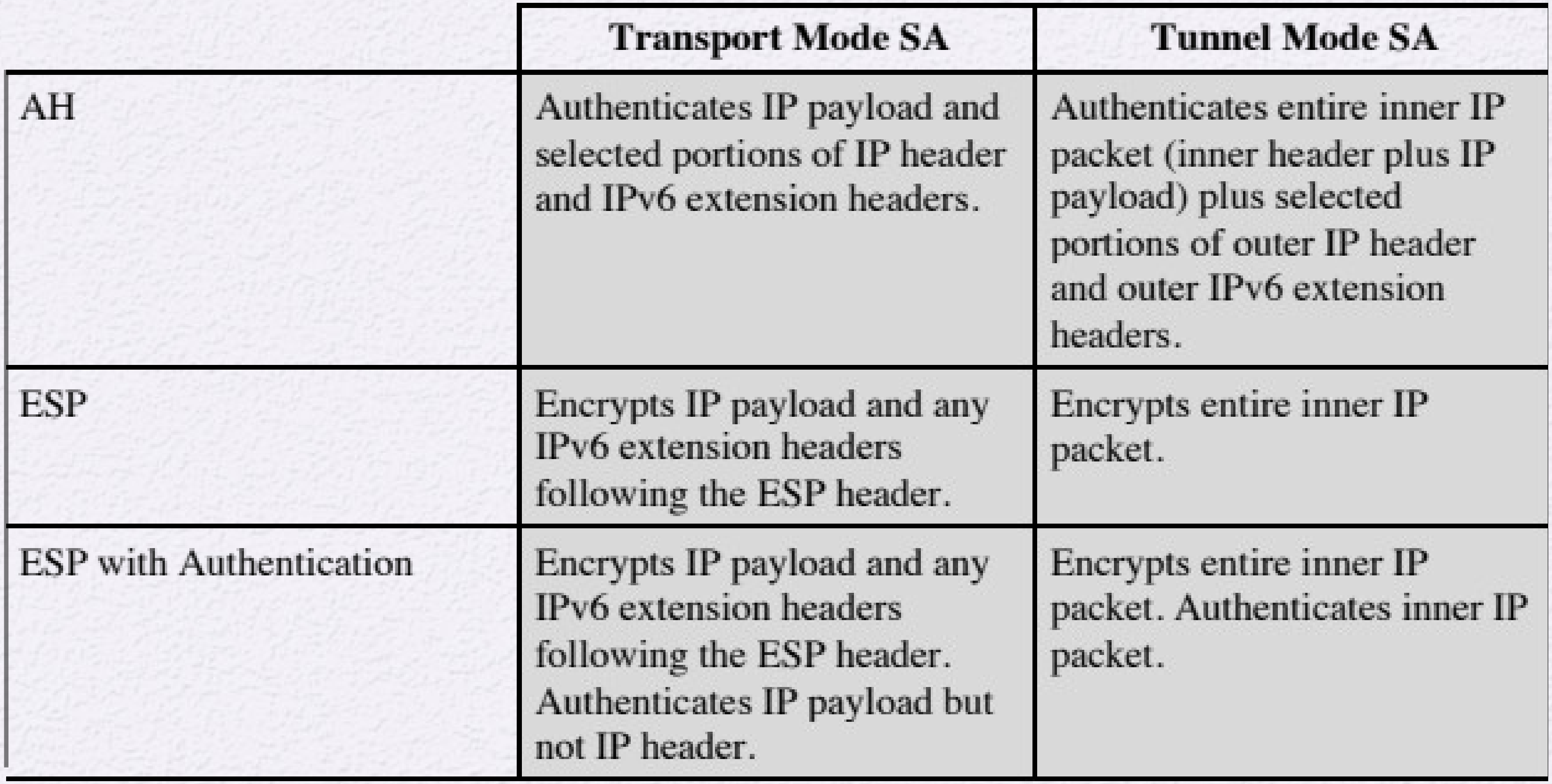
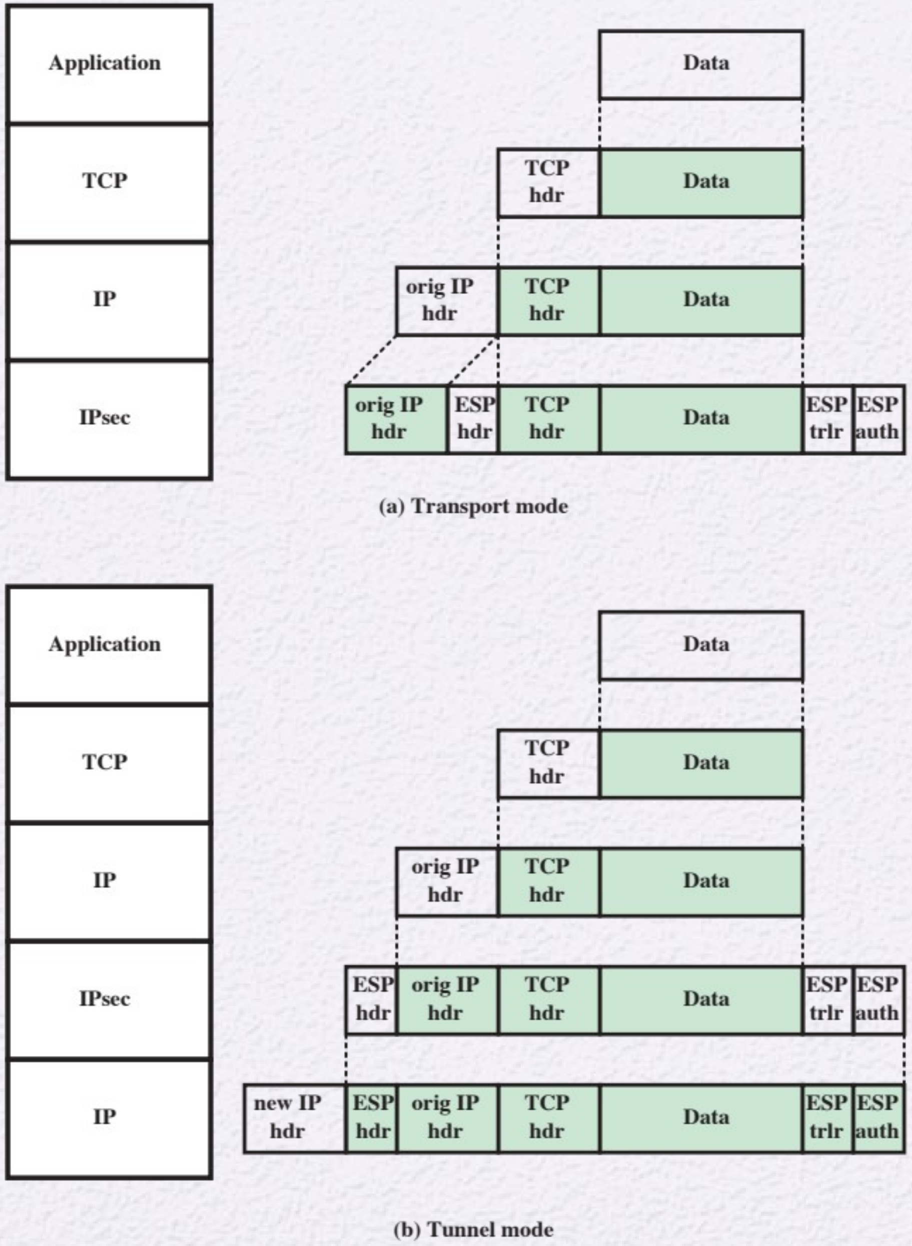


Figure 20.8 Example of Virtual Private Network Implemented with IPsec Tunnel Mode

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.



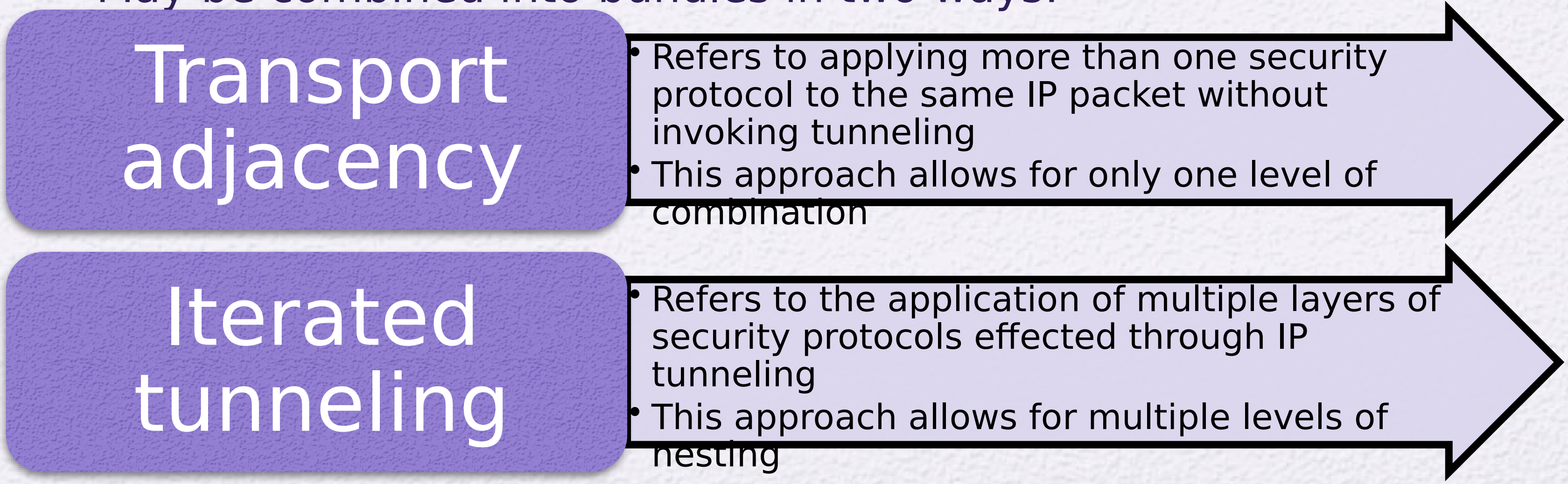
(a) Transport mode

(b) Tunnel mode

Figure 20.9 Protocol Operation for ESP

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

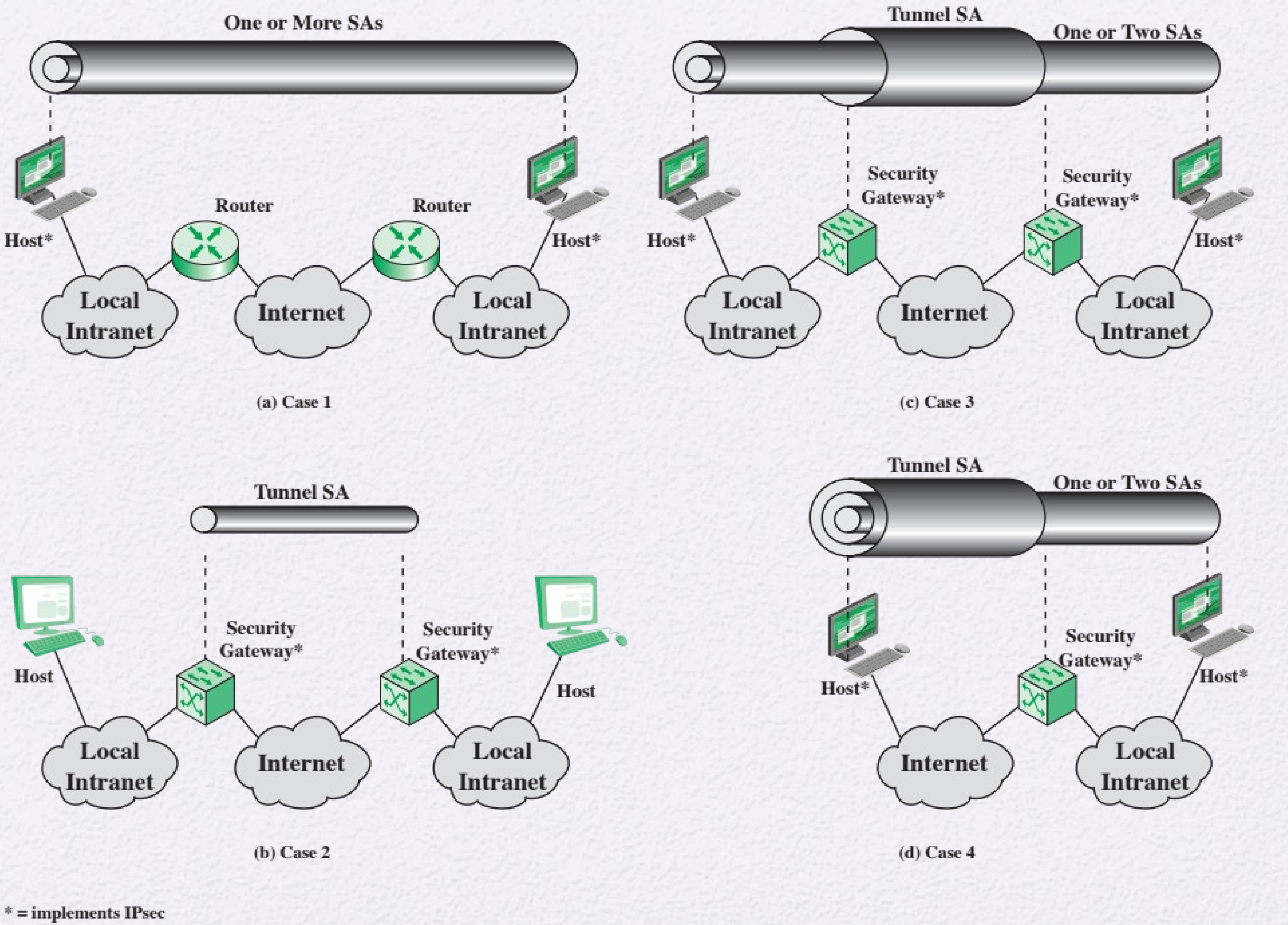
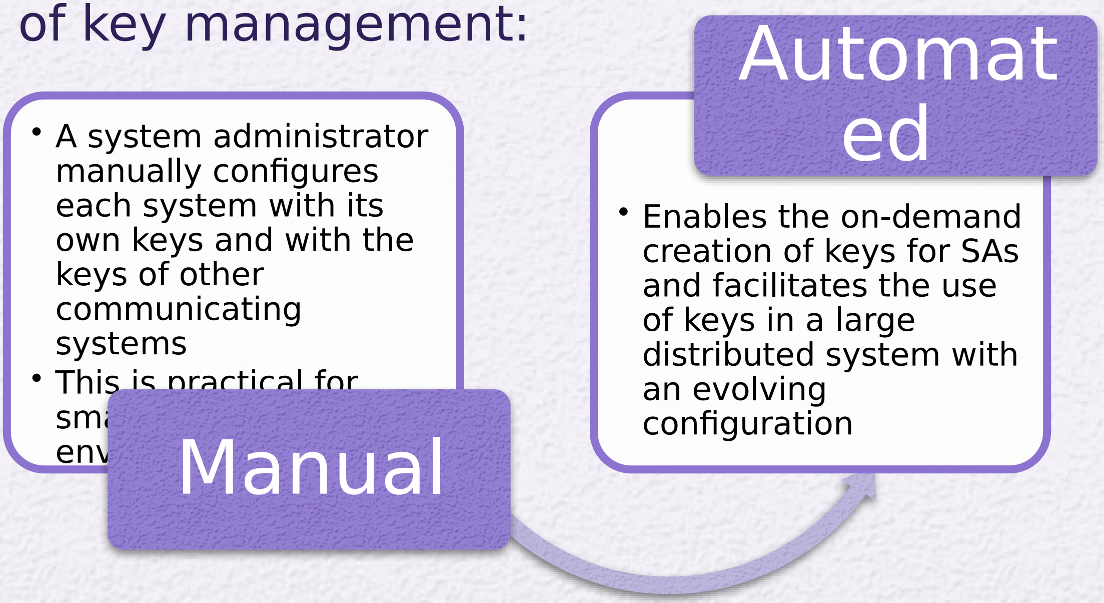


Figure 20.10 Basic Combinations of Security Associations

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 sma env

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

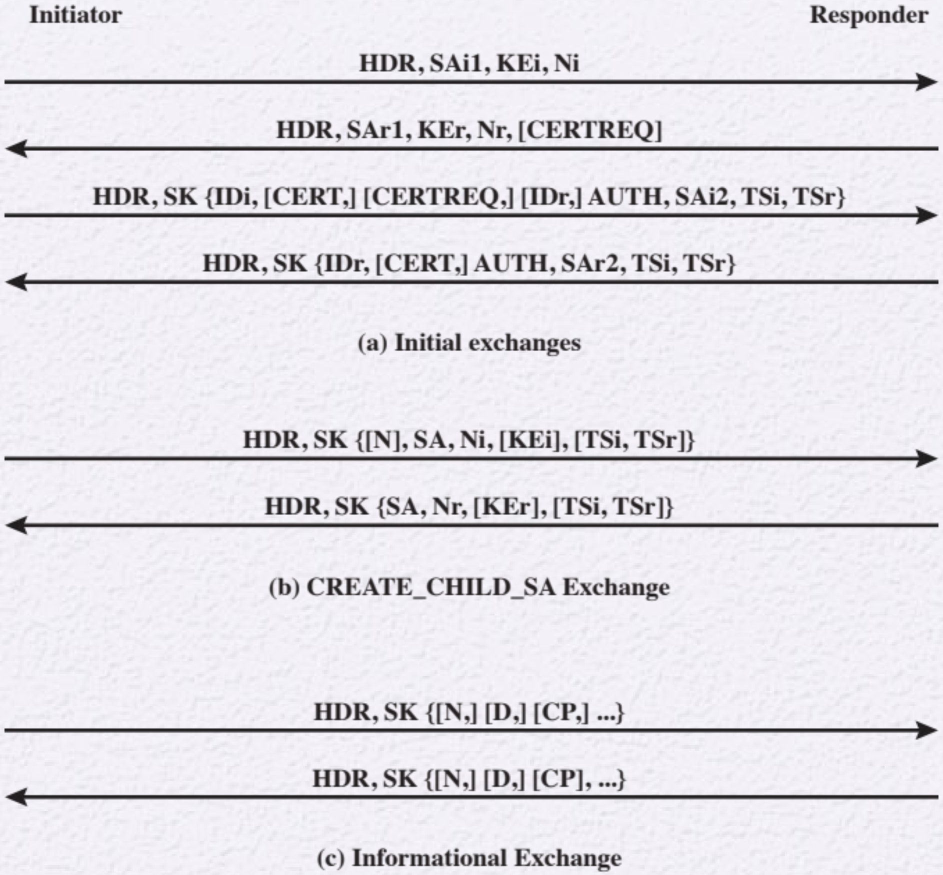
ISAKMP/Oakley

- 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,] ...}

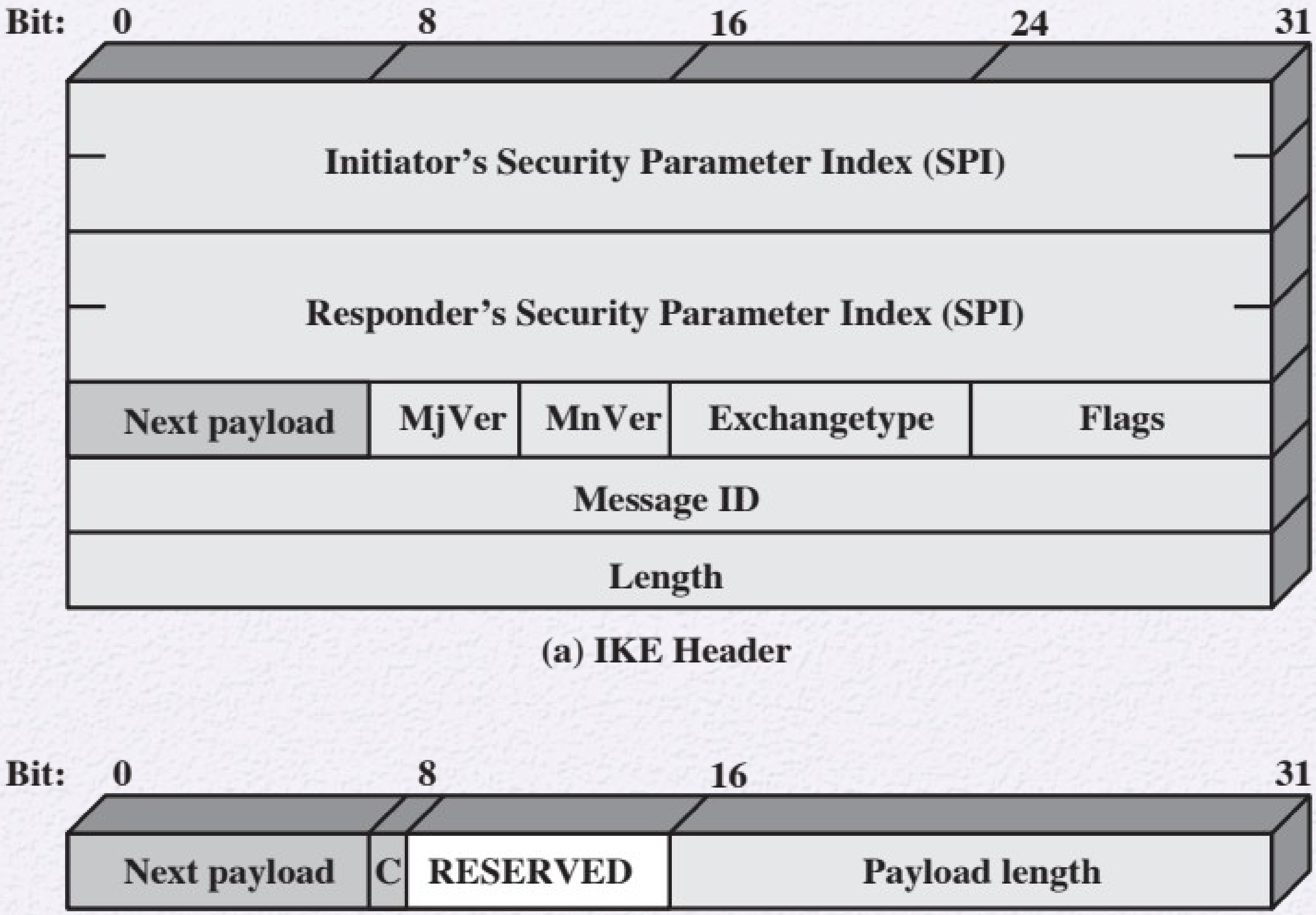
HDR, SK {[N,] [D,] [CP], ...}

(c) Informational Exchange

HDR = IKE header
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



Bit: 0 8 16 24 31

Initiator's Security Parameter Index (SPI)

Responder's Security Parameter Index (SPI)

Next payload | MjVer | MnVer | Exchangetype | Flags

Message ID

Length

(a) IKE Header

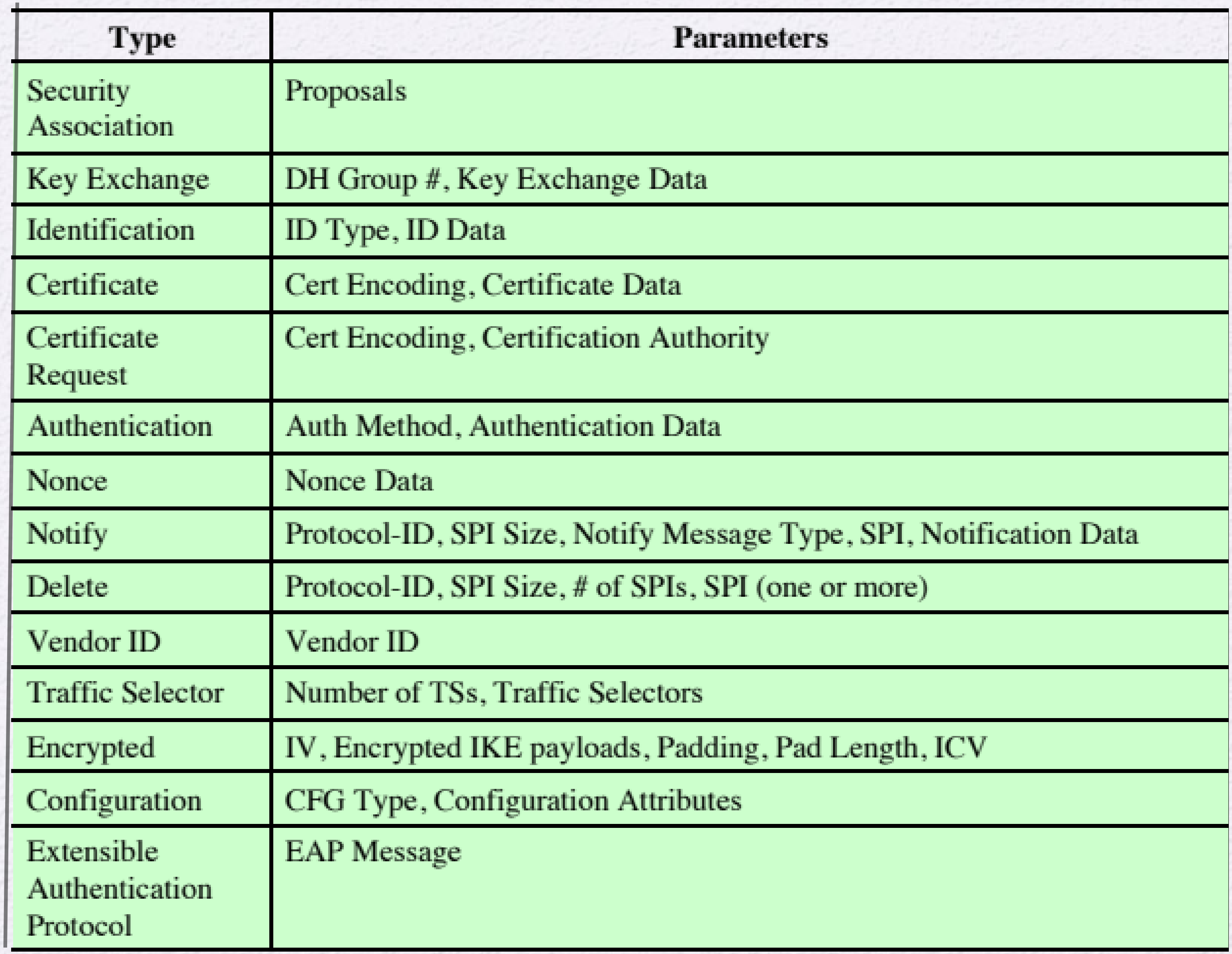
Bit: 0 8 16 31

Next payload | C | RESERVED | Payload length

(b) Generic Payload Header

Figure 20.12 IKE Formats

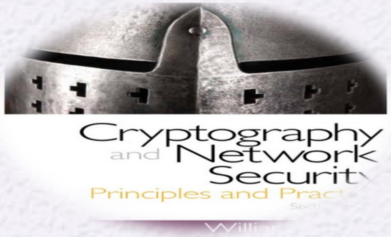
Table 20.3 IKE Payload Types



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

Summary

- Present an overview of IP security (IPsec)
- Explain the difference between transport mode and tunnel mode
- Understand the concept of security association
- Explain the difference between the security association database and the security policy database
- Present an overview of Encapsulating Security Payload



- Summarize the traffic processing functions performed by IPsec for out- bound packets and for inbound packets
- Discuss the alternatives for combining security associations
- Present an overview of Internet Key Exchange
- Summarize the alternative cryptographic suites approved for use with IPsec