Fundamentos de Segurança Informática

LEI

2025/2026

T8 – IP Security

Security approaches in the context of the TCP/IP stack

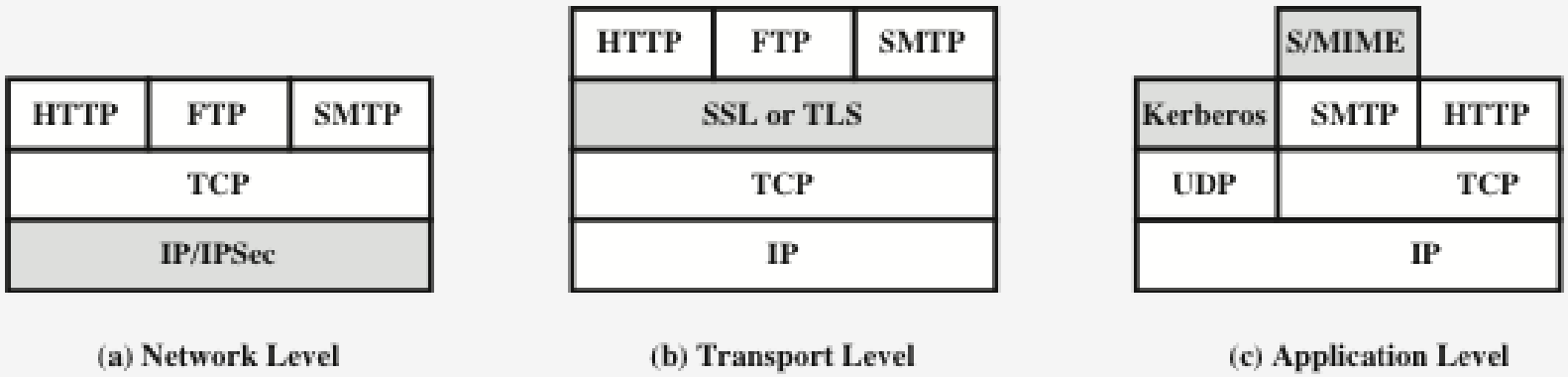


Figure 17.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

IP Security Overview

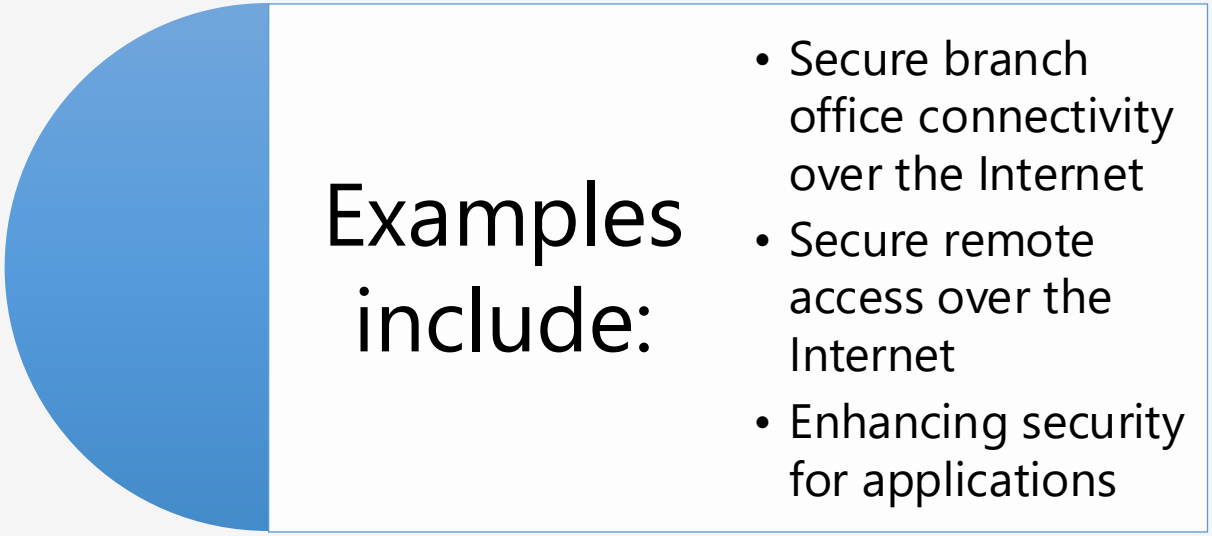
- Security at the IP (network) level provides transversal secure networking for applications

- IP-level security encompasses: authentication, confidentiality and key management

- "Security in the Internet Architecture", RFC 1636 (1994):
  - ✓ Identifies key areas for security mechanisms: secure the network infrastructure from unauthorized monitoring and control of network traffic, and secure end-user-to-end-user traffic using authentication and encryption mechanisms
  - ✓ Authentication and encryption as necessary security features in the next generation IP (IPv6)
  - ➢ **The IPsec (IP Security) 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



- Principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the **IP level (network layer)**

- All distributed applications (remote logon, client/server, e-mail, file transfer, web access, etc.) can benefit from **secure end-to-end communications**

A typical IPSec usage scenario

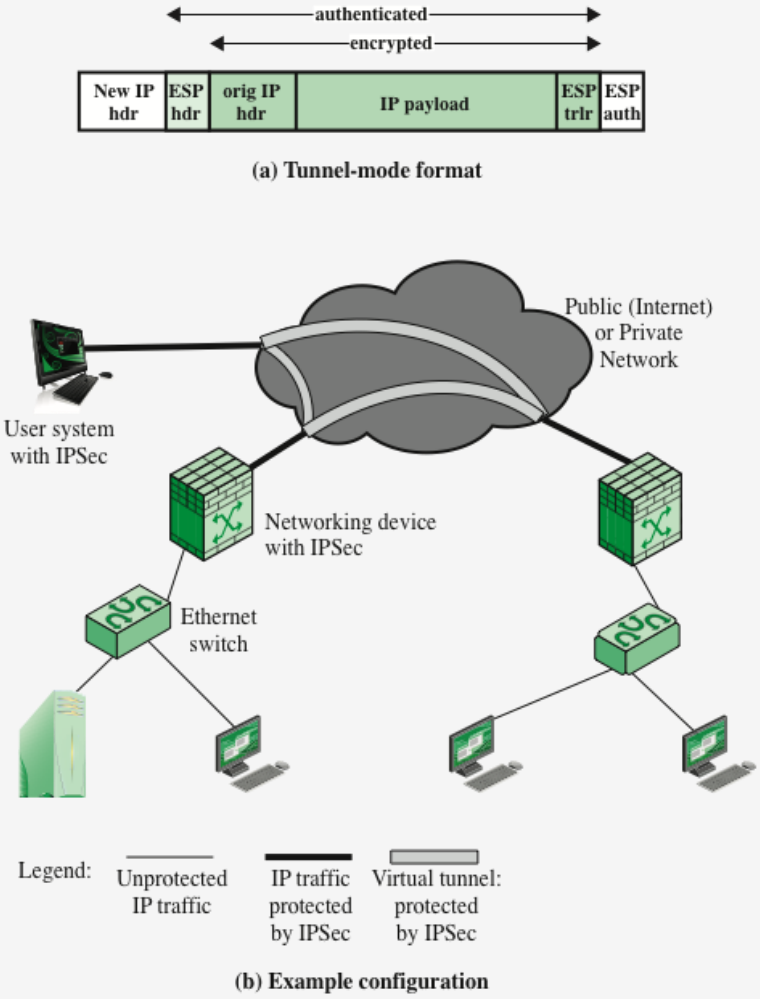
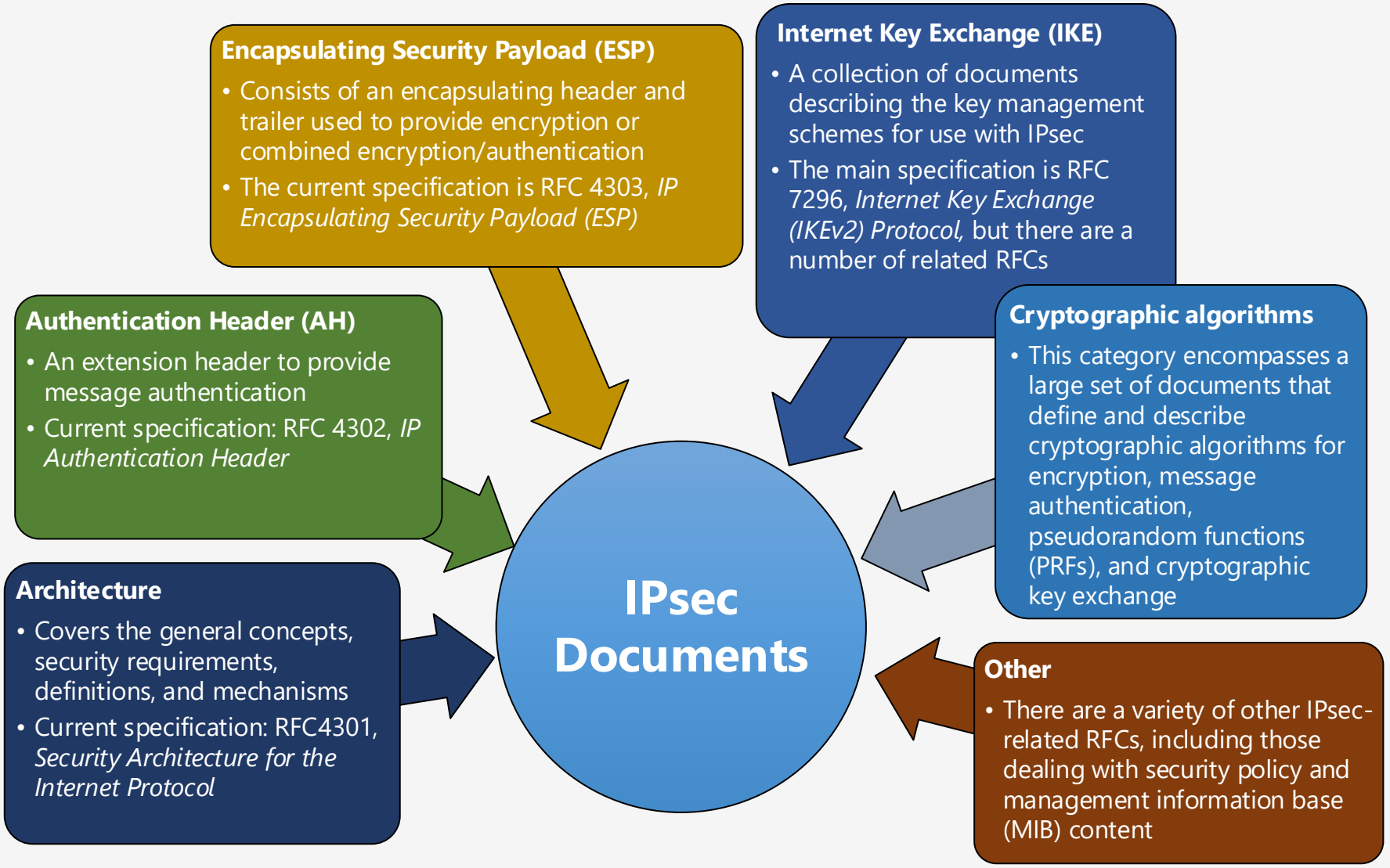


Figure 20.1 An IPSec VPN Scenario

Benefits of IPSec

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications
- IPsec can be transparent to end users
- IPsec can provide security for individual users if needed (e.g. road warrior VPN scenario)
- Can play a vital role in securing the routing architecture (routing protocols can run on top of security associations between routers established using IPSec)

IPSec Specifications



Transport and Tunnel Modes

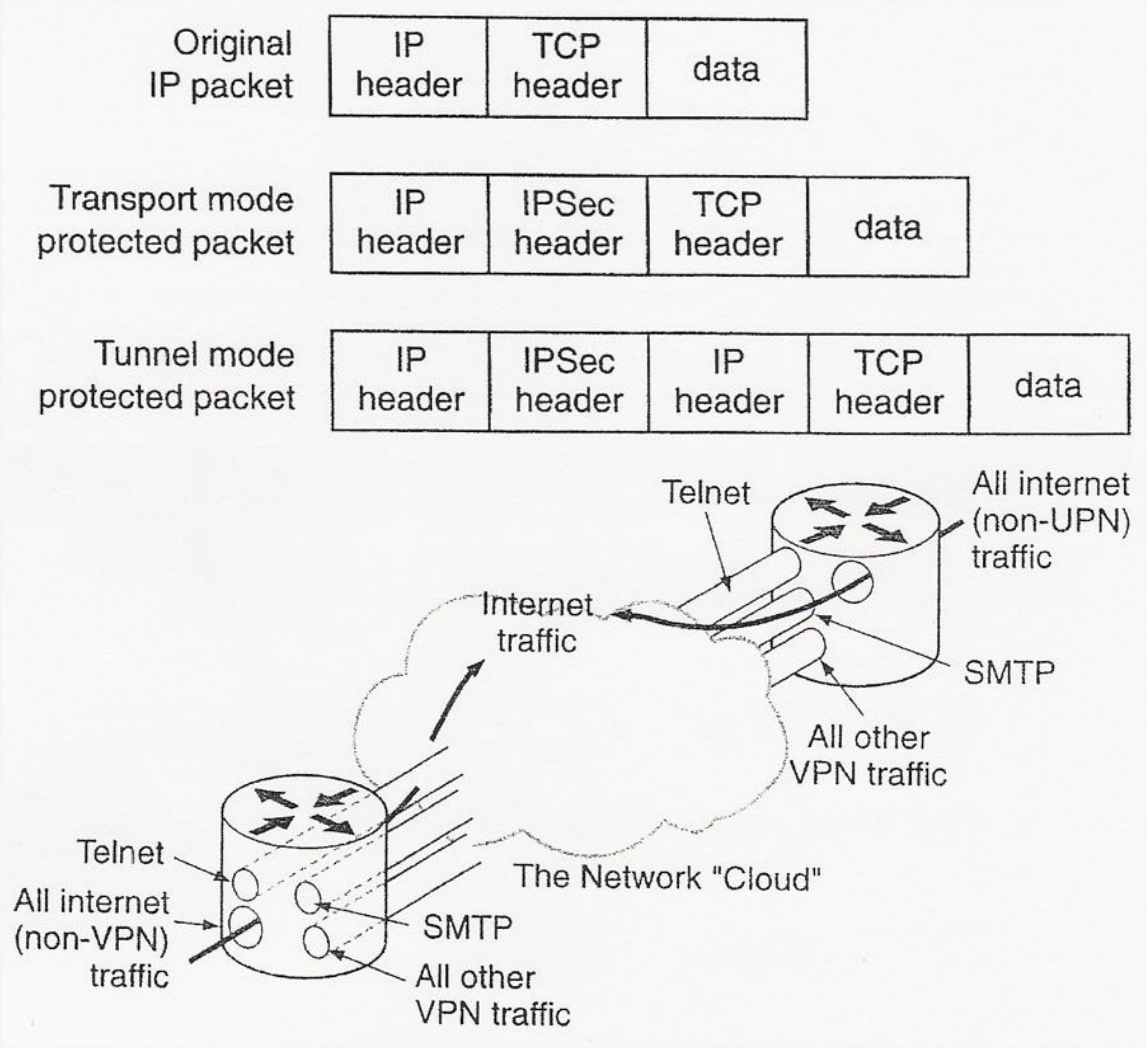
Transport Mode

- 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

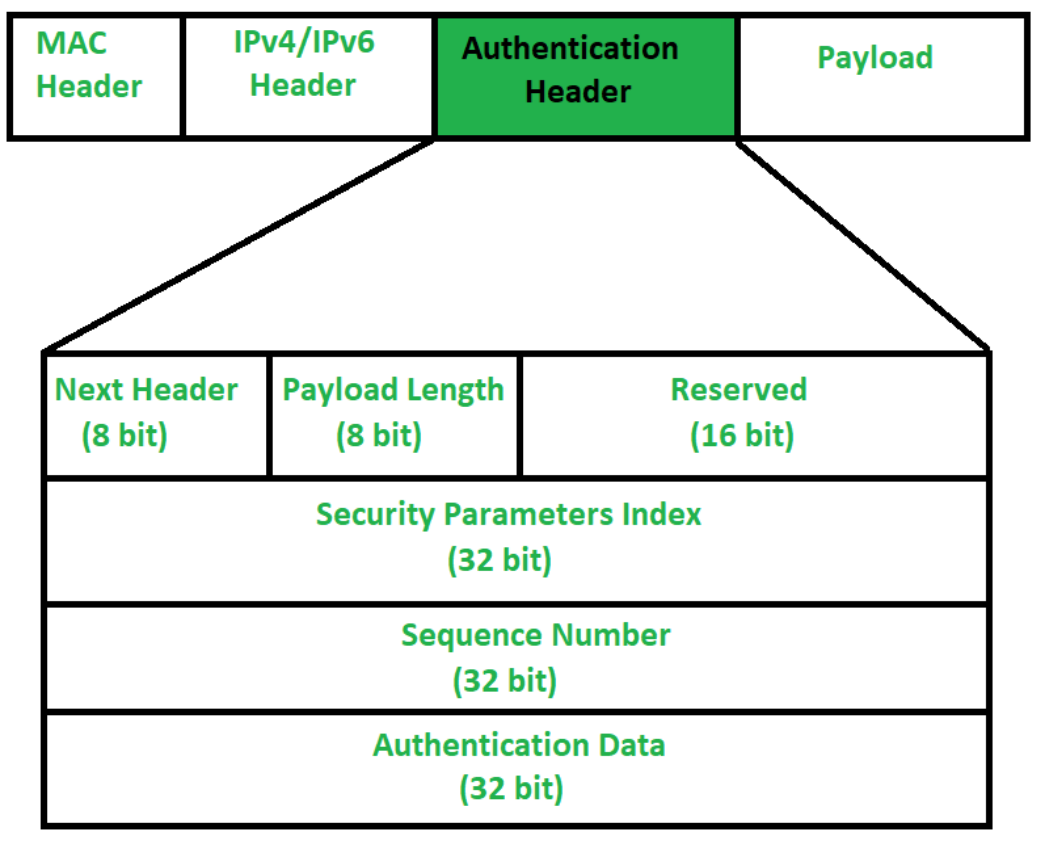
Transport and Tunnel Modes



AH (IP Authentication Header)

AH - IP Authentication Header

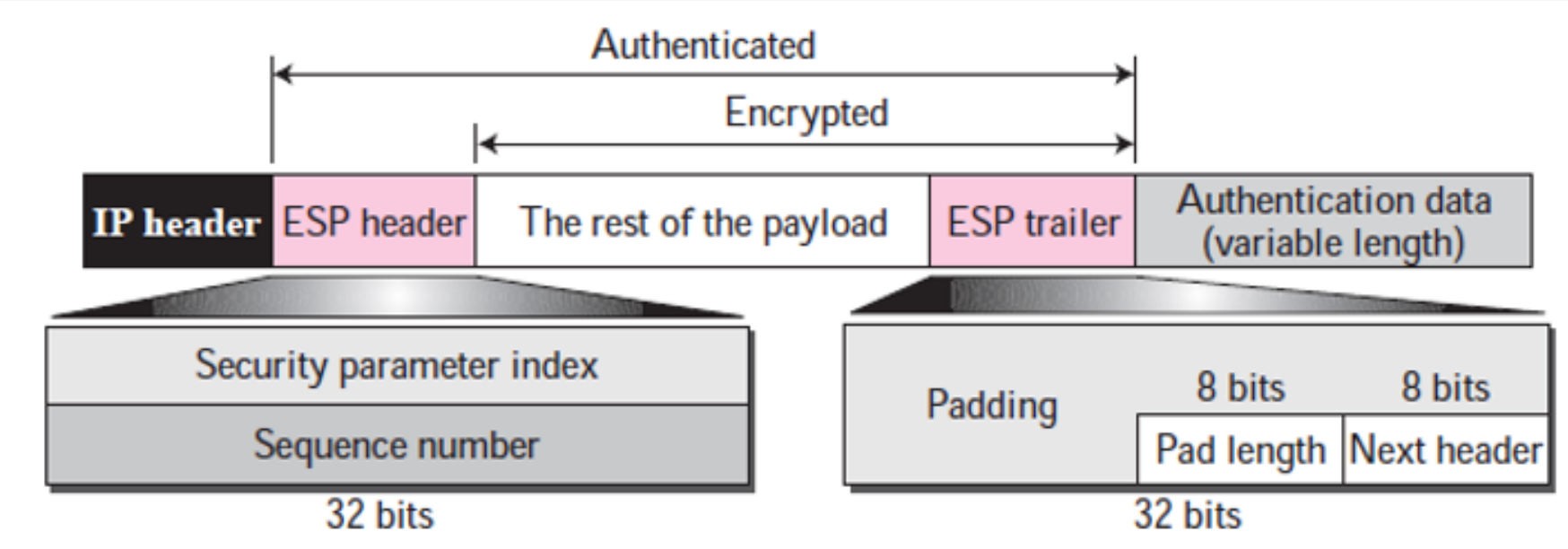
- Defined in RFC 2402
- Provides integrity for IP packets
- Provides authentication for IP packets
- Doesn't support confidentiality



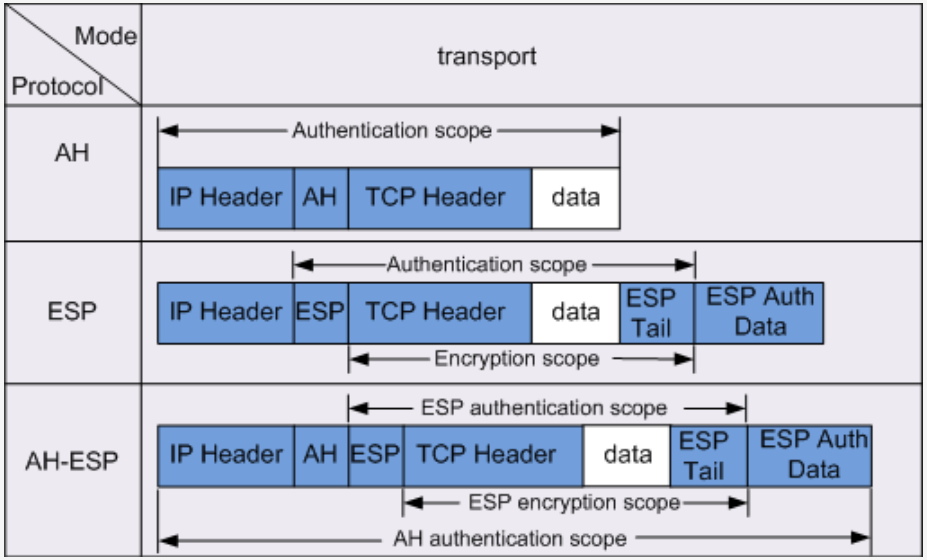
ESP (IP Encapsulated Security Payload)

ESP - IP Encapsulated Security Payload

- Defined in RFC 1827
- Provides integrity of IP packets
- Provides authentication of IP packets
- Provides confidentiality

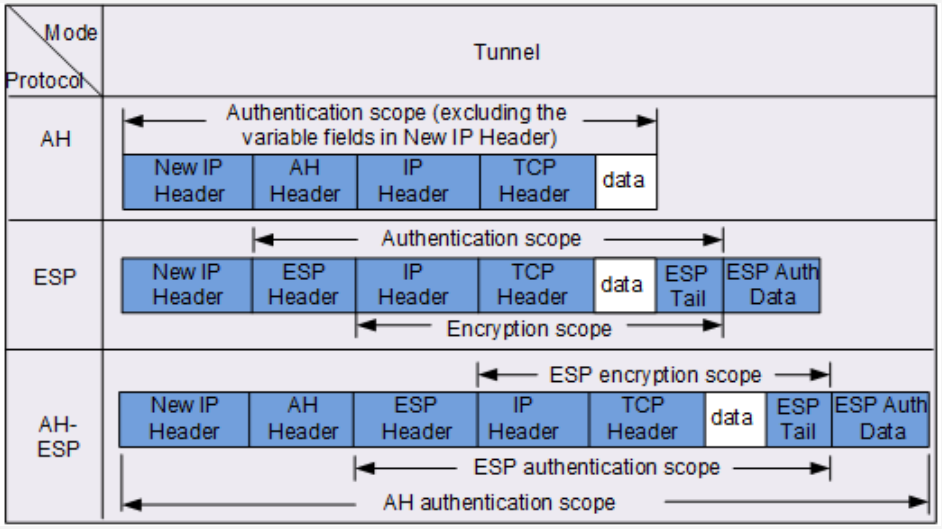


Transport and Tunnel Modes



Transport mode:

- AH verifies the entire IP packet during integrity verification, it fails if the contents of packet (payload or header) changes
- Thus, AH cannot coexist with NAT
- ESP does not authenticate the IP header, can coexist with NAT
- Typical in host-to-host direct communications



Tunnel mode:

- The original IP packet can be authenticated and encrypted completely, and the internal IP address, protocol type and ports are hidden
- Because of an extra IP header requires mode bandwidth
- Gateway-to-gateway communications, for net-to-net VPB tunnels

IPSec Architecture

- A **security policy** is applied to each IP packet that transits from a source to a destination
- An IPSec policy is determined by the interaction of two databases, the **SAD (Security Association Database)** and the **SPD (Security Policy Database)**

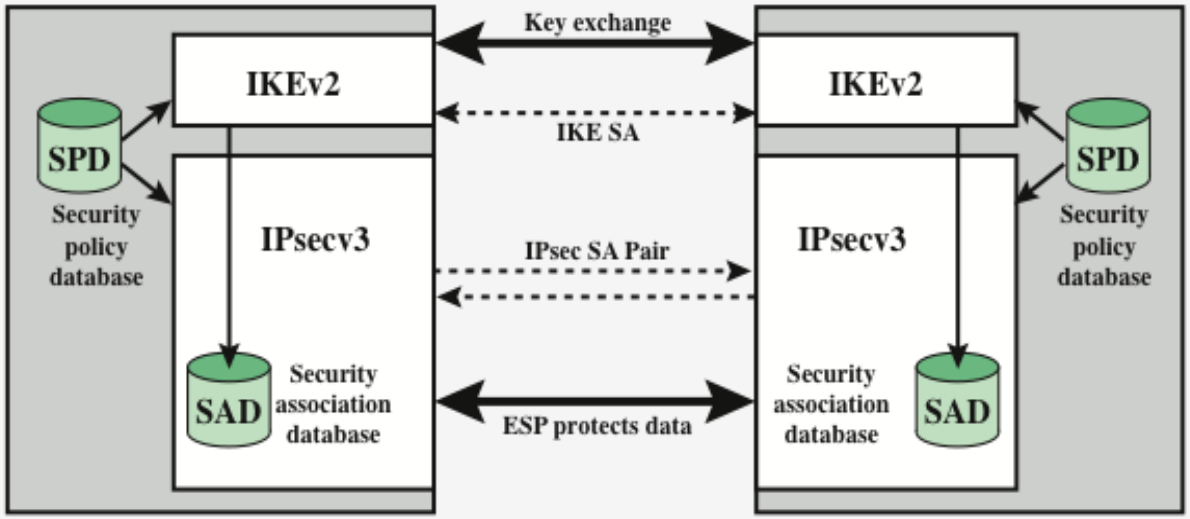
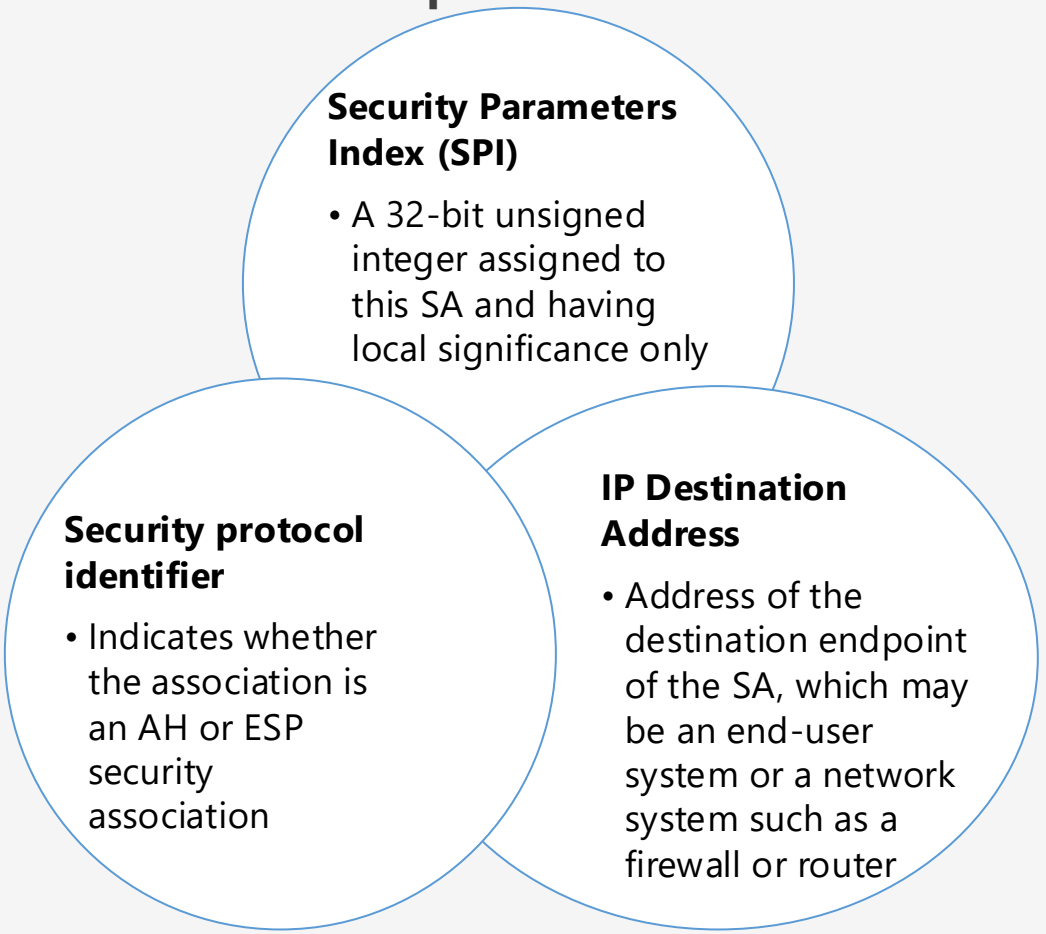


Figure 20.2 IPsec Architecture

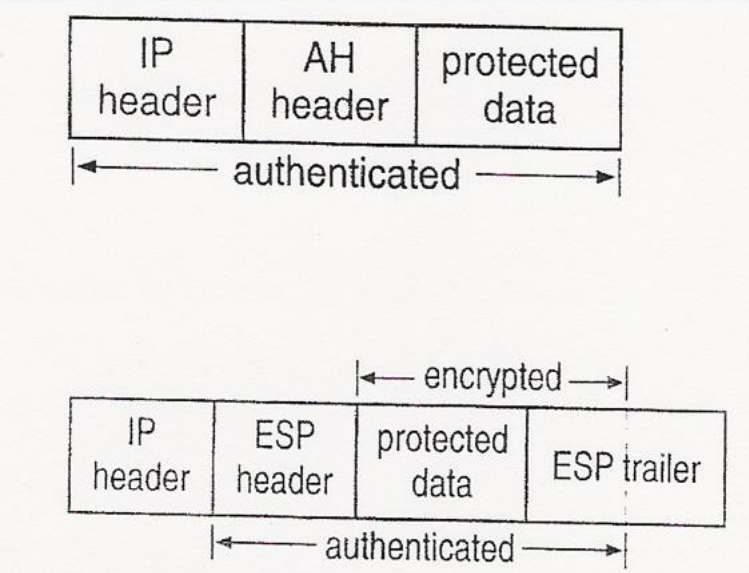
Security Association (SA)

- A one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it
- For a two-way secure exchange, two SA are needed
- 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)

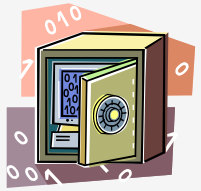
Uniquely identified by three parameters:



Security Association (SA)



Security Association Database (SAD)

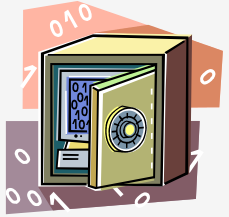


- Defines the parameters associated with each SA

- Normally defined by the following parameters in a SAD entry:
  - **Security parameter index**: uniquely identifies the SA
  - **Sequence number counter**: to generate sequence numbers for AH and ESP
  - **Sequence counter overflow**: a flag controlling whether overflow of the sequence number counter generates an event
  - **Anti-replay window**: used to determine whether inbound AH or ESP packet is a replay
  - **AH information**: authentication algorithms, keys, key lifetimes, etc.
  - **ESP information**: encryption and authentication algorithms, keys, IVs, key lifetimes, etc.
  - **Lifetime** of this security association: time interval or byte count to replace this SA with a new SA
  - **IPsec protocol mode**: tunnel, transport or wildcard
  - **Path MTU**: observed path maximum transmission unit

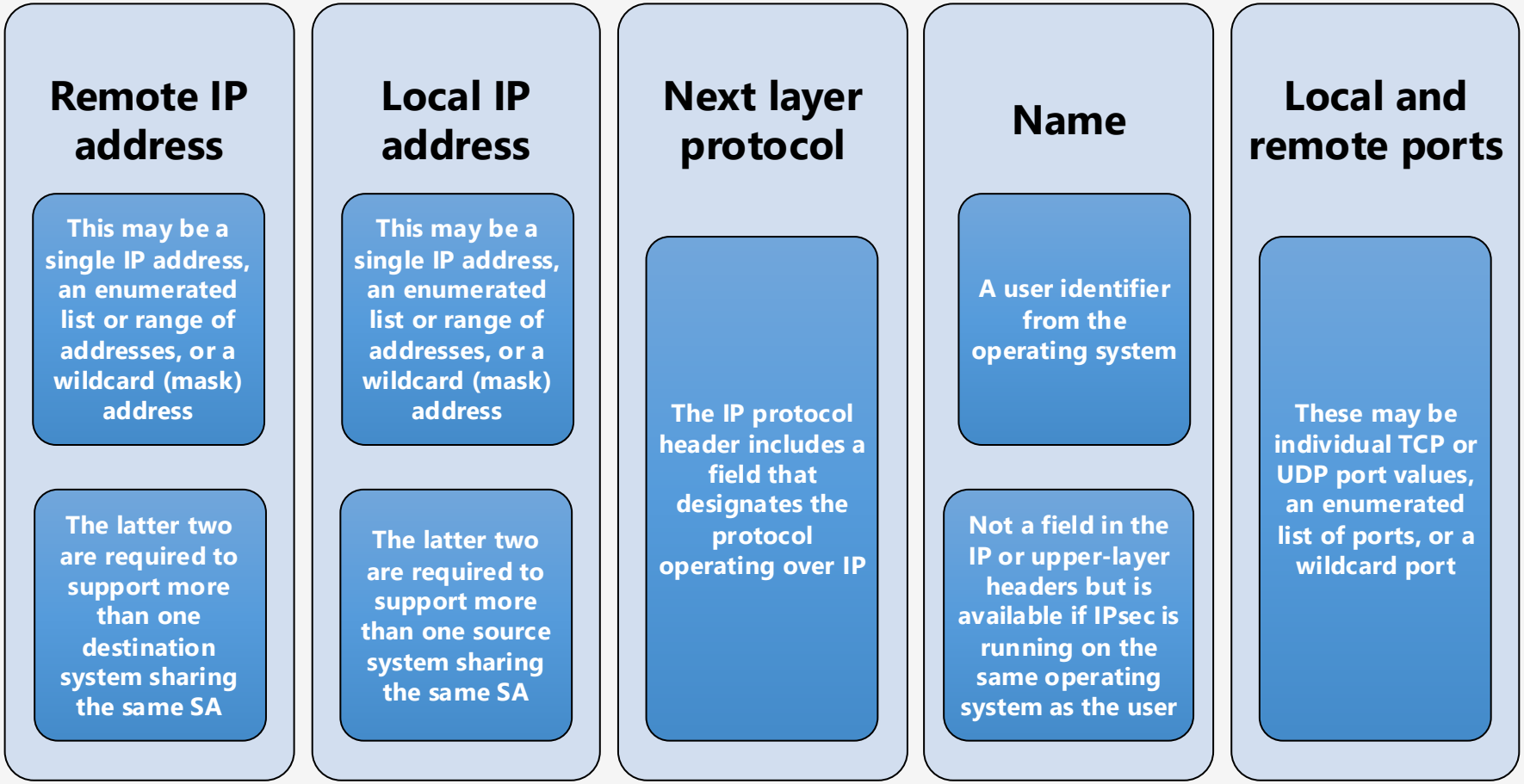
Security Policy Database (SPD)

- 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

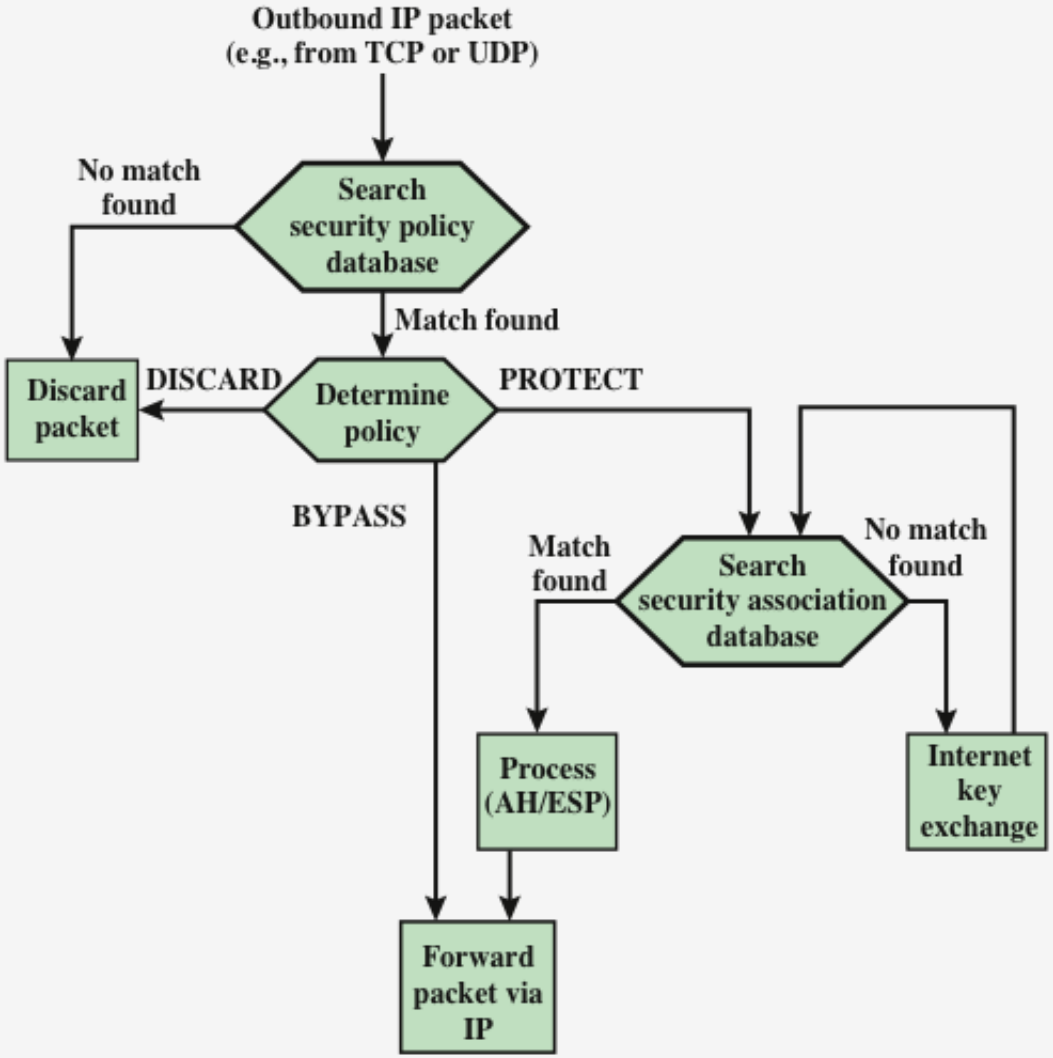
- The following selectors determine an **SPD entry**:



Example of SPD on a *host* system

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

Processing packets in IPSec: Outbound



Processing packets in IPSec: Inbound

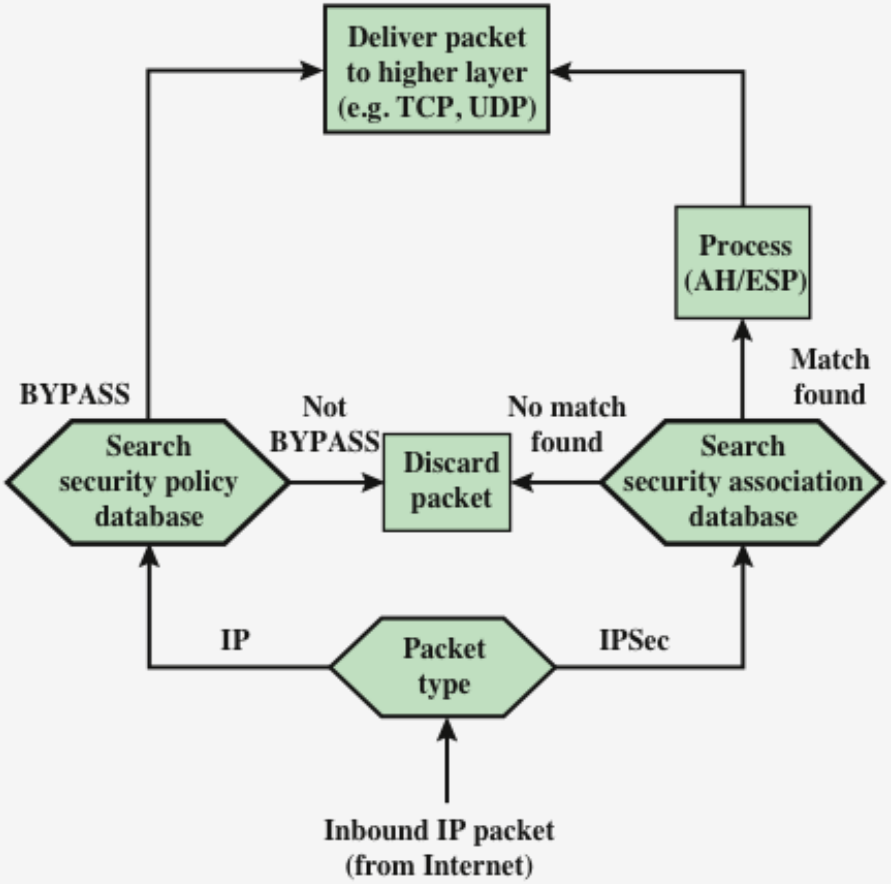


Figure 20.4 Processing Model for Inbound Packets

Anti-Replay Mechanism

- IP is a connectionless and unreliable service
- IPSec implements an anti-replay mechanisms using a window mechanism
- Packets received and to the left of the window or if not authenticated are discarded and an auditable event is generated

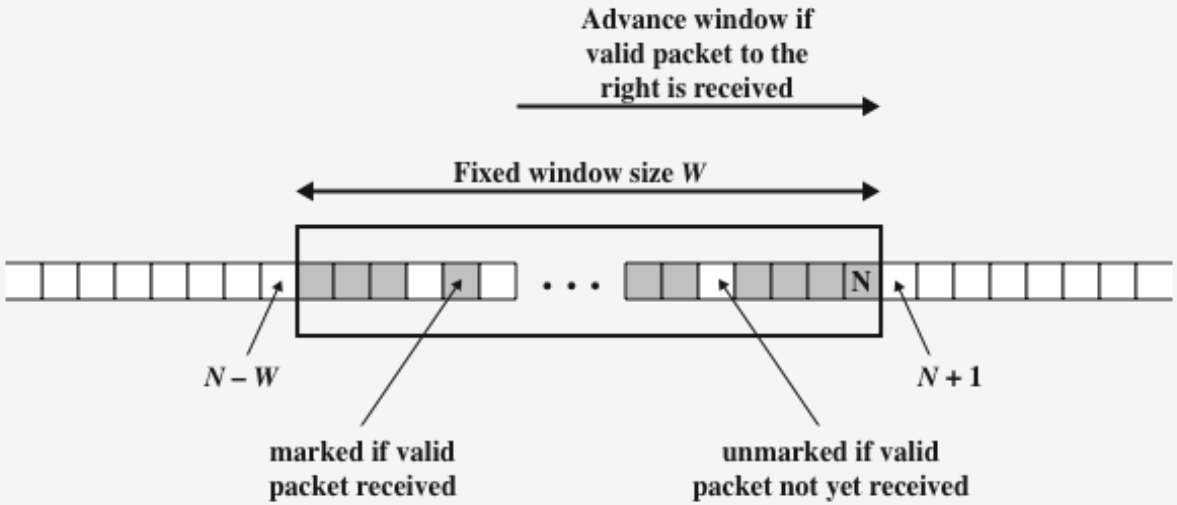


Figure 20.6 Anti-Replay Mechanism

Transport-Mode vs. Tunnel-Mode Encryption

- Transport-mode provides security directly between hosts
- Tunnel-mode supports Virtual Private Network (VPN) scenarios

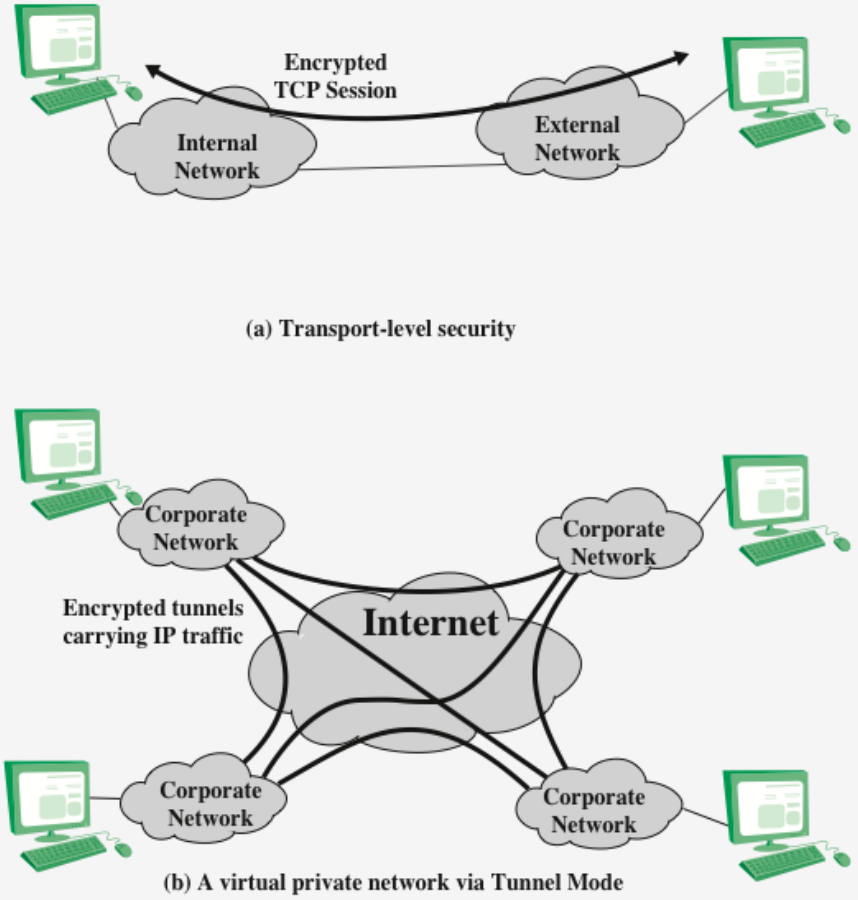
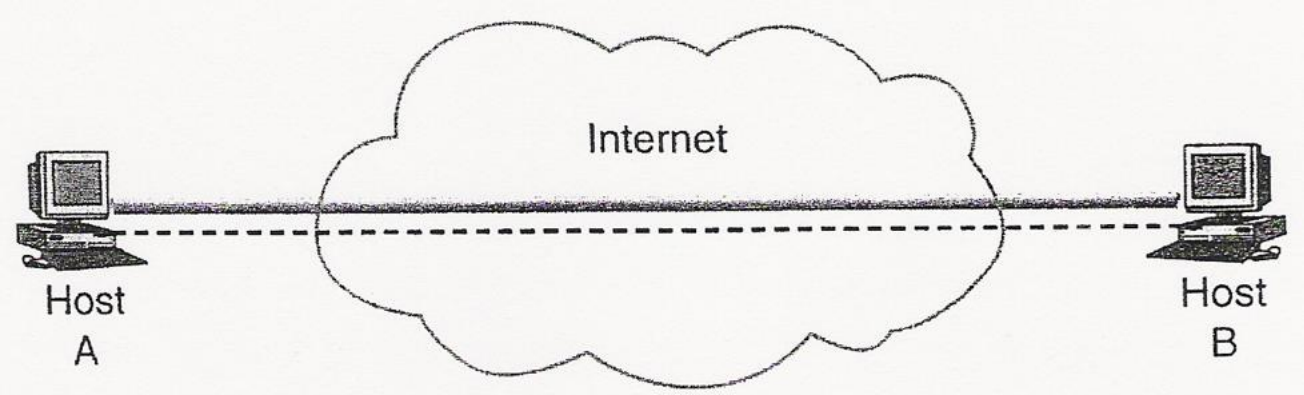
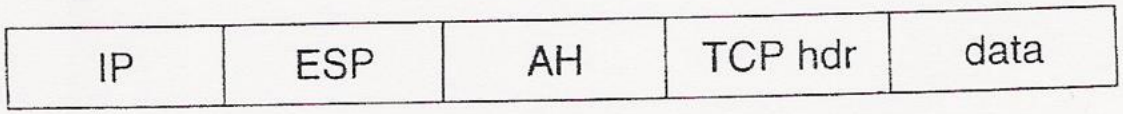


Figure 20.7 Transport-Mode vs. Tunnel-Mode Encryption

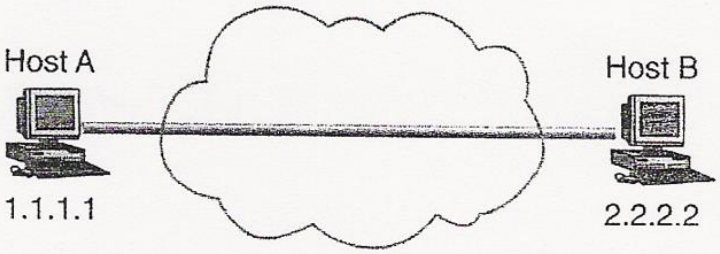
Transport-Mode





Packet format with ESP and AH

Transport-Mode (example)



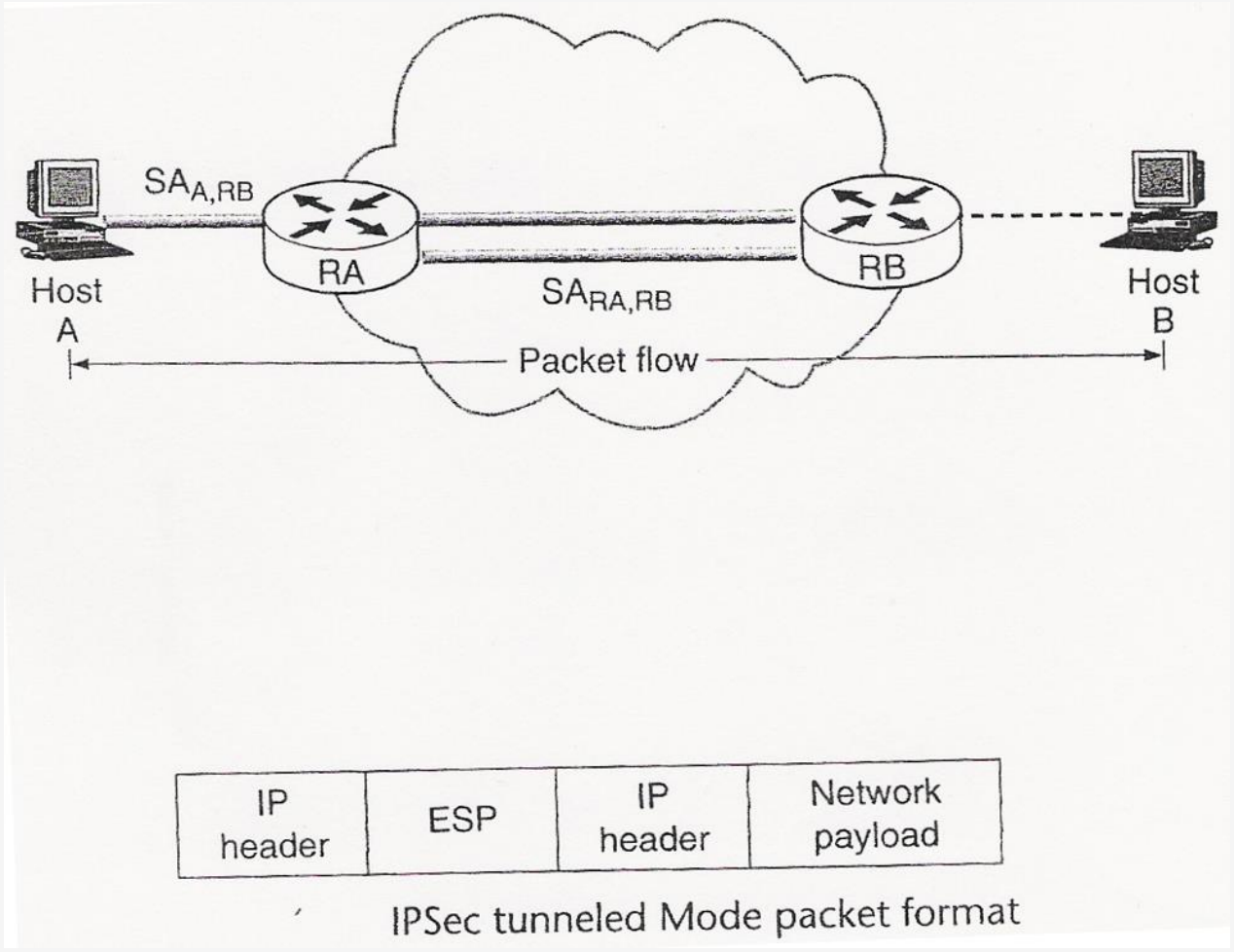
SPD

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	TCP	1000	ESP with 3 DES
1.1.1.1	2.2.2.2	*	*	ESP with DES

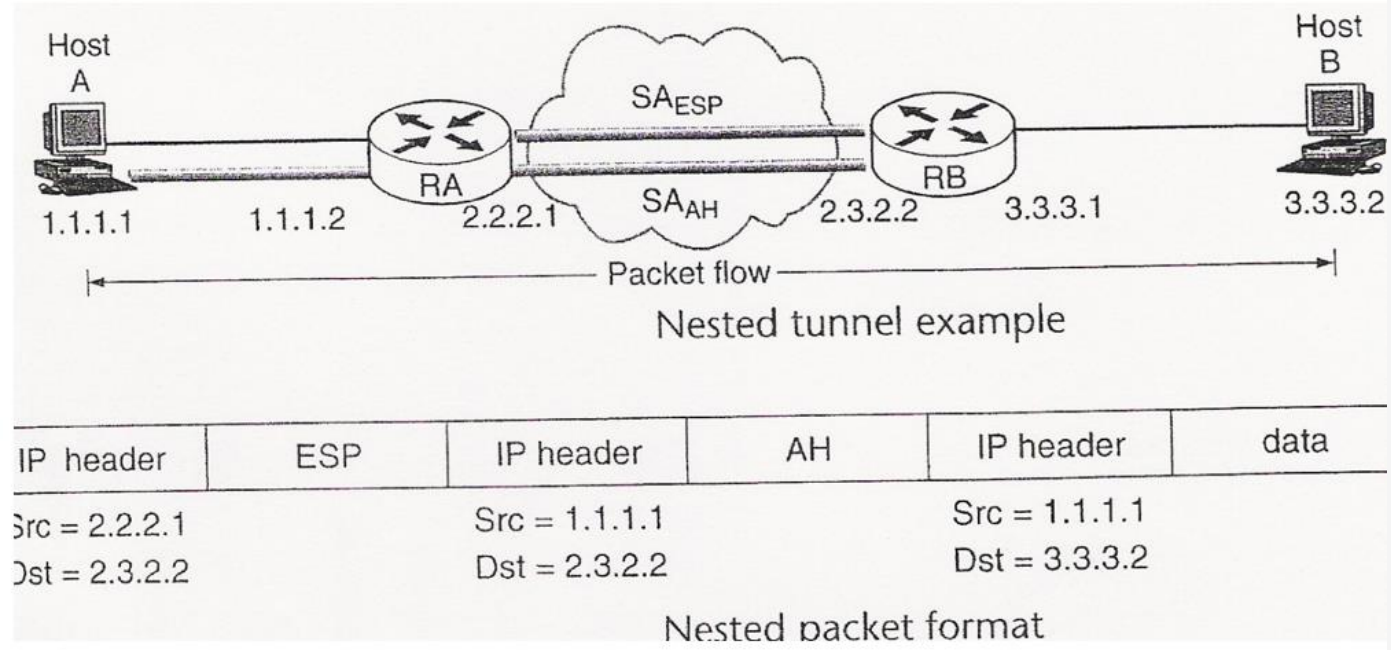
Inbound SADB

Src	Dst	Protocol	Spi	SA RECORD	
2.2.2.2	1.1.1.1	ESP	10	64 bit DES key	SA_2
2.2.2.2	1.1.1.1	ESP	11	168 bit 3 DES key	SA_1

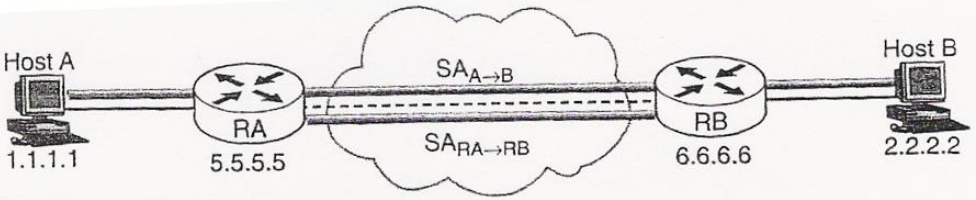
Tunnel-Mode



Tunnel-Mode (examples)



Tunnel-Mode (examples)



A's SPD

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	Any	Any	Transport AH with HMAC MD5

A's Outbound SADB

Src	Dst	Protocol	Spi	SA Record
1.1.1.1	2.2.2.2	AH	10	MD5 key

$SA_{A \rightarrow B}$

RA's SPD

From	To	Protocol	Port	Policy	Tunnel Dst
1.1.1/24	2.2.2/24	Any	Any	Tunnel ESP with 3DES	6.6.6.6

RA's Outbound SADB

Src	Dst	Protocol	Spi	SA Record
5.5.5.5	6.6.6.6	ESP tunnel	11	168 bit 3 DES key

$SA_{RA \rightarrow RB}$

Protocol architecture for ESP in tunnel and transport modes

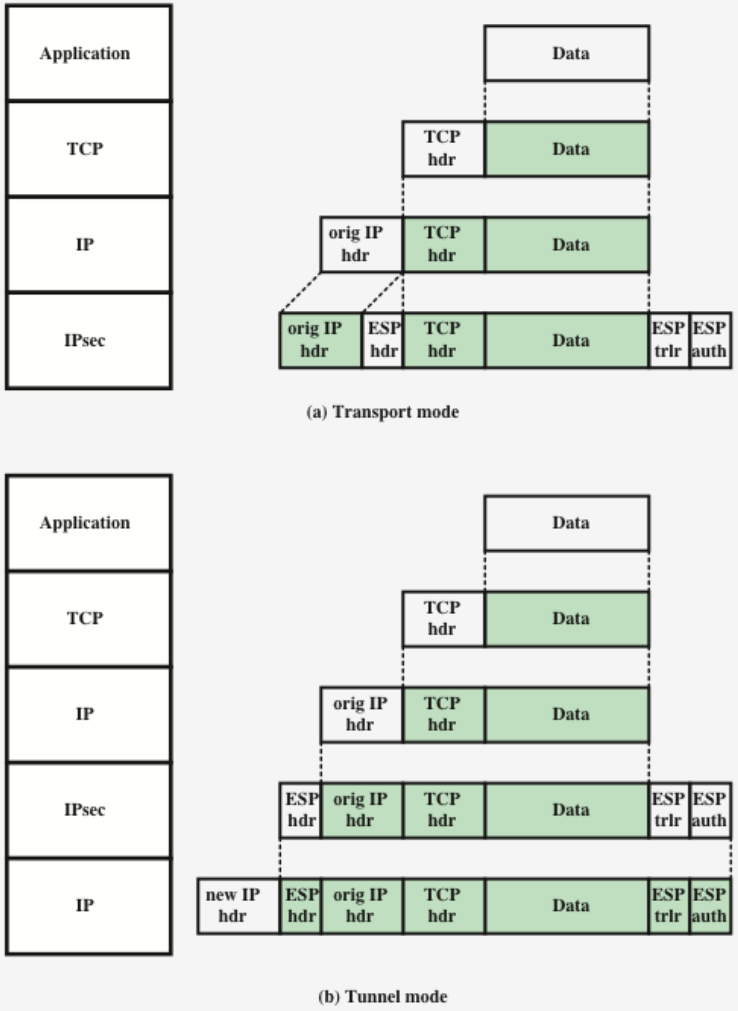


Figure 20.9 Protocol Operation for ESP

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

Combinations of Security Associations

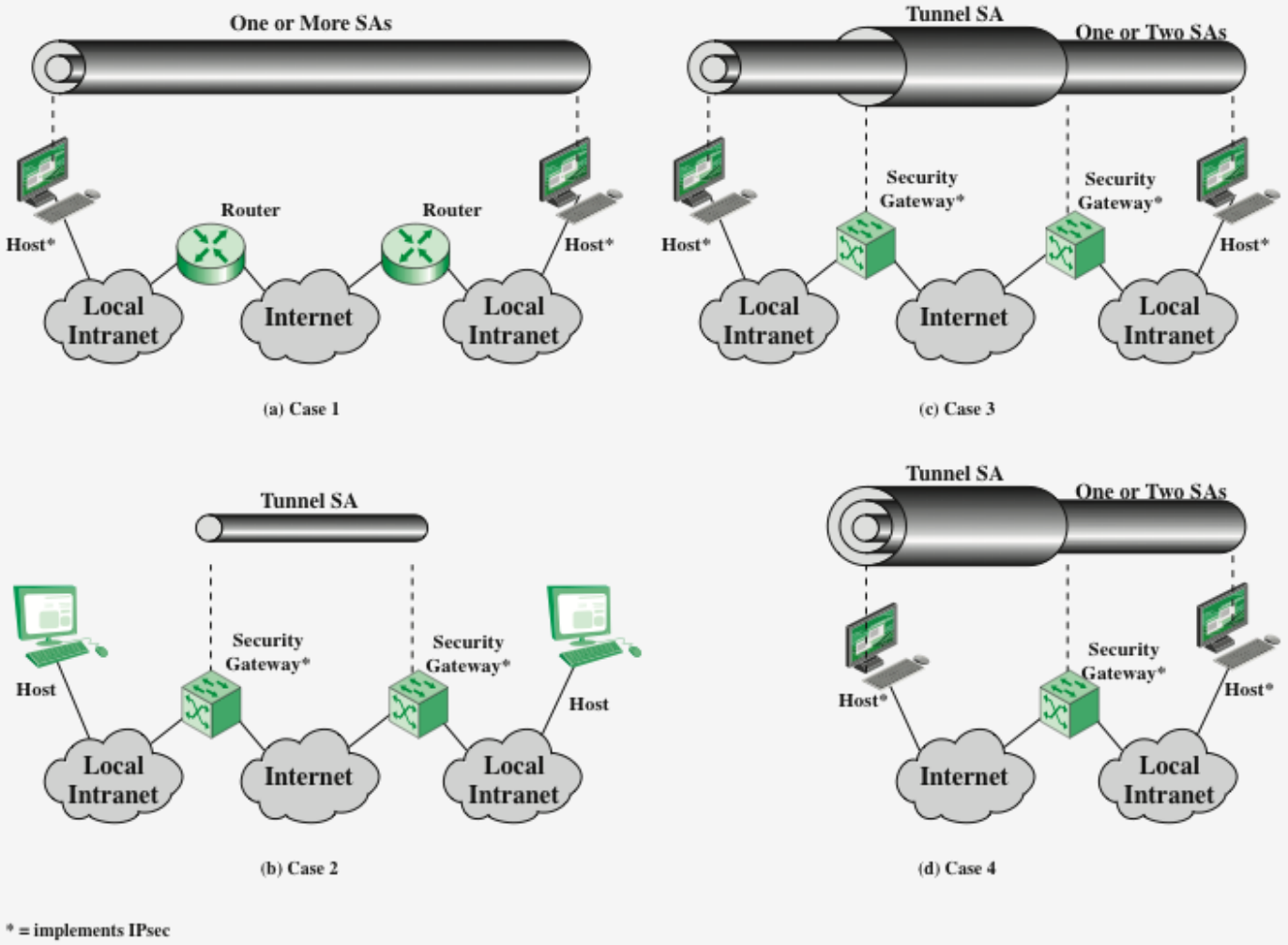
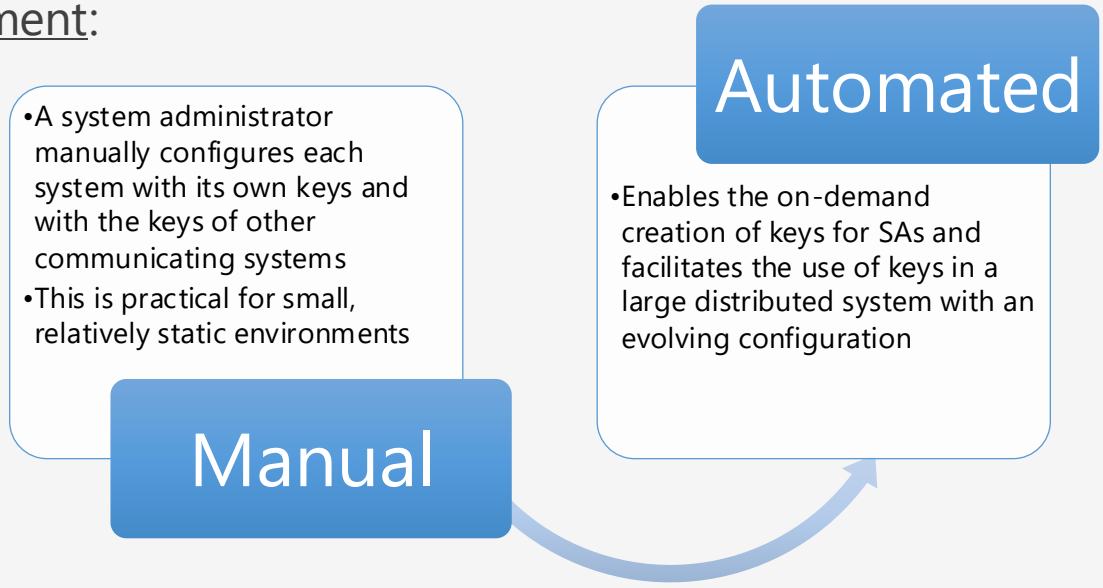


Figure 20.10 Basic Combinations of Security Associations

IKE (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:



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

Cryptographic Suites for IPSec

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

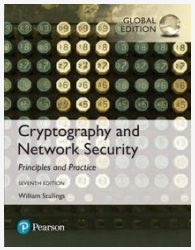
Summary

- 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
  - ✓ Anti-replay service
  - ✓ Transport and tunnel modes
- Combining security associations
  - ✓ Authentication plus confidentiality
  - ✓ Basic combinations of security associations
- Internet key exchange fundamentals

Bibliography

Cryptography and network security, Stallings, Pearson, 2017, Chapter 20: IP Security



Segurança em Redes Informáticas, André Zúquete, FCA, Capítulo 8: Redes Privadas Virtuais (VPN)