**Universidad de Oviedo**

*Departamento de Informática*

*Campus de Gijón*

# Protocolos de Seguridad: IPsec

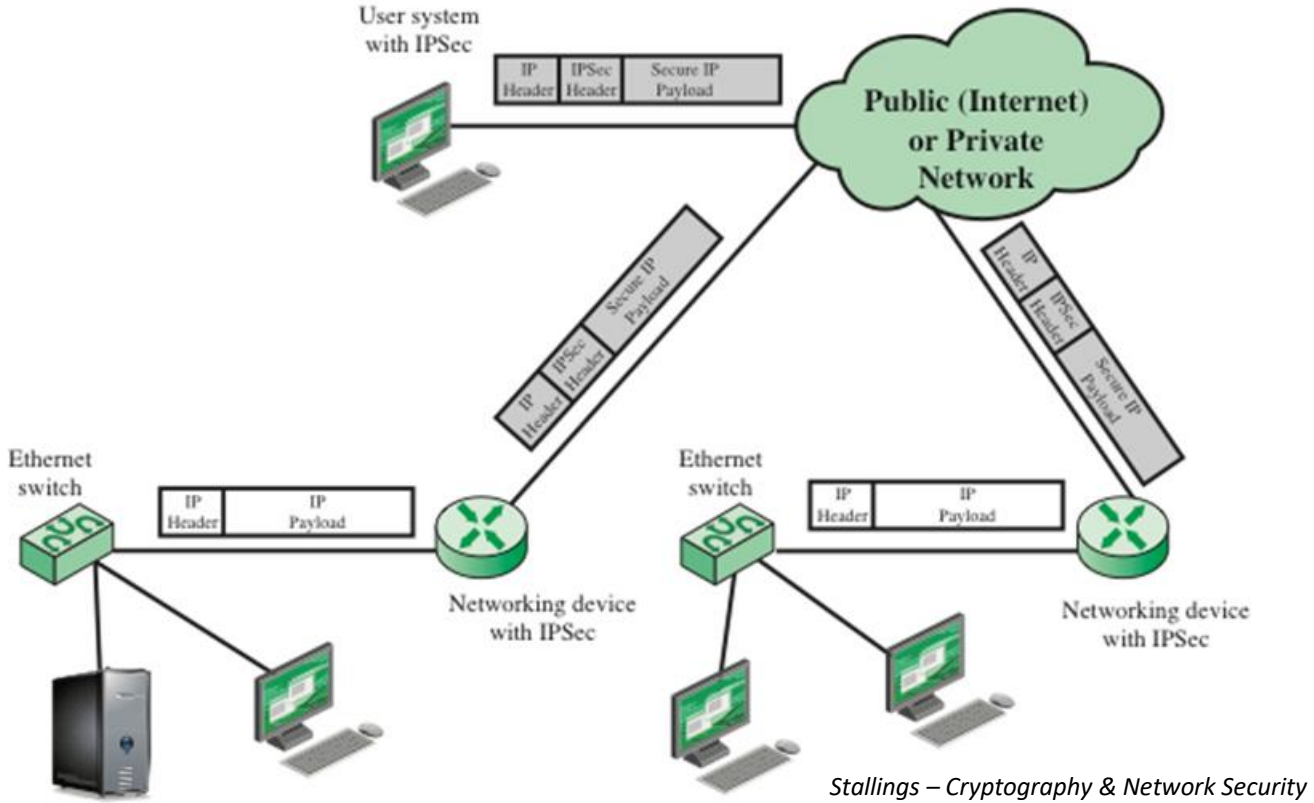
*Presentación*

Daniel F. García

# Introducción a IPsec

IPsec (*Internet Protocol Security*) es un conjunto de protocolos para asegurar las comunicaciones con el protocolo IP autenticando y/o cifrando cada paquete IP de una comunicación

También incluye protocolos para establecer las claves de cifrado




*Stallings – Cryptography & Network Security*

IPsec proporciona los servicios de seguridad en la capa IP (Ubicada en el nivel 3 o nivel de red del modelo ISO/OSI)

Transparente a aplicaciones / usuarios
Protege todo el tráfico basado en IP

# Protocolo IPsec – Documentación

La documentación es muy extensa → Muchos RFCs interrelacionados

Usar como índice la última versión de "***IPsec document roadmap***"

2011 Feb RFC-6071 IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap
https://www.rfc-editor.org/rfc/pdfrfc/rfc6071.txt.pdf

Documentos básicos:

**IPsec-v2 (antiguo)**

1998 Nov RFC-2401 Security Architecture for the Internet Protocol

1998 Nov RFC-2402 IP Authentication Header (AH)

1998 Nov RFC-2406 IP Encapsulating Security Payload (ESP)

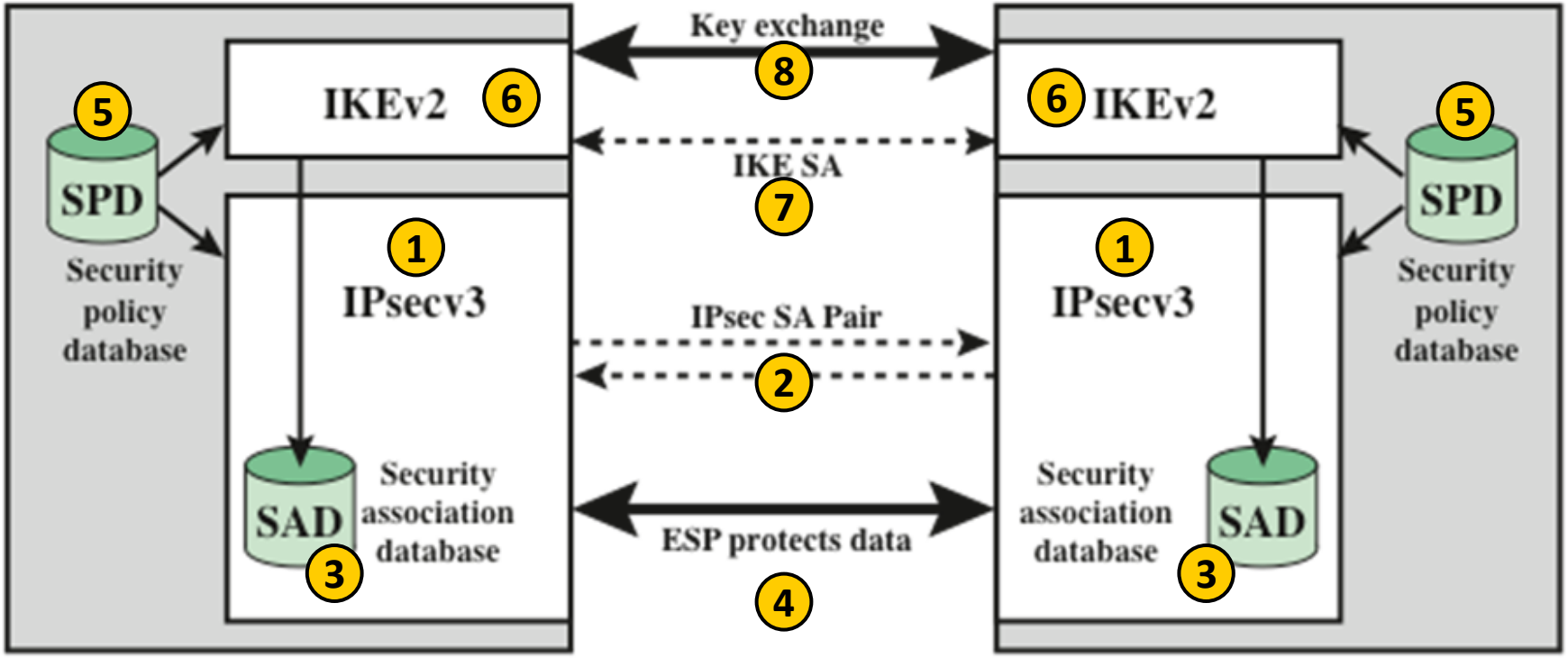
**IPsec-v3 (actual)**

2005 Dic RFC-4301 Security Architecture for the Internet Protocol
https://www.rfc-editor.org/rfc/pdfrfc/rfc4301.txt.pdf

2005 Dic RFC-4302 IP Authentication Header (AH)
https://www.rfc-editor.org/rfc/pdfrfc/rfc4302.txt.pdf

2005 Dic RFC-4303 IP Encapsulating Security Payload (ESP)
https://www.rfc-editor.org/rfc/pdfrfc/rfc4303.txt.pdf

# Arquitectura general de IPsec




*Stallings – Cryptography & Network Security*

# Protocolos de seguridad usados por IPsec (1)

IPsec utiliza dos protocolos para proporcionar los servicios de seguridad:

- **AH** – Authentication Header
  Proporciona integridad, autenticación y no repudio
- **ESP** – Encapsulating Security Payload
  Proporciona confidencialidad, y opcionalmente, integridad y autenticación

Las implementaciones de IPsec **DEBEN soportar ESP** y deberían soportar AH

Ambos protocolos pueden funcionar en 2 modos → { Transporte, Túnel }

## Modo Transporte

Solo se cifra y/o autentica la carga útil del paquete IP (los datos que se transfieren)

Como no se cifra la cabecera IP el enrutamiento del paquete es posible

Modo típicamente usado para comunicaciones extremo-a-extremo entre 2 hosts (un cliente y un servidor, o dos workstations)

# Protocolos de seguridad usados por IPsec (2)

## Modo Túnel

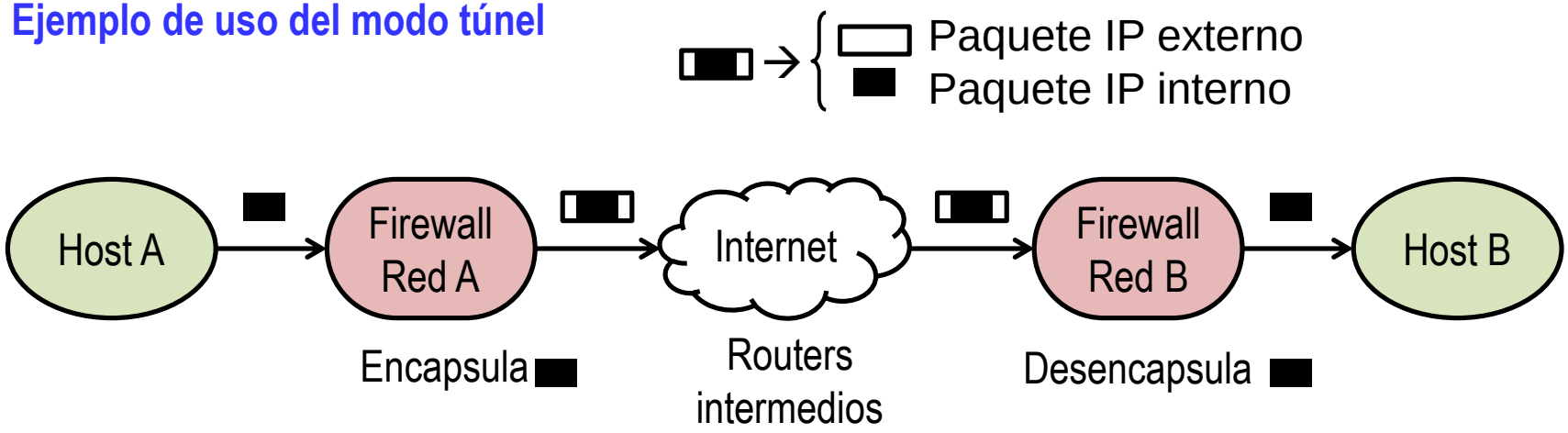
Se cifra y/o autentica TODO el paquete IP (cabeceras + datos del mensaje)

Al cifrar la cabecera IP el enrutamiento del paquete es imposible

Hay que encapsular el paquete IP y las cabeceras de seguridad añadidas en un nuevo paquete IP cuyas cabeceras sean accesibles y modificables por los routers

Modo típicamente usado cuando uno o ambos extremos de una comunicación es un equipo de seguridad de una red (firewall o router que usan IPsec)

### Ejemplo de uso del modo túnel



# Asociaciones de seguridad

Una asociación de seguridad (*SA, Security Association*) es una **conexión lógica unidireccional** entre un emisor y un receptor que especifica como proporcionar seguridad al tráfico IP entre el emisor y el receptor

Si se necesita intercambiar datos de modo seguro en las dos direcciones E → R y E ← R, se necesitan dos asociaciones de seguridad

## Identificación de una asociación de seguridad

- Índice de parámetros de seguridad (*SPI, Security Parameter Index*)
  - Entero sin signo de 32 bits asignado a la SA
  - El SPI se integra en las cabeceras de los protocolos AH y ESP para que el equipo receptor pueda seleccionar la SA que especifica como procesar el paquete recibido
- Dirección IP de destino (*IP Destination Address*)
  - Es la dirección IP del extremo destino de la SA
- Identificador del protocolo de seguridad (*Security Protocol Identifier*)
  - Indica si la SA utiliza AH o ESP

# Base de datos de Políticas de Seguridad (1)

La Base de Datos de Políticas de Seguridad (*SPD, Security Policy Database*) permite relacionar cada paquete IP con una SA concreta
(o con ninguna si se permite a los paquetes evitar a IPsec)

Cada entrada de la SPD define un subconjunto del tráfico IP y lo relaciona a una SA

## Selectores

Cada entrada de una SPD contiene un conjunto de **valores** que pueden aparecer en los campos de las cabeceras del protocolo IP y de los protocolos superiores (TCP, UDP)

Estos **valores** son los **selectores** y sirven para seleccionar una entrada concreta de la SPD

- Direcciones IP local y remota (*Local and Remote IP Addresses*)
  Dirección IP individual, lista enumerada, rango o máscara (*wildcard*) de direcciones
- Protocolo de la capa siguiente (*Next Layer Protocol*)
  Puede ser el número de un protocolo, ó ANY, o para IPv6, OPAQUE
- Puertos locales y remotos (*Local and Remote Ports*)
  Puertos TCP ó UDP individuales, lista enumerada o una máscara de puertos

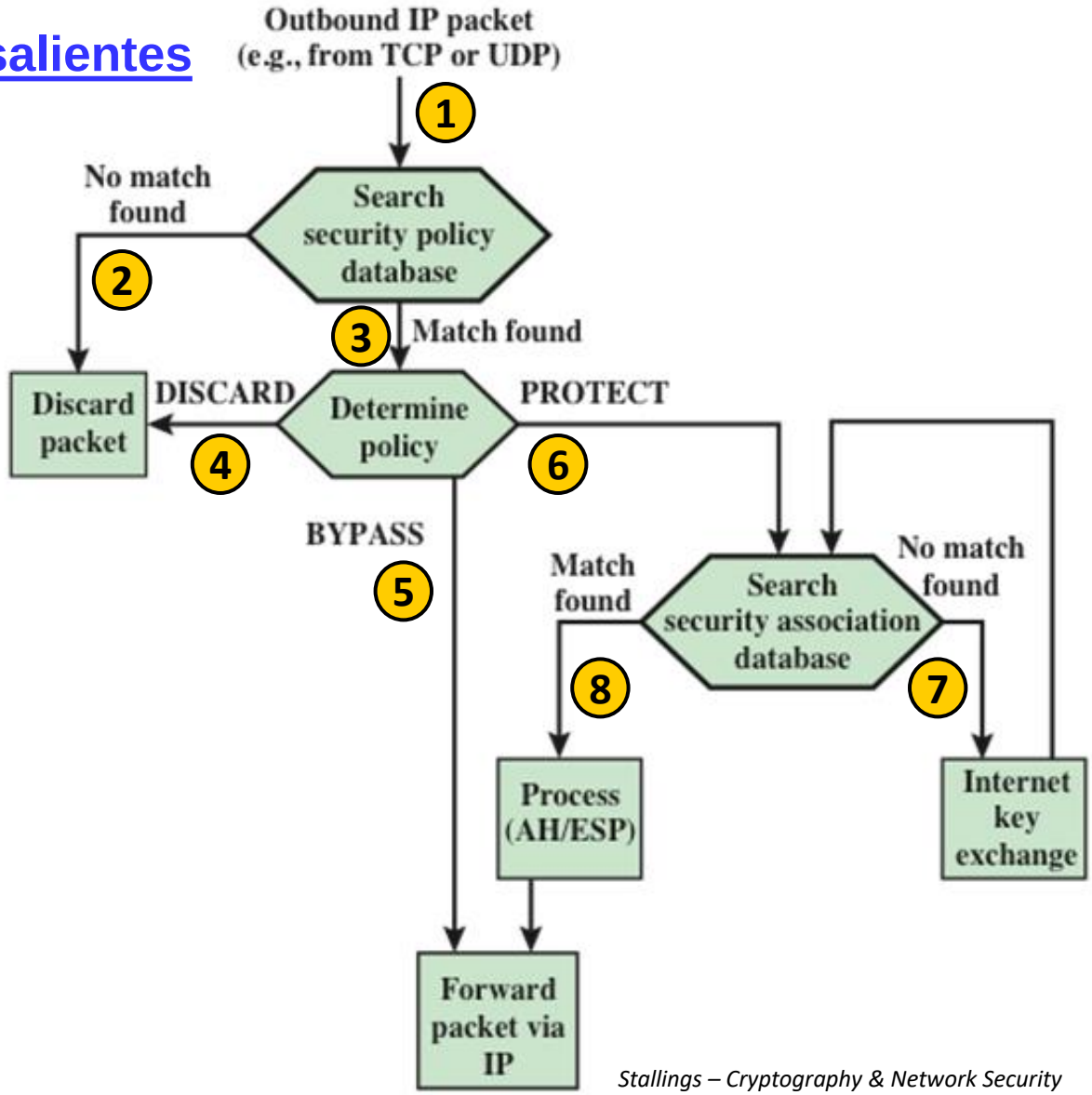
# Base de datos de Políticas de Seguridad (2)

## Ejemplo de BD de Políticas de Seguridad de un Computador

| 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 |

# Procesamiento del tráfico IP con IPsec (1)

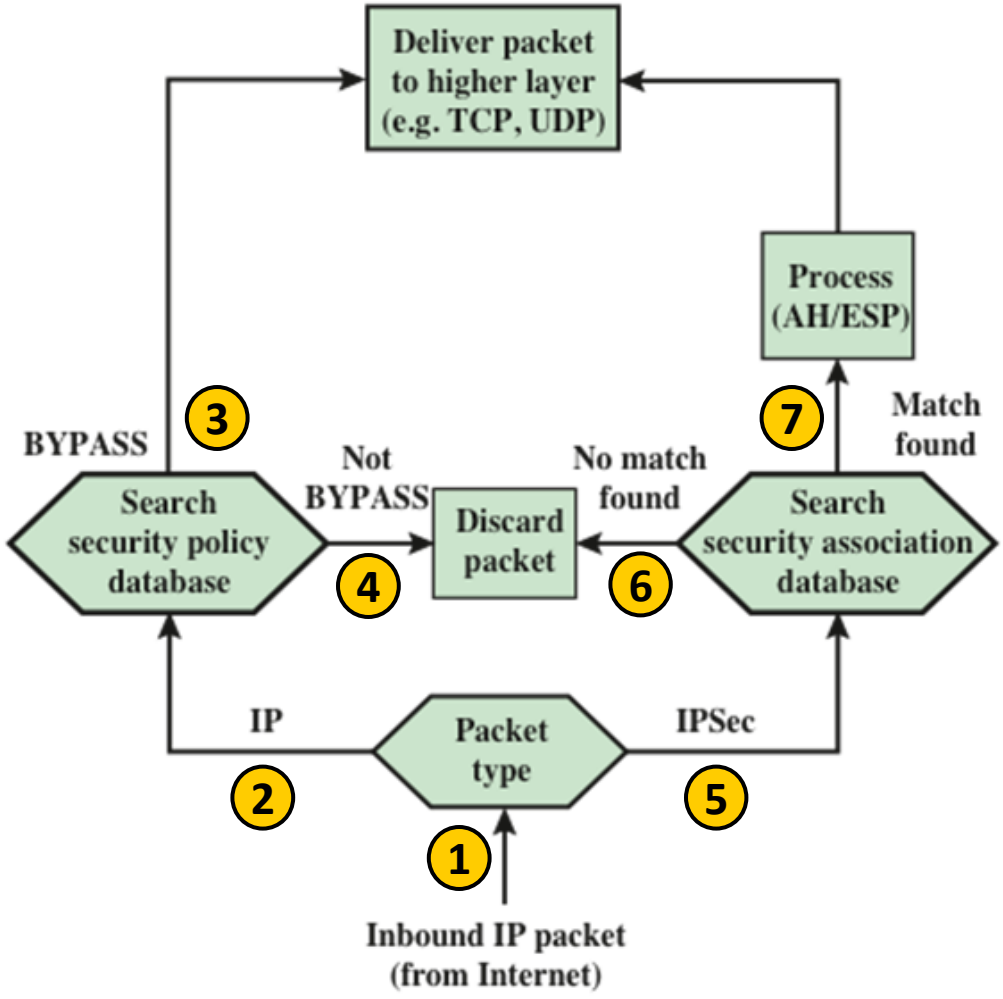
## Paquetes salientes




*Stallings – Cryptography & Network Security*

# Procesamiento del tráfico IP con IPsec (2)

## Paquetes entrantes




*Stallings – Cryptography & Network Security*

# El protocolo ESP (1) Introducción

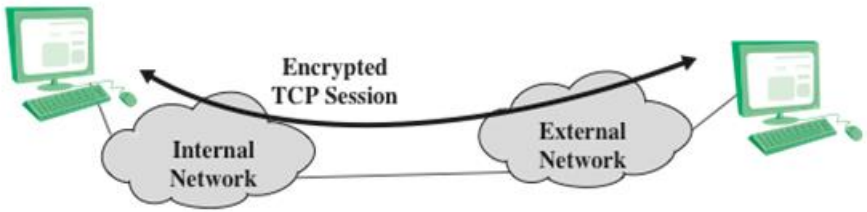
IPsec utiliza ESP (***Encapsulating Security Payload***) para proporcionar: confidencialidad, autenticación del origen de los datos, integridad, …

**El conjunto de servicios depende de las opciones seleccionadas al establecer la SA**

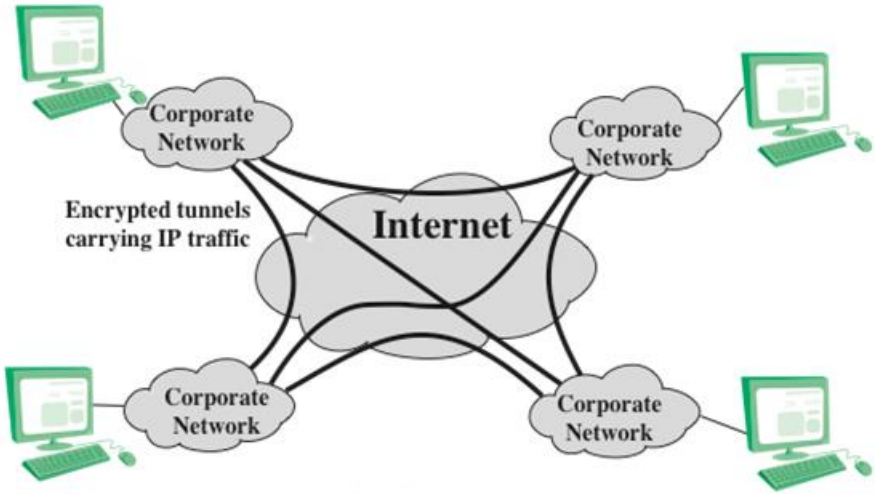
ESP puede trabajar con diversos algoritmos de cifrado y autenticación

ESP puede funcionar en dos modos → { Transporte, Túnel }

**ESP en modo Transporte**

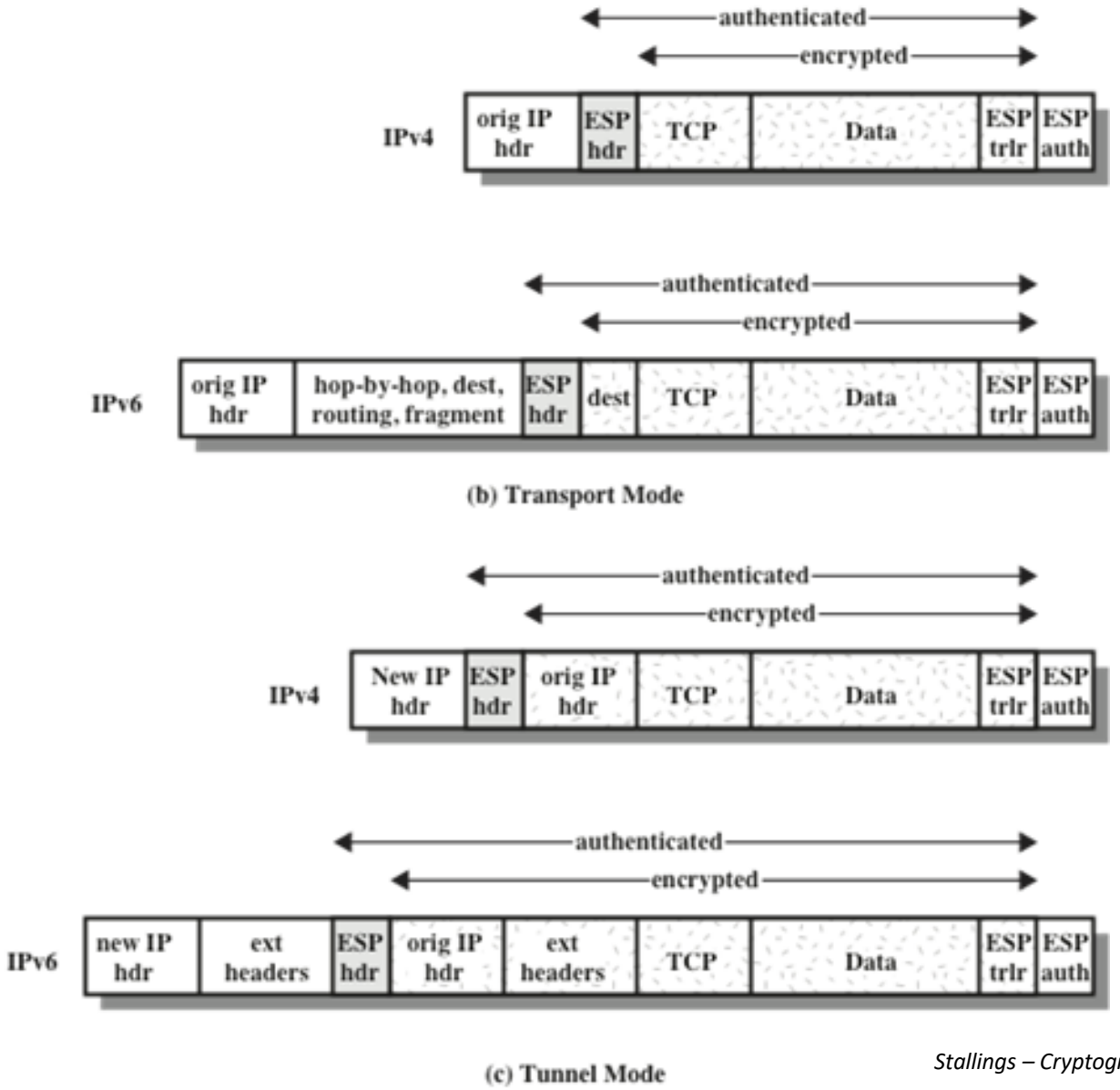



**ESP en modo Túnel**




*Stallings – Cryptography & Network Security*

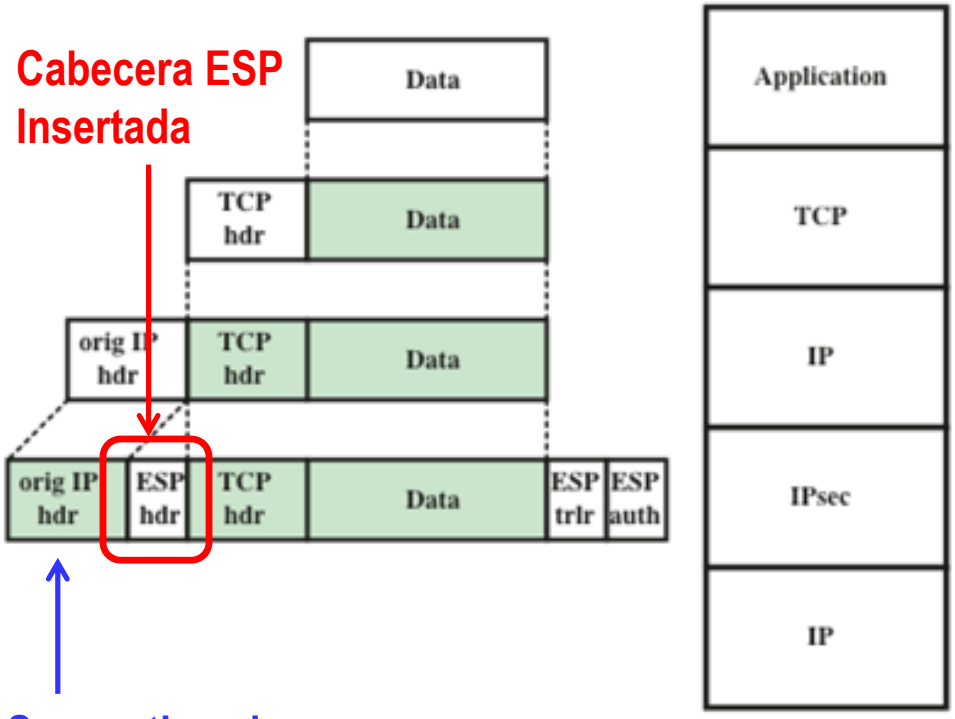
# El protocolo ESP (2) Ámbitos de cifrado y autenticación




*Stallings – Cryptography & Network Security*

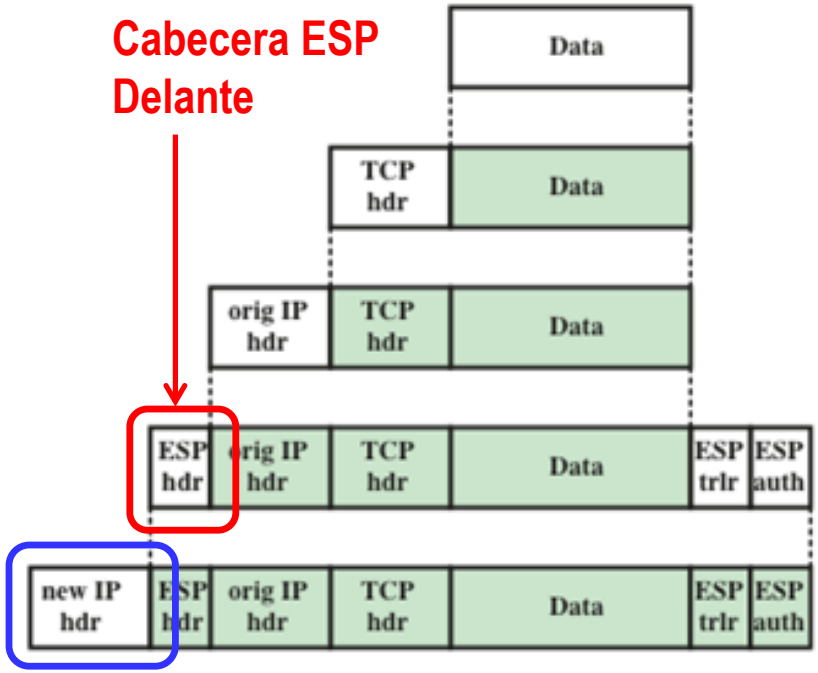
# El protocolo ESP (3) Comparación de modos

## ESP en modo Transporte




Se mantiene la
Cabecera IP original

## ESP en modo Túnel




Se añade Cabecera IP EXTERNA
Encapsulando al paquete original

# El protocolo AH

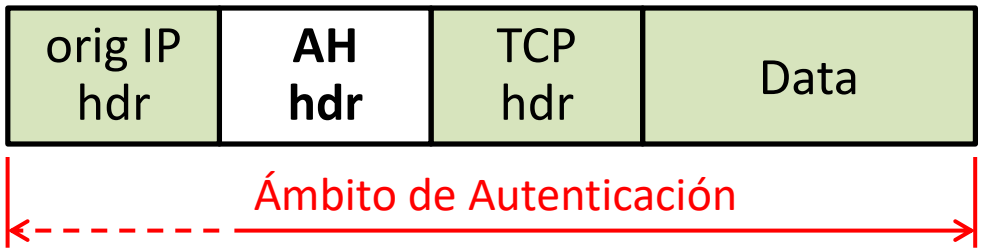
Solo proporciona autenticación (integridad) de los paquetes IP

Añade una cabecera AH al paquete IP

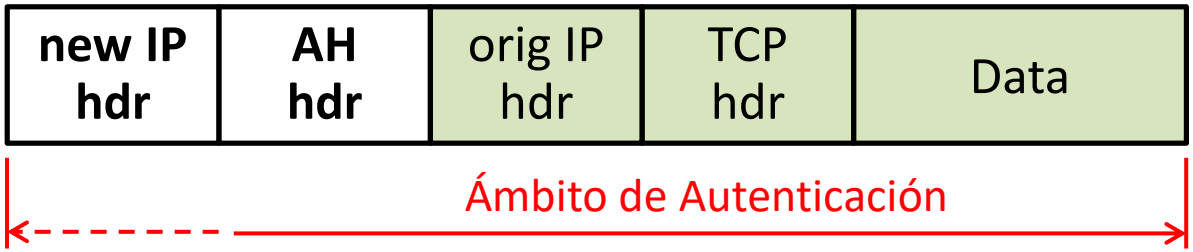
La cabecera AH **contiene un ICV** (*Integrity Check Value*) calculado sobre:

- Todos los campos detrás de la cabecera AH
- Los campos inmutables de la cabecera IP antes de la cabecera AH

**AH en modo Transporte** (IPv4)




**AH en modo Túnel** (IPv4)



# Protocolo IKE (*Internet Key Exchange*)

IPsec necesita mantener un "**estado compartido**" entre el productor y el consumidor de datagramas IP

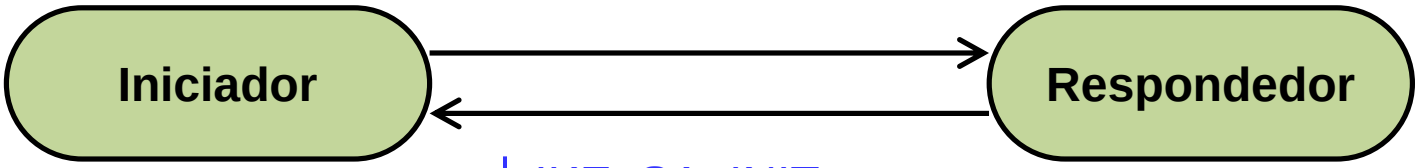
Estado compartido ←→
- Servicios a proveer a los datagramas
- Alg. criptográficos que necesitan los servicios
- Claves que necesitan los alg. criptográficos

El protocolo IKE se utiliza para establecer y gestionar el estado compartido

---

Todas las comunicaciones IKE consisten en pares de mensajes: petición+respuesta

A un par de mensajes se le denomina un Intercambio (*Exchange*)




Garantiza la fiabilidad

Tipos de Intercambios →
- IKE_SA_INIT
- IKE_AUTH
- CREATE_CHILD_SA
- INFORMATIONAL

# Protocolo IKE – Documentación

Todo el protocolo IKE se describe en múltiples RFCs

Documentos básicos:

**IKE-v1 (antiguo)**

1998 Nov RFC-2409 The Internet Key Exchange (IKE)

1998 Nov RFC-2408 Internet Security Association and Key Management Protocol (ISAKMP)

1998 Nov RFC-2407 The Internet IP Security Domain of Interpretation for ISAKMP

1998 Nov RFC-2412 The OAKLEY Key Determination Protocol

**IKE-v2 (actual)**

2005 Dic RFC-4306 Internet Key Exchange (IKEv2) Protocol

2006 Oct RFC-4718 IKEv2 Clarifications and Implementation Guidelines

2010 Sep RFC-5996 Internet Key Exchange Protocol Version 2 (IKEv2)

https://www.rfc-editor.org/rfc/pdfrfc/rfc5996.txt.pdf

# IPsec: Juegos (suites) Criptográficos

2005 Dic RFC-4308 Cryptographic Suites for IPsec https://www.rfc-editor.org/rfc/pdfrfc/rfc4308.txt.pdf

| | 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 |

← Soporte de Redes Privadas Virtuales

VPN-A para IKEv1 → 3DES y HMAC-SHA1

VPN-B para IKEv2 → AES

2007 Abr RFC-4869 Suite B Cryptographic Suites for IPsec https://www.rfc-editor.org/rfc/pdfrfc/rfc4869.txt.pdf

2011 Oct RFC-6379 https://www.rfc-editor.org/rfc/pdfrfc/rfc6379.txt.pdf

| | 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 |

GCM = Galois/Counter Mode

Cifrado & Autenticación (con un solo algoritmo)

GMAC: GCM solo autenticando

Para IKE: AES y HMAC-SHAn

# Combinación de Asociaciones de Seguridad (1)

Una SA individual puede implementar cualquiera de los protocolos AH o ESP pero no ambos

En ocasiones un determinado flujo de tráfico puede necesitar:

- La combinación de servicios proporcionados por AH y ESP
- Unos servicios entre los hosts y otros servicios entre los gateways

Una Combinación de Asociaciones de Seguridad (*Security Association Bundle*) es una secuencia de SAs a través de la cual se procesa un flujo de tráfico para proporcionarle un conjunto de servicios IPsec deseados

Una combinación puede empezar y terminar en el mismo equipo o en equipos distintos

**Hay dos formas básicas de realizar la combinación:**

| | |
|---|---|
| Adyacencia de transporte | Se refiere a aplicar más de un protocolo de seguridad al mismo paquete IP sin usar túneles (sólo es útil aplicar una combinación de ESP y AH) |
| Tunelado iterativo | Consiste en aplicar múltiples protocolos de seguridad al mismo paquete IP usando túneles sucesivos (puede ser útil aplicar varias combinaciones) |

# Combinación de Asociaciones de Seguridad (2)

## Estrategias de combinación de SAs (1)

Las combinaciones se usan para proporcionar confidencialidad + autenticación (integridad)

¿Qué hay que proporcionar primero o después? ¿la confidencialidad o la autenticación?

**1** ESP con autenticación = NO Combinación

Estrategia: 1º Confidencialidad + 2º Autenticación

ESP-Transporte con Aut → 1º Cifra Carga IP + 2º Autentica Cab ESP y Carga IP

NO protege la cabecera IP

ESP-Túnel con Aut → 1º Cifra Cab y Carga IP + 2º Autentica Cab ESP, Cab IP y Carga IP

SI protege la cabecera IP

**2** Adyacencia de transporte = Combinar 2 SAs en modo transporte

Estrategia: 1º Confidencialidad + 2º Autenticación

1ª SA interna: ESP-Transporte sin autenticación – Cifra Carga IP

2ª SA externa: AH-Transporte – Autentica Cab ESP y Cab IP (excepto campos modificables)

Respecto a la estrategia (1):

- **Ventaja**: Autentica parte de Cab IP (No los campos modificables)
- **Desventaja**: Más sobrecarga al usar 2 SAs

# Combinación de Asociaciones de Seguridad (3)

## Estrategias de combinación de SAs (2)

**3** Combinación Transporte-Túnel

Estrategia: 1º Autenticación + 2º Confidencialidad

1ª SA interna: AH-Transporte – Autentica Cab IP (excepto campos modificables) y Carga IP

2ª SA externa: ESP-Túnel sin autenticación – Cifra Paquete Interno y Añade nueva Cab IP

**Ventajas**:

El cifrado externo protege directamente al autenticador interno

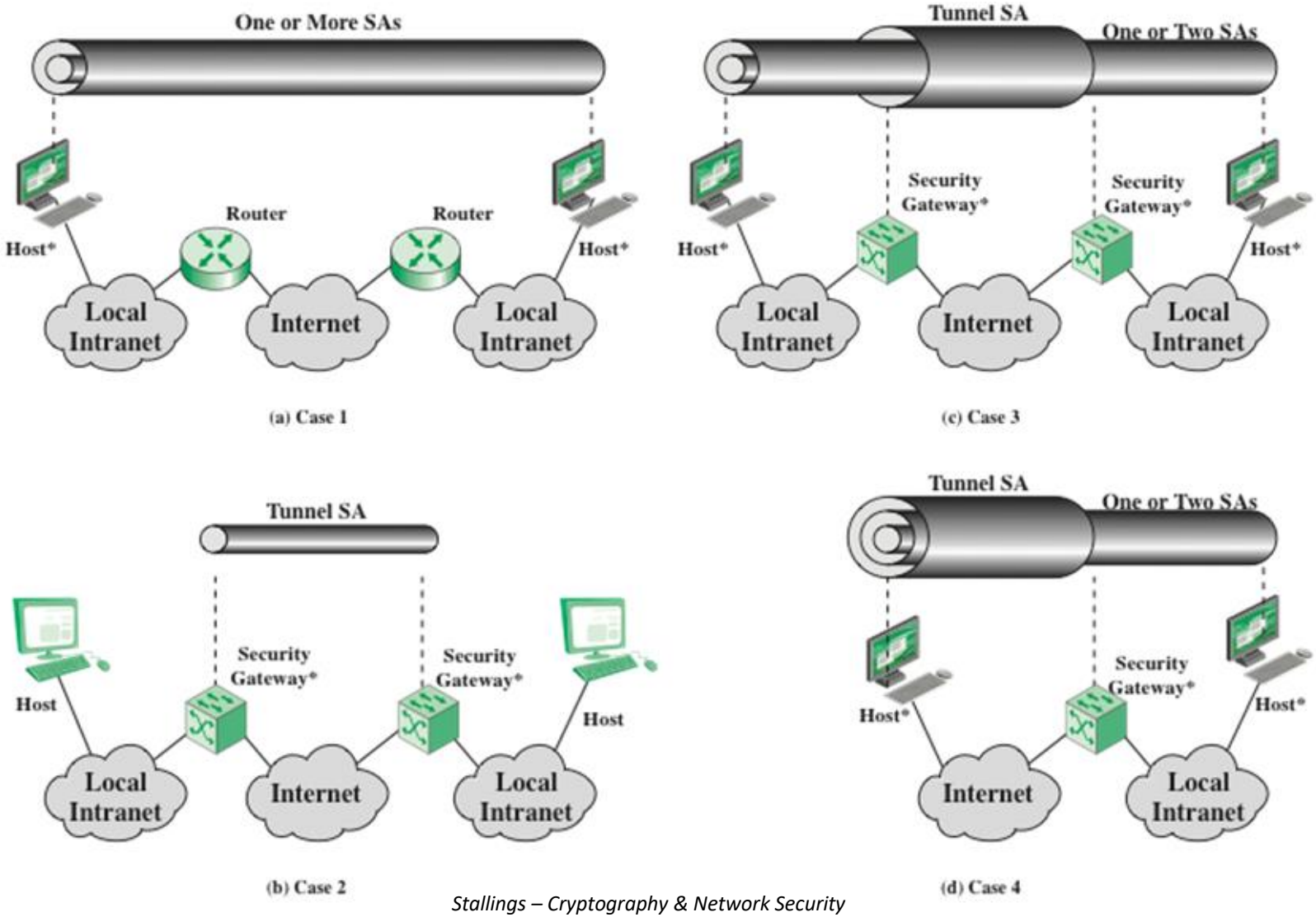
En (1) y (2) hay que proteger (cifrar) el autenticador

Permite guardar el autenticador junto con el mensaje

En (1) y (2) hay que recifrar para usar el autenticador

# Combinación de Asociaciones de Seguridad (4)

**Estrategias de combinación que debe soportar una implementación de IPsec**




*Stallings – Cryptography & Network Security*