Grupo de Seguridad Informática

Fundamentos de la Seguridad Informática

Seguridad en Redes

Mecanismos de mitigación

Seguridad IP (IPSec)

Introducción

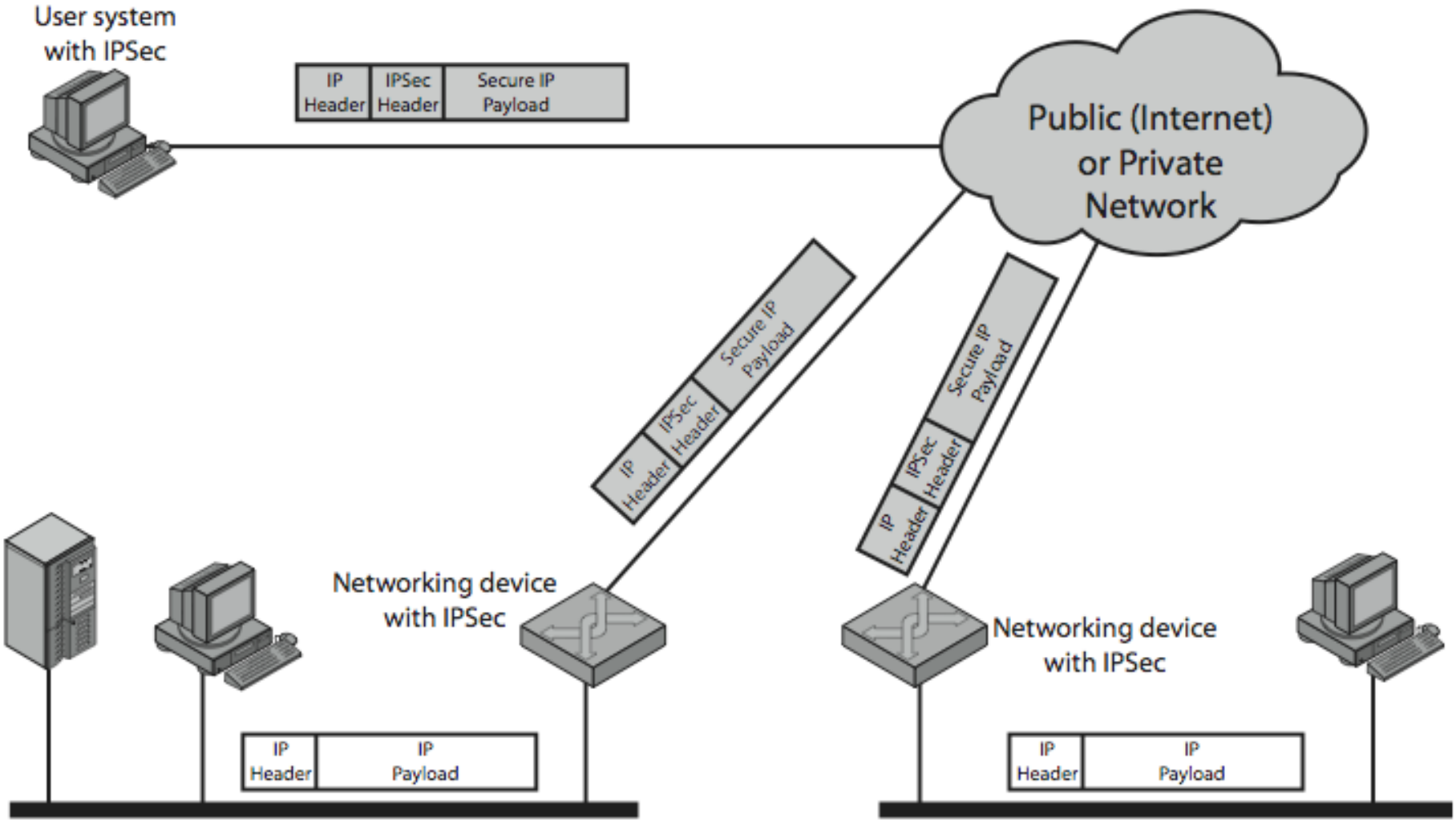
- IP es un protocolo de mejor esfuerzo, sin ninguna previsión respecto a la seguridad
- IPSec (IP Security) agrega previsiones para lograr confidencialidad, autenticación, control de integridad
- Agregar seguridad en capa 3 permite asegurar aplicaciones sin modificarlas
- Su uso más común hoy en día es para la realización de redes privadas virtuales (VPN)

IPsec

- rfc 4301 definición de arquitectura de seguridad de IPsec (1998, revisado en 2005)
- rfc 6071, IPsec and IKE document roadmap
- Opcional para IPv4, obligatorio para IPv6
  - Obligatorio implementarlo, no usarlo :)
- Provee 2 mecanismos (protocolos) de seguridad
  - Authentication Header (**AH**) rfc 4302
  - Encapsulating Security Payload (**ESP**) rfc 4303

Uso típico de IPSec

(Stallings. Criptography and network security. Fig. 16.1)



Servicios de IPSec

- Control de acceso
- Integridad
- Autenticación de origen
- Rechazo de paquetes replay
- Confidencialidad
- Confidencialidad limitada de flujo de tráfico

Asociaciones de seguridad (SA)

- Define en una conexión IPsec una relación unidireccional entre emisor y receptor.
- Es el estado que deben compartir los hosts para una comunicación unidireccional
- Típicamente se crean en pares
- Definido por:
  - SPI (Security Parameters Index)
  - IP (origen y) destino
  - Identificador del protocolo de seguridad AH (51) o ESP (50)

Asociaciones de Seguridad (SA)

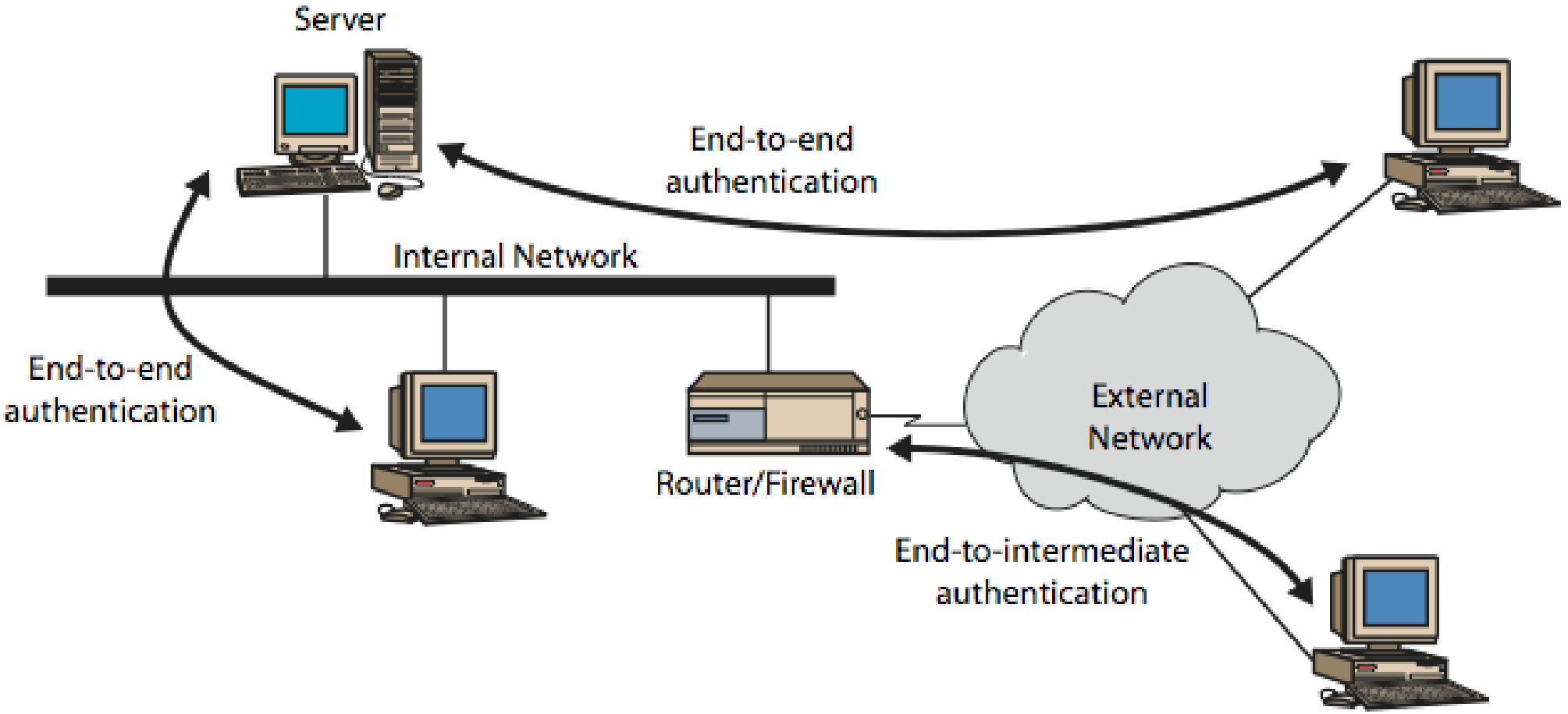
- La SA del emisor tiene asociado los parámetros necesarios para la comunicación:
  - Número de Secuencia (32 bit)
  - Datos criptográficos (algoritmos, claves, duración de las claves, vectores de inicialización)
  - Modo (túnel o transporte)
  - Maximun Transmission Unit (MTU)
- Cada equipo tiene una base de datos de SA (**SAD**)
- El SPI viaja en el encabezado AH o ESP
- Vamos a poder tener SA anidadas (ver ejemplo)

Modos de funcionamiento

- Modo transporte
  - Pensado para encriptación punta a punta
  - Encripta el contenido y autentica todo el paquete
- Modo túnel
  - Pensado para encriptación entre equipos intermedios
  - El paquete a proteger se encapsula completo dentro de otro paquete IP
  - Encripta y autentica todo el paquete original

Modo túnel y modo transporte

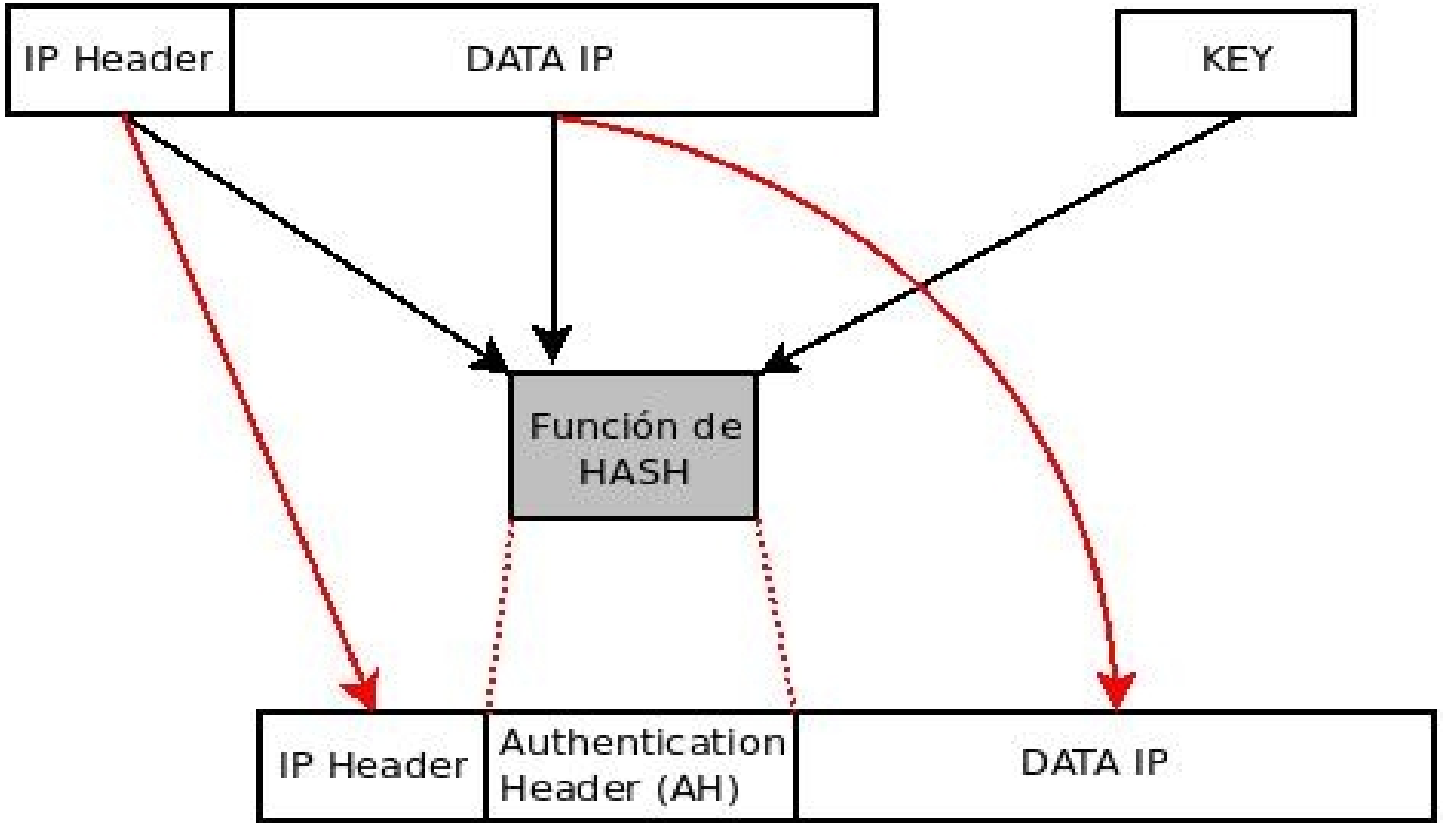
(Stallings. Cryptography and network security. Fig. 16.5)



AH (Authentication Header)

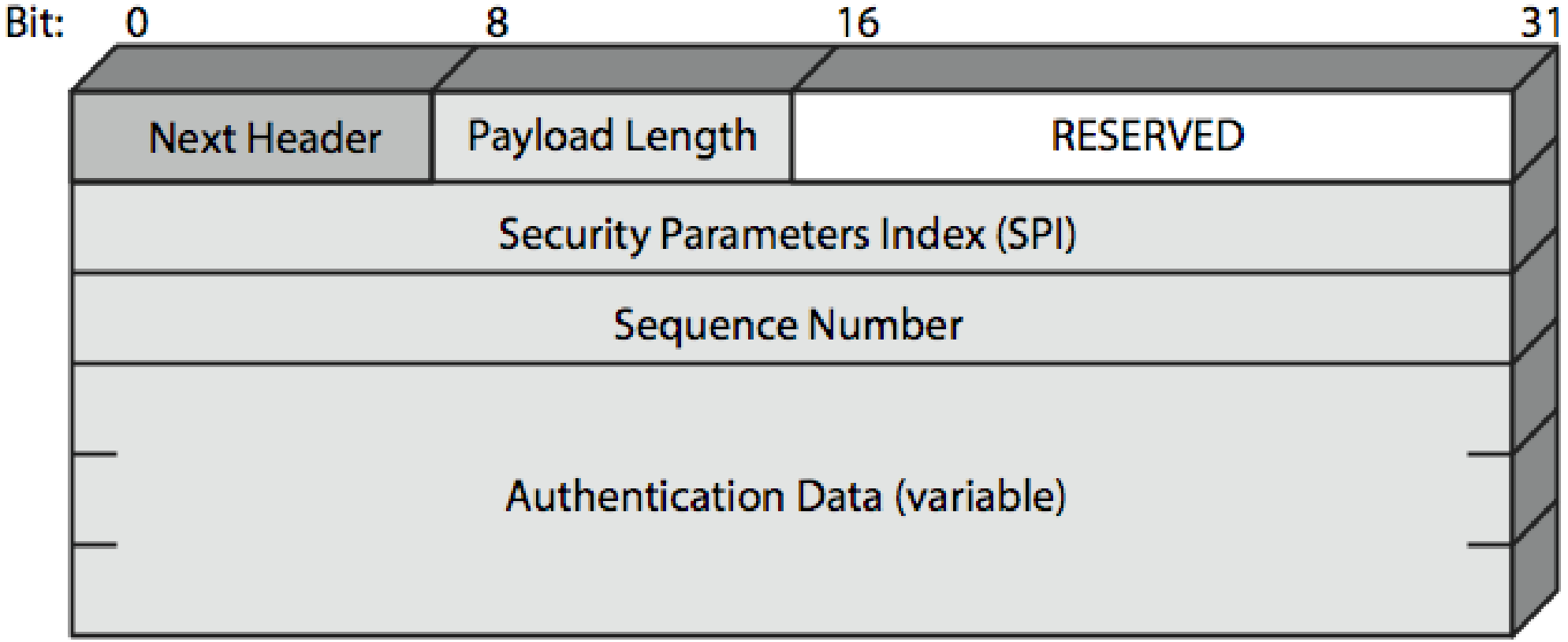
- Provee solo **integridad** y **autenticación** de paquetes IP, no confidencialidad
- Se basa en el uso de un código de autenticación de mensaje (MAC)
  - HMAC-MD5-96 or HMAC-SHA-1-96
  - Emisor y receptor deben compartir una clave secreta

Authentication Header



Atención: La función de HASH (HMAC) se calcula solo sobre aquellos campos del “IP Header” que no se modifican en tránsito (inmutables)

Formato del encabezado AH

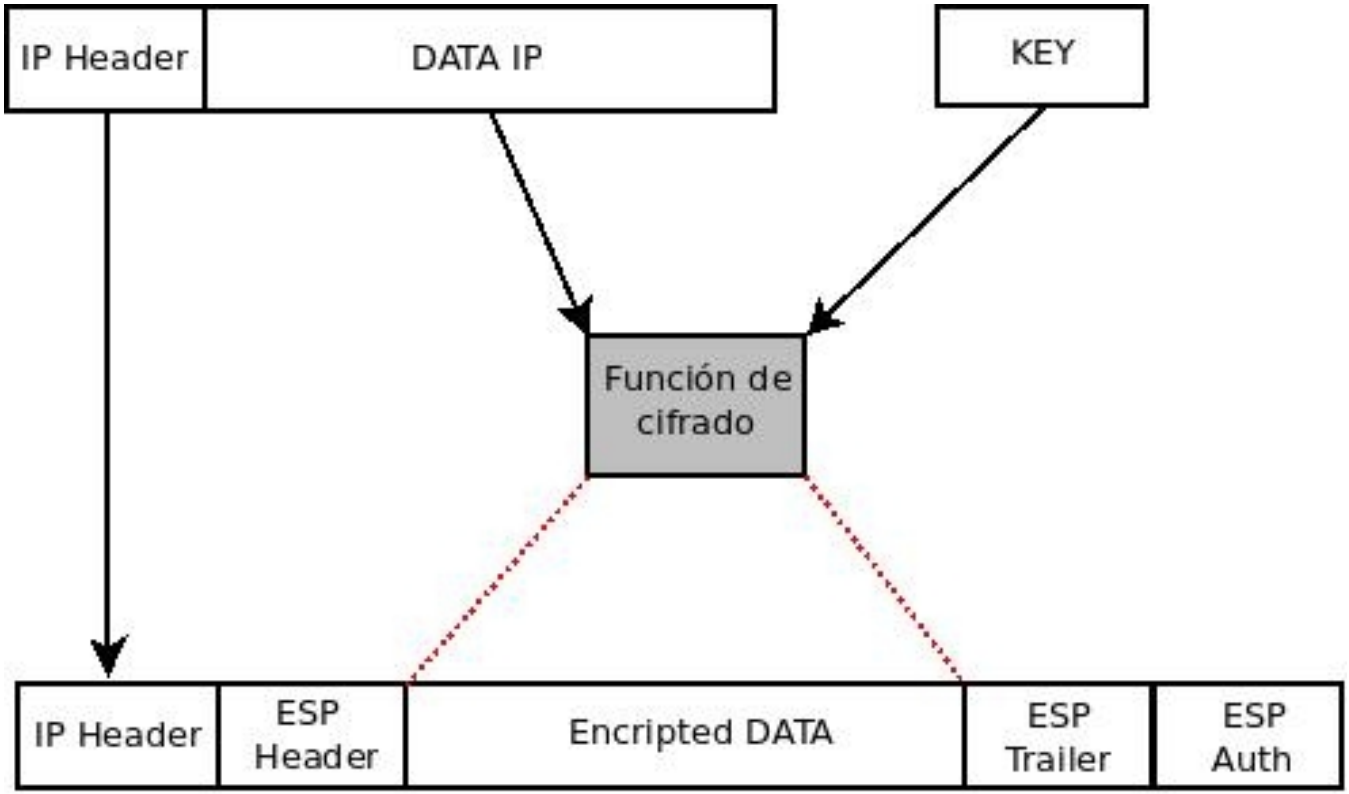


(Stallings. Criptography and network security. Fig. 16.3)

ESP (Encapsulating Security Payload)

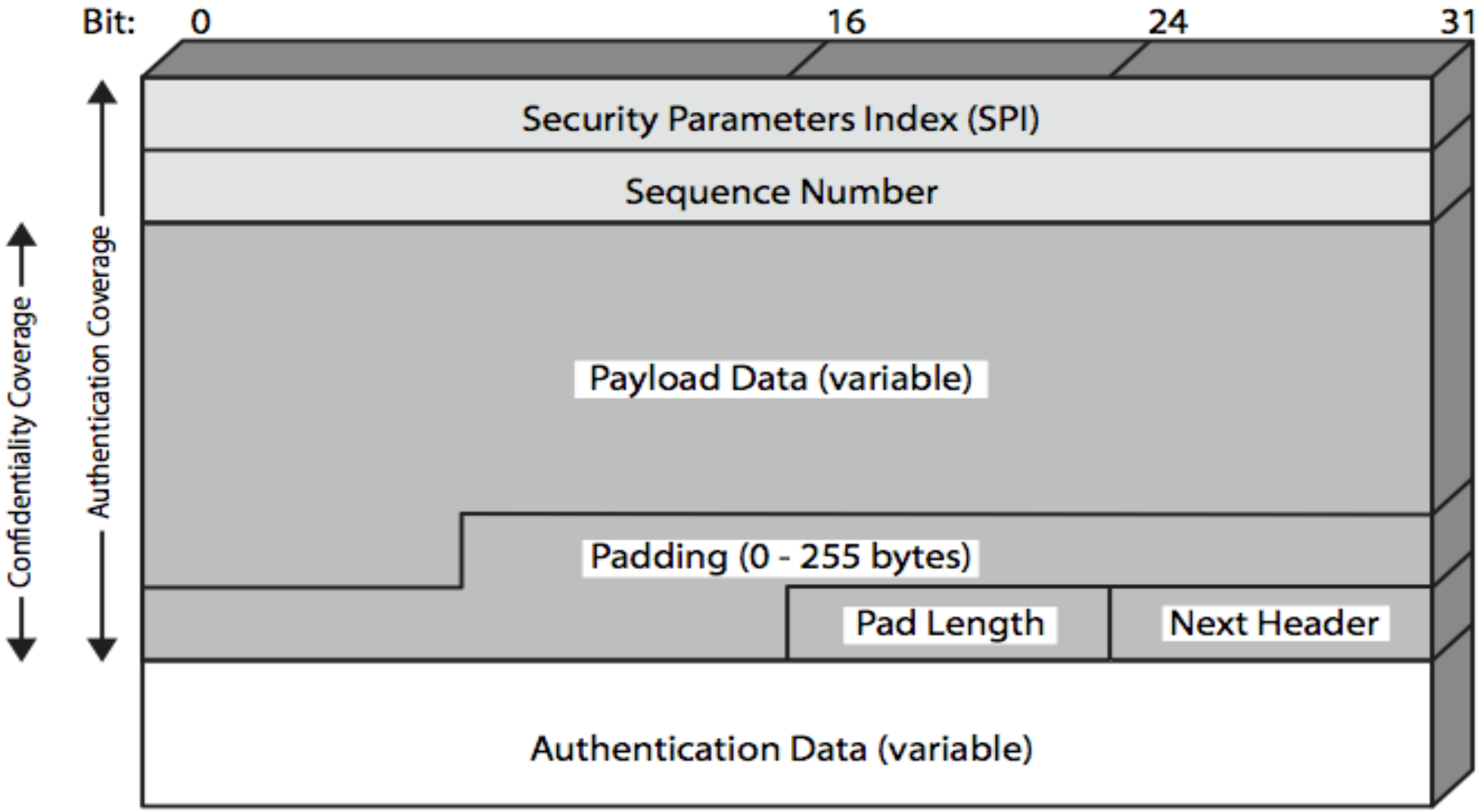
- Confidencialidad
- (Opcionalmente) los mismos servicios de autenticación que AH
- Soporta varios algoritmos de encriptación:
  - DES, DES triple, AES, RC5, IDEA, etc
  - CBC y otros modos
  - Relleno, para llenar el bloque requerido por el protocolo y para dificultar el análisis de tráfico

Encription Header

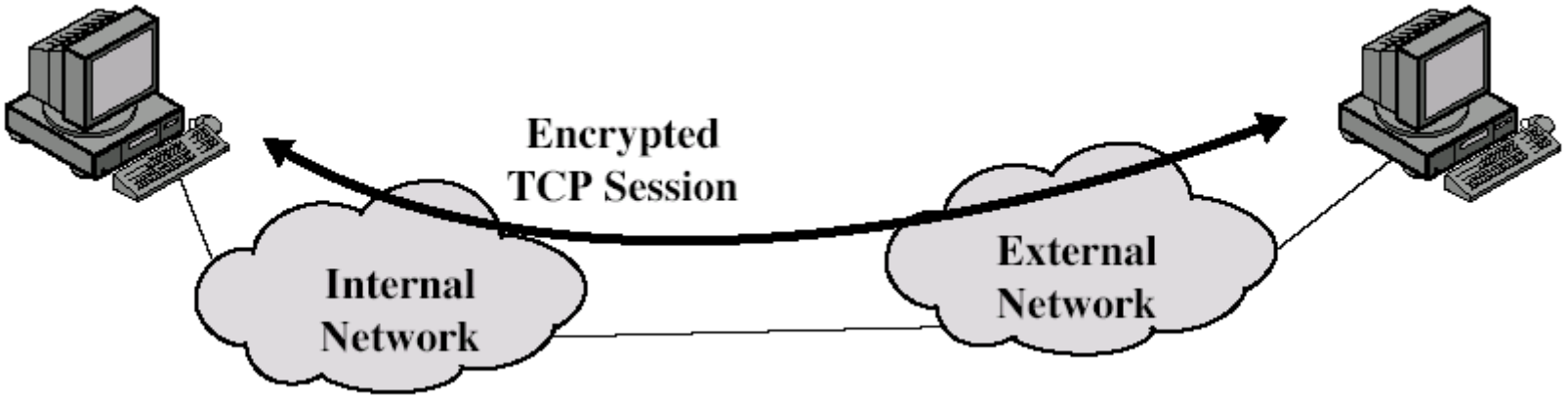


Nota: ESP AUTH **no** se calcula igual que en el protocolo AH
No toma en cuenta el encabezado IP en la función MAC

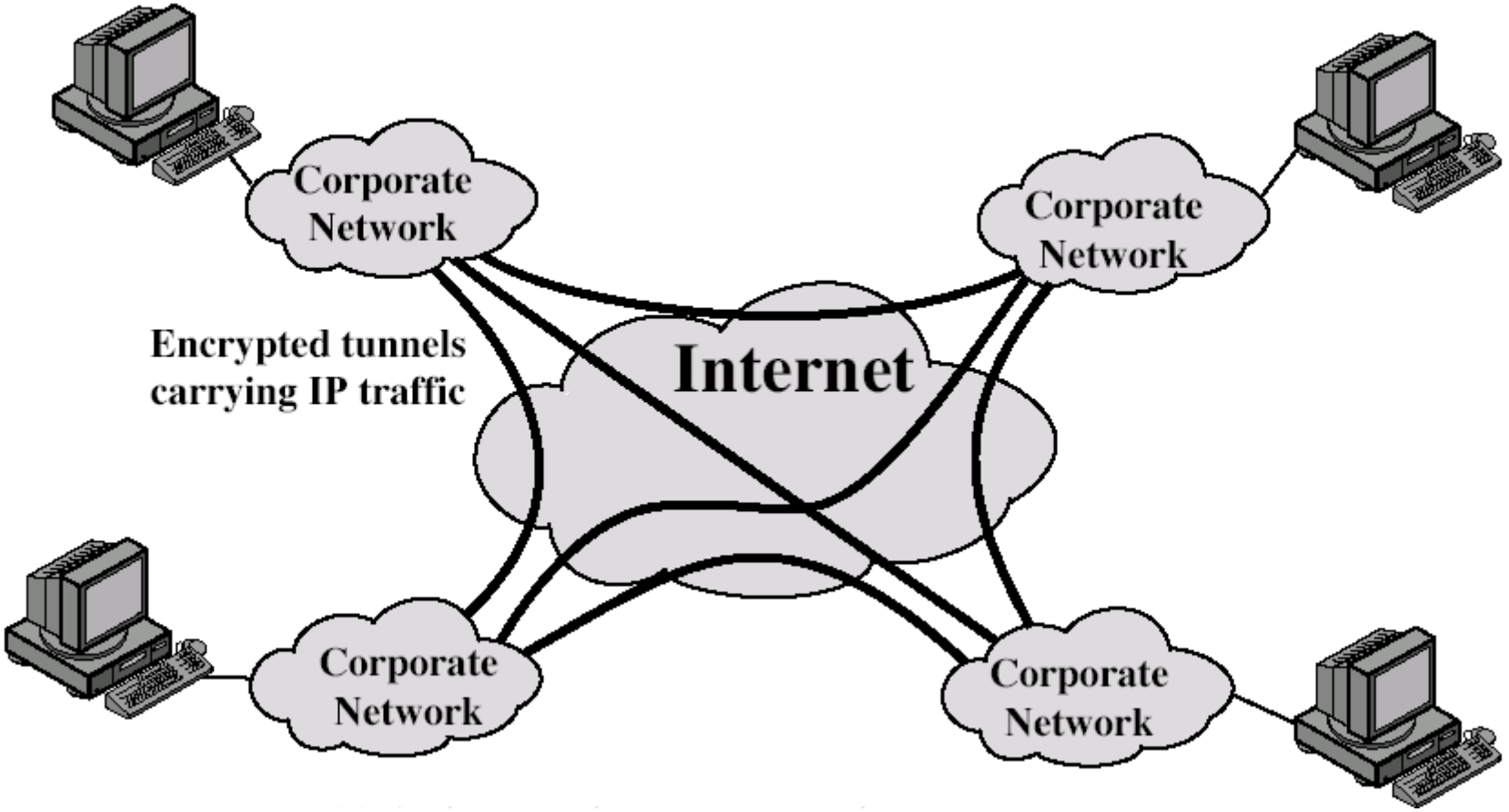
ESP


Bit:
0
16
24
31
Security Parameters Index (SPI)
Sequence Number
Payload Data (variable)
Padding (0 - 255 bytes)
Pad Length
Next Header
Authentication Data (variable)
Authentication Coverage
Confidentiality Coverage

Uso en modo transporte

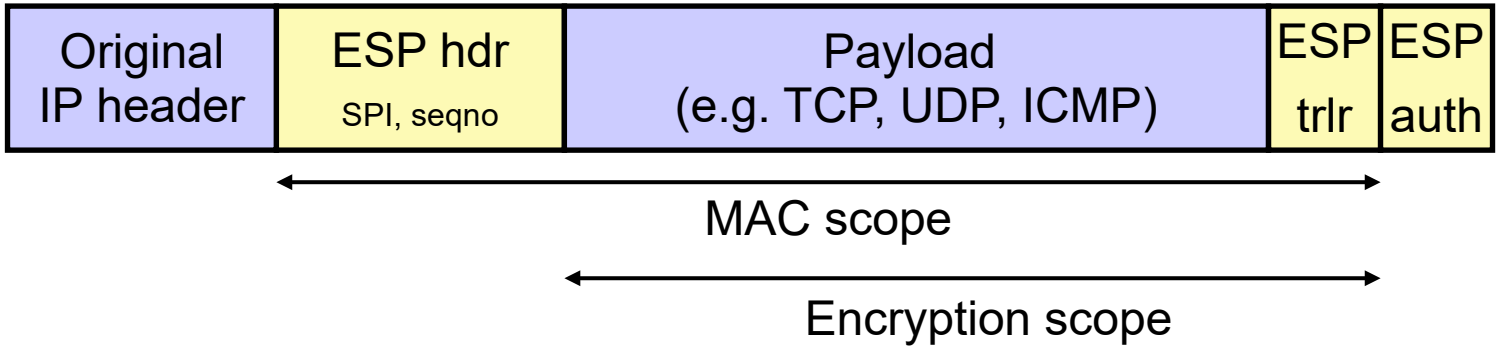


Uso en modo túnel

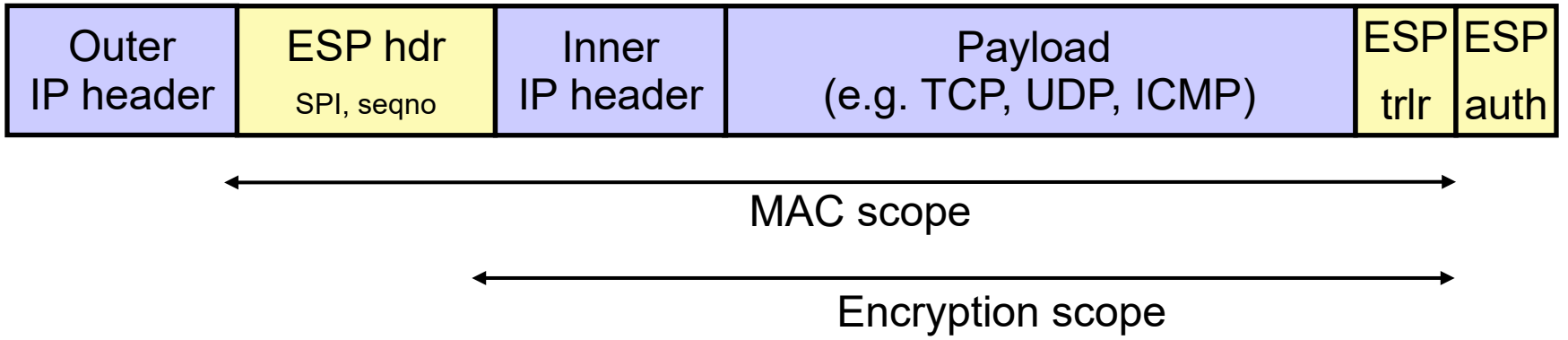


Transporte & Tunnel

ESP in transport mode:



ESP in tunnel mode:



IPSec Key Management

- IPsec necesita una gran cantidad de claves simétricas:
  - Una clave por cada SA.
  - Distintas SA para cada combinación de:
    {ESP,AH} x {tunnel,transport} x {sender, receiver}
- Soluciones:
  - Configurar manualmente las claves y SA
  - IKE: Internet Key Exchange [RFC 2409]
  - Oakley / ISAKMP

Internet Key Exchange (IKE)

- Autenticación de entidades y generación de una clave compartida (usada para generar las otras claves)
- Negociación de algoritmos
- 2 fases
  - Fase 1: Establecimiento de un SA inicial, autenticación de entidades, intercambio de claves
  - Autenticación basada en firmas y claves compartidas, o en criptografía de clave pública
  - Fase 2: Se negocian SAs para uso general

Políticas de IPSec

- Indican el procesamiento de seguridad que debe aplicarse a un paquete IP
- Puede seleccionarse por
  - Direcciones IP de origen y/o destino (rangos, subredes)
  - Protocolo de transporte
  - Puertos de capa de transporte
  - etc.

IPSec y filtrado

- IKE: UDP puerto 500
- AH: IP protocolo 51
- ESP: IP protocolo 50

- ¿Qué pasa con los firewalls centralizados si se populariza la encriptación extremo a extremo?

Bibliografía y referencias

- **R. Anderson**, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2001.
- **D. Gollman**, *Computer Security*, Wiley, 2006.
- **W. Stallings,** *Cryptography and Network Security. 4ta. ed.* Prentice Hall, 2005