

# *Criptografía y Seguridad de Datos*

## **Seguridad IP - IPSec**

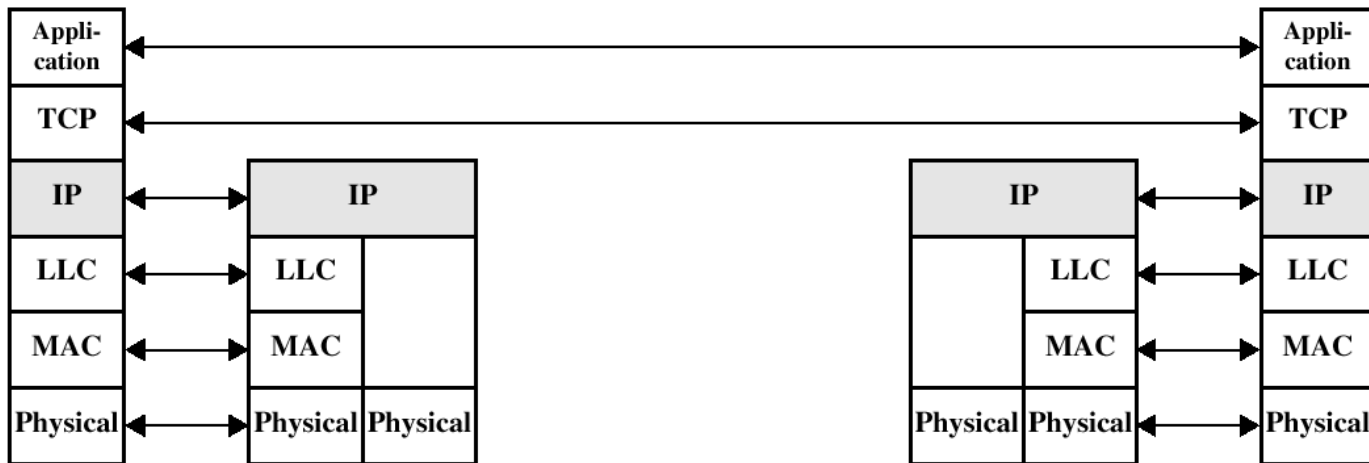
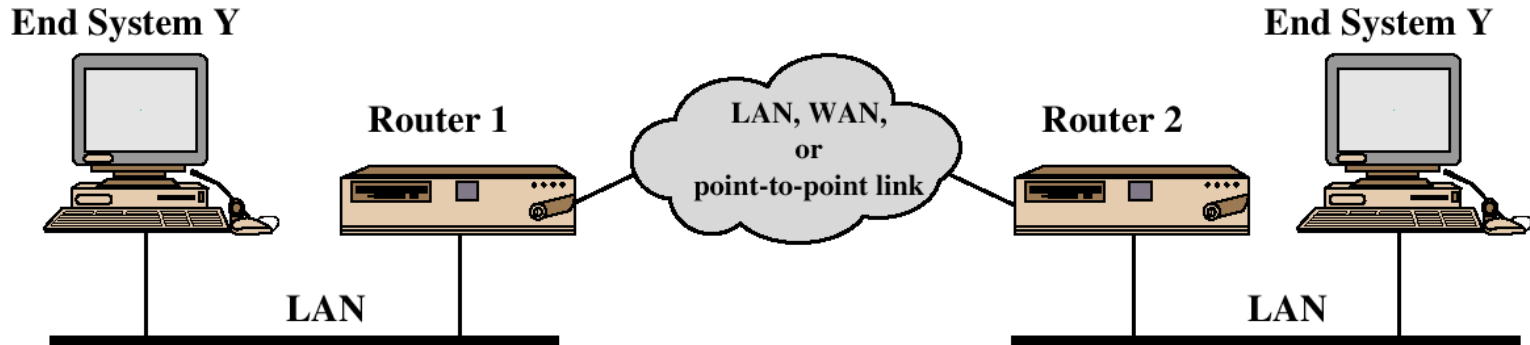
*Profs. Rodolfo Sumoza/Carlos Figueira, Universidad  
Simón Bolívar (figueira@usb.ve)*

*Basado en una presentación de Henric Johnson, Blekinge  
Institute of Technology, Sweden*

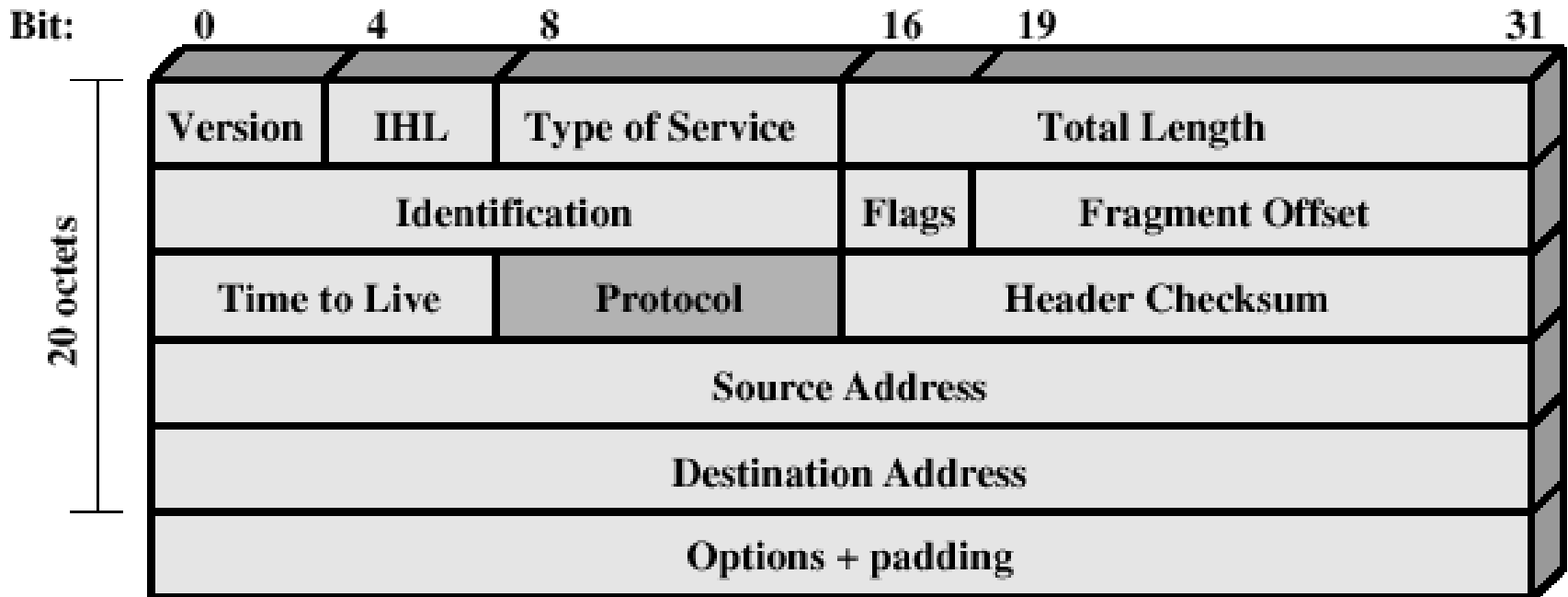
# Contenido

- Internetworking y Protocolos de Internet
- Seguridad IP - Generalidades
- Arquitectura de la Seguridad IP
- Encabezados de Autenticación (AH)
- Encapsulado de Carga Útil de Seguridad (ESP)
- Combinaciones de Asociaciones de Seguridad
- Gestión de Claves

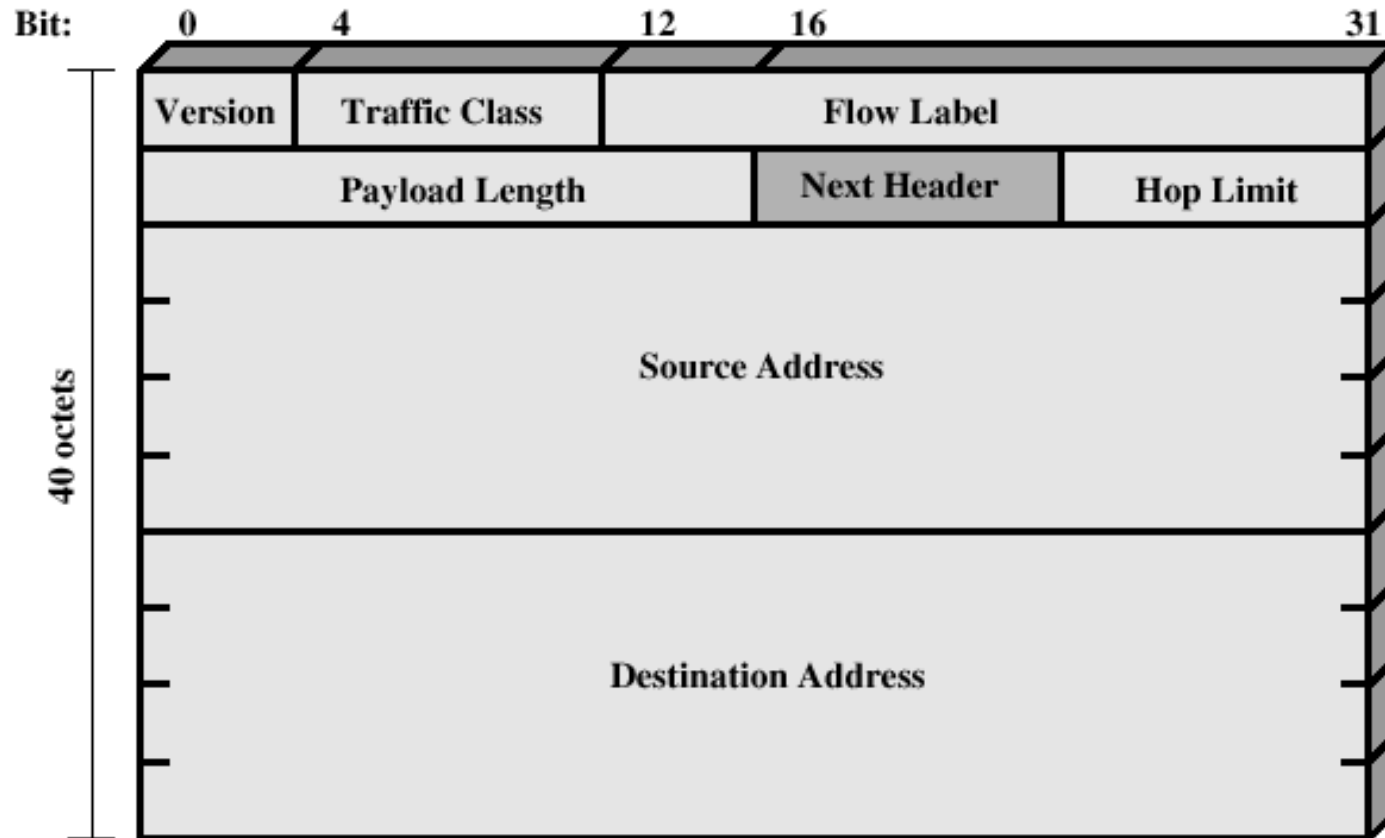
# Ejemplo TCP/IP



# Encabezado IPv4



# Encabezado IPv6



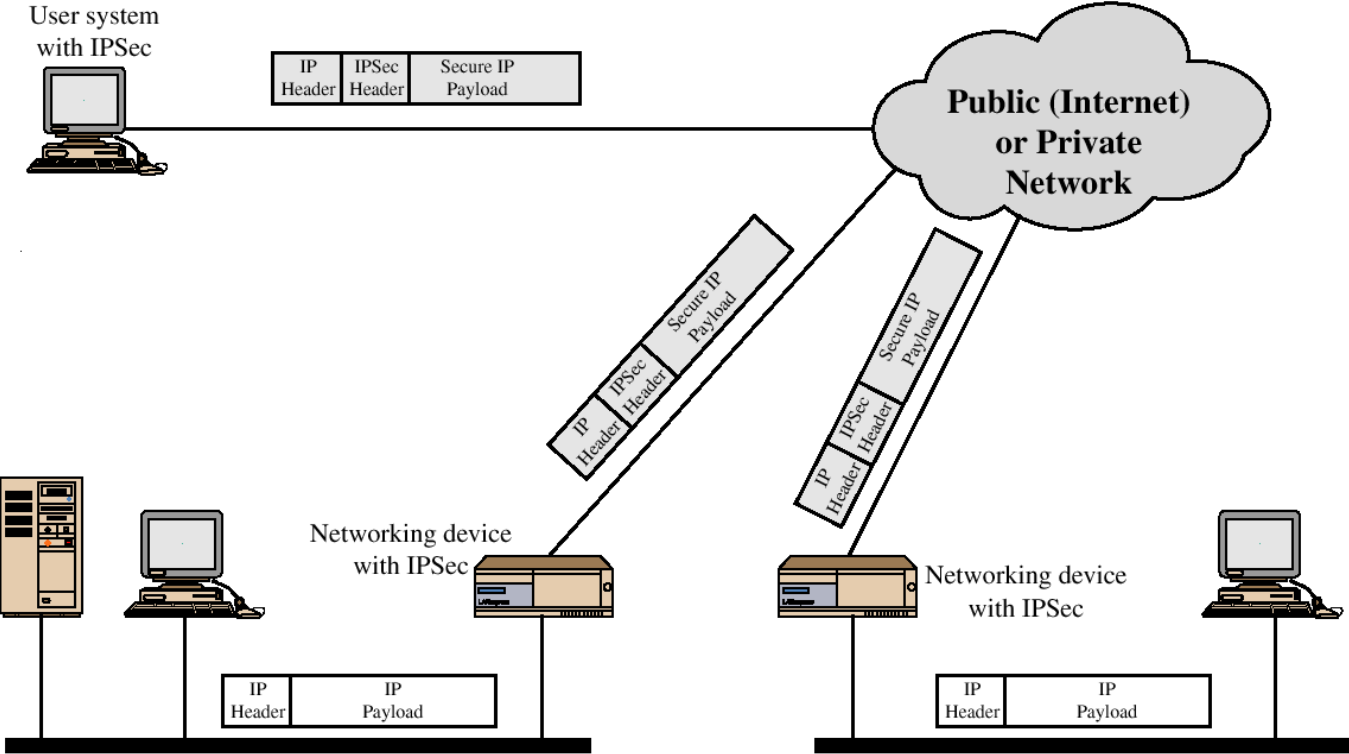
# IPSec

IPSec no es un protocolo simple, sino que provee un conjunto de algoritmos de seguridad más un contexto general que permite a un par de entidades utilizarlos para proveer la seguridad apropiada en sus comunicaciones.

# Aplicaciones de IPSec

- Seguridad a nivel de sucursales comerciales conectadas a través de Internet
- Acceso remoto seguro sobre Internet
- Establecimiento de la conectividad con socios en extranets e intranets
- Permite el comercio electrónico seguro

# Escenario de Seguridad IP



# Seguridad IP

- Beneficios de IPSec
  - Transparente para las aplicaciones sobre la capa de transporte (TCP, UDP)
  - Provee seguridad para los usuarios individuales
- IPSec puede asegurar que:
  - El anuncio de un encaminador o vecino viene desde un nodo autorizado
  - Un mensaje redirigido viene desde encamin. al cual el paquete original fue enviado
  - Una actualización de rutas no puede ser falsificada

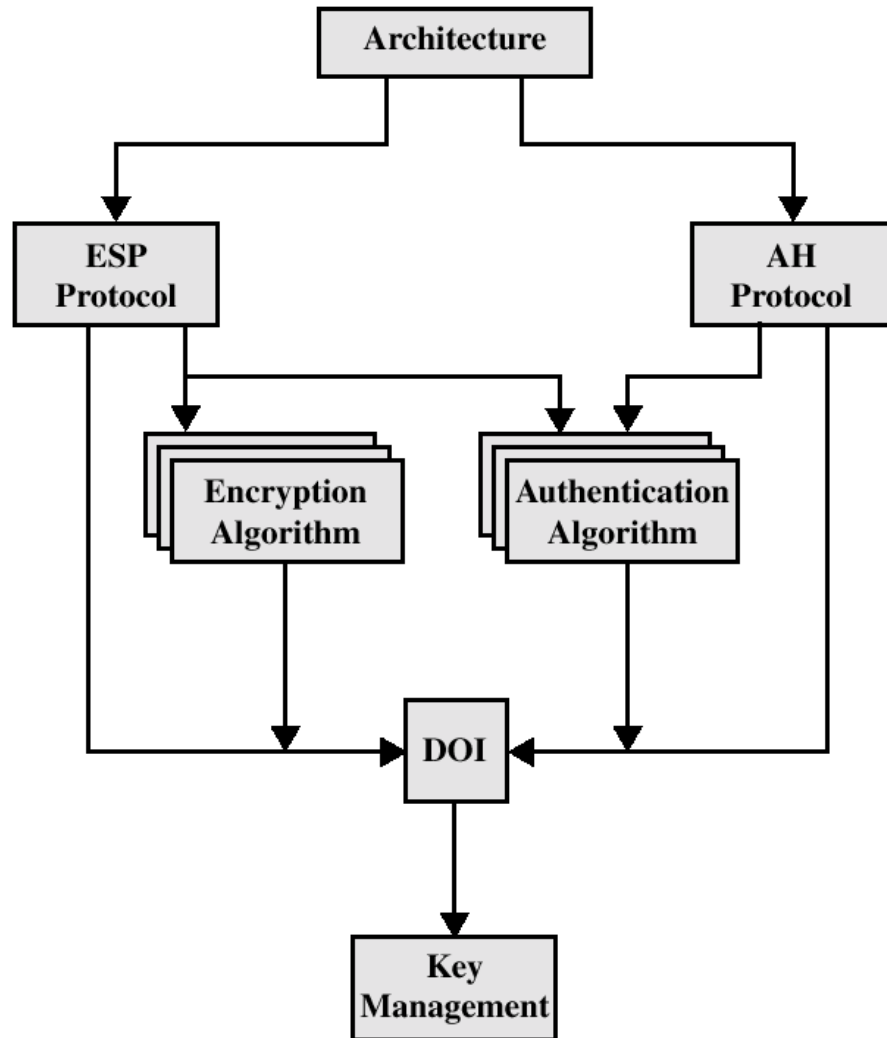
# IPSec: Arquitectura (1)

- Documentos IPSec (1998): sustituye versión original de 1995
  - RFC 2401: Descripción General de una arquitectura de seguridad
  - RFC 2402: Descripción de la extensión de autenticación de un paquete a IPv4 y IPv6
  - RFC 2406: Descripción de la extensión de cifrado de un paquete a IPv4 y IPv6
  - RFC 2408: Especificación de las capacidades de la gestión de claves

# IPsec: Arquitectura (2)

- Documentos IPSec (2005), extienden los anteriores
- RFC 4301-4309
- Incluye estándar para intercambio de claves

# IPSec: Documentos



# IPSec: Servicios

- Control de acceso
- Integridad
- Autenticación del Origen de los Datos
- Rechazo de repetición de paquetes
- Confidencialidad (cifrado)
- Confidencialidad limitada del flujo de tráfico

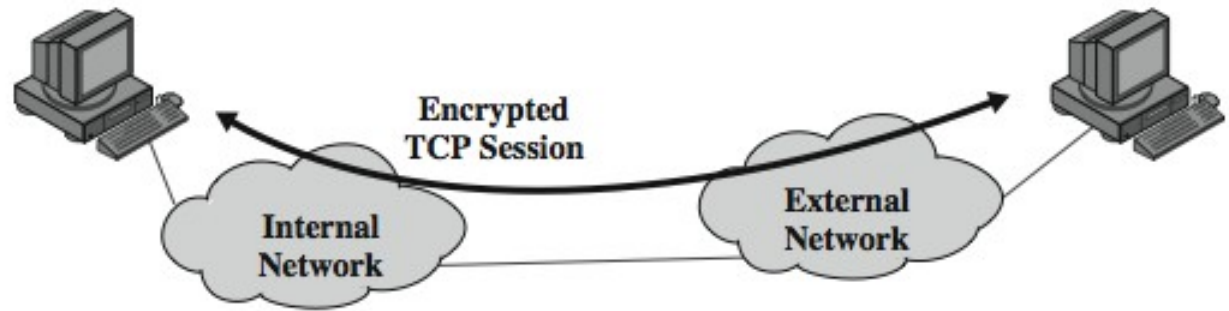
# Modo Transporte

- Agrega información al paquete IP original
- Para cifrar/autenticar campo de datos IP
- Vulnerable a análisis de tráfico pero eficiente
- Bueno para tráfico ESP extremo-extremo

# Modo Túnel

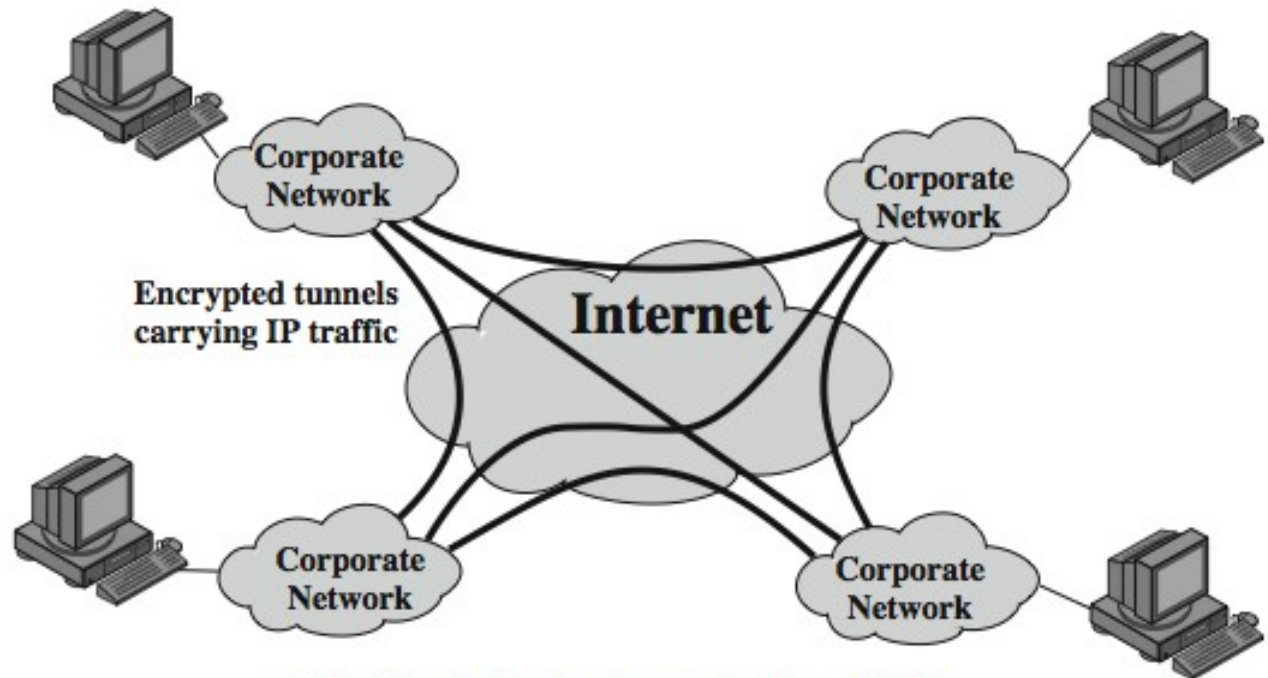
- Se crea un paquete IP nuevo que contiene al original
- Cifra paquete IP entero
- Nuevo encabezado en cada salto
- Enrutadores intermedios no pueden examinar encabezados IP internos
- Buenos para VPNs, seguridad pasarela-pasarela

# Modo Transporte



(a) Transport-level security

# Modo Túnel



(b) A virtual private network via Tunnel Mode

# Asociaciones de Seguridad (AS)

- Relación unidireccional entre un emisor y un receptor.
- Identificado por tres parámetros:
  - Índice de Parámetros de Seguridad (SPI)
  - Dirección IP de Destino
  - Identificador del Protocolo Seguridad (AH o ESP)

# Parámetros de las AS

- Contador de Secuencia
- Desbordamiento del Contador de Secuencia
- Ventana contra repeticiones
- Información AH y ESP
- Tiempo de vida
- Modo (transporte o túnel)

# Selectores de AS

- Son campos del prot. IP y de protocolos de capa superiores
- Se implementan como registros en la Base de Datos de Políticas de seguridad (SPD).
- Cada registro define un subconjunto de tráfico y una AS asociada.

# ...Selectores

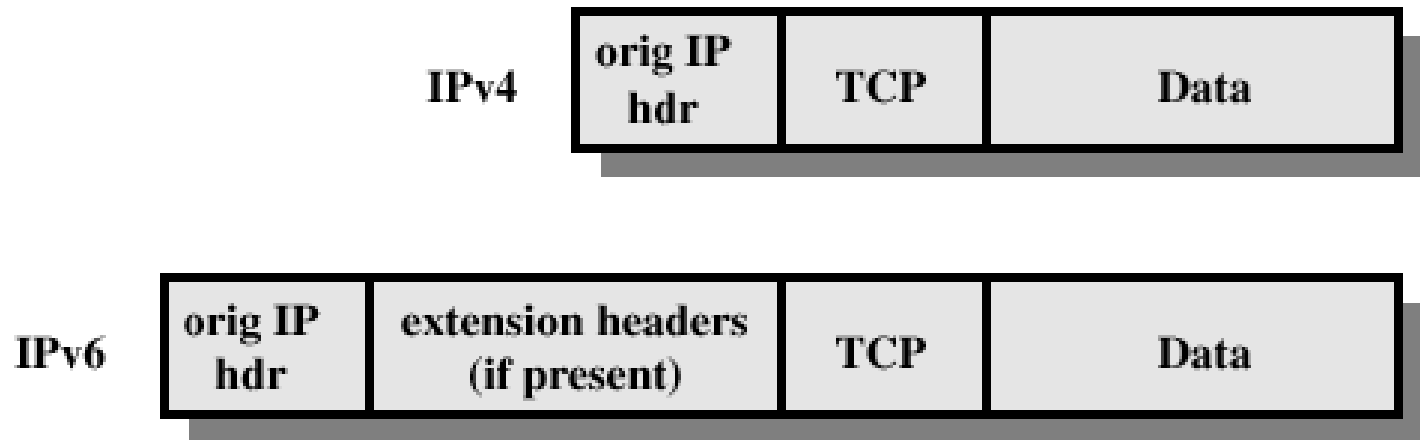
- Filtran el tráfico saliente
- Selectores: IP destino, IP fuente, ID de usuario, Nivel de confidencialidad, Protocolo de Capa de Transporte, Protocolo IPSec, Puertos fuente y destino, Clase IPv6, Etiqueta de Flujo IPv6, Tipo de Servicio IPv4 (TOS).

# BD Políticas de Seguridad

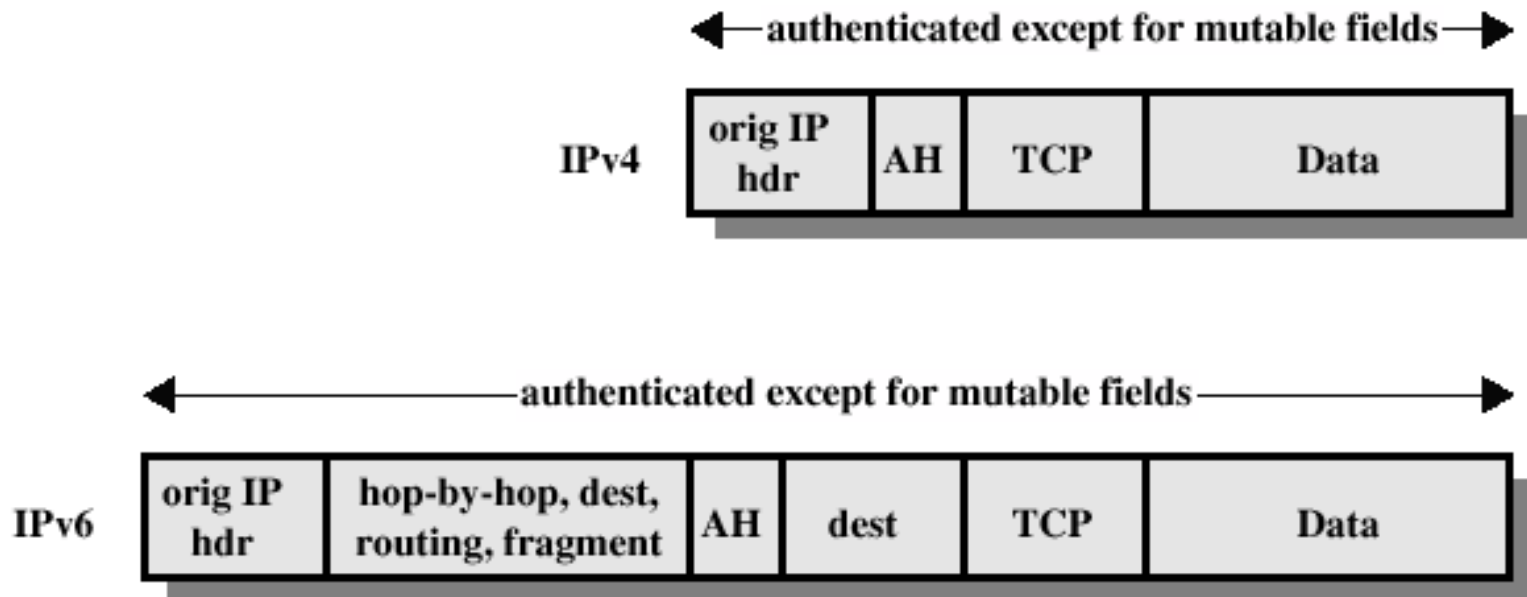
Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	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

	AS Modo Transporte	AS Modo Túnel
AH	Autentica la carga útil IP y selecciona porciones del encabezado IP y extensiones de encabezados IPv6	Autentica completo el paquete IP más porciones seleccionadas del encabezado IP externo
ESP	Cifra la carga útil IP y cualquier extensión de encabezado IPv6	Cifra todo el paquete IP
ESP con autenticación	Cifra carga útil IP y cualquier extensión de encabeza. IPv6. Autentica carga útil IP pero no encabezado IP	Cifra todo el paquete IP. Autentica todo el paquete IP.

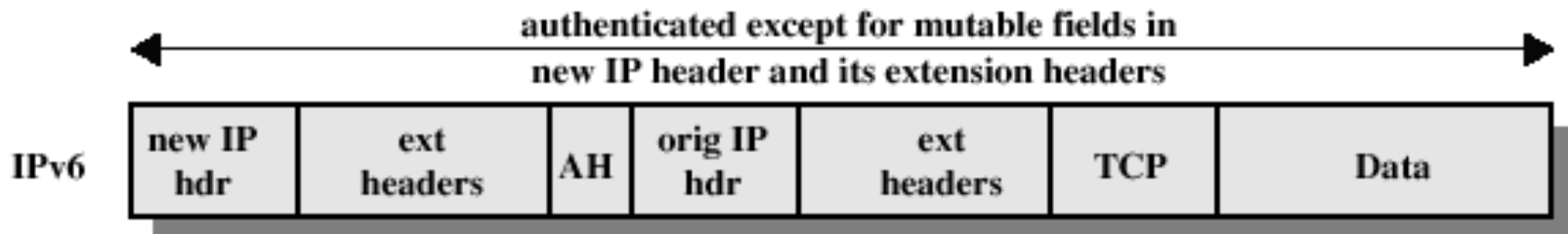
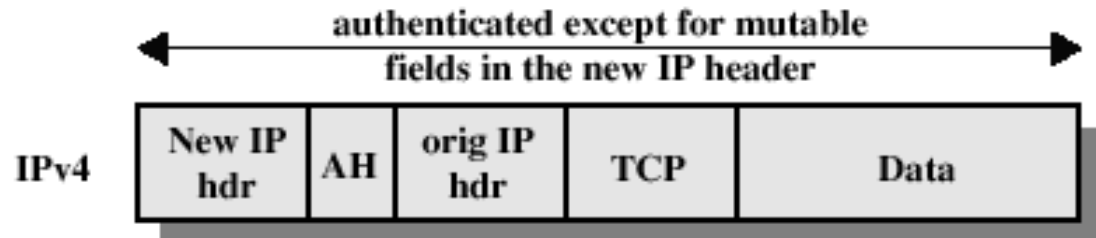
# Antes de aplicar el AH



# Modo Transporte (AH)



# Modo Túnel (AH)



# Encabezado de Autenticación AH

- Provee soporte para la integridad de los datos y la autenticación (código MAC) de paquetes IP.
- Protege contra ataques de repetición.

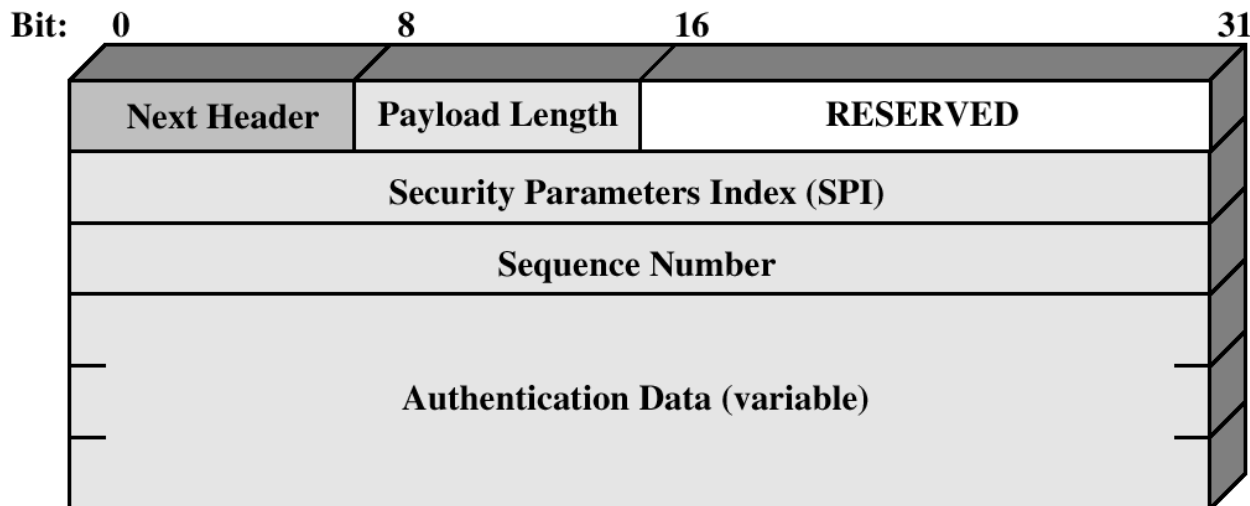
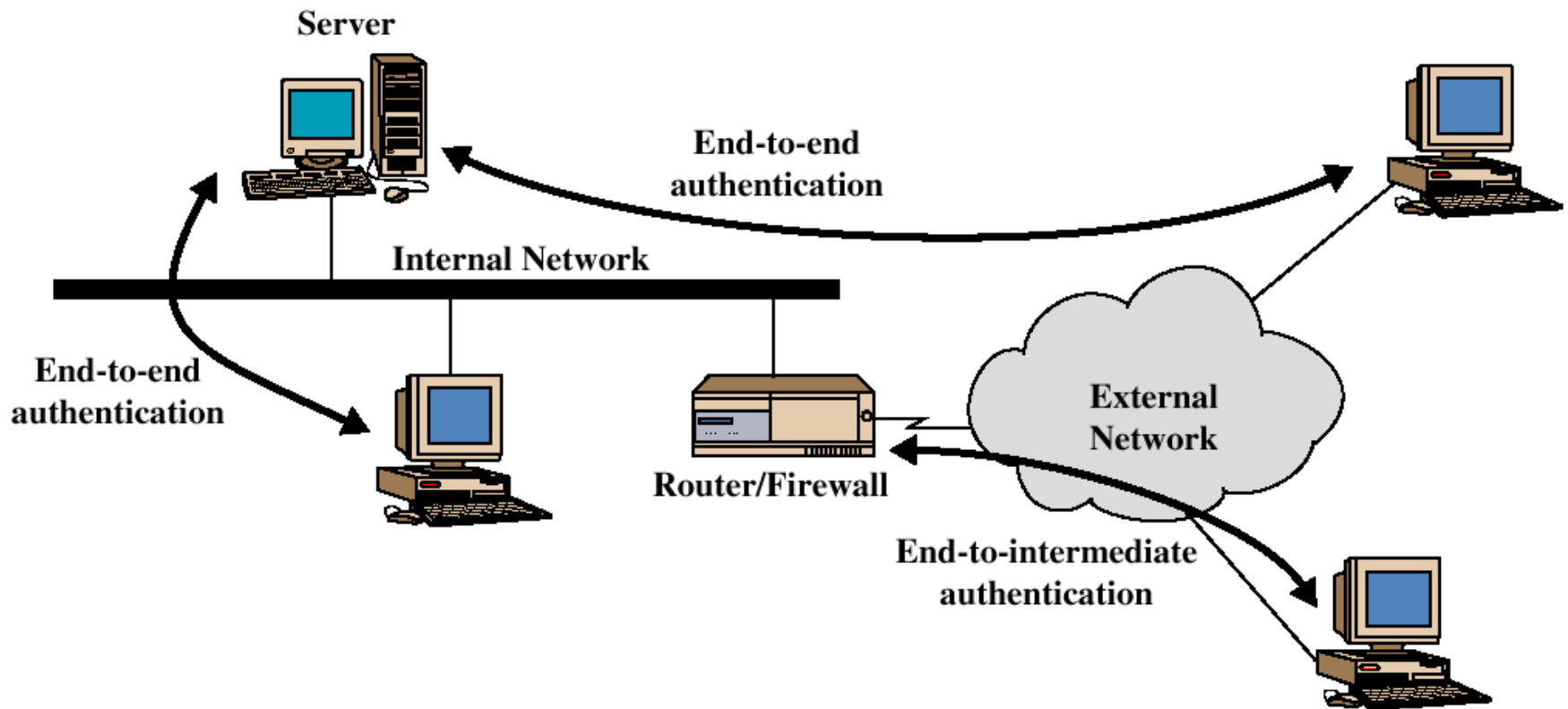


Figure 6.3 IPsec Authentication Header

# Autenticación Ext-a-Ext versus Ext-a-Intermedio



# Encapsulado de Seguridad de la carga útil (ESP)

- ESP provee servicios de confidencialidad

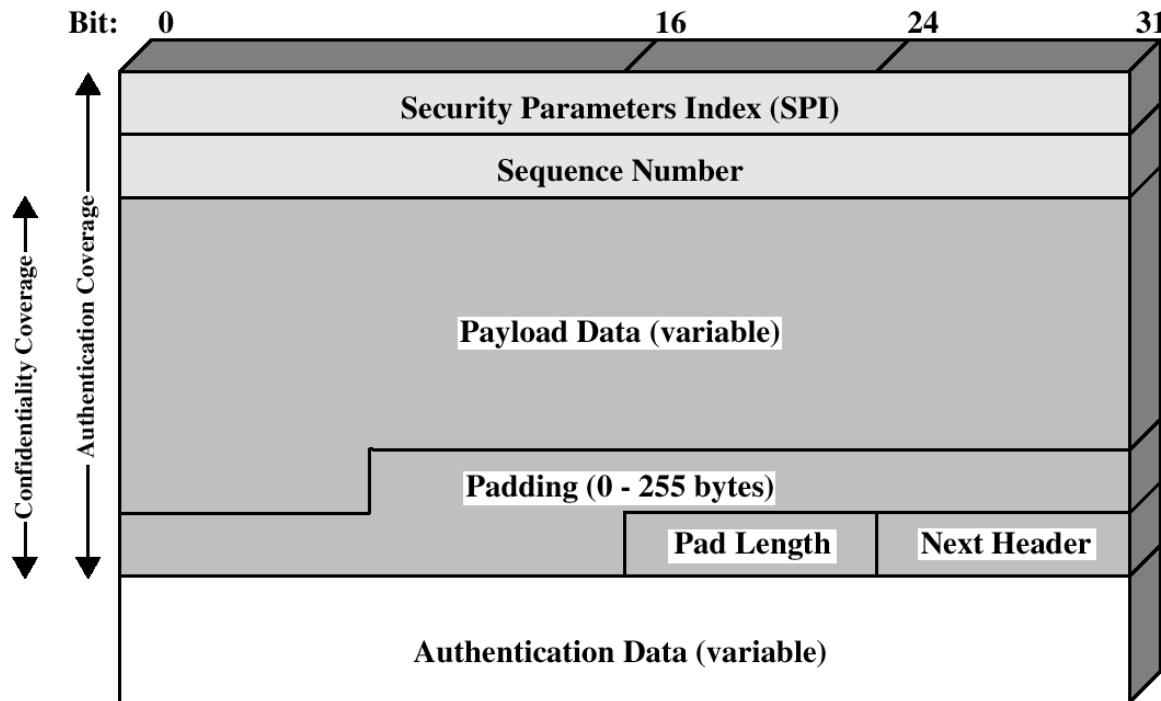
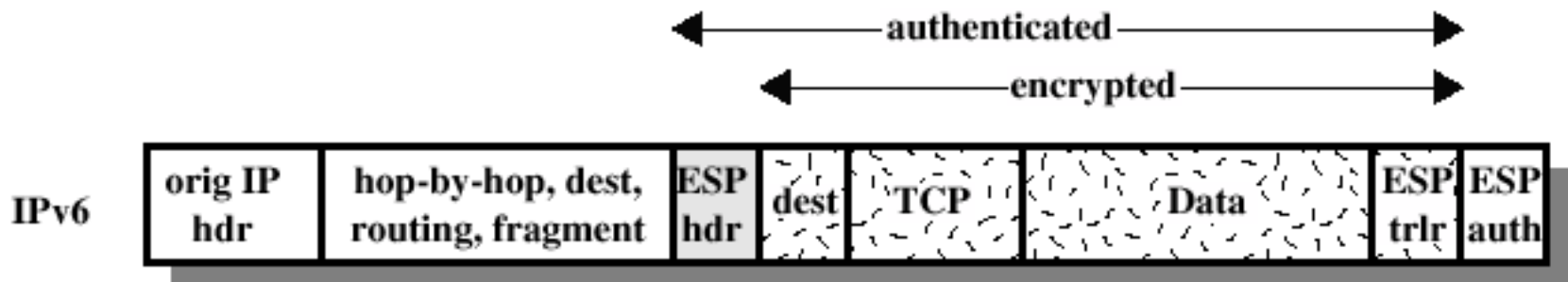
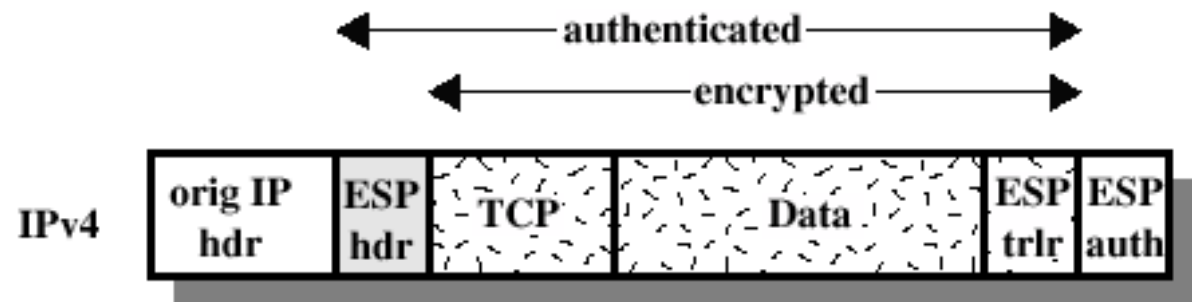


Figure 6.7 IPsec ESP Format

# Cifrado y Algoritmos de Autenticación

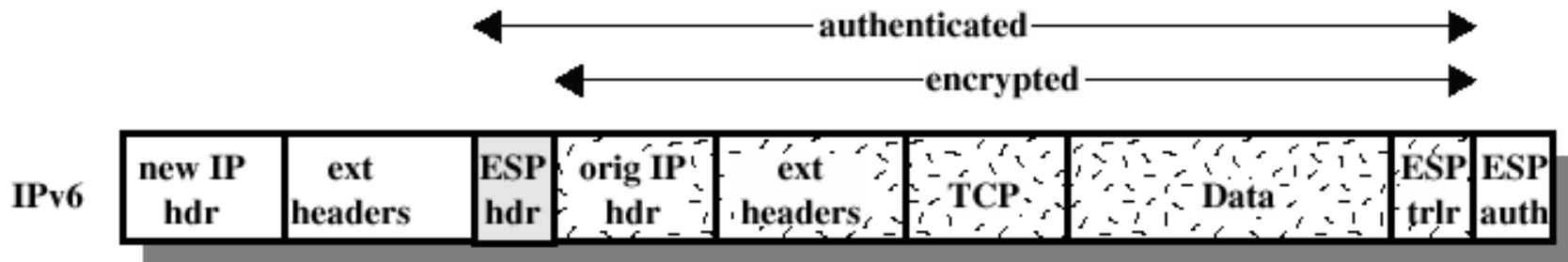
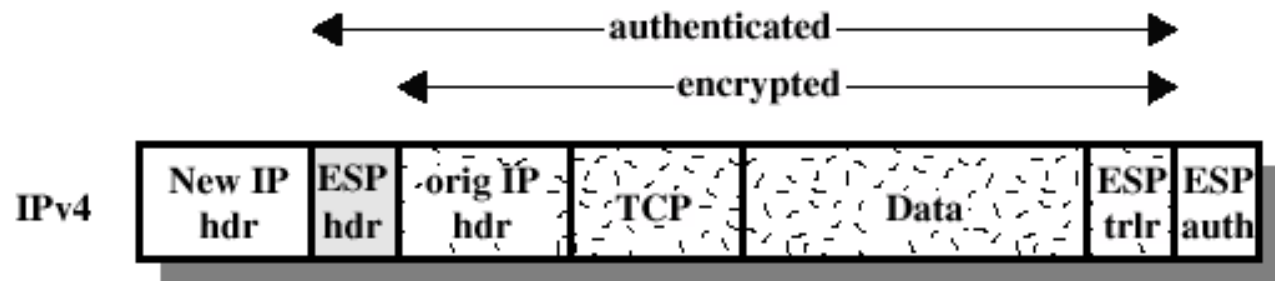
- RFC4308: conjuntos criptográficos para VPN
  - VPN-A para compatibilidad (3DES & HMAC)
    - VPN-B para las nuevas VPN con IPsecv3 e IKEv2 con AES
- RFC4869 define 4 conjuntos criptográficos compatibles con especificaciones NSA

# ESP Cifrado y Autenticación



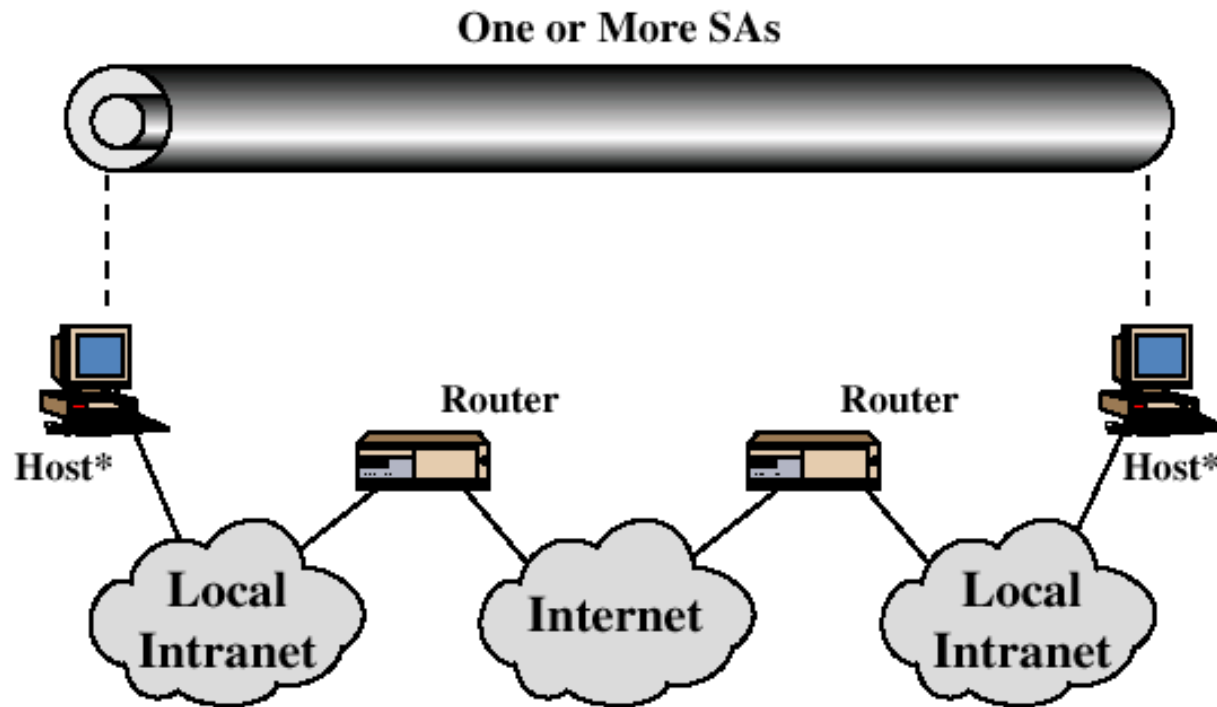
(a) Transport Mode

# ESP Cifrado y Autenticación



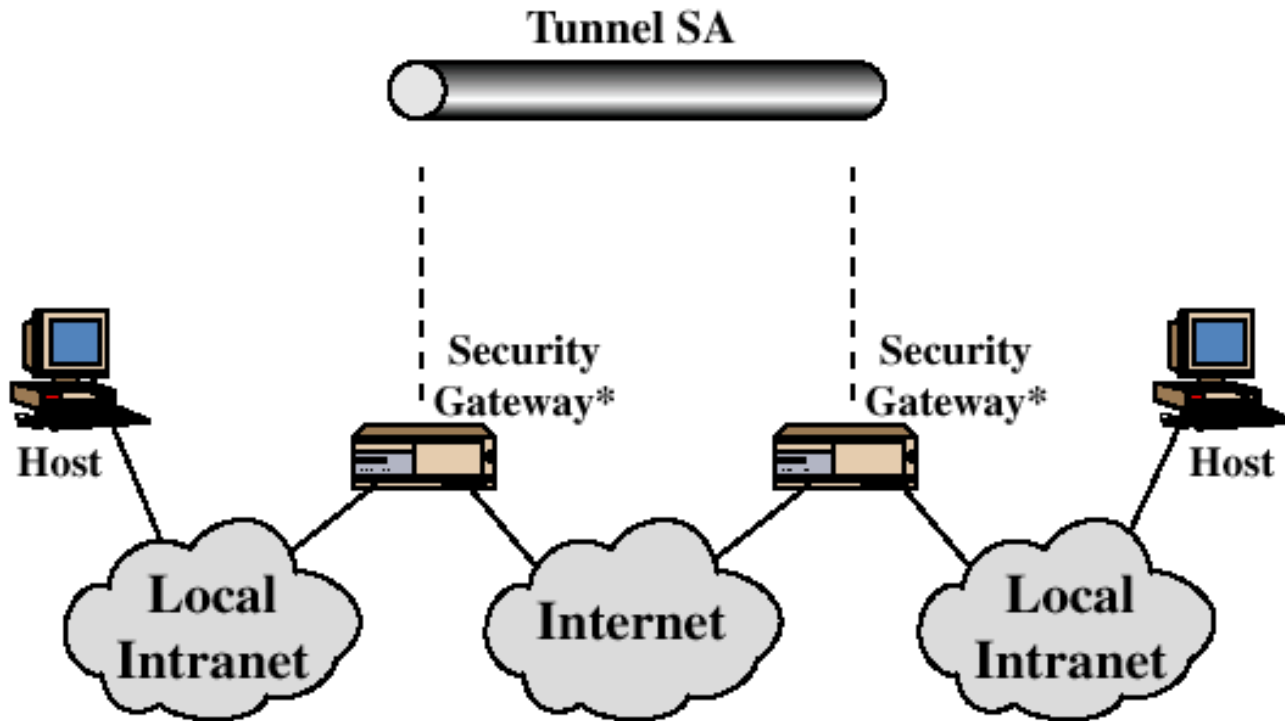
(b) Tunnel Mode

# Combinaciones de AS



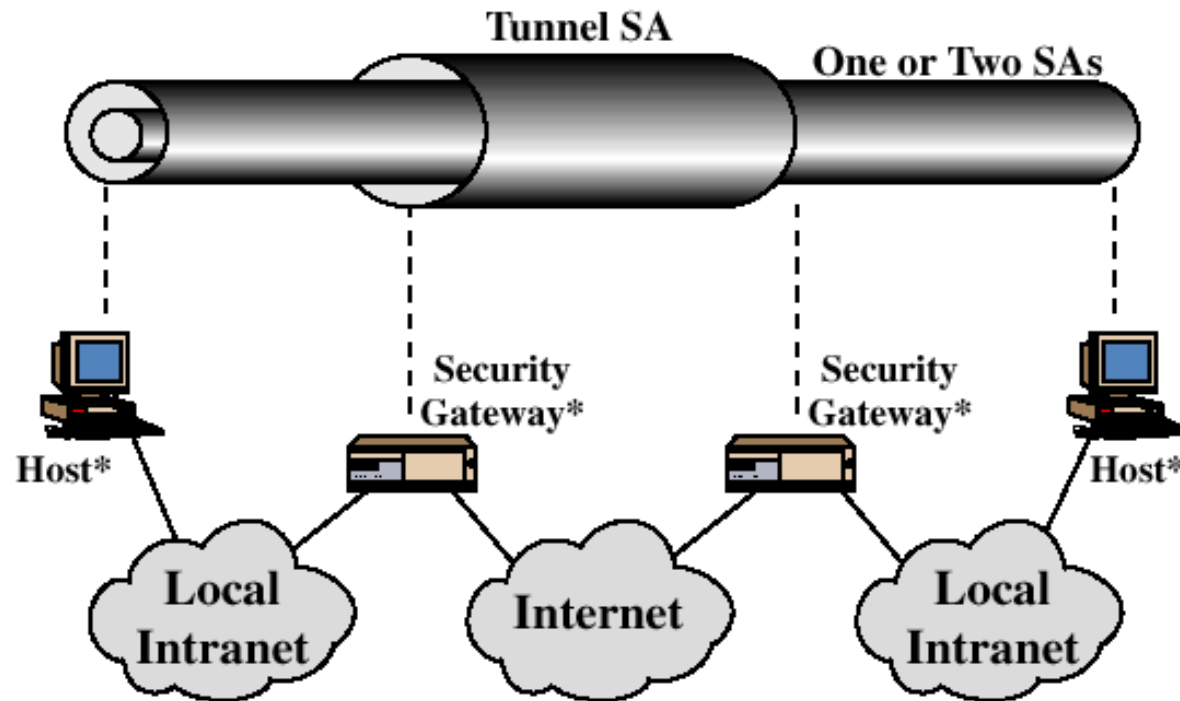
(a) Case 1

# Combinaciones de AS



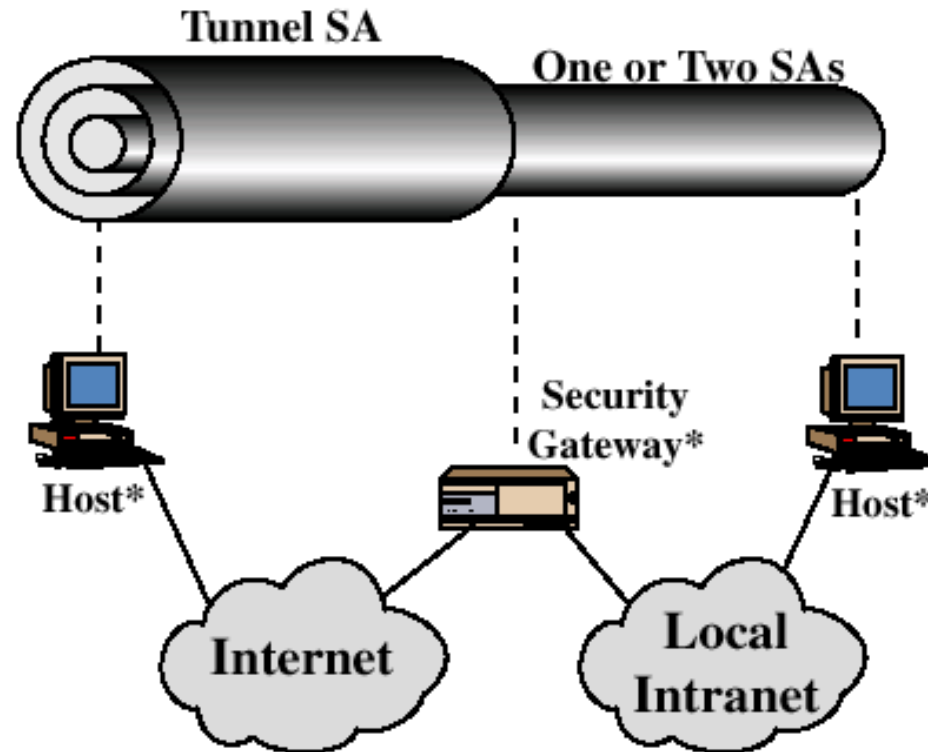
(b) Case 2

# Combinaciones de AS



(c) Case 3

# Combinaciones de AS



(d) Case 4

# Gestión de Claves

- Manual
- Automática
  - *RFC4306 (**Internet Key Exchange IKEv2**, 2005) definió estándar que unifica los RFC anteriores*
    - *Utiliza Internet Security Association and Key Management Protocol (ISAKMP) para establecer AS base (fase 1)*
    - *Fase 2 negocia AS's para IPsec*

# Implementaciones

- GNU/Linux (y OpenSwan) Demonio IKE en espacio usuario,
- Pila IPSec implementada en el kernel (versiones  $\geq 2.6$ )
- IKE negocia claves y se las pasa a IPSec

# **Anexo: ISAKMP**

# ISAKMP

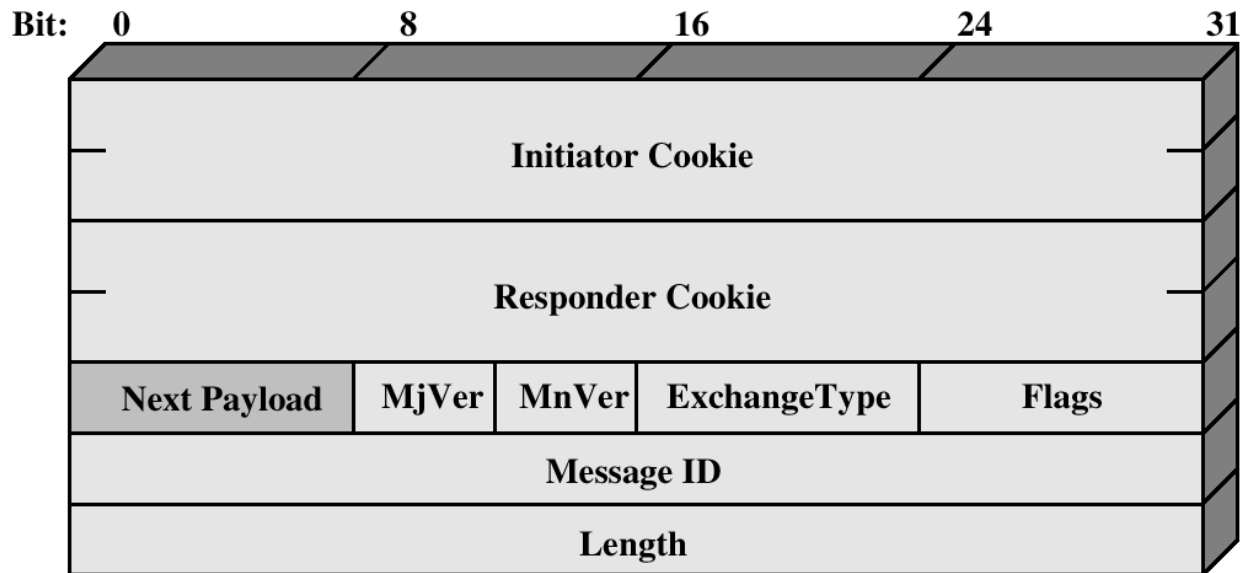
*(Internet Security Association and  
Key Management Protocol)*

- Define los procedimientos y formatos de paquetes para establecer, negociar, modificar y eliminar AS
- Define cargas útiles para intercambiar generación de claves y datos de autenticación

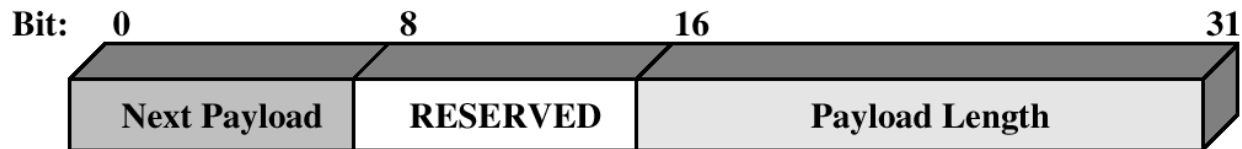
# ISAKMP

- Tipos de carga útil:
  - De propuesta.(negociación AS)
  - De transformación (ej. 3DES para ESP)
  - Intercambio de claves (ej. Oakley, RSA)
  - De identificación (ej. IP)
  - Del Certificado
  - Hash, de firma, nonce, notificación,

# ISAKMP



(a) ISAKMP Header



(b) Generic Payload Header

Figure 6.12 ISAKMP Formats

# **Campos (*encabezado*) ISAKMP**

- Cookie iniciador (64 bits): entidad que inicia establecimiento, notificación o eliminación de AS
- Próxima carga útil: tipo de la 1ra carga
- Versión mayor, menor
- Indicadores: opciones para este intercambio ISAKMP (cifrado y commit)

# ISAKMP

- Intercambio de Mensajes
  - Base: incluye intercambio de claves y material para autenticación
  - Protección de Identidad
  - Sólo autenticación
  - Agresivo: reduce # de intercambios