Capítulo 8, Sección 8.6: IPsec

Material basado en el Texto:

Computer Networking: A Top Down Approach Featuring the Internet, Jim Kurose, Keith Ross.

Capítulo 8 contenidos

8.1 ¿Qué es la seguridad en la red?

8.2 Principios de criptografía

8.3 Integridad de mensajes

8.4 Dando seguridad a e-mail

8.5 Conexiones TCP seguras: SSL

8.6 Seguridad en capa de Red: IPsec

8.7 Seguridad en redes locales inalámbricas

8.8 Cortafuegos y Sistemas de detección de intrusión (IDS)

¿Qué es confidencialidad en la capa de red ?

Entre la capa de red de dos nodos:

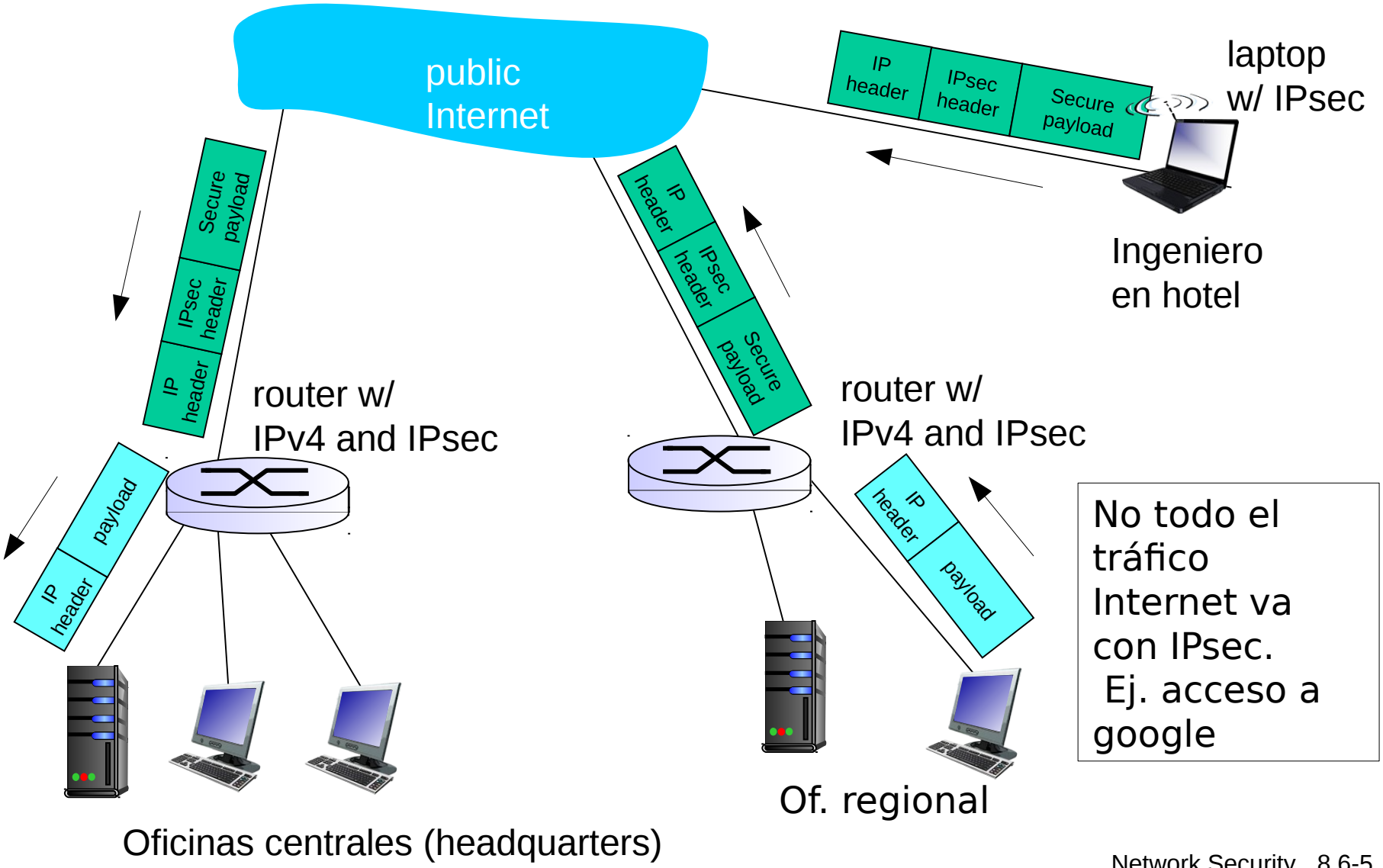
- Quien envía encripta los datos del datagrama (no su encabezado), posibles tipos de datos:
  - Segmento TCP o UDP, mensajes ICMP, OSPF
- Los datos enviados de un nodo a otro se ocultan:
  - Páginas web, e-mail, archivos P2P, paquetes SYN de TCP.

Virtual Private Networks (VPNs)

motivación:

- Las instituciones requieren a menudo redes privadas por seguridad.
  - Son costosas: se debe contar con routers, links, DNS.
- Con VPN: el tráfico entre oficinas -distantes- de la institución es enviado a través de Internet pública.
  - Se encripta antes de ingresar a la red pública, se descifra luego de salir de la red pública.
  - Hay una separación lógica, no física, de otros tráficos.

Virtual Private Networks (VPNs)



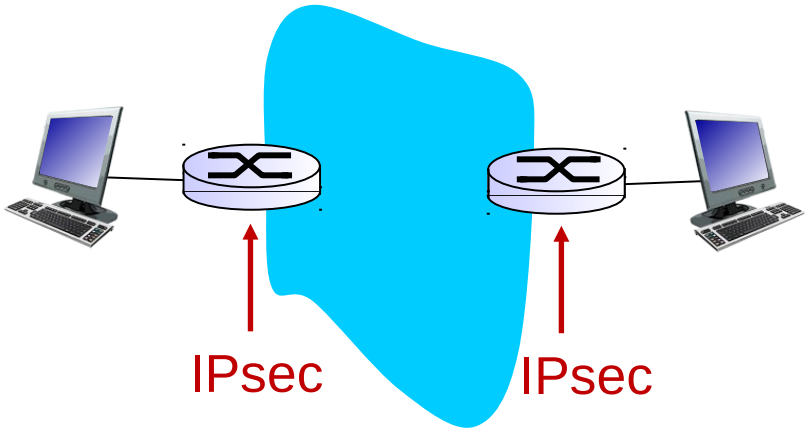
Servicios IPsec

- Integridad de datos
- Autenticación de origen
- Prevención de ataque de reproducción
- confidencialidad

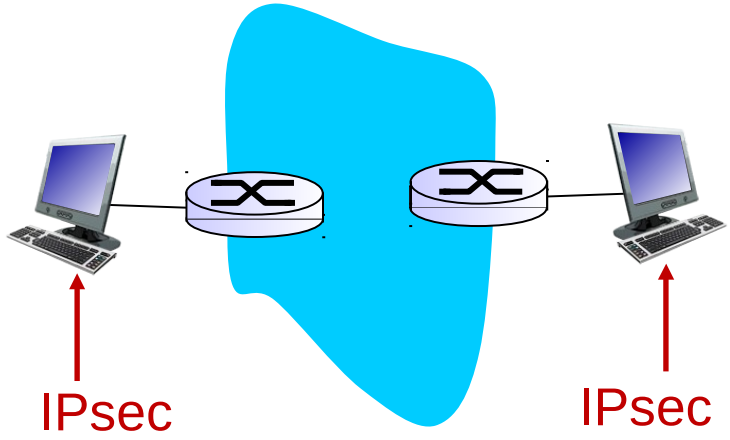
- Características:
  - Datagrama IPsec es emitido y recibido por sistemas extremos
  - Protege protocolos de capas superiores
  - Apropiado para VPNs

- Dos protocolos con modelos de servicio diferentes:
  - AH (Authentication Header): Autentica fuente y da integridad.
  - ESP (Encapsulation Security Payload): Igual que AH más confidencialidad.

Modos en IPsec: túnel y transporte



- Túnel: IPsec en routers de borde



- Transporte: IPsec en Hosts

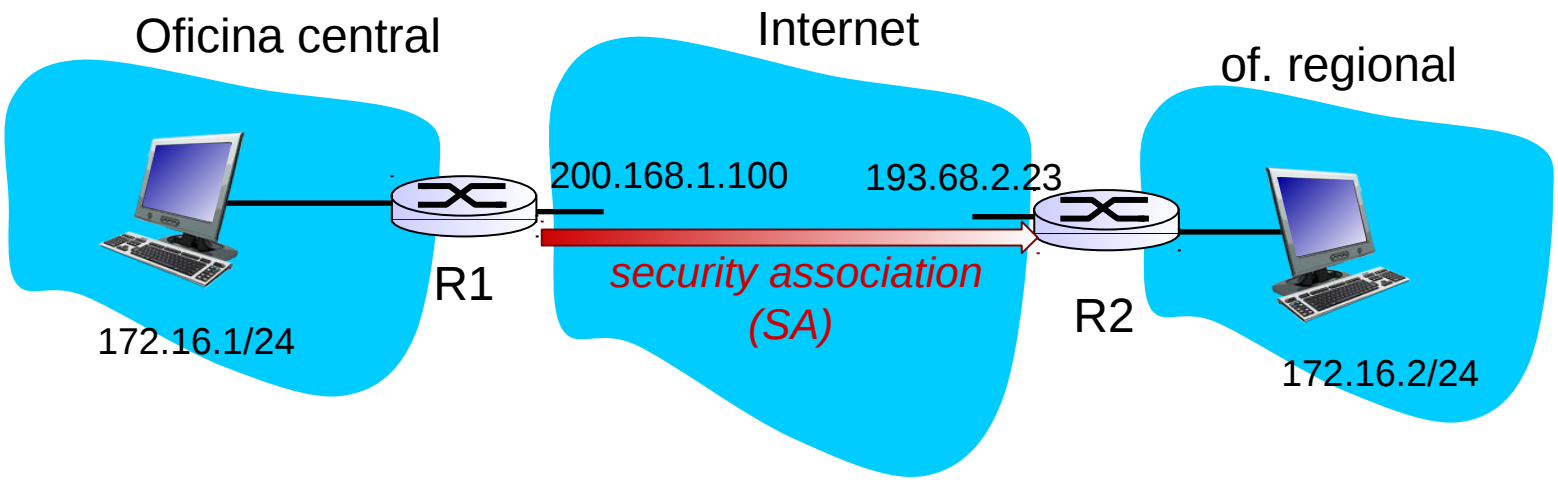
Dos Protocolos IPsec

- Protocolo Authentication Header (AH)
  - Provee: autenticación de fuente e integridad de datos, pero no confidencialidad.
- Protocolo Encapsulation Security Payload (ESP)
  - Provee: autenticación de fuente, integridad de datos y *confidencialidad*
  - ESP es más usado que AH
  - ESP, según su configuración, puede proveer sólo encriptación (no es recomendado), sólo autenticación.

Asociaciones de Seguridad (SAs)

- Antes de enviar datos, se establece una "asociación de seguridad (security association SA)" desde la fuente al destino IPsec
  - SAs son simplex: en una dirección
  - Si hay datos de regreso, la otra fuente arma otra asociación
- Los nodos extremos en IPsec mantienen información de estado sobre la SA.
  - Recordar: extremos en TCP también mantienen estado
  - IP es sin conexión; pero IPsec es orientado a la conexión!
- ¿Cuántas SAs hay en una oficina central que se interconecta con una oficina regional y con n ingenieros en terreno?

Ejemplo de SA de R1 a R2

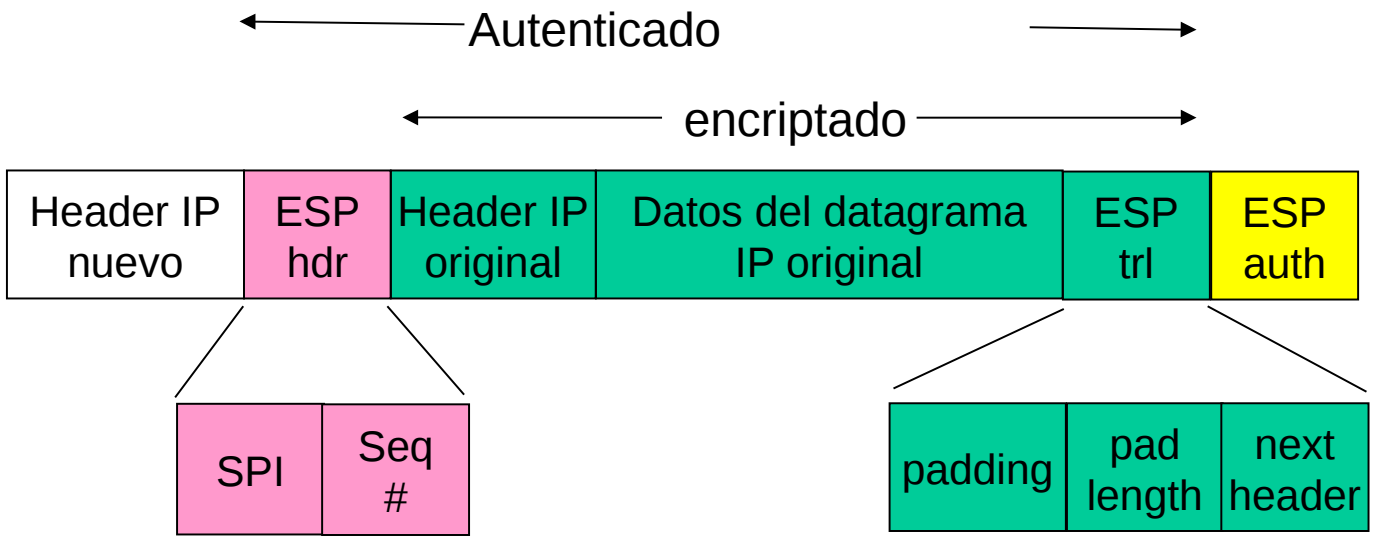


En base de datos, R1 almacena para cada SA:

- Identificador de SA de 32-bit: *Security Parameter Index (SPI)*
- Interfaz SA origen (200.168.1.100)
- Interfaz SA destino (193.68.2.23)
- Tipo de encriptación usada (e.g., 3DES con CBC)
- Clave de encriptación
- Tipo de chequeo de integridad usado (e.g., HMAC con MD5)
- Clave de autenticación

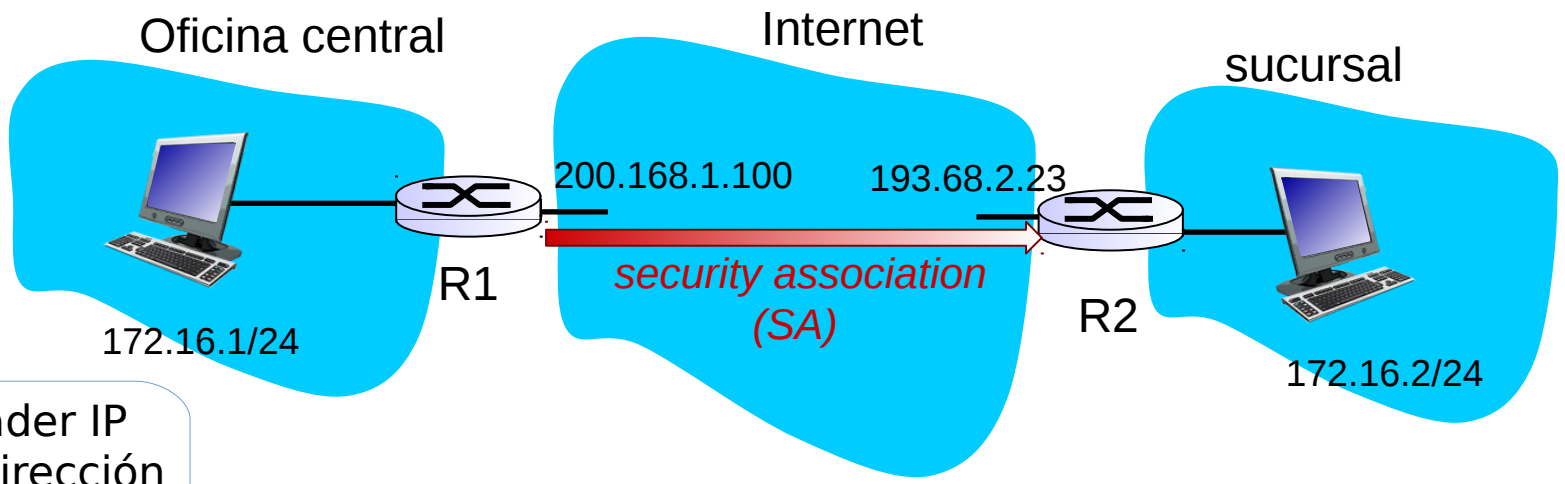
Datagrama IPsec

Caso modo túnel con ESP



Caso modo transporte, ESP no provee integridad y autenticación a todo el paquete IP; el encabezado IP no puede ir encriptado.

¿Cómo R1 arma el datagra ma?



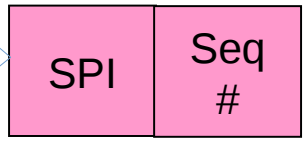
Header IP con dirección origen R1 y destino R2

Autenticado

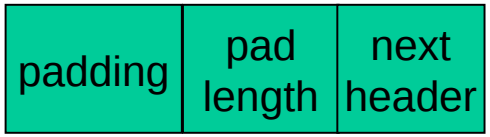
encriptado

Código de Autenticación de Mensaje

Para que R2 busque en DB datos de esa SA



Parra reconocer ataque de reproducción



Resumen: servicio IPsec

- Si el atacante se ubica entre R1 y R2. Si éste no conoce las claves,
  - ¿Será capaz de ver el contenido del datagrama original? Verá dirección fuente y destino? Protocolo de transporte? Puerto de la aplicación?
  - ¿Podrá cambiar los bits sin ser detectado?
  - ¿repetir un datagrama antiguo sin ser detectado?

IKE: Internet Key Exchange

- *Ejemplos previos:* supusimos establecimiento manual de IPsec SAs en puntos extremos:

  Ejemplo SA

  SPI: 12345
  Source IP: 200.168.1.100
  Dest IP: 193.68.2.23
  Protocol: ESP
  Encryption algorithm: 3DES-cbc
  HMAC algorithm: MD5
  Encryption key: 0x7aeaca…
  HMAC key:0xc0291f…

- Configuración manual no es práctica para VPN con centenas de puntos de llegada.
- En su lugar se usa *IPsec IKE (Internet Key Exchange)*

Resumen IPsec

- Se intercambian mensajes IKE para definir algoritmos, claves secretas, números SPI.
- Se usa protocolo AH o ESP (o ambos)
  - AH provee integridad, autenticación de fuente
  - ESP (con AH) provee adicionalmente encriptación
- Pares IPsec pueden ser dos sistemas terminales, dos routers/cortafuegos, o un router/cortafuegos y un sistema terminal

Capítulo 8 contenidos

8.1 ¿Qué es la seguridad en la red?

8.2 Principios de criptografía

8.3 Integridad de mensajes

8.4 Dando seguridad a e-mail

8.5 Conexiones TCP seguras: SSL

8.6 Seguridad en capa de Red: IPsec

8.7 Seguridad en redes locales inalámbricas

8.8 Cortafuegos y Sistemas de detección de intrusión (IDS)