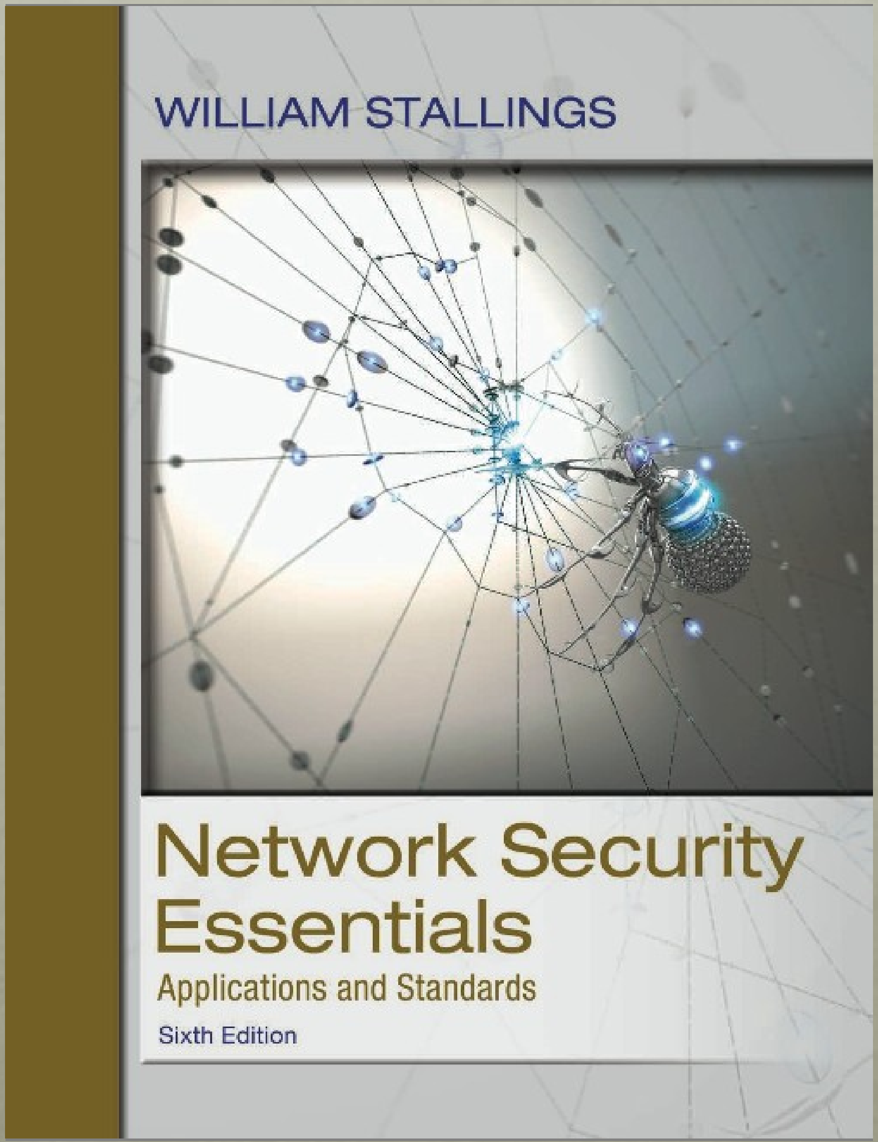
Network Security Essentials

Sixth Edition

by William Stallings



Chapter 9

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

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

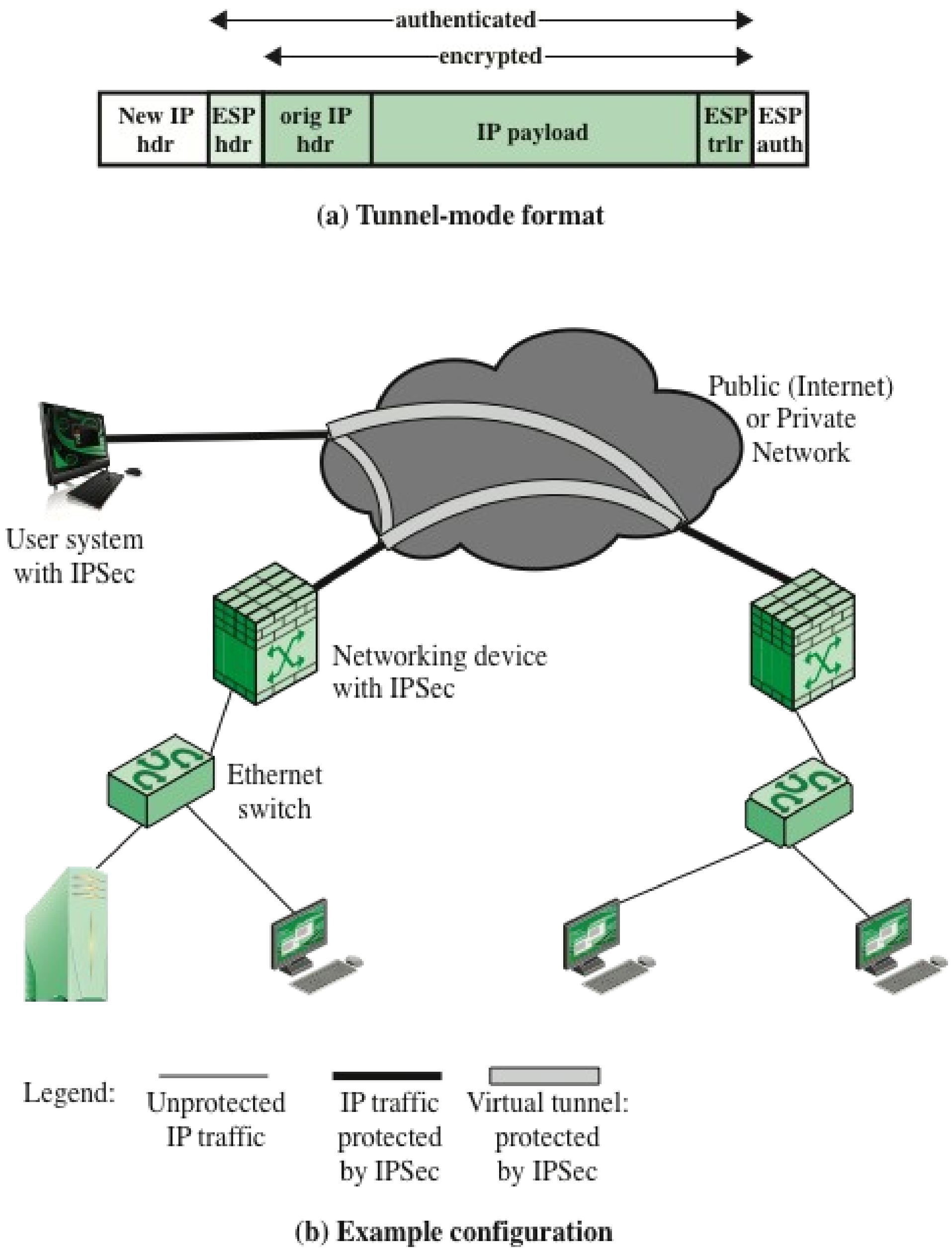
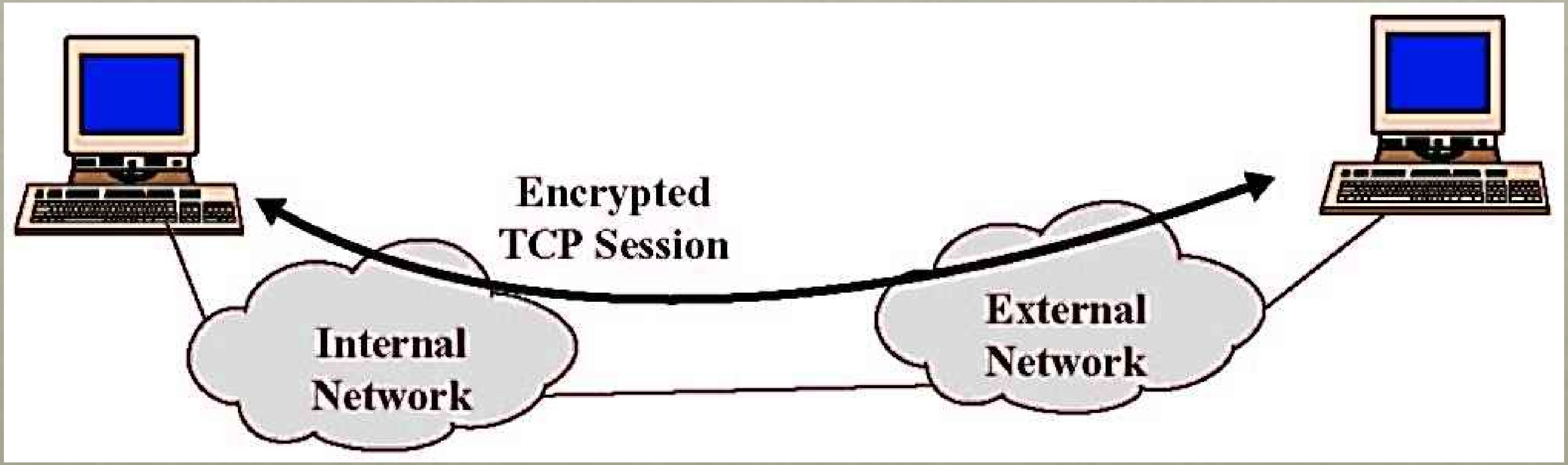


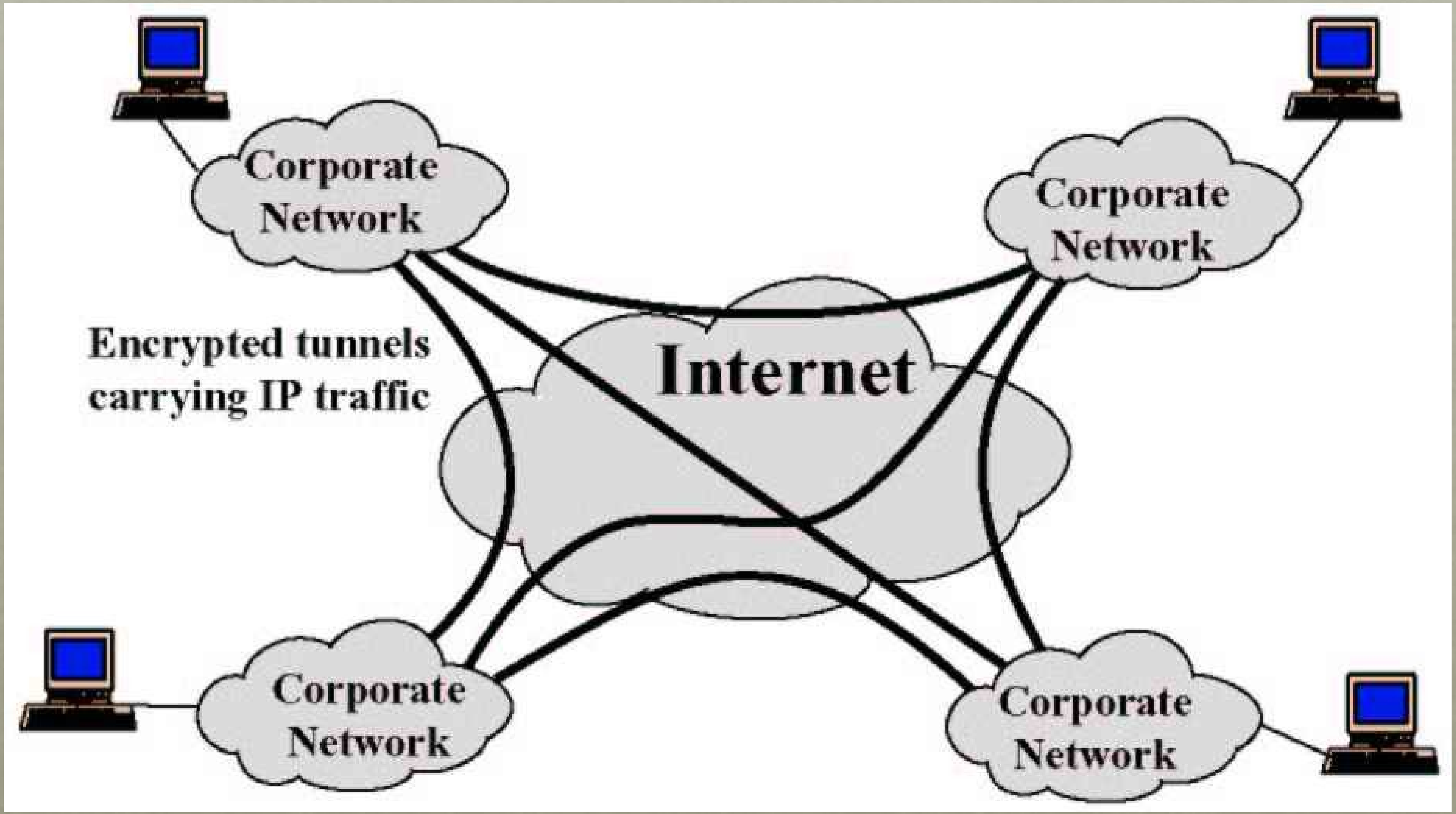
Figure 9.1 An IPSec VPN Scenario

ESP in modalità trasporto



VPN punto-punto – IPSec sui due punti

ESP in modalità tunnel



VPN fra i router/firewall (intermediari) delle varie reti aziendali

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

IPsec Documents

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 there are a number of related RFCs

Authentication Header (AH)

- An nsion ader to p id essa a enti on
- Th urren ification is R
Authentication Header

Cryptographic algorithms

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

Architecture

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

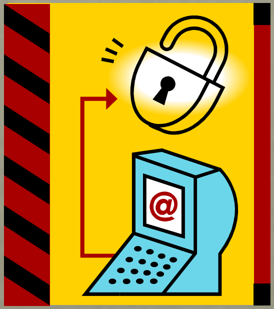
Other

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

IPsec Services (more on this)

- 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 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.

Quali strumenti usa IPsec

Sicurezza ➡ segretezza, autenticazione, integrità

Per garantirle si serve di tre protocolli:

- **Authentication Header** (AH) → integrità e autenticazione dell’origine dei dati
- **Encapsulating Security Payload** (ESP) → criptazione, segretezza e opzionalmente integrità e autenticazione
- **Internet Key Exchange** (IKE) → scambio delle chiavi

e di tre strutture:

1. **Security Policy Database** (SPD) al cui interno vanno elencate le regole di sicurezza relative al flusso di dati IP (out o in)
2. **Security Association Database** (SAD) che memorizza tutte le connessioni stipulate con altre macchine
3. **Security Association** (SA) connessione orientata e univocamente determinata da IPdestinazione – parametro – ID tipo protocollo sicuro.

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

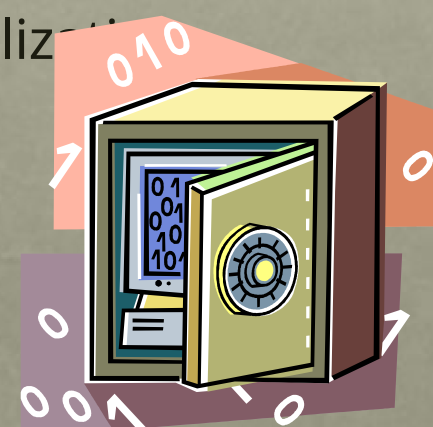
- Indicates whether the association is an AH or ESP security association

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/ESP information (enc/auth alg, keys, Initializ values, lifetime)
  - Lifetime of this security association
  - IPsec protocol mode (tunnel/transport)
  - 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 9.2
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

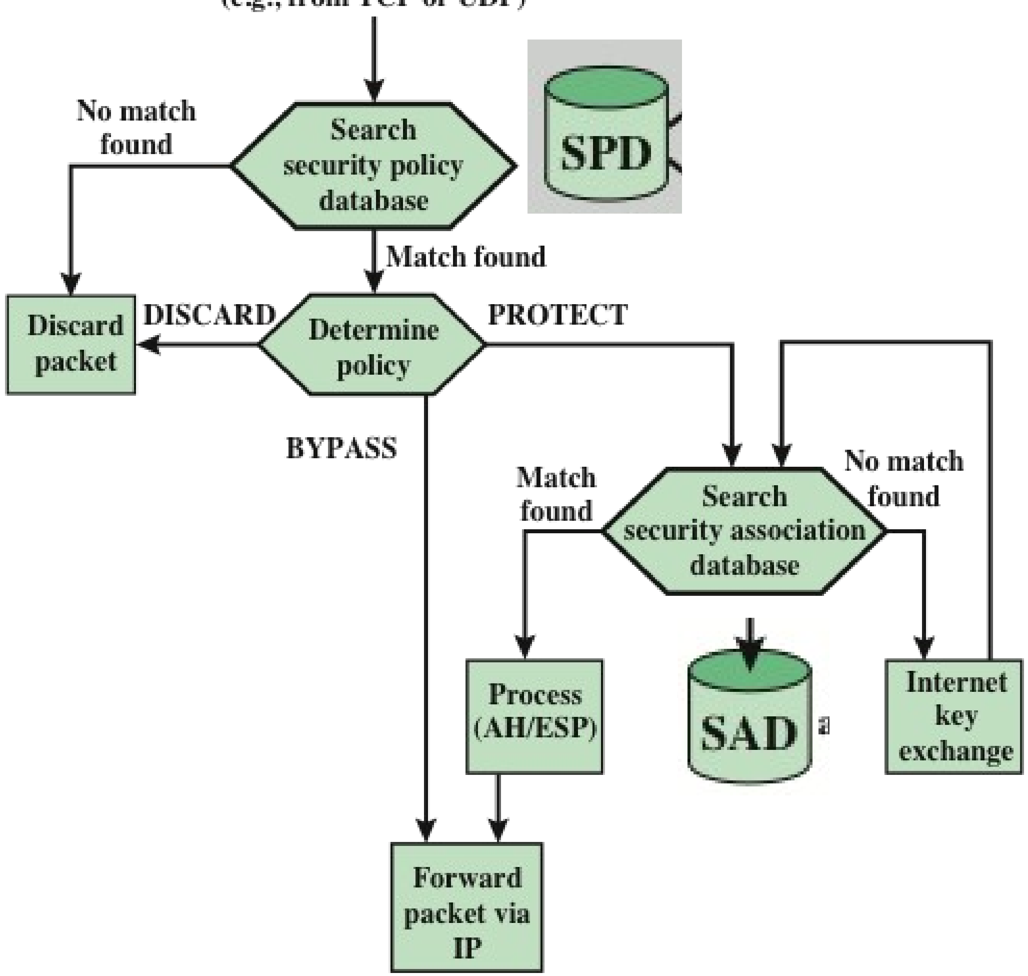


Figure 9.3 Processing Model for Outbound Packets

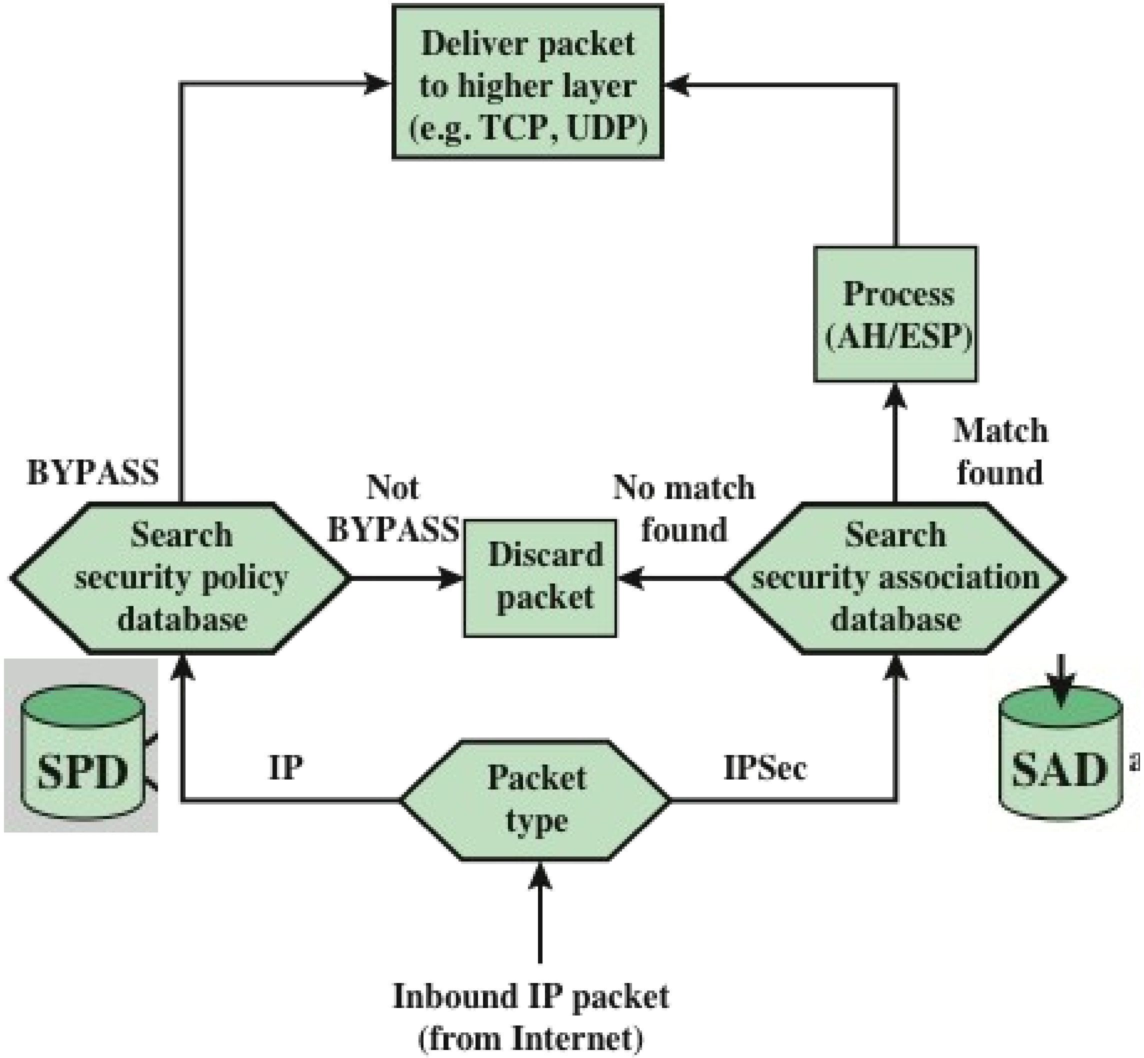
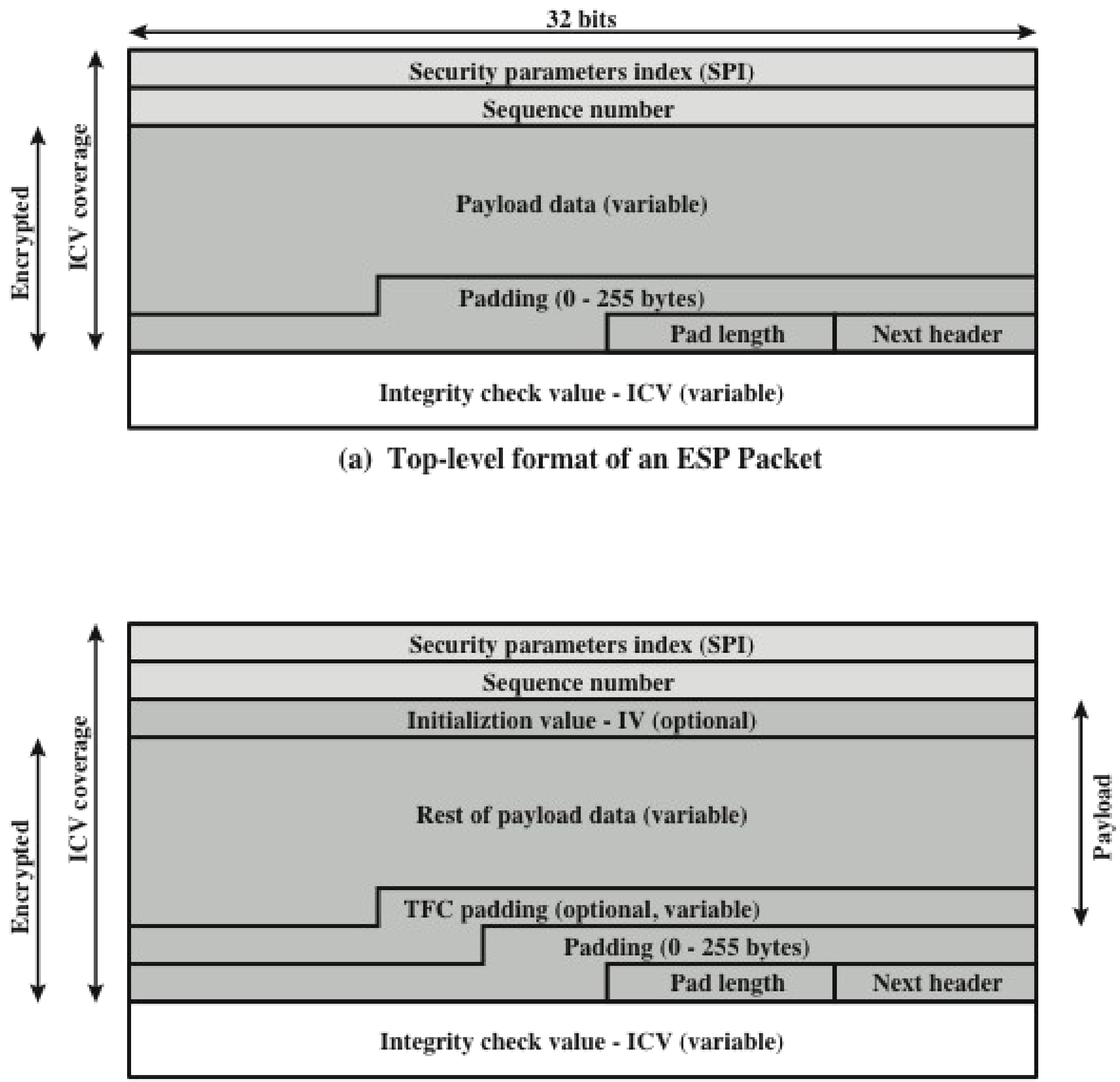


Figure 9.4 Processing Model for Inbound Packets

ESP

- Confidentiality
- Data origin authentication
- Connection-less integrity
- Anty-replay service (partial sequence integrity)
- Traffic flow confidentiality



(a) Top-level format of an ESP Packet

(b) Substructure of payload data

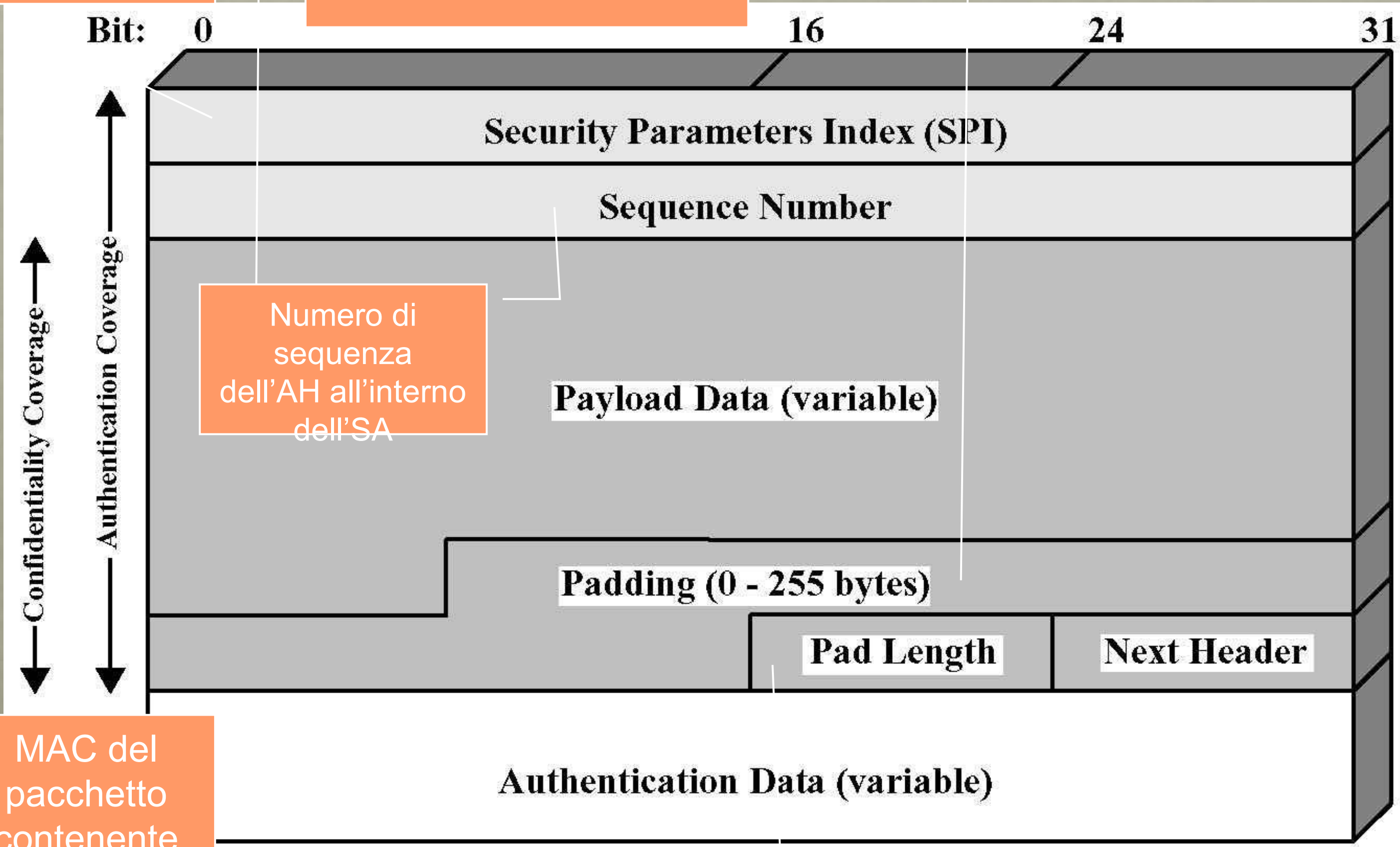
Figure 9.5 ESP Packet Format

ESP – formato

Parte dell'SA: serve a selezionare l'SA in un SAD

Codifica dei dati del pacchetto (trasporto) o dell'intero pacchetto (tunnel)

Padding (riempimento) necessario per certi tipi di crypto



Numero di sequenza dell'AH all'interno dell'SA

Header ESP

Trailer ESP

Authenticator ESP

MAC del pacchetto contenente questo AH

Lunghezza del padding

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

Prevenzione dei replay attack

- I pacchetti, anche se autenticati, non possono essere replicati grazie al campo Sequence Number dell'ESP
- Il mittente inserisce da 0 a 2^{32}-1
- Se ha bisogno di altri pacchetti, deve negoziare una nuova SA
- Il ricevente deve scartare i pacchetti
  - vecchi o ripetuti o falsificati

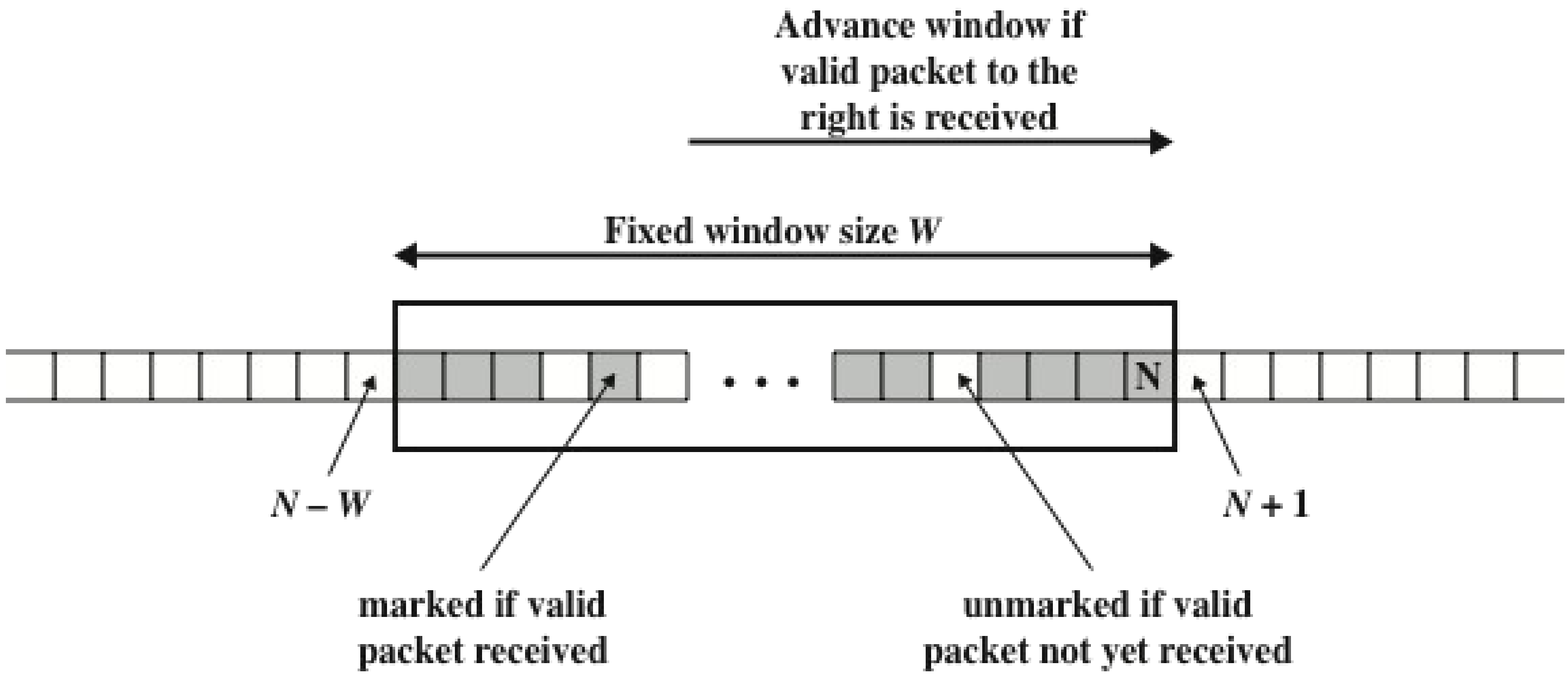
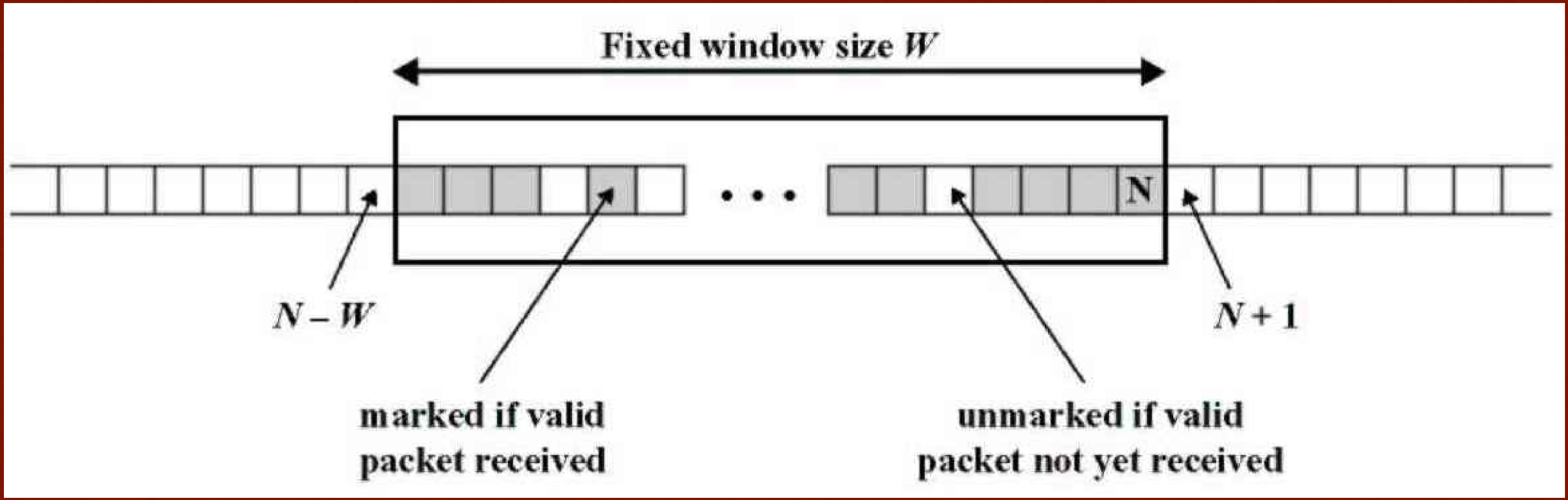


Figure 9.6 Anti-Replay Mechanism

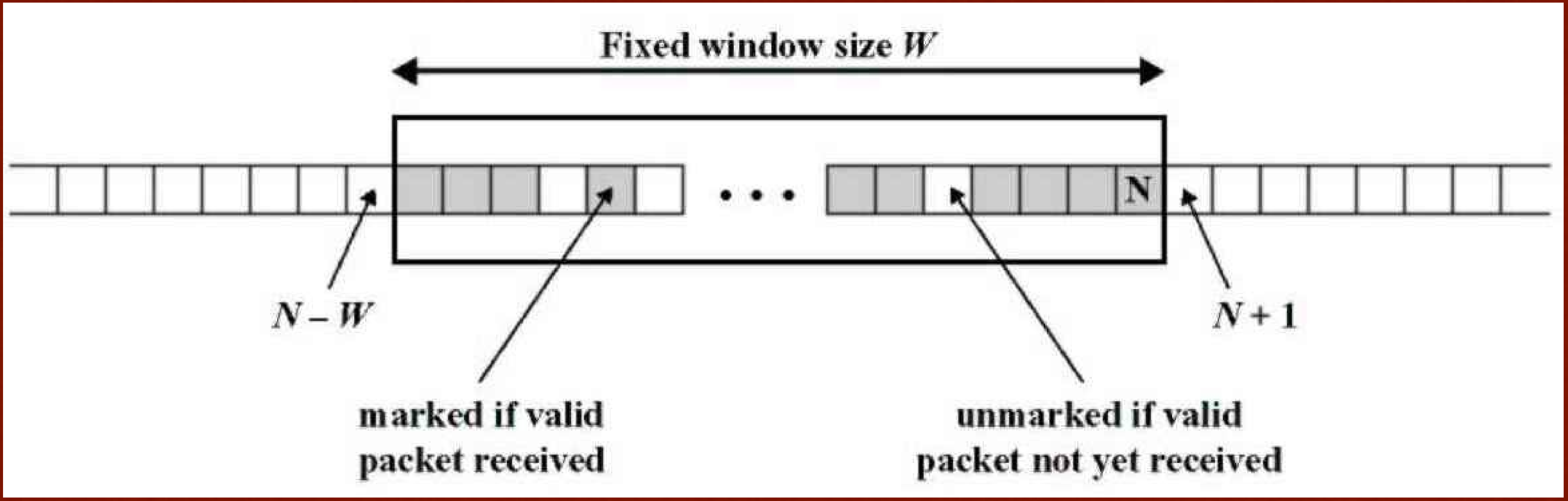
Prevenzione dei replay attack

1. Il ricevente accetta una "finestra" di dimensione W (tipicamente W=64) di numeri di sequenza. N sia il massimo numero nella finestra



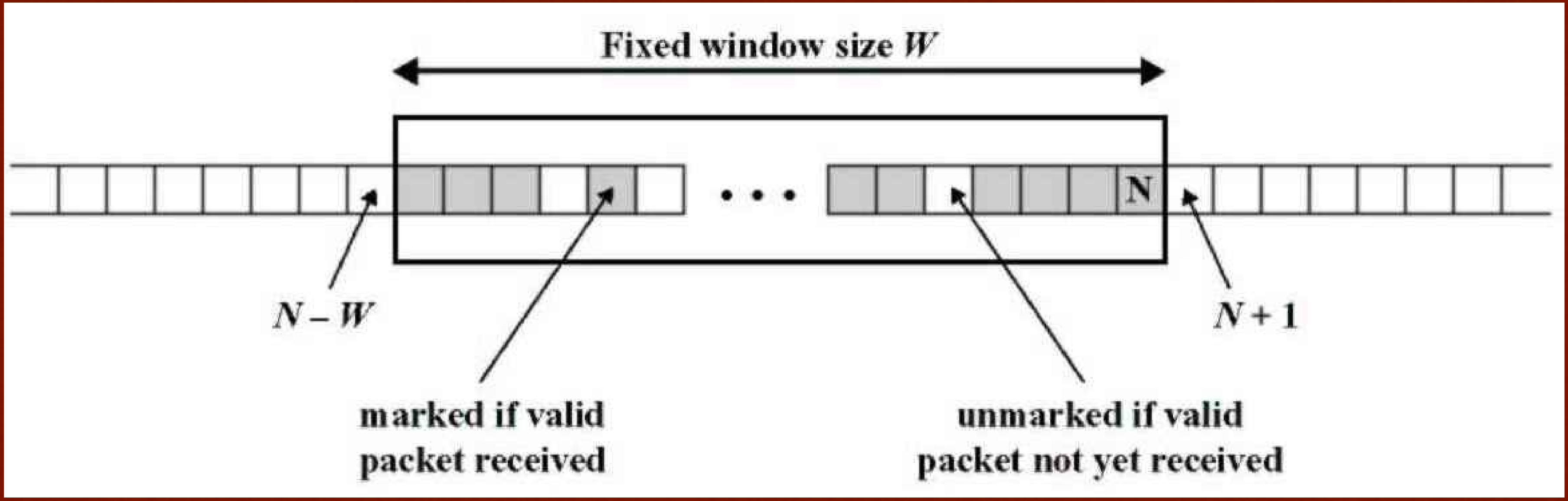
Prevenzione dei replay attack

2. Se il numero di un pacchetto in arrivo **rientra nella finestra**, il pacchetto **non è presente** ed è **autenticato** mediante MAC, viene marcata la posizione relativa



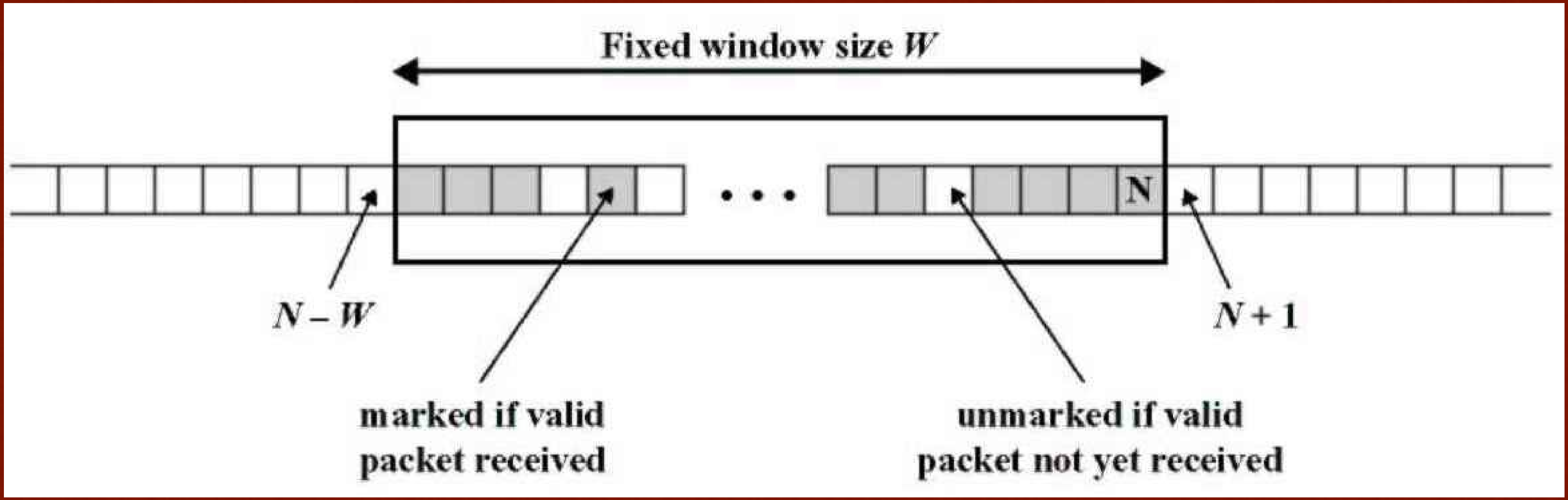
Prevenzione dei replay attack

3. Se il numero di un pacchetto in arrivo è **M>N**, il pacchetto non è presente ed è autenticato mediante MAC, viene estesa la finestra dalla destra fino a M



Prevenzione dei replay attack

4. Se il numero di un pacchetto in arrivo è **M≤N-W**, oppure il pacchetto **è già presente**, oppure **non è autenticato** dalla MAC, viene segnalata un'anomalia



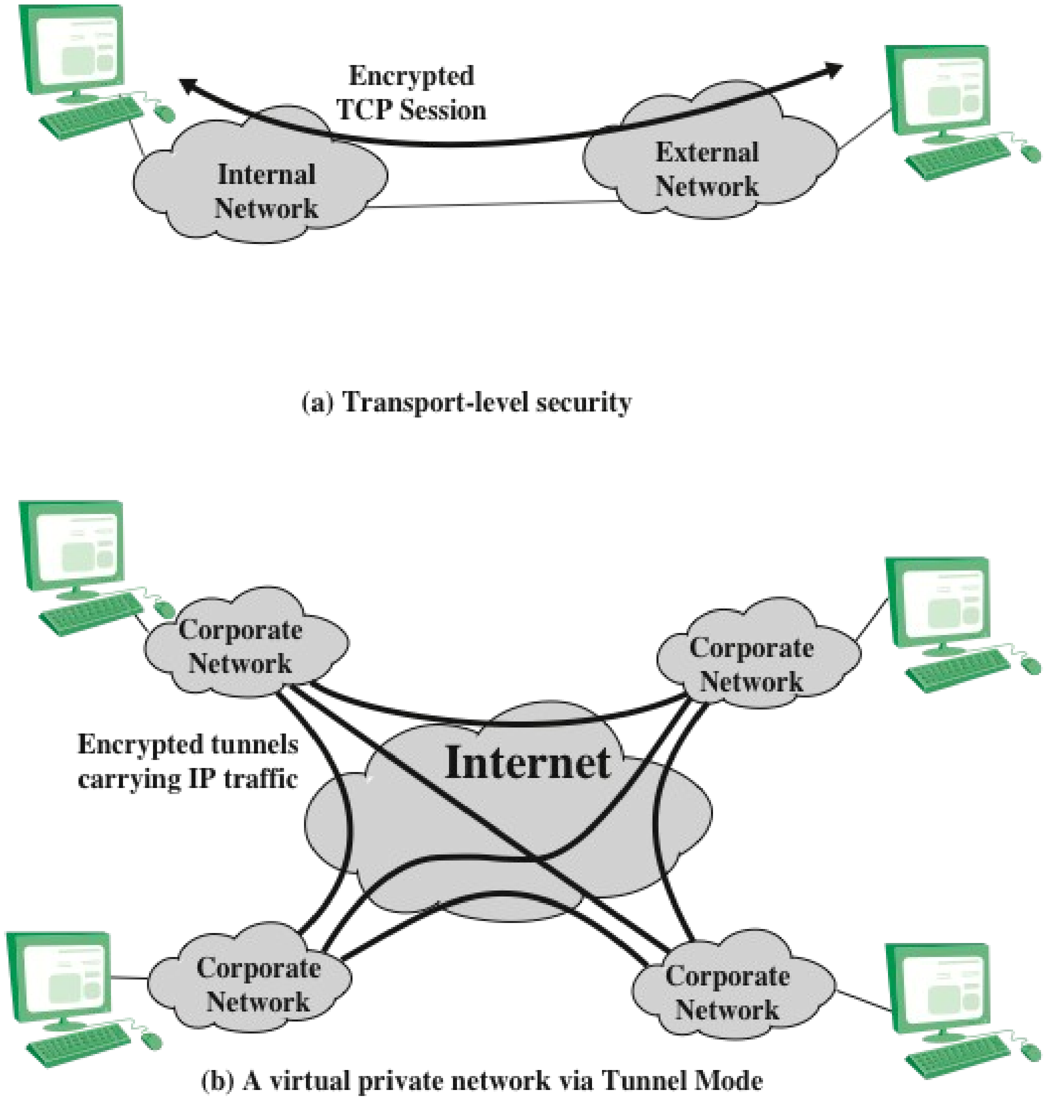


Figure 9.7 Transport-Mode vs. Tunnel-Mode Encryption

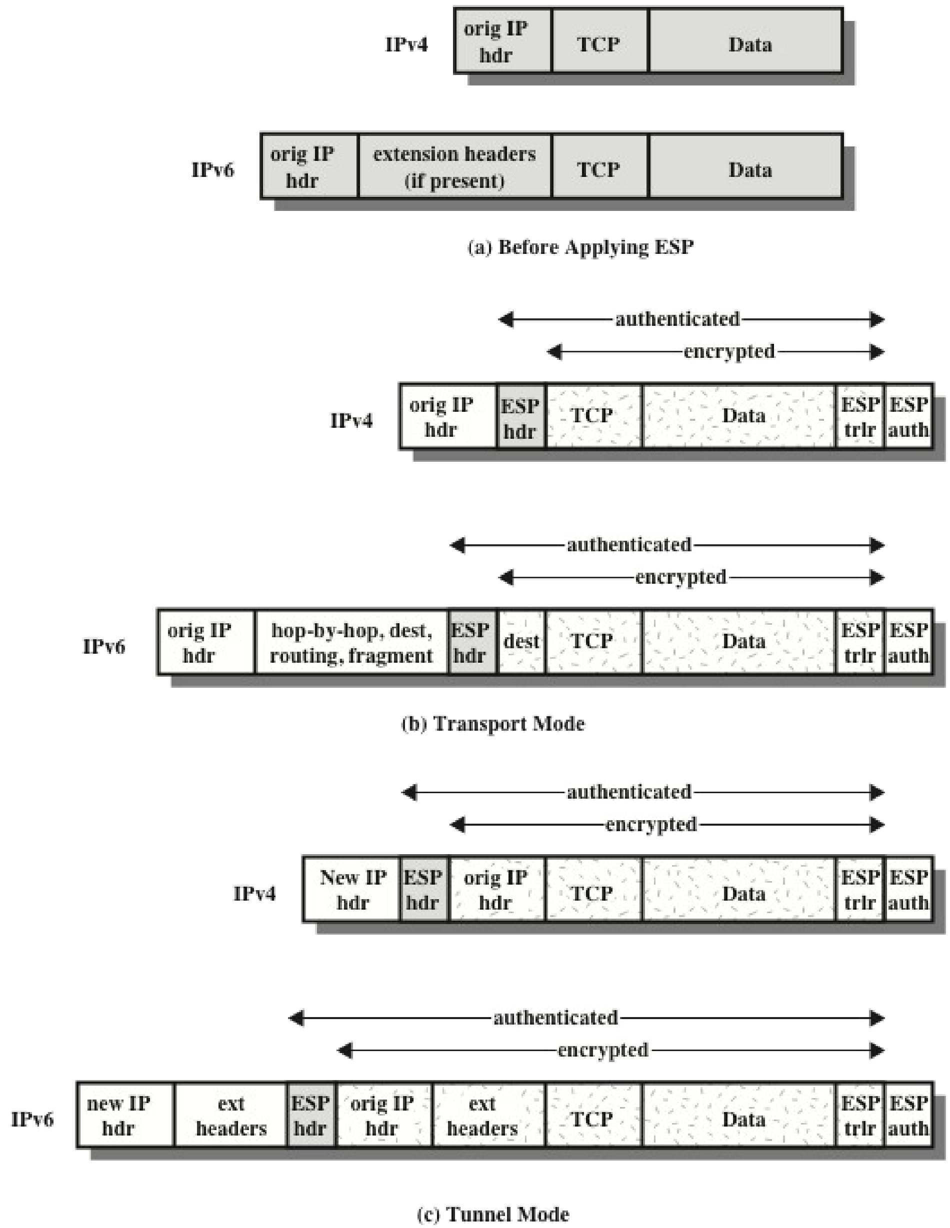
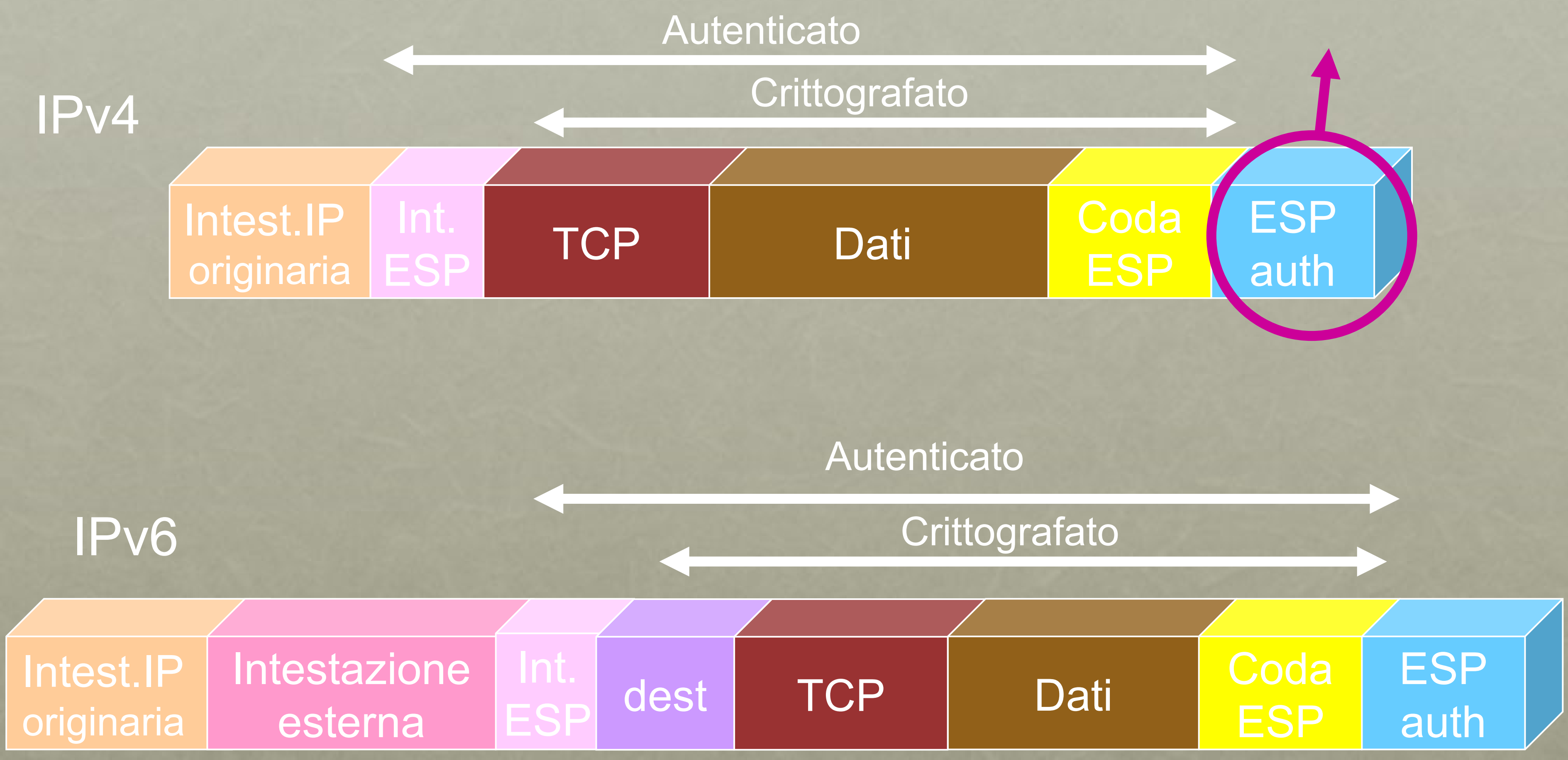


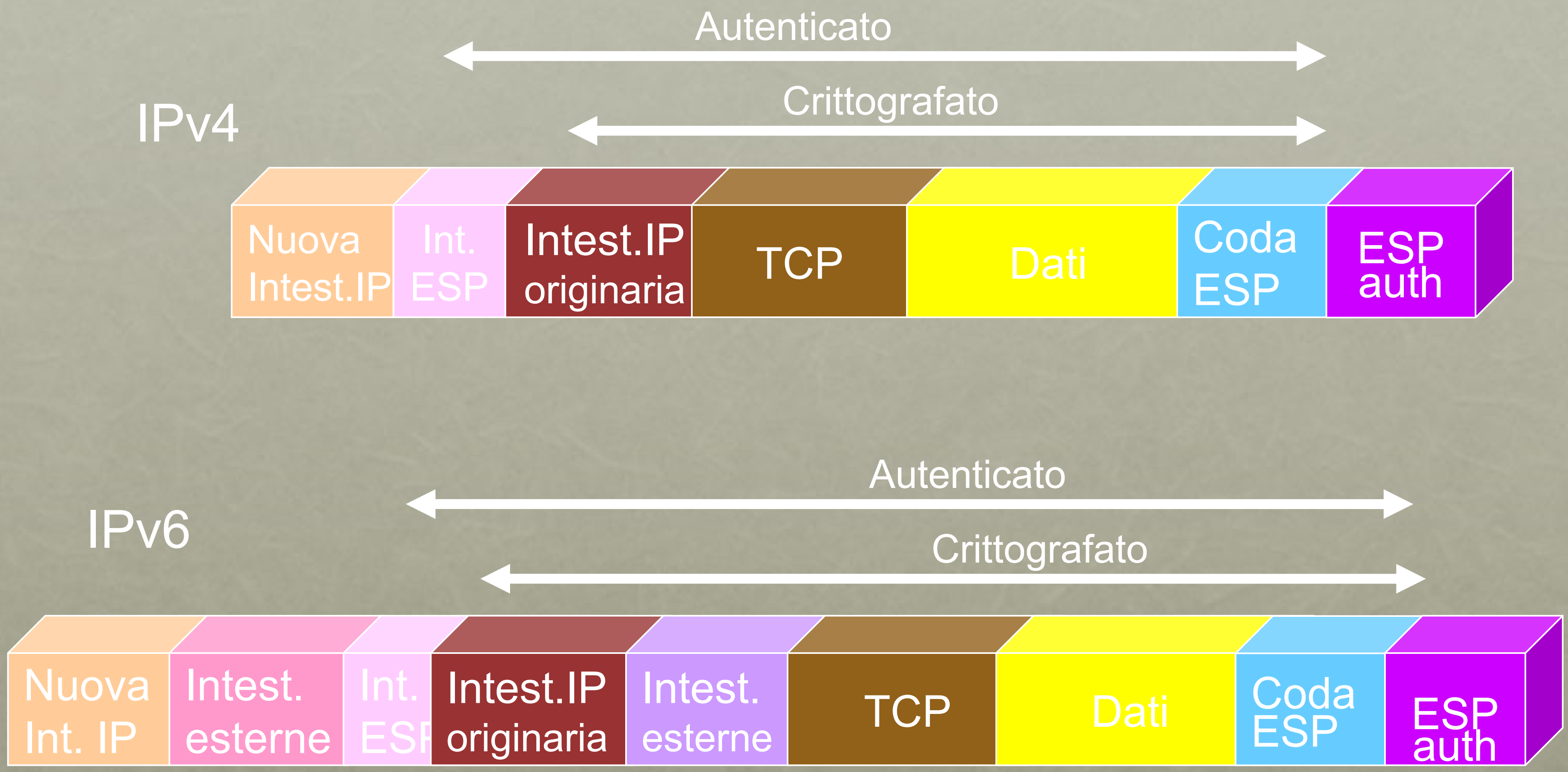
Figure 9.8 Scope of ESP Encryption and Authentication

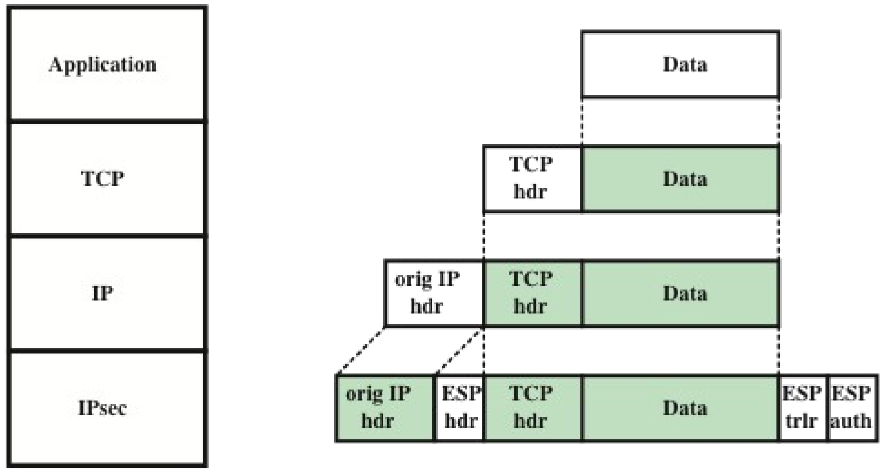
modalità transport

L'autenticazione viene applicata al testo cifrato

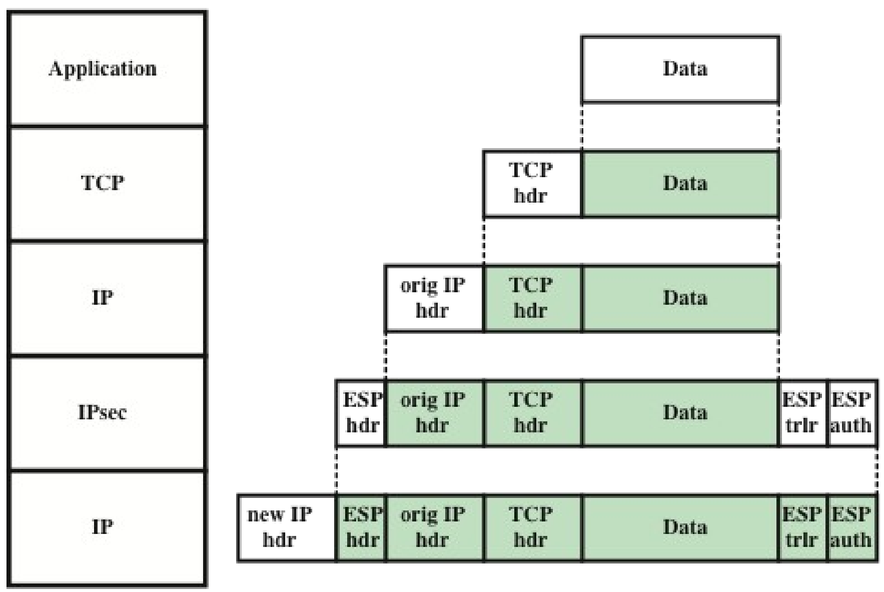


modalità tunnel





(a) Transport mode



(b) Tunnel mode

Figure 9.9 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 (dep?)

- 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 (dep?)

- 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

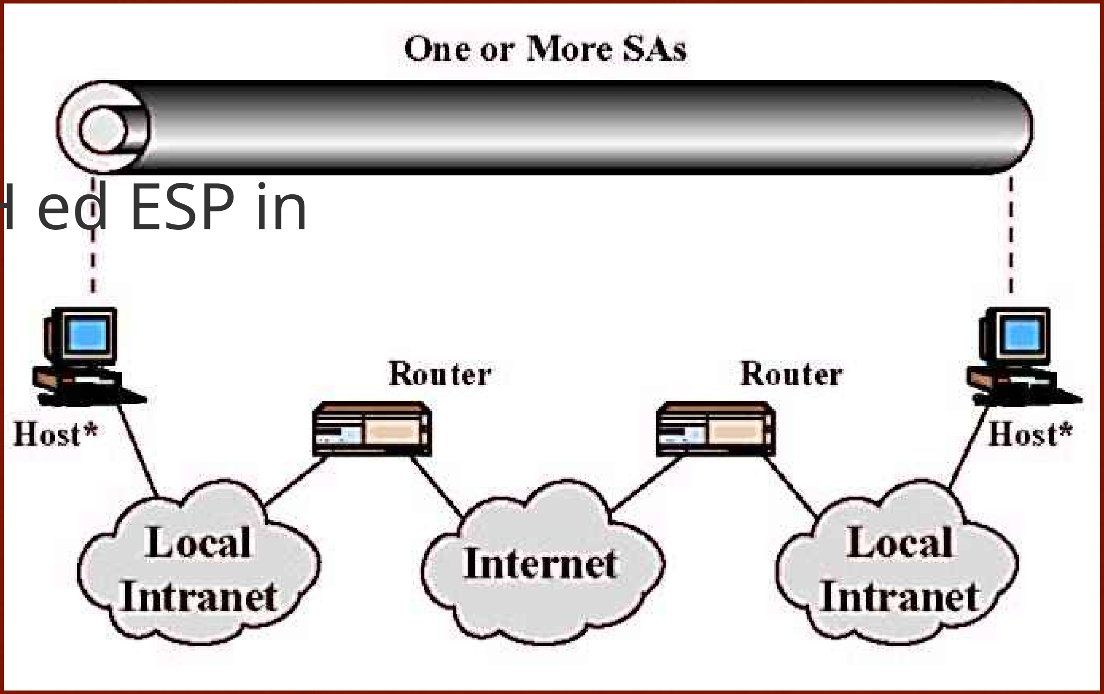
- One approach is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
  - Authentication is applied to the IP payload plus the IP header
  - The resulting IP packet is then processed in tunnel mode by ESP
    - The result is that the entire authenticated inner packet is encrypted and a new outer IP header is added

Combinazioni di SA

- Non ha senso combinare più di due modalità di trasporto
  - ESP in trasporto & AH in trasporto
- Può servire combinare (sovrapporre) molteplici tunnel
  - Ogni tunnel può avere propri nodi di inizio e fine
- Ogni nodo compatibile IPSec deve supportare 4 tipi di combinazioni SA

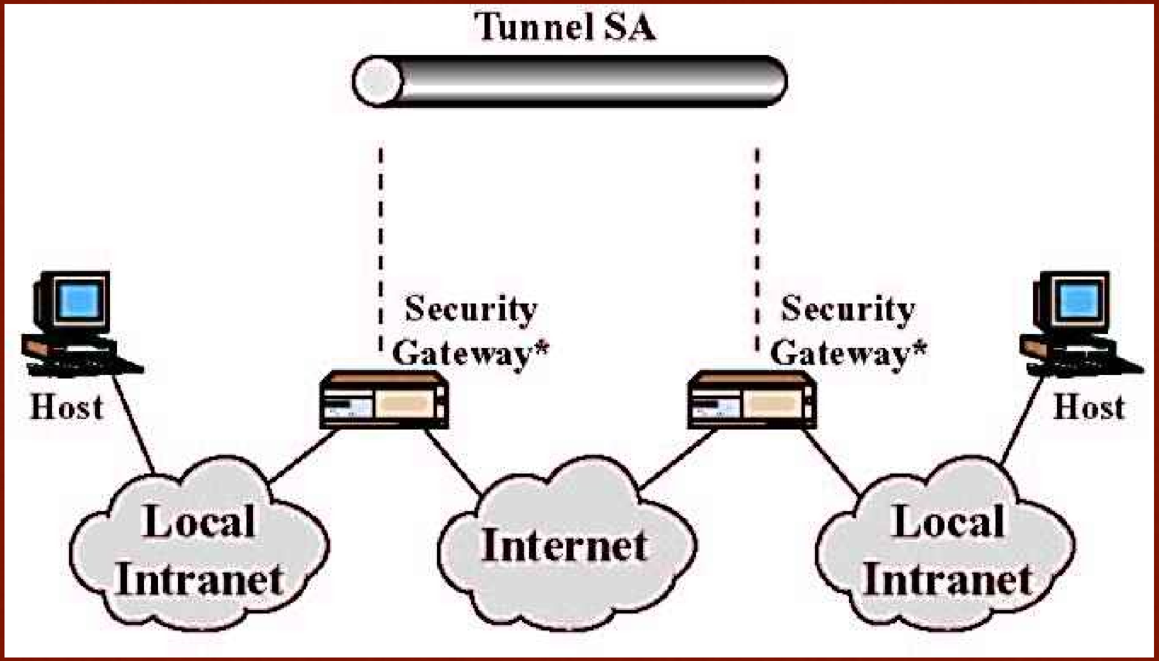
Tipo 1 di combinazioni SA: sicurezza punto-punto

1. ESP in trasporto
2. Evewntualmente AH ed ESP in cascata (deprecato)



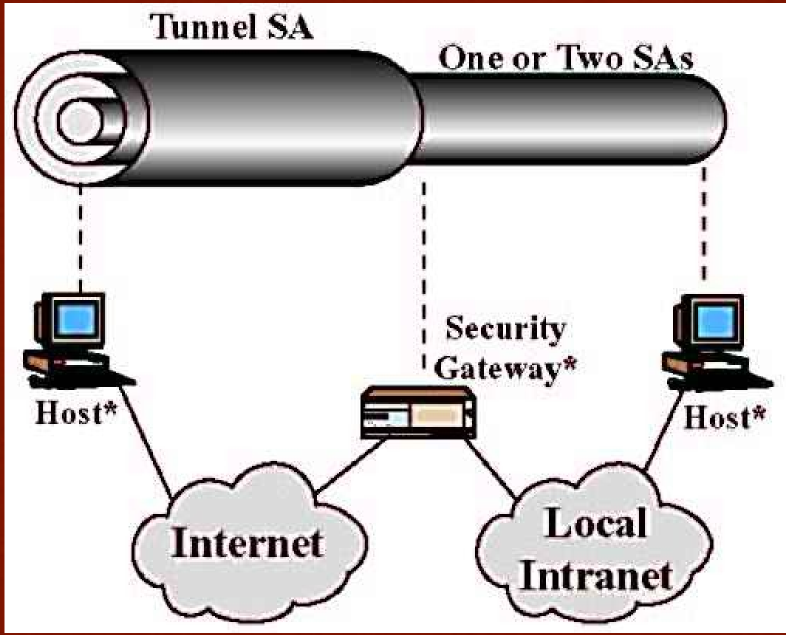
Tipo 2 di combinazioni SA: sicurezza fra intermediari

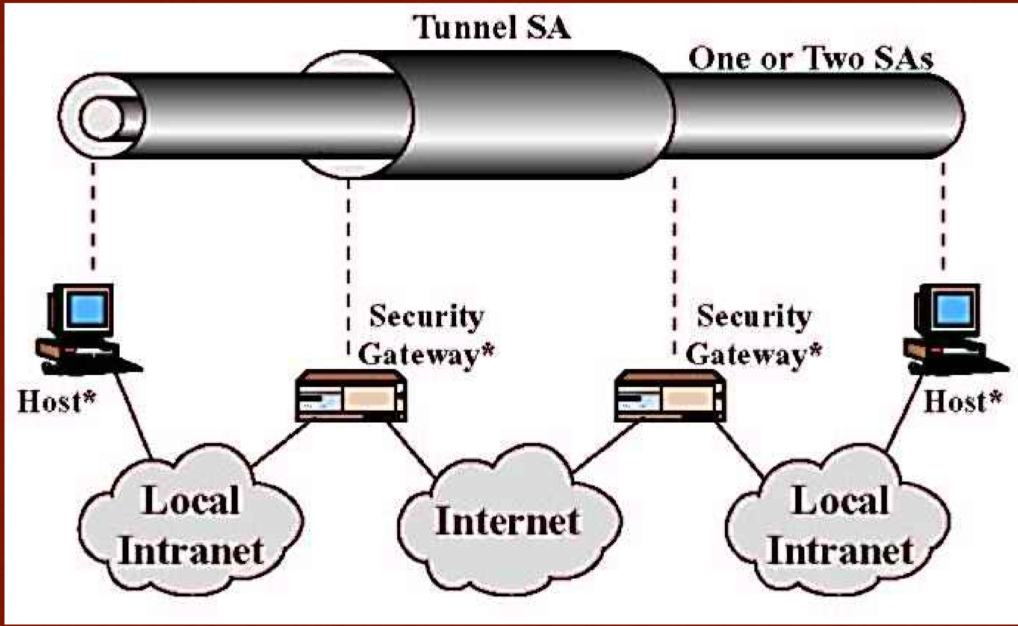
1. ESP in tunnel



Tipo 3/4 di combinazioni SA: tipo 1 & tipo 2

1. Combinazione di tipo 1 punto-punto & combinazione di tipo 2 fra intermediari





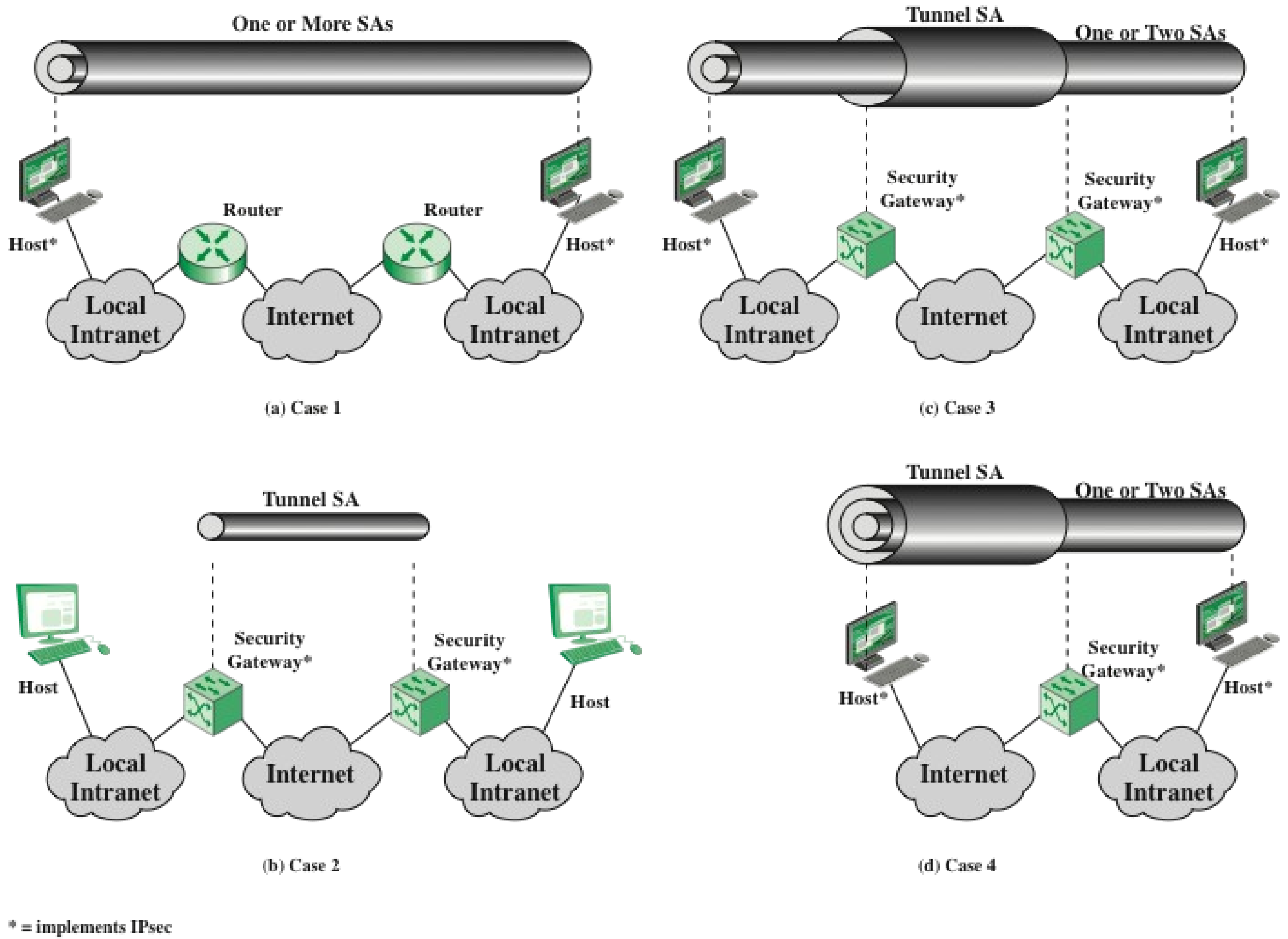


Figure 9.10 Basic Combinations of Security Associations

IKE

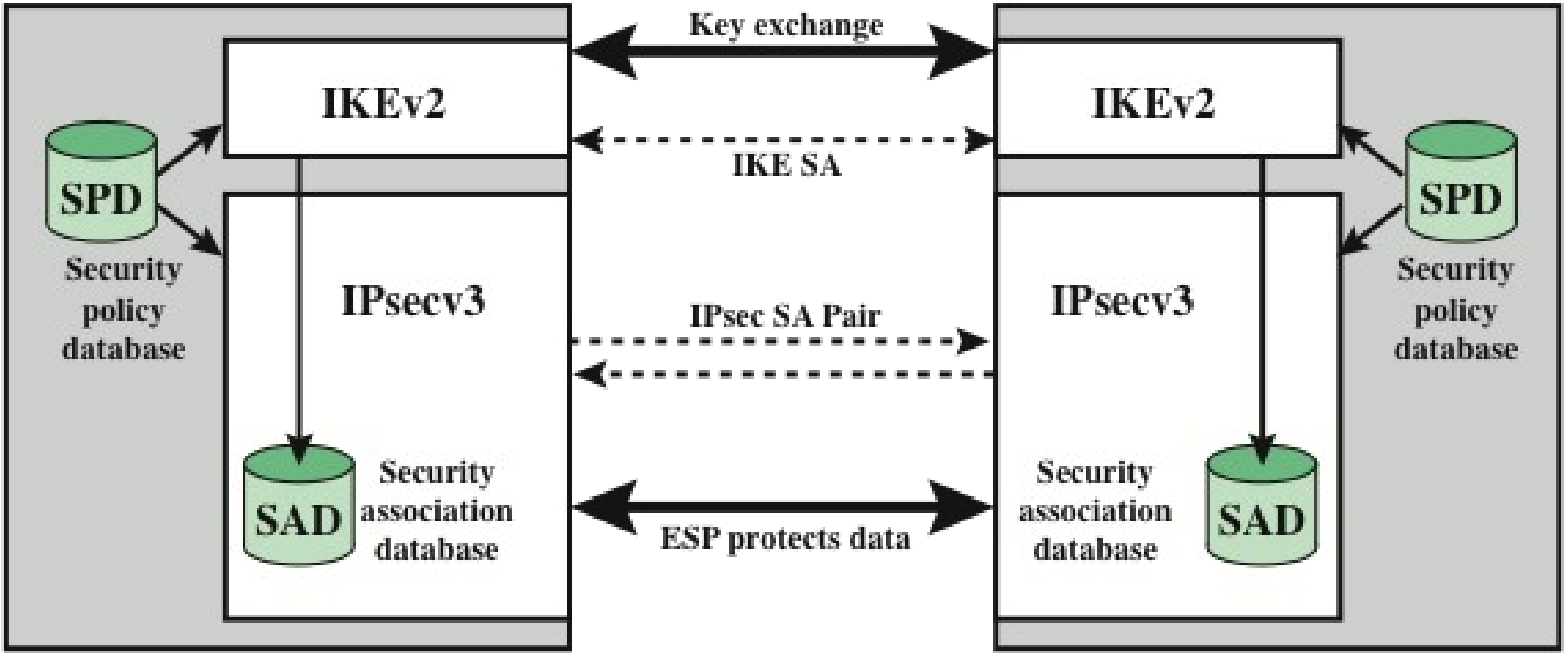


Figure 9.2 IPsec Architecture

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 environ

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

IKE1: 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 IKE2 Key Determination

- Algorithm is characterized by five important features:

1. It employs a mechanism known as cookies to thwart clogging attacks (DoS)
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

Features of IKE2 Key Determination

- Algorithm is characterized by five important features:

1.
- It employs a mechanism known as cookies to thwart clogging attacks (DoS)

- Cookie exchange require each part send ack. Opponent can only frce a user to generate ack but not to do expensive calculation (Diffie-Hellman modular exponentiation)
  - Cookie must depend on the specific party (to avoid masquerading)
  - Cookies connected to some local secret information
  - Cookie generation and verification need to be fast

2.
- Use a fast hash (MD5) over IP and UDP source and destination and a local secret nounce

IKE groups for key generation and authentication methods

- Groups
  - Modular esponentiation with 768-bit or 1024-bit or 1536-bit modules
  - Elliptic curves group over 2^155 or 2^185
  - Use nounces (to avoid replay attacks)
- 3 different authentication methods
  - Digital signatures
  - Publick key encryption
  - Symmetric encryption

Protocollo Diffie-Hellmann

- A e B concordano i parametri pubblici α e β
- Inventato Xa a caso, A crea $Ya = \alpha^{Xa} \bmod \beta$
- Inventato Xb a caso, B crea $Yb = \alpha^{Xb} \bmod \beta$

1. $A \rightarrow B : Ya$
2. $B \rightarrow A : Yb$

- A calcola $K = Yb^{Xa} \bmod \beta$
- B calcola $K = Ya^{Xb} \bmod \beta$

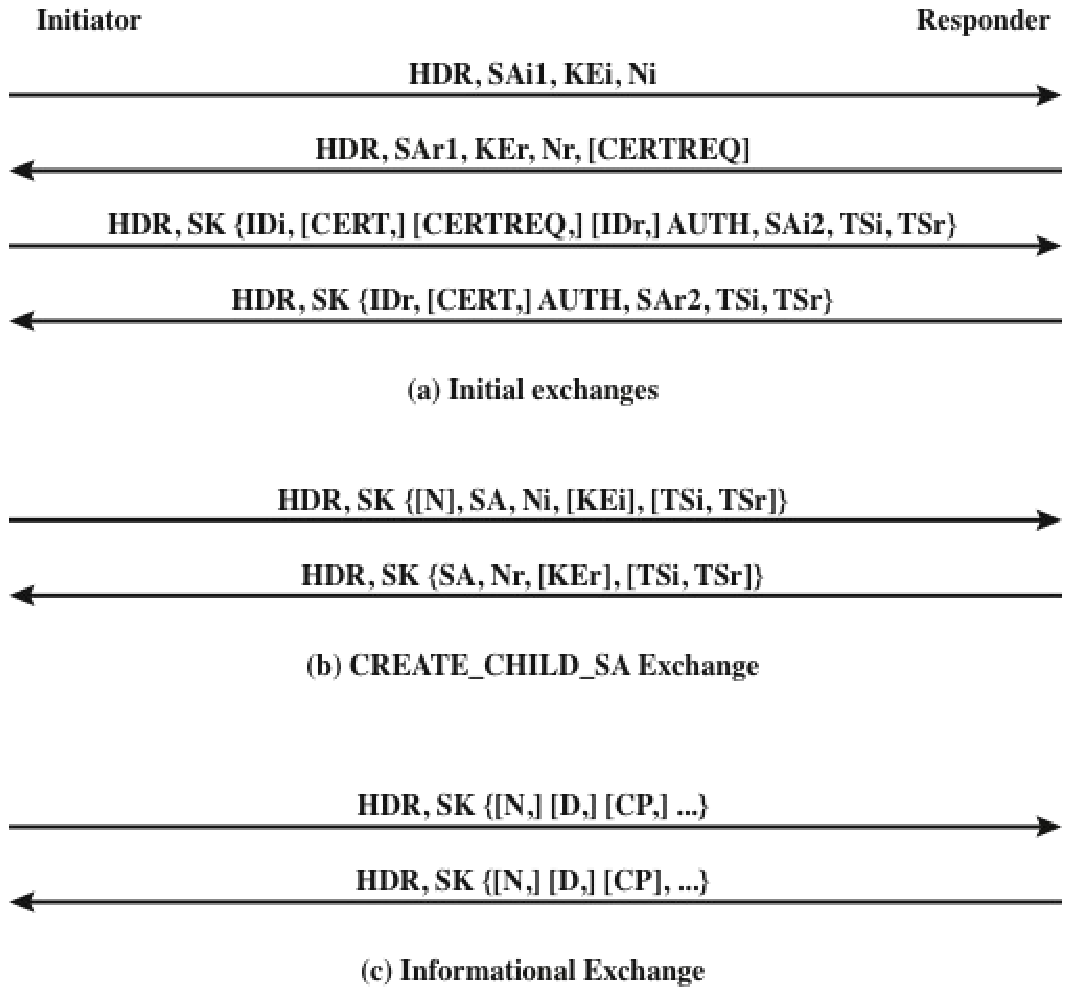
Vulnerabilità di Diffie-Hellmann

1. Nessuna forma di autenticazione
2. Possibile attacco man-in-the-middle
3. È computazionalmente costoso, quindi si presta bene per DoS sul ricevente (calcolare $K = Ya^{Xb} \bmod \beta$ è costoso)

Man-in-the-middle su Diffie-Hellmann

1. A $\rightarrow$ B : Ya   (intercettato da C)
1. C(A) $\rightarrow$ B : Yc
2. B $\rightarrow$ A : Yb   (intercettato da C)
2. C(B) $\rightarrow$ A : Yc

- A calcola K1 = Yc^{Xa} mod β
- B calcola K2 = Yc^{Xb} mod β
- C calcola K1 = Ya^{Xc} mod β
  K2 = Yb^{Xc} mod β



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

Oakley risolve le vulnerabilità

1. Ambedue i messaggi sono autenticati
   - Firma digitale, o
   - Codifica con la chiave privata del mittente, o
   - Codifica con chiave simmetrica negoziata diversamente
2. Appropriato uso di nonce
3. Complicazione dell’accesso mediante cookie

Protocollo Oakley

1. $A \rightarrow B$: Ca, {A, B, Na, Ya}SKa
2. $B \rightarrow A$: Cb, Ca, {B, A, Nb, Na, Yb, Ya}SKb
3. $A \rightarrow B$: Ca, Cb, {A, B, Na, Nb, Ya, Yb}SKa

Autenticazione. No man-in-the-middle.
B esegue l'esponenziazione solo quando A si è impegnata fino al passo 3.

ISAKMP/Oakley

- Combinazione dei due protocolli a livello applicazione (porta UDP 500)
- Studiamo il contenuto (**payload**) dei pacchetti, tralasciandone il formato completo
- Studiamo il funzionamento di base

ISAKMP – alcuni payload

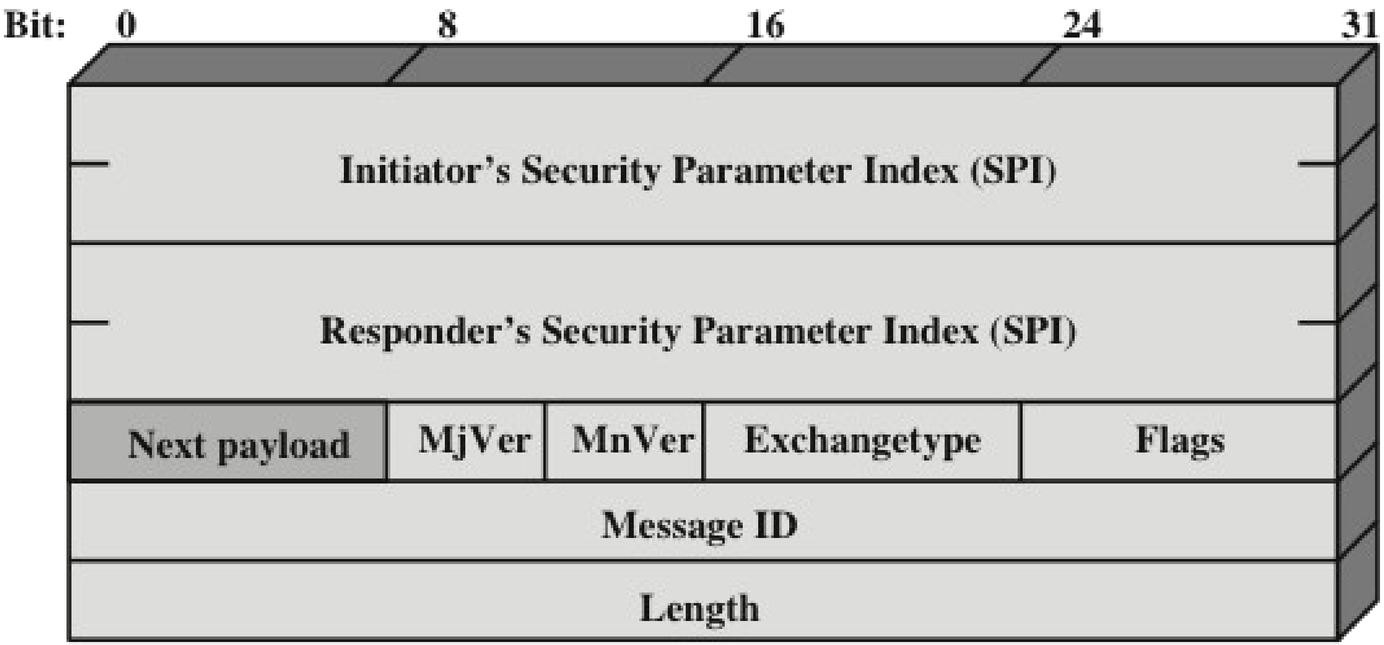
- **SA**: l’associazione che si sta negoziando
- **Proposta** (Proposal): quale protocollo usare per questa SA, se AH, ESP o ESP con autenticazione
  - No combinazioni di protocolli: una SA per prot.
- **Trasformazione** (Transform): quali hash usare per il MAC
- **Hash**: per autentica/integrità del pacchetto

ISAKMP – funzionamento di base

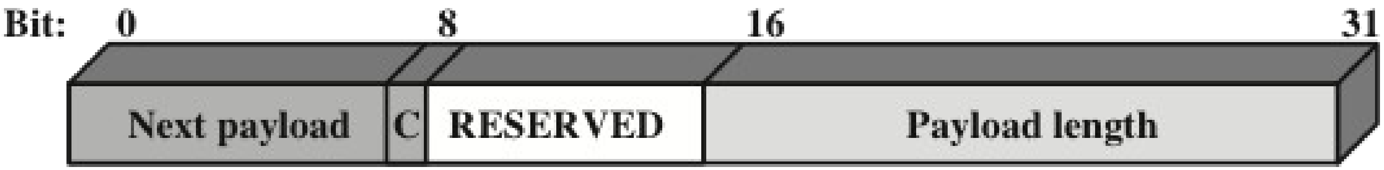
- **Scambio base**: simile a Oakley ma semplificato dei meccanismi di firma e arricchito con la negoziazione della SA completa di protocollo e trasformazione
- **Scambio con protezione dell'identità**: come il precedente più i meccanismi di firma e scambio dei certificati relativi

ISAKMP – funzionamento di base

- **Scambio solo autentica**: per mutua autentica ma senza scambio chiavi
- **Scambio aggressivo**: semplifica al massimo i messaggi (anche rispetto a 1) perdendo protezione dell'identità
- **Scambio informativo**: per gestione di SA esistenti (*notifica d'errore, cancellazione*)



(a) IKE Header



(b) Generic Payload Header

Figure 9.12 IKE Formats

ISAKMP – tutti i payload

Type	Parameters	Description
Security Association (SA)	Domain of Interpretation, Situation	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Transform #, Transform-ID, SA Attributes	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Key Exchange Data	Supports a variety of key exchange techniques.
Identification (ID)	ID Type, ID Data	Used to exchange identification information.
Certificate (CERT)	Cert Encoding, Certificate Data	Used to transport certificates and other certificate-related information.
Certificate Request (CR)	# Cert Types, Certificate Types, # Cert Auths, Certificate Authorities	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Hash Data	Contains data generated by a hash function.
Signature (SIG)	Signature Data	Contains data generated by a digital signa wture function.
Nonce (NONCE)	Nonce Data	Contains a nonce.
Notification (N)	DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data	Used to transmit notification data, such as an error condition.
Delete (D)	DOI, Protocol-ID, SPI Size, # of SPIs, SPI (one or more)	Indicates an SA that is no longer valid.

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)

ESP Encryption Algorithms

Name	Status	AEAD	Comment
ENCR_NULL	MUST	No	[RFC2410]
ENCR_AES_CBC	MUST	No	[RFC3602][1]
ENCR_AES_CCM_8	SHOULD	Yes	[RFC4309](IoT)
ENCR_AES_GCM_16	MUST	Yes	[RFC4106][1]
ENCR_CHACHA20_POLY1305	SHOULD	Yes	[RFC7634]

ESP Authentication Algorithms

Name	Status	Comment
AUTH_NONE	MUST / MUST NOT	[RFC7296][RFC5282] AEAD-only
AUTH_HMAC_SHA1_96	MUST-	[RFC2404][RFC7296]
AUTH_AES_XCBC_96	SHOULD / MAY	[RFC3566][RFC7296] (IoT)
AUTH_AES_128_GMAC	MAY	[RFC4543]
AUTH_AES_256_GMAC	MAY	[RFC4543]
AUTH_HMAC_SHA2_256_128	MUST	[RFC4868]
AUTH_HMAC_SHA2_512_256	SHOULD	[RFC4868]

ESP Compression Algorithms

Name	Status	Comment
IPCOMP_DEFLATE	MAY	[RFC3173]
IPCOMP_LZS	MAY	[RFC2395]
IPCOMP_LZJH	MAY	[RFC3051]

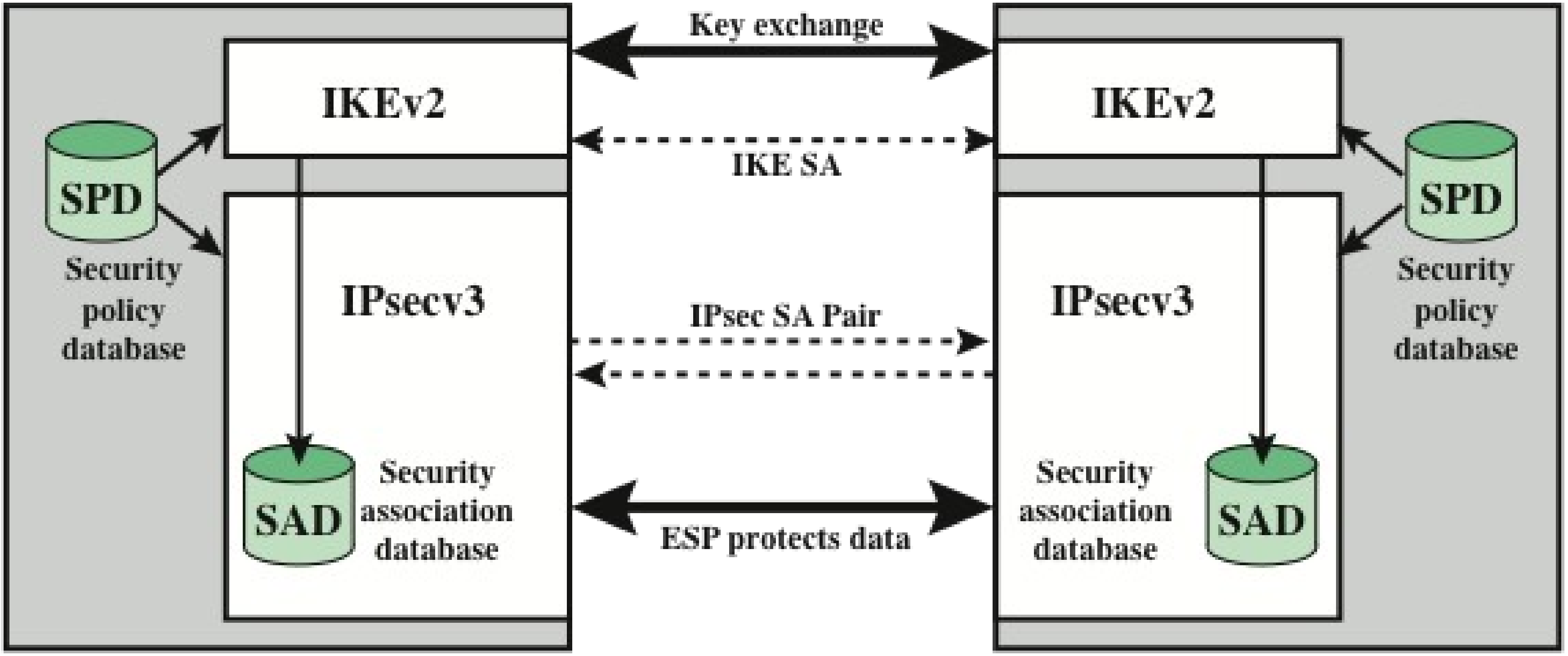


Figure 9.2 IPsec Architecture

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