10

SEGURIDAD EN LA CAPA DE RED
VPN CON PROTOCOLO IPsec

Manual de clases

Objetivo

- Describir el protocolo IPsec que proporciona seguridad a los datagramas IP intercambiados por hosts y routers de la capa de red. y hace posible la creación de redes VPN empresariales.

Última modificación:
16 de mayo de 2023

Tema 10 de:
SEGURIDAD EN REDES

Edison Coimbra G.

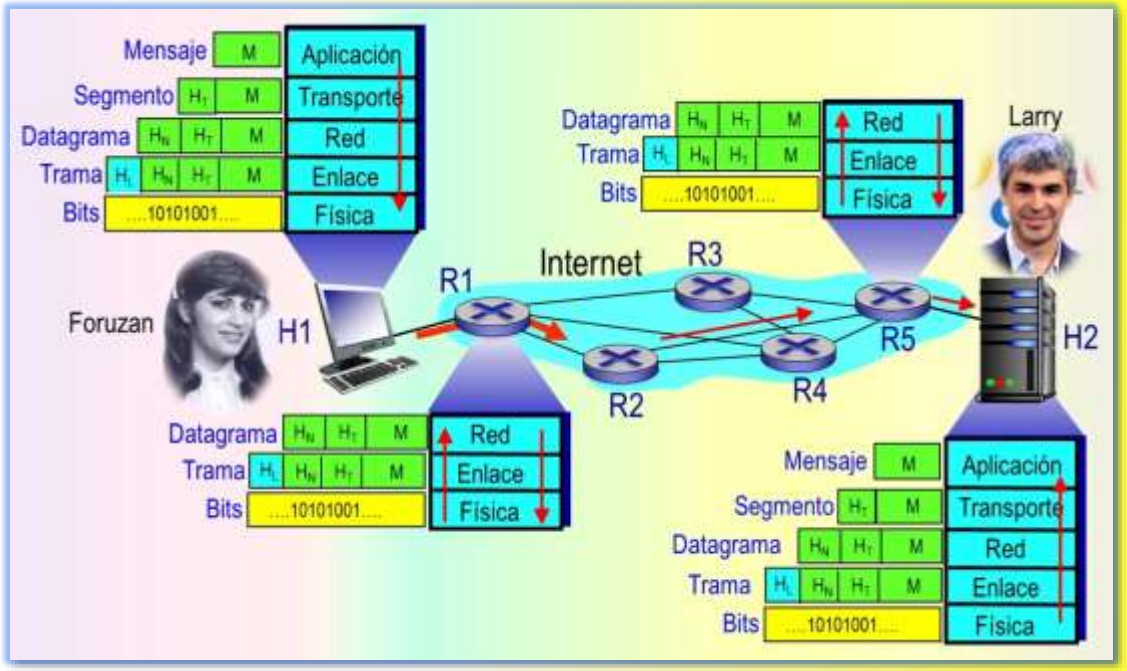
1.- SEGURIDAD EN LA CAPA DE RED

VPN CON PROTOCOLO IPsec

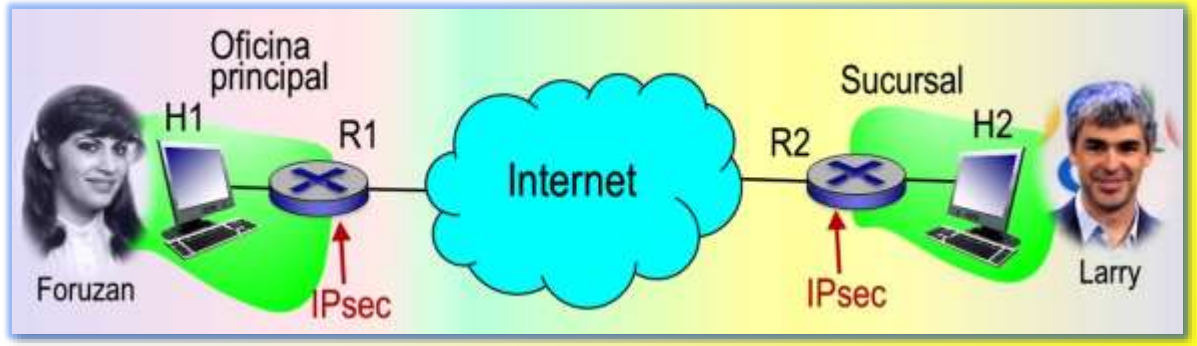
(Kurose, 2017)

Servicios que proporciona la capa de red

- **El protocolo** de la capa de red de Internet es el protocolo IP que proporciona una comunicación lógica entre hosts. El modelo de servicio de IP es un servicio de entrega de mejor esfuerzo.
  - ⊠ Esto quiere decir que IP hace todo lo que puede por entregar los segmentos entre los host que se están comunicando, pero no garantiza la entrega.
  - ⊠ En particular, no garantiza la entrega de los segmentos, no garantiza que los segmentos se entreguen en orden y no garantiza la integridad de los datos contenidos en los segmentos. Por estas razones, se dice que IP es un servicio no fiable.



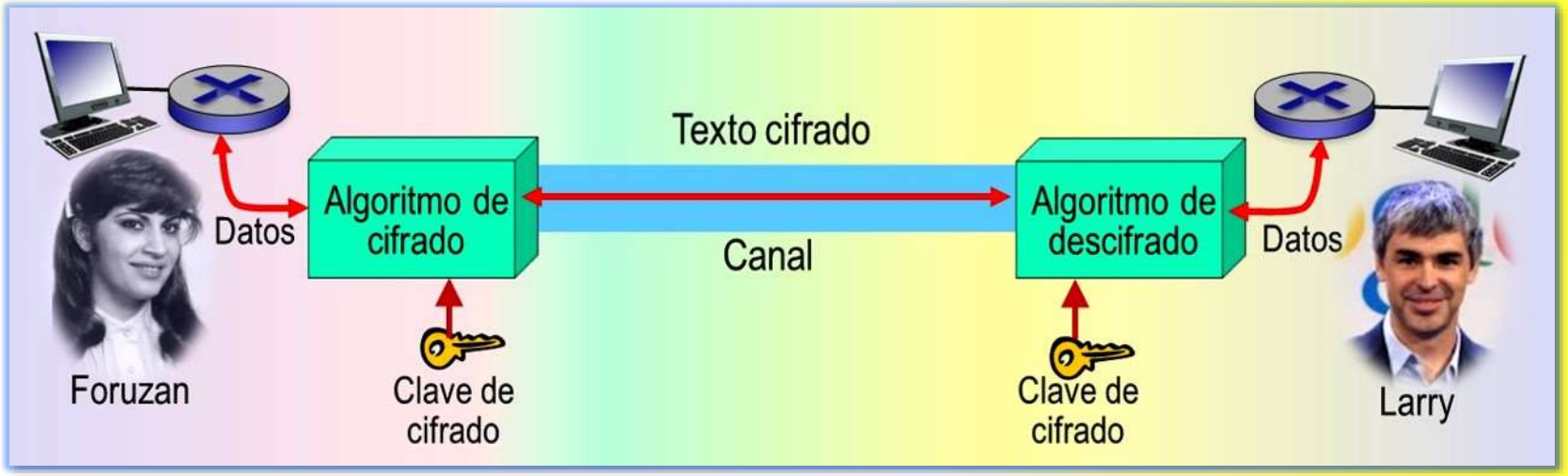
- **¿Cómo dotar de seguridad a la capa de red?** Utilizando el protocolo de seguridad IP, más conocido como IPsec, que proporciona seguridad a los datagramas IP intercambiados por hosts y routers de la capa de red.
- **Muchas instituciones**, como corporaciones, agencias gubernamentales, etc., utilizan IPsec para crear redes privadas virtuales VPN, que funcionan sobre la Internet pública y que necesitan confidencialidad.



VPN CON PROTOCOLO IPsec

Confidencialidad en la capa de red (Kurose, 2017)

- **¿Qué implica proporcionar confidencialidad en la capa de red?** La confidencialidad entre Silvia y Bill, y más específicamente entre dos routers, o entre dos hosts o entre un router y un host, implica que el emisor cifra las cargas útiles (datos) de todos los datagramas que envía hacia el receptor.



- **La carga útil** cifrada podría ser un segmento TCP, un segmento UDP, un mensaje ICMP, etc. Si se dispusiera de tal servicio en la capa de red, todos los datos enviados de un emisor a un receptor (incluyendo los mensajes de correo electrónico, las páginas web, los mensajes de acuerdo TCP y los mensajes de administración, como ICMP y SNMP) estarían ocultos a ojos de posibles terceros que pudieran estar husmeando los mensajes que circulan por la red.
- **Por esta razón**, se dice que la seguridad en la capa de red proporciona un servicio básico de ocultación.

VPN CON PROTOCOLO IPsec

Otros servicios de seguridad

(Kurose, 2017)

- **Además de la confidencialidad**, un protocolo de seguridad de la capa de red podría potencialmente proporcionar otros servicios de seguridad. Por ejemplo:
  - ▶Un servicio de integridad de los datos, de modo que el receptor pueda comprobar si se ha producido alguna alteración del datagrama mientras este se encontraba en tránsito.
  - ▶Mecanismos de autenticación del origen, de modo que el receptor pueda verificar cuál es el origen del datagrama seguro.
  - ▶Mecanismos para prevenir ataques por reproducción, lo que significa que se podría detectar cualquier datagrama duplicado que un atacante pudiera insertar.

Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**
Cifrado PGP para correo	Cifrado PGP para correo	Cifrado PGP para correo	Firewalls (Filtros de paquetes. Filtros con memoria del estado. Gateways de aplicación)
Protocolo TCP-SSL	Protocolo TCP-SSL	Protocolos de autenticación (Contraseñas y números distintivos)	Sistemas de Detección y de Prevención de Intrusiones
Protocolo IPsec (ESP)	Protocolo IPsec (AH, ESP)	Protocolo TCP-SSL Protocolo IPsec (AH, ESP)	Zonas de seguridad y zonas desmilitarizadas

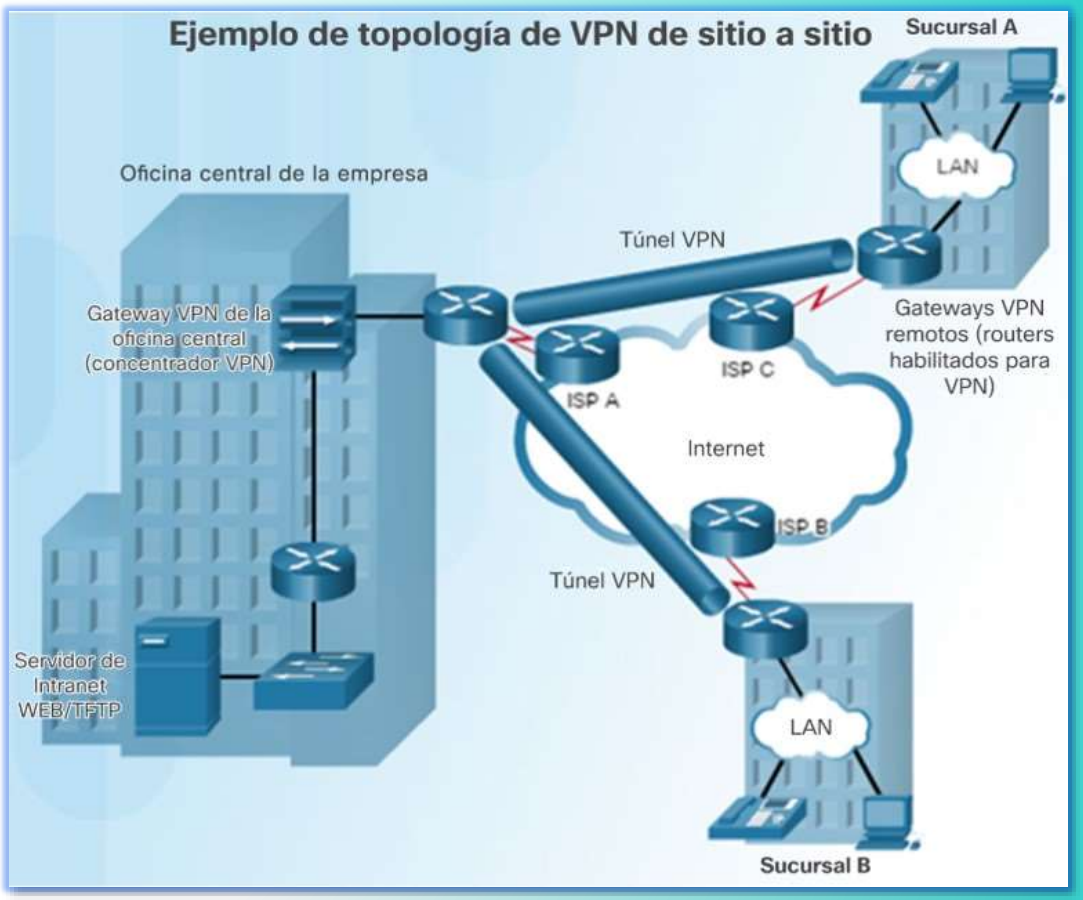
- **IPsec**, de hecho, proporciona mecanismos para todos estos servicios de seguridad es decir, para la confidencialidad, la integridad de los datos, la autentificación de origen y la prevención de los ataques por reproducción.

2.- VPN EN LA INTERNET PÚBLICA

VPN CON PROTOCOLO IPsec

Redes Privadas virtuales VPN

(CISCO, 2016)



- **Una institución** que abarque múltiples regiones geográficas deseará disponer de su propia red IP, de modo que sus hosts y servidores puedan intercambiar datos de forma segura y confidencial.
- **Para conseguir** este objetivo, esta institución podría implantar una red física independiente (incluyendo routers, enlaces y una infraestructura DNS) que esté completamente separada de la internet pública.
- **Dicha red separada**, dedicada a una institución concreta, se denomina red privada. No es sorprendente que tales redes privadas puedan llegar a ser muy costosas, ya que la institución necesitará comprar, instalar y mantener su propia infraestructura física de red.
- **Sin embargo**, en lugar de implantar y mantener una red privada, muchas instituciones crean actualmente redes privadas virtuales VPN. Una VPN es una conexión cifrada entre redes privadas a través de la Internet pública.
- **En vez de usar** una conexión dedicada de capa 2, como una línea arrendada físicamente independiente, una VPN usa conexiones virtuales llamadas “túneles VPN”, que se enrutan a través de Internet desde la red de la oficina central de la empresa hasta la red de las sucursales remotas o de lo empleados remotos.

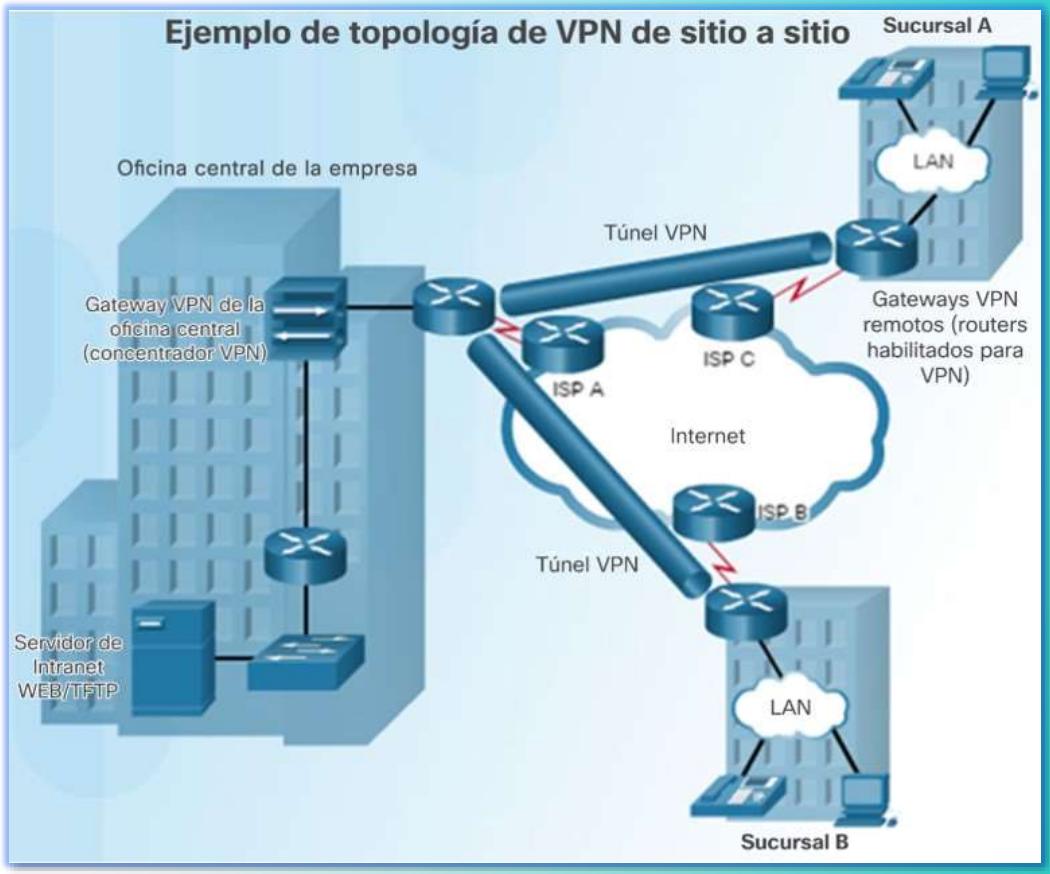
VPN en la Internet pública

VPN CON PROTOCOLO IPsec

Tipos de acceso a VPN

(Kurose, 2017) (CISCO, 2016)

- **Existen dos tipos** de acceso a VPN:
  - ▶VPN de sitio a sitio. Conecta redes enteras entre sí, por ejemplo, puede conectar la red de una sucursal a la red de la oficina central de una empresa.
  - ▶VPN de acceso remoto. Permite que los empleados a distancia, los usuarios móviles y los consumidores de extranets accedan a la red de una empresa de manera segura a través de Internet.
    - ✉ Cuando un trabajador remoto o un trabajador en una oficina remota utiliza un servicio de banda ancha para acceder a la WAN corporativa a través de Internet, se generan riesgos de seguridad y por eso son necesarias las VPN.
- **Para proporcionar confidencailidad**, el tráfico entre sucursales se cifra antes de entrar en la Internet pública.



3.- VPN CON EL PROTOCOLO IPSEC

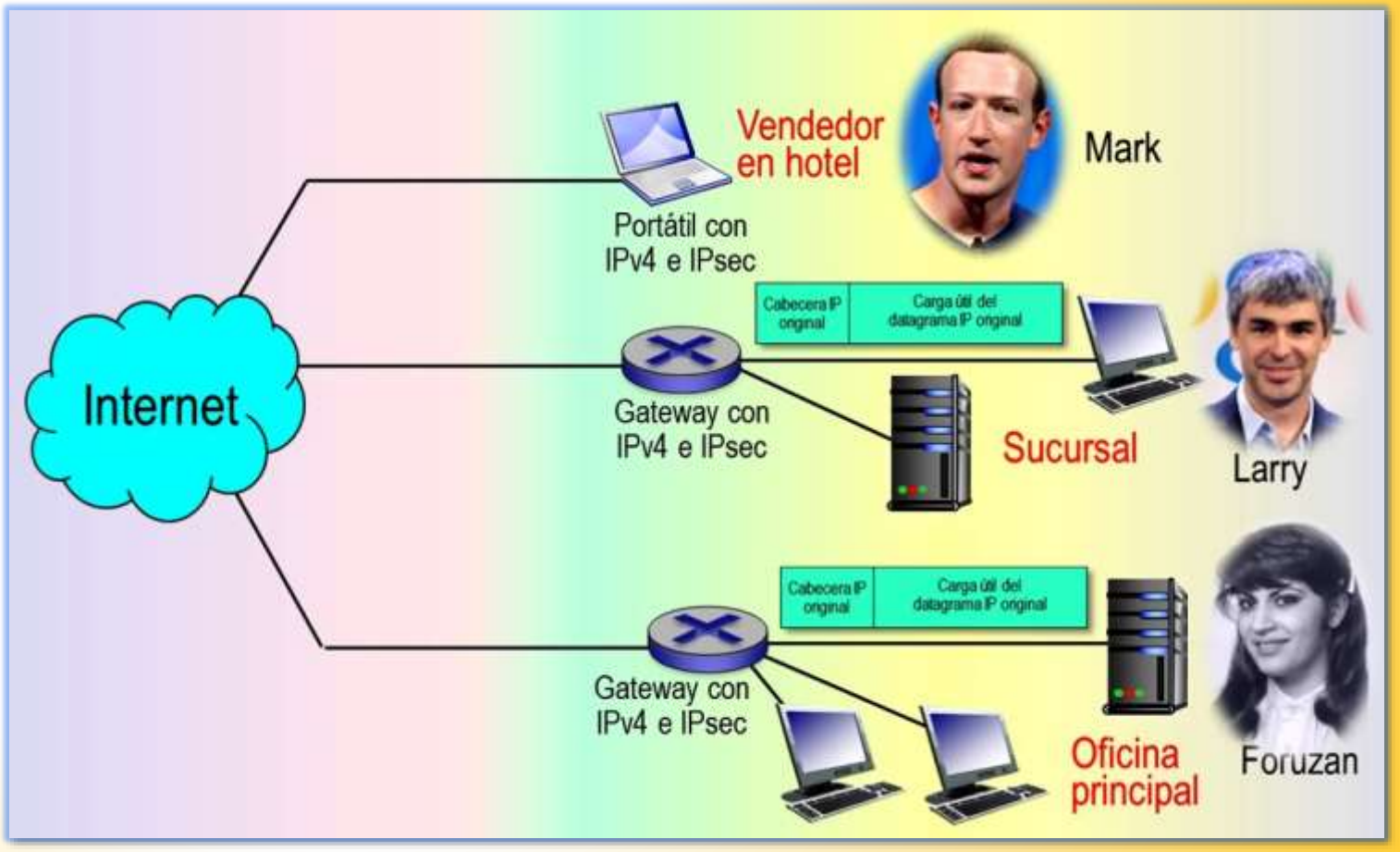
VPN CON PROTOCOLO IPsec

Un ejemplo de VPN con IPsec

(Kurose, 2017)

- **En la figura** se muestra un ejemplo simple de red VPN. Aquí, la institución está compuesta por una oficina principal, una sucursal y una serie de vendedores itinerantes que suelen acceder a Internet desde la habitación de su hotel (solo se muestra uno de esos vendedores).

- **En esta VPN**, cuando dos hosts situados en la oficina principal se intercambian datagramas IP o cuando dos host de la sucursal quieren comunicarse, utilizan el protocolo simple y tradicional IPv4.

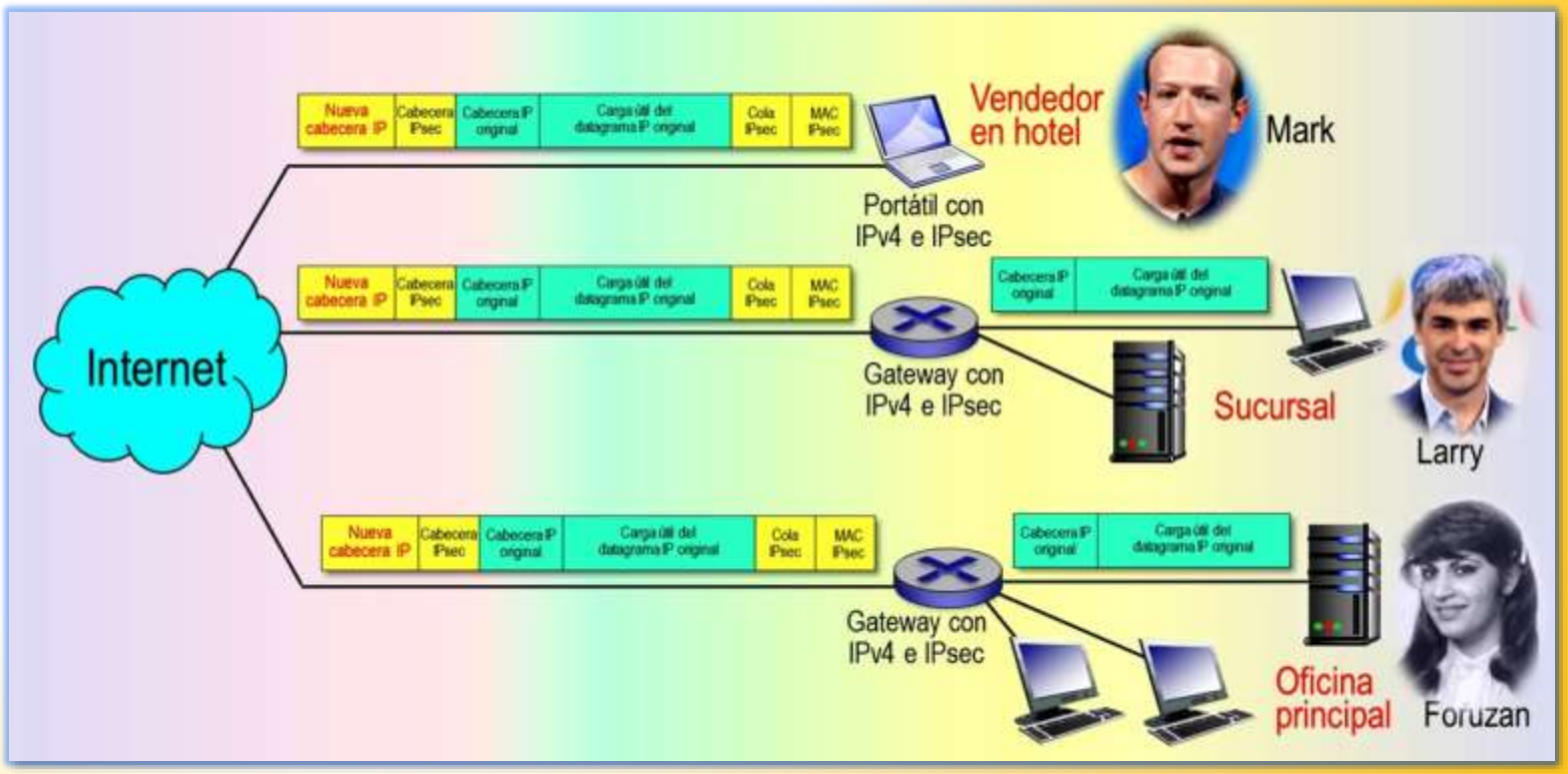


VPN CON PROTOCOLO IPsec

Un ejemplo de VPN con IPsec (cont.)

(Kurose, 2017)

- **Sin embargo**, cuando, por ejemplo, un host de la oficina principal (el host de Foruzan) envía un datagrama IP a un vendedor (Mark) que se encuentra en un hotel, el tráfico se cifra antes de entrar a Internet.
  - ✉ Este cifrado lo realiza el router gateway de la oficina principal, convirtiendo el datagrama IP simple en un datagrama IPsec y luego reenvía dicho datagrama hacia Internet.
- **Este datagrama IPsec** tiene de hecho una nueva cabecera IP tradicional, de modo que los routers de Internet procesan el datagrama como si se tratara de un datagrama IP normal, para ellos el datagrama es, de hecho, como cualquier otro.



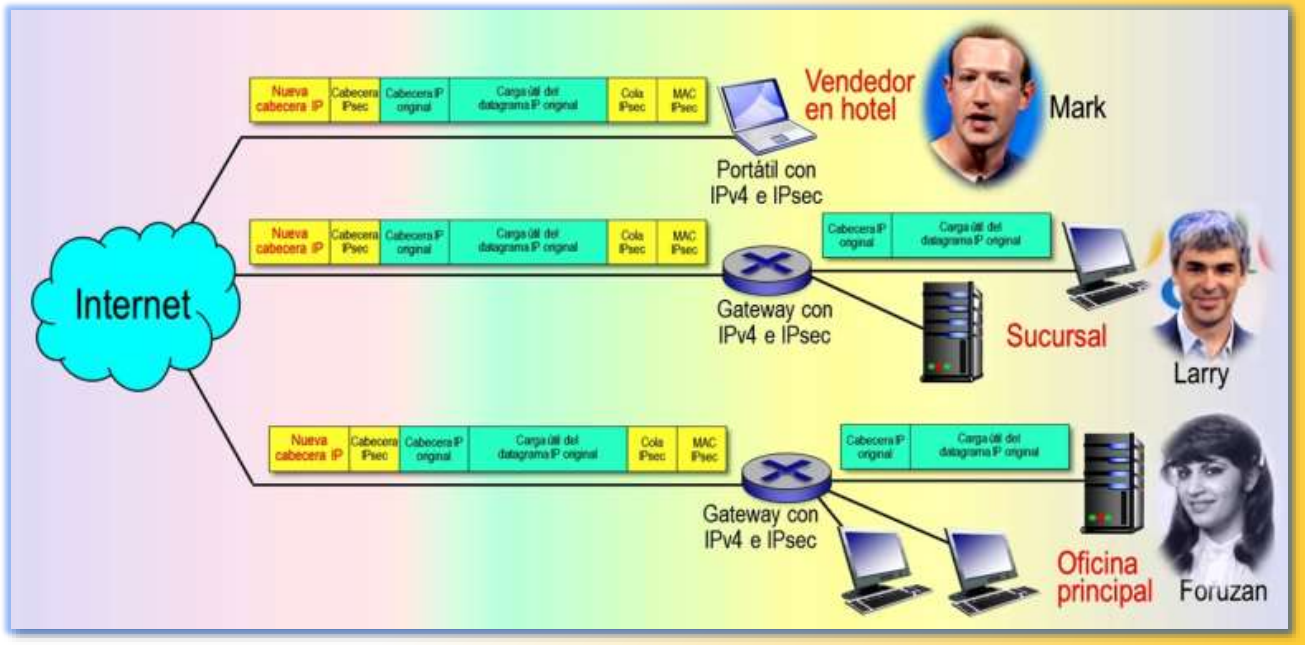
VPN CON PROTOCOLO IPsec

Formato del datagrama IPsec

(Kurose, 2017)

- **La carga útil** del datagrama IPsec incluye una cola IPsec, que es utilizada para el procesamiento IPsec, además, la carga útil del datagrama IPsec está cifrada.

- **Cuando el datagrama IPsec** llega al PC del vendedor Mark, el sistema operativo del equipo descifra la carga útil y proporciona algunos otros servicios de seguridad, como la verificación de la integridad de los datos, y pasa la carga útil descifrada hacia el protocolo de la capa superior, TCP o UDP.



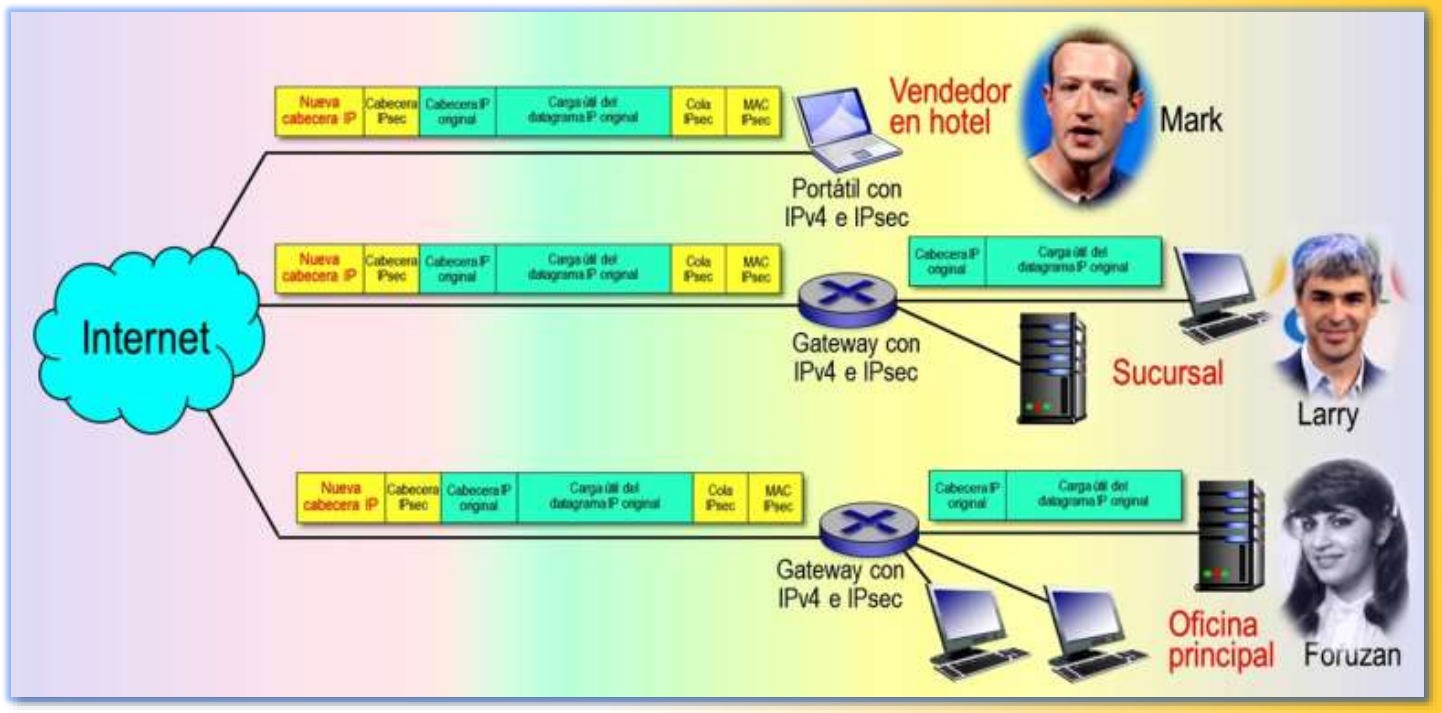
- **Esto es solo** una pequeña panorámica de como una institución puede utilizar IPsec para crear una red VPN.

VPN CON PROTOCOLO IPsec

IPsec y los protocolos AH y ESP

(Kurose, 2017)

- **IPsec** está conformado por una serie de protocolos que conforman a su vez la arquitectura global de seguridad IP. Existen en esta serie, dos protocolos importantes:
  - ▶**1.**El protocolo AH, protocolo de cabecera de autenticación.
  - ▶**2.**El protocolo ESP, protocolo de carga útil de seguridad para encapsulación.
- **Cuando un host o router IPsec** de origen envía datagramas seguros a un host o router de destino, lo hace con el protocolo AH o con el ESP.
  - ▶El protocolo AH proporciona la integridad de los datos y autenticación del origen, pero no confidencialidad.
  - ▶El protocolo ESP proporciona confidencialidad, integridad de los datos y autenticación del origen. Puesto que la confidencialidad a menudo es crítica para las redes VPN y otras aplicaciones IPsec, el protocolo ESP se utiliza más ampliamente.



4.- ASOCIACIONES DE SEGURIDAD

VPN CON PROTOCOLO IPsec

¿Qué son las asociaciones de seguridad? (Kurose, 2017)

- **Los datagramas IPsec** se intercambian entre parejas, como por ejemplo entre dos hosts, dos routers, o entre un host y un router.

- **Antes de enviar** datagramas IPsec, por ejemplo, desde el router de origen R1 al de destino, R2, ambas crean una conexión lógica en la capa de red. Esta conexión lógica se denomina asociación de seguridad.

- **Una asociación de seguridad** es una conexión lógica de tipo simple, es decir, una conexión unidireccional desde el origen al destino. Si ambos routers desean enviarse datagramas seguros entre sí, entonces será necesario establecer una asociación de seguridad en cada dirección.

- ▶**Ejemplo 1.** Considere una VPN institucional. Esta institución consta de una oficina principal, una sucursal y un cierto número *n* de vendedores itinerantes. Suponga, que existe tráfico IPsec bidireccional entre la oficina principal y la sucursal y entre la oficina principal y los vendedores. En esta VPN, ¿cuántas asociaciones de seguridad existirán?
  - ▶Hay dos asociaciones entre el router gateway de la oficina principal y el gateway de la sucursal (una en cada dirección).
  - ▶Para la PC portátil de cada vendedor tambien hay dos asociaciones entre el router gateway de la oficina principal y la portátil.

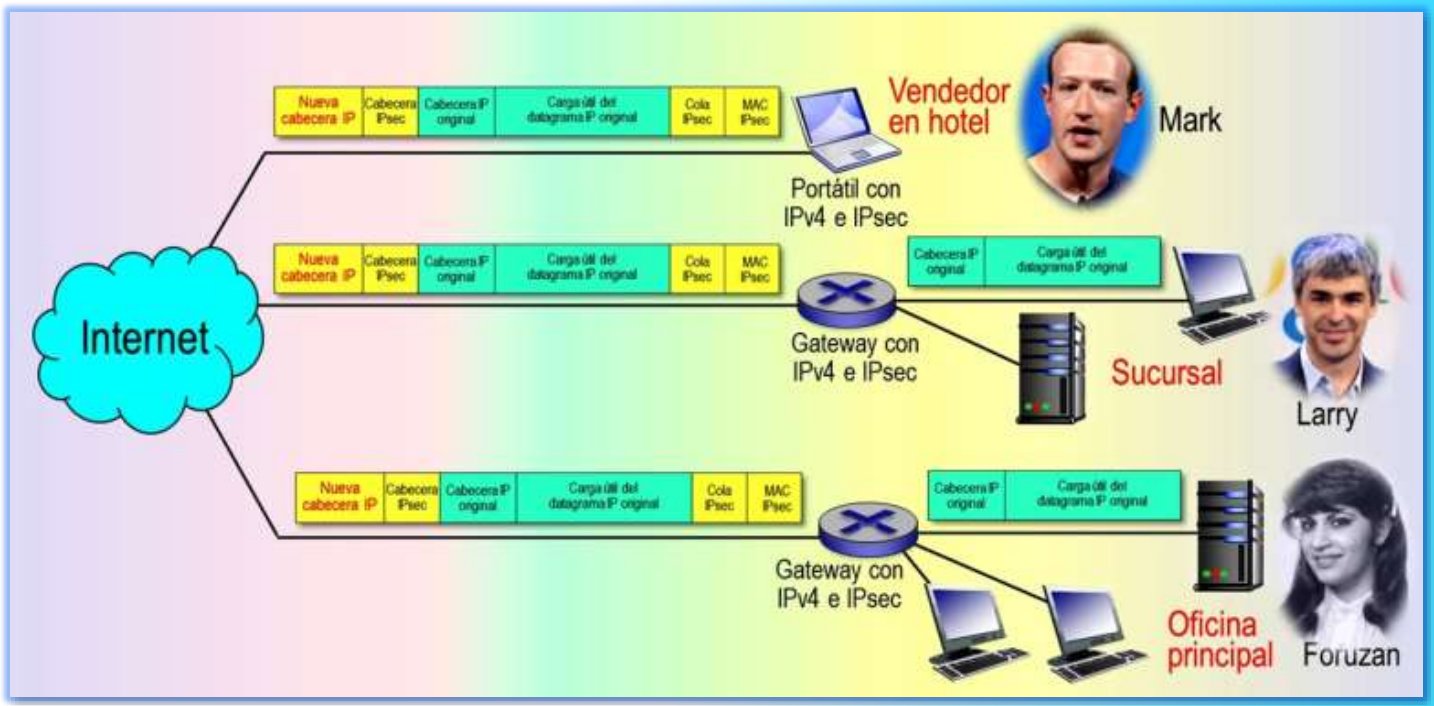
Asociaciones de seguridad

VPN CON PROTOCOLO IPsec

Las asociaciones de seguridad

(Kurose, 2017)

- ▶**Ejemplo 2.** En la figura habrán (2 +2*n*) asociaciones de seguridad, siendo *n* la cantidad de vendedores itinerantes.
- **Cabe hacer notar** que no todo el tráfico enviado hacia Internet por los gateways o por las PC portátiles estará protegido mediante IPsec.
  - ✉ Un host situado en la oficina principal o en la sucursal o las portátiles de los vendedores podrían querer acceder a un servidor web (como Amazon o Google) disponible en la Internet pública.
- **Por tanto**, los routers gateway y las portátiles enviarán hacia Internet tanto datagramas IP normales como datagramas dotados de seguridad IPsec.



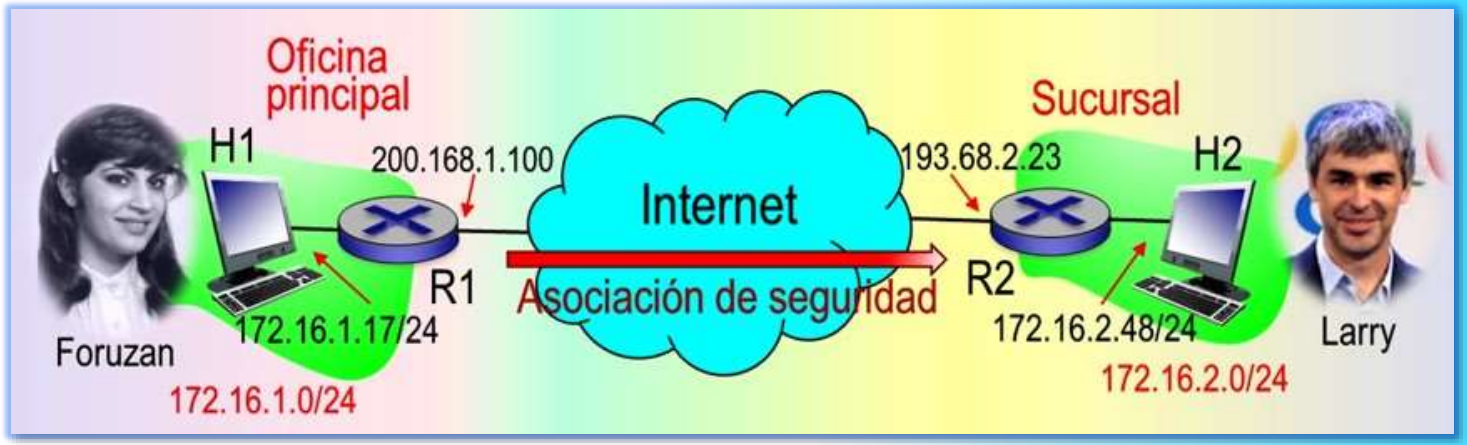
Asociaciones de seguridad

VPN CON PROTOCOLO IPsec

Detalles de una asociación de seguridad

(Kurose, 2017)

- ▶**Ejemplo 3.** Una asociación de seguridad, es, por ejemplo, la existente entre los routers R1 y R2 de la figura (ambos son los gateways de la oficina principal y de la sucursal, respectivamente).



- **El router R1** mantendrá una cierta información de estado acerca de esta asociación, la cual incluirá:
  - ▶Un identificador de 32 bits para la asociación de seguridad, denominado Índice de parámetro de seguridad SPI.
  - ▶La interfaz de origen de la asociación (en este caso 200.168.1.100) y la interfaz de destino (en este caso 193.68.2.23).
  - ▶El tipo de cifrado que se va a utilizar (por ejemplo, algoritmo de cifrado 3DES con descifrado CBC).
  - ▶La clave de cifrado.
  - ▶El tipo de comprobación de integridad (por ejemplo, código de autenticación HMAC calculado con función hash criptográfica MD5).
  - ▶La clave de autenticación.

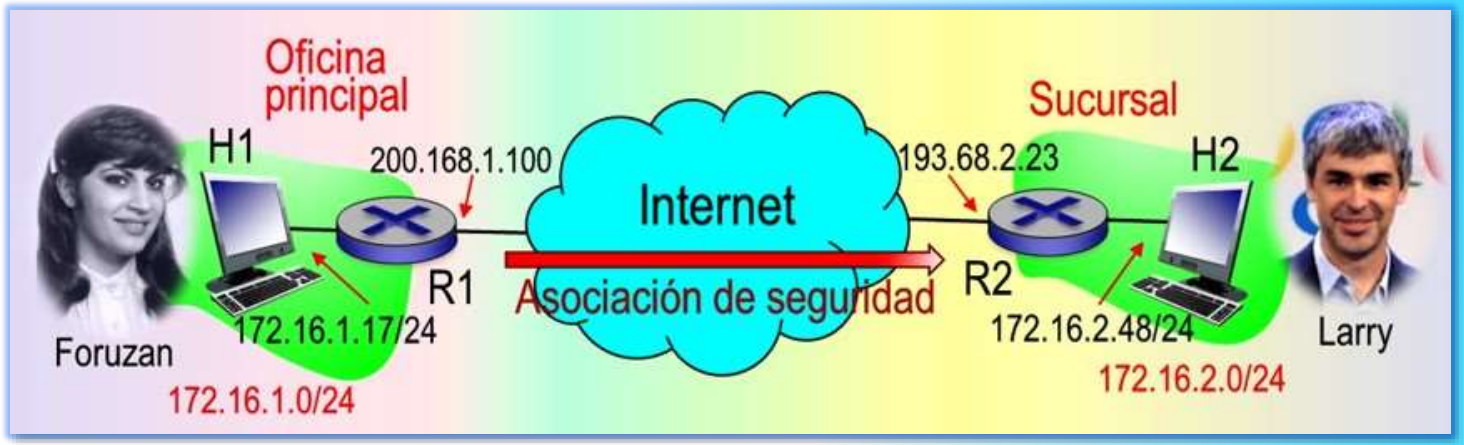
Asociaciones de seguridad

VPN CON PROTOCOLO IPsec

Detalles de una asociación de seguridad (cont.)

(Kurose, 2017)

- **Cada vez** que el router R1 necesite construir un datagrama IPsec para reenviarlo a través de esta asociación de seguridad, accederá a la información de estado para determinar cómo debe autenticar y cifrar el datagrama.
- **De forma similar**, el router R2 mantendrá la misma información de estado para esta asociación de seguridad y utilizará esta información para autenticar y descifrar todos los datagramas IPsec que lleguen desde dicha asociación.



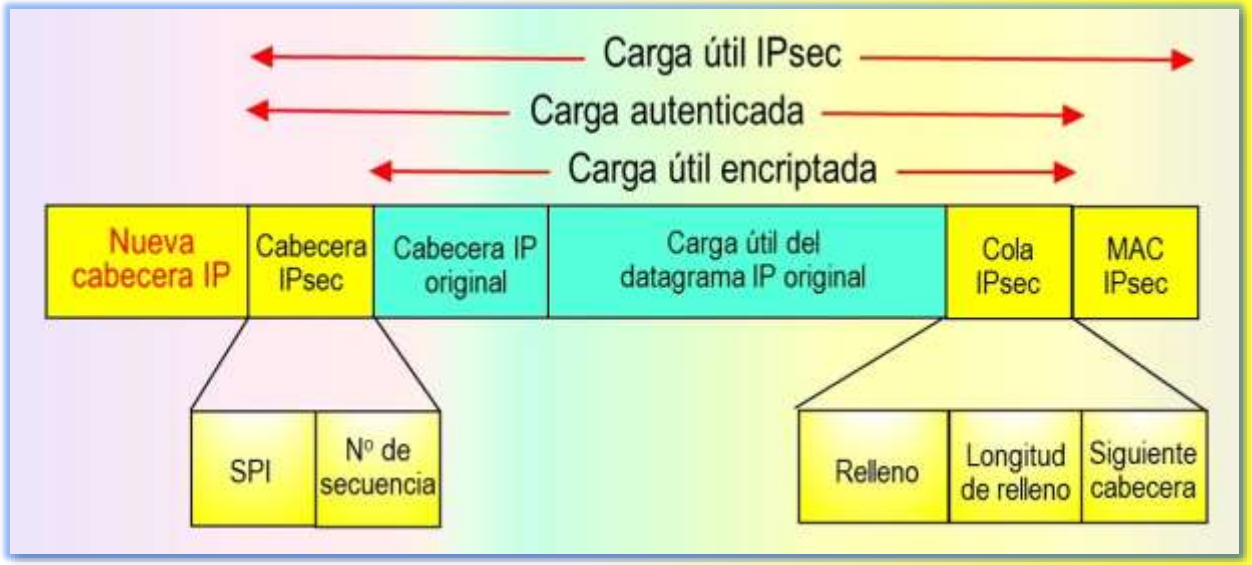
- **Cada host o router IPsec** suele mantener información de estado para muchas asociaciones de seguridad.
  - ▶Por ejemplo, en la red VPN del ejemplo, con *n* vendedores, el gateway de la oficina principal mantiene información de estado para (2+ 2*n*) asociaciones de seguridad.
- **Cada host o router IPsec** almacena la información de estado para todas sus asociaciones de seguridad en su base de datos de asociaciones de seguridad SAD, que es una estructura de datos contenida en el kernel del sistema operativo de esa entidad.

5.- EL DATAGRAMA IPsec

VPN CON PROTOCOLO IPsec

Formato del datagrama IPsec (Kurose, 2017)

- **El análisis** se centrará en el modo túnel, que es el más apropiado para las redes VPN y está mas ampliamente implantado. Existe también el modo transporte.
- **El formato** del datagrama IPsec se muestra en la figura. Suponga que el router gateway R1 recibe un datagrama IP normal procedente de un host situado en la red de la oficina principal, destinado a otro host de la sucursal. Utiliza la siguiente receta para convertir este datagrama IP original en un datagrama Ipsec:



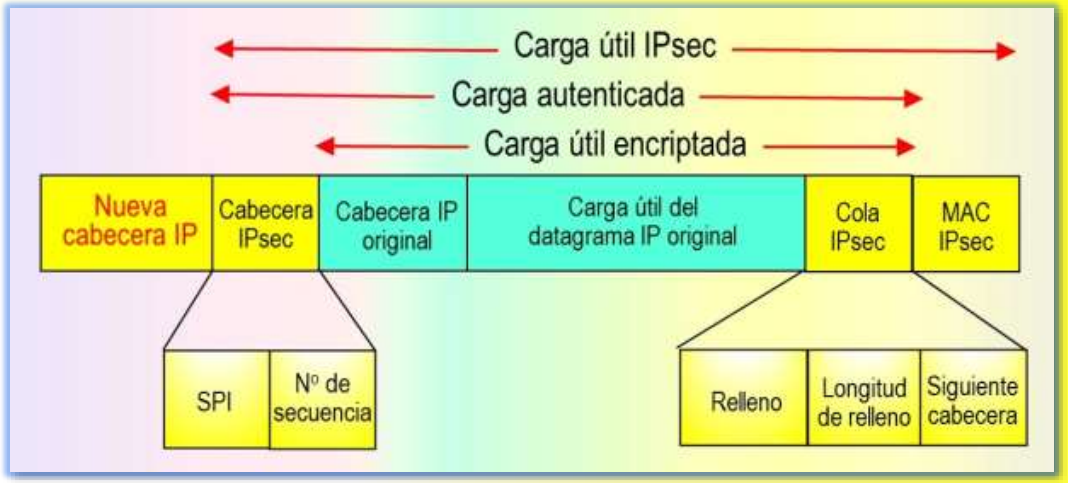
- ▶**1.** Añade al final del datagrama IP original un campo especial de Cola IPsec.
- ▶**2.** Cifra el resultado (encripta) utilizando el algoritmo y la clave especificados por la asociación de seguridad.
- ▶**3.** Añade al principio de este paquete cifrado un campo denominado Cabecera IPsec, que contiene un SPI (Índice de Parámetro de Seguridad) y un número de secuencia. El paquete resultante se conoce como carga autenticada.
- ▶**4.** Crea un valor MAC IPsec de autenticación para toda la carga autenticada utilizando el algoritmo y la clave especificados por la asociación de seguridad.
- ▶**5.** Añade el valor MAC IPsec al final de la carga autenticada formando así la carga útil IPsec.
- ▶**6.** Por último, crea una Nueva cabecera IP con todos los campos clásicos de la cabecera IP y añade dicha cabecera al principio de la carga útil IPsec.

El datagrama IPsec

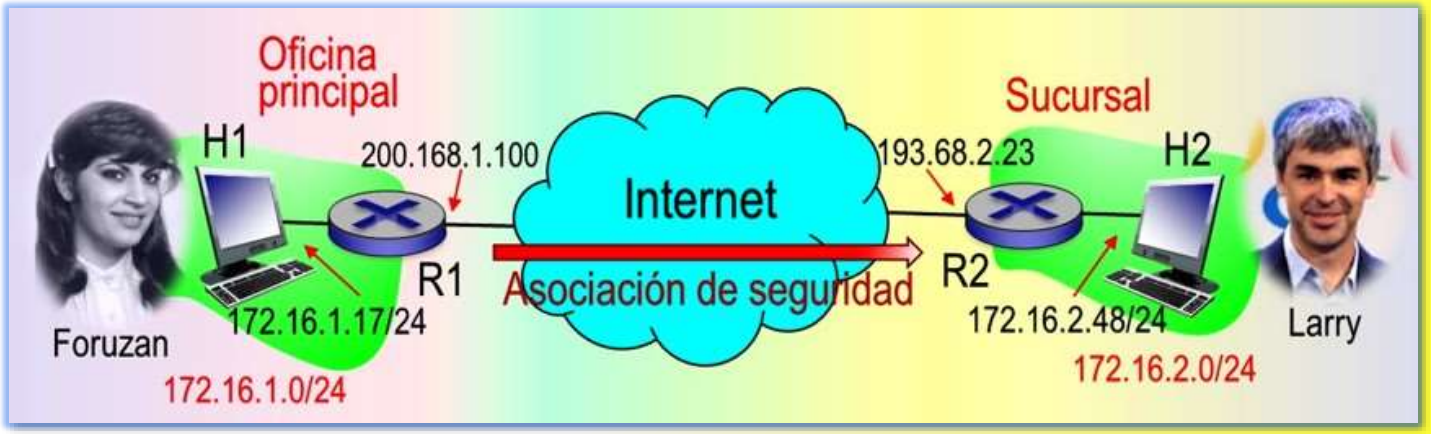
VPN CON PROTOCOLO IPsec

Datagrama IPsec resultante

(Kurose, 2017)



- **El datagrama IPsec** resultante es un datagrama IP perfectamente normal, con los campos tradicionales de cabecera IP seguidos de una carga útil.
- **Pero** en este caso la carga útil contiene una Cabecera IPsec, el datagrama IP original, una Cola IPsec y un campo de autenticación MAC IPsec (estando cifrados el datagrama original y la Cola IPsec).
- ▶**Ejemplo 4.** En el ejemplo de la figura, el datagrama IP original tiene 172.16.1.7 como dirección IP de origen y 172.16.2.48 como IP de destino. Puesto que el datagrama IPsec incluye el datagrama IP original, estas direcciones se incluyen (y se cifran) como parte de la carga útil del paquete IPsec.



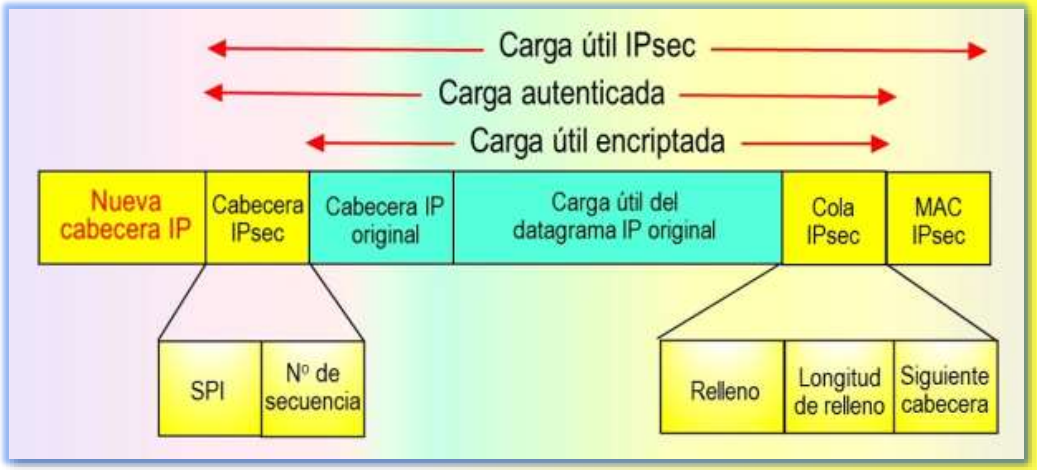
- **¿Pero que sucede** con las direcciones IP de origen y de destino contenidas en la Nueva cabecera IP?
- **Como cabria** esperar, esos valores se configuran con las direcciones de las interfaces de router de origen y de destino situadas en los dos extremos de los túneles, es decir, con los valores 200.168.1.100 y 193.68.2.23.

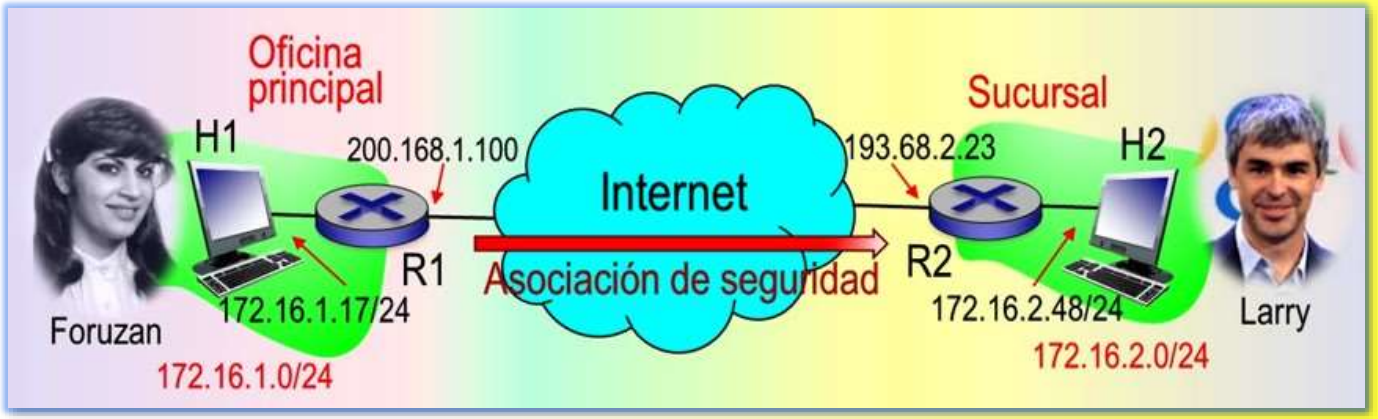
VPN CON PROTOCOLO IPsec

Datagrama IPsec resultante (cont.)

(Kurose, 2017)

- **Así mismo**, el número de protocolo en este nuevo campo de cabecera IP no se configura con el valor correspondiente a TCP, UDP o STMP, sino con el valor 50, que indica que se trata de un datagrama IPsec que está empleando el protocolo IPsec (o más propiamente el protocolo ESP).
- **Después de que** R1 envíe el datagrama IPsec hacia la Internet pública, este pasará a través de muchos routers antes de alcanzar R2.
- **Cada uno de estos** routers procesará el datagrama como si fuera un datagrama normal. De hecho, todos estos routers no son conscientes de que el datagrama esté transportando datos cifrados mediante IPsec.
- **Para estos routers** de la Internet pública, el destino último del datagrama es R2, puesto que la dirección IP de destino en la cabecera externa es R2.



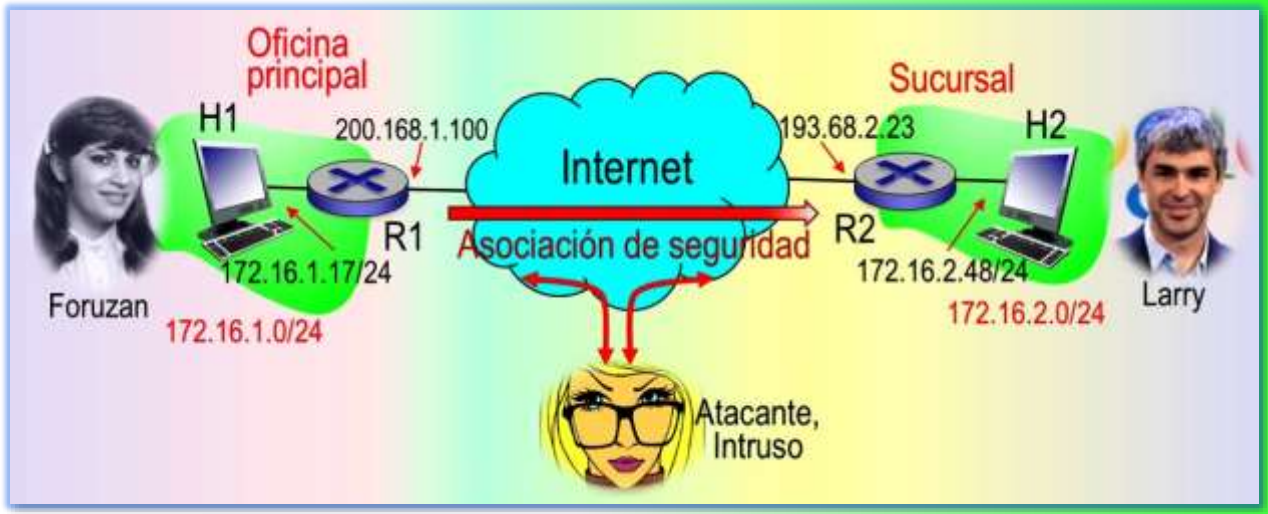


6.- VISTA PANORÁMICA DE LOS SERVICIOS IPsec

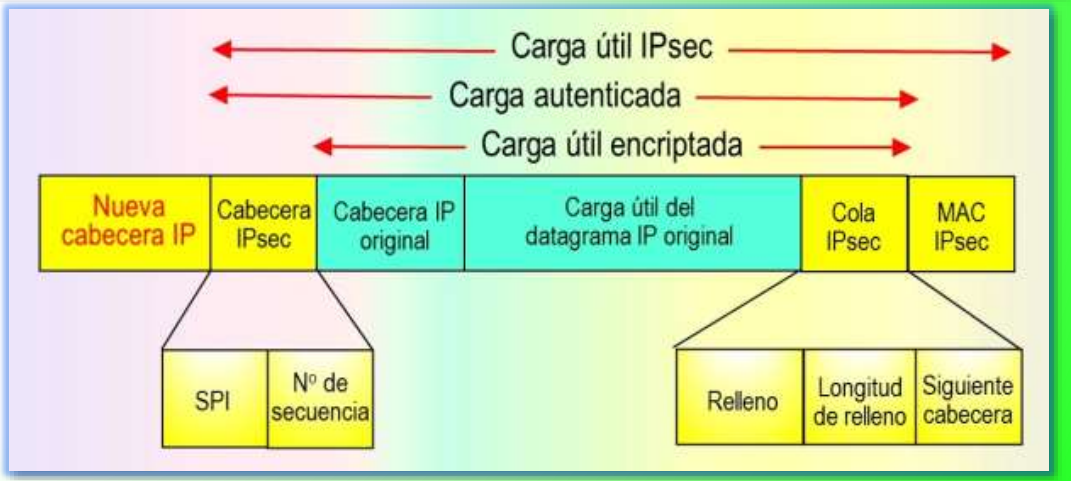
VPN CON PROTOCOLO IPsec

¿Qué servicios proporciona IPsec?

(Kurose, 2017)



- ▶**Ejemplo 5.** Se hará un resumen desde la perspectiva de un Atacante que se ha interpuesto en la comunicación, situado en algún lugar de la ruta entre los routers R1 y R2 de la figura.
- **Suponga** que el Atacante no conoce las claves de cifrado ni de autenticación empleadas por la asociación de seguridad. ¿Qué cosas puede hacer el Atacante y cuáles no?
- ▶**1.** Confidencialidad. El Atacante no puede ver el datagrama original. De hecho, no solo están los datos del datagrama original ocultos (cifrados) a sus ojos, sino que también lo están el número de protocolo, la dirección IP de origen y de destino.
  - ⌧ Para los datagramas enviados, el Atacante solo sabe que el datagrama tiene su origen en algún host de la red 172.16.1.0/24 y que está destinado a algún host de la red 172.16.2.0/24.
  - ⌧ El Atacante no sabe si el datagrama está transportando datos TCP, UDP o ICMP; no sabe si está transportando HTTP, SMTP o algún otro tipo de datos de aplicación.



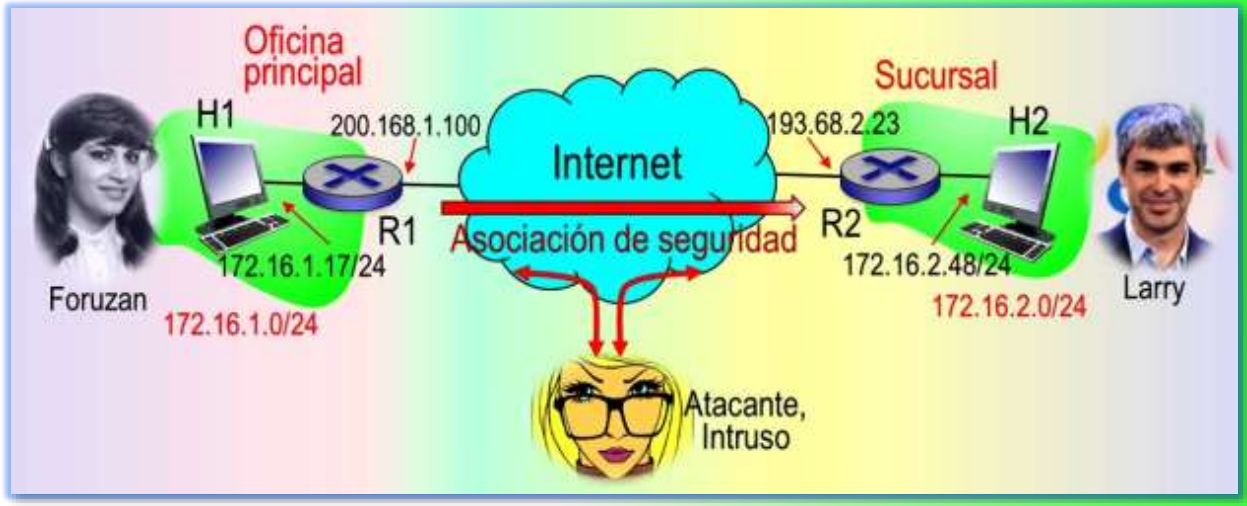
Vista panorámica de los servicios IPsec

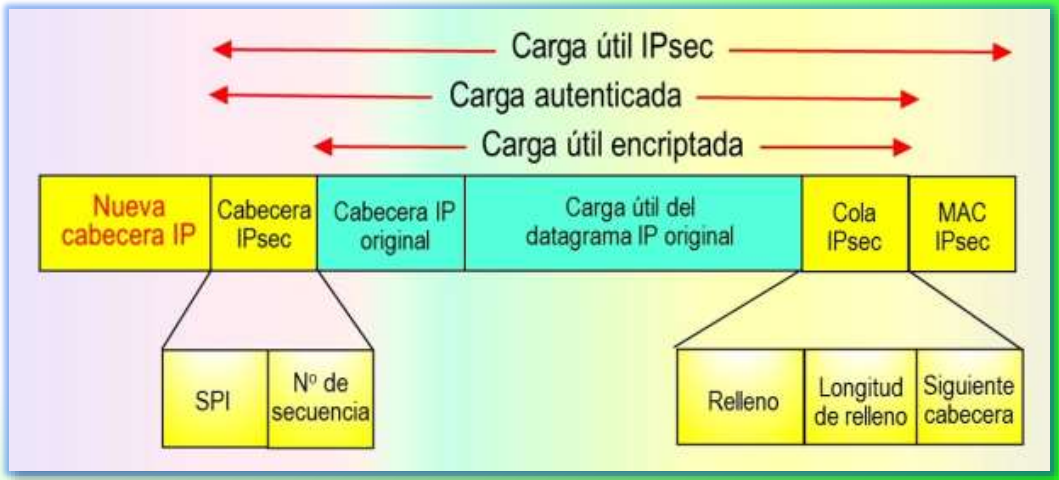
VPN CON PROTOCOLO IPsec

¿Qué servicios proporciona IPsec? (cont.)

(Kurose, 2017)

- ▶**2.** Integridad. Suponga que el Atacante trata de alterar un datagrama modificando algunos de sus bits. Cuando este datagrama alterado llegue a R2 no pasará las comprobaciones de integridad (utilizando el valor MAC IPsec), desbaratando las intenciones del Atacante.
- ▶**3.** Autenticación. Suponga que el Atacante intenta hacerse pasar por R1, creando un datagrama IPsec cuyo origen sea 200.168.1.100 y cuyo destino sea 193.68.2.23. El ataque no tendrá ningún efecto, ya que este datagrama de nuevo no pasará la comprobación de autenticación realizada por R2.
- ▶**4.** Ataques por reproducción. Puesto que la Cabecera IPsec incluye números de secuencia, el Atacante no podrá desarrollar con éxito ningún ataque por reproducción.
- **En resumen**, IPsec proporciona, entre cualquier pareja de dispositivos que procesen paquetes en la capa de red, mecanismos de:
  - ▶Confidencialidad
  - ▶Integridad de los datos
  - ▶Autenticación del origen
  - ▶Prevención de los ataques por reproducción.

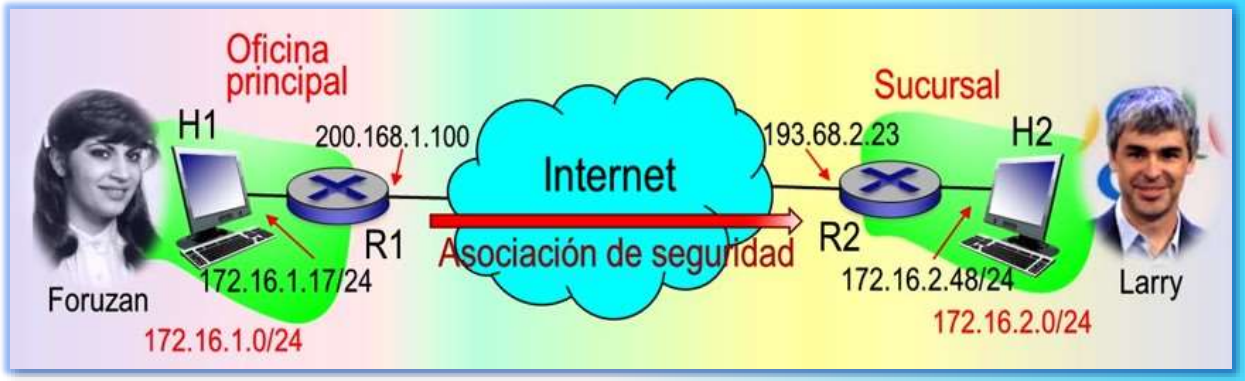




VPN CON PROTOCOLO IPsec

Protocolo de Intercambio de Claves en Internet IKE

(Kurose, 2017)



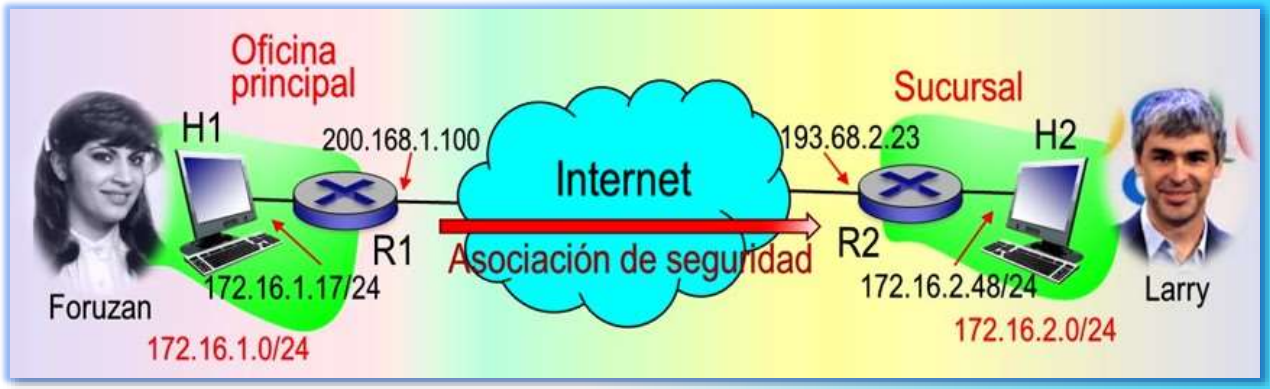
- **Cuando una VPN** tiene un pequeño número de terminales (por ejemplo, solo dos routers, el administrador de la red puede introducir manualmente la información de la asociación de seguridad (claves y algoritmos de cifrado/autenticación y los índices SPI) en las bases de datos SAD de los puntos terminales.
- **Este tipo de** "introducción manual" de las claves resulta obviamente poco práctico para una VPN de gran tamaño, que puede constar de centenares o incluso miles de hosts y routers IPsec.
- **Las tareas de implantación** de gran envergadura geográficamente distribuidas requieren un mecanismo automatizado para la creación de las asociaciones de seguridad . IPsec lleva a cabo este tipo de tarea mediante el protocolo de Intercambio de Claves de Internet (IKE), especificado en RFC 5996.
- **Cada entidad IPsec** tiene un certificado, que incluye la clave pública de la entidad. El protocolo IKE exige que las dos entidades intercambien certificados, negocien los algoritmos de autenticación y cifrado e intercambien de modo seguro el material necesario para crear claves de sesión para las asociaciones de seguridad de IPsec. IKE emplea dos fases para llevar a cabo estas tareas.

VPN CON PROTOCOLO IPsec

Fase 1 de IKE para el intercambio de claves

(Kurose, 2017)

- ▶**Durante el primer** intercambio de mensajes los dos lados utilizan el algoritmo de intercambio de claves de Diffie – Hellman para crear una IKE SA bidireccional entre los routers.
  - ✉ La IKE SA proporciona, por tanto, un canal autenticado y cifrado entre los dos routers. Durante este primer intercambio de parejas de mensajes se establecen las claves de cifrado y autenticación para la IKE SA.



- ✉ También se establece un valor secreto maestro que se utilizará para calcular las claves IPsec SA posteriormente en la Fase 2. Observe que durante este primer paso no se utilizan claves públicas ni privadas RSA. En particular ni R1 ni R2 revelan su identidad firmando un mensaje con su clave privada.

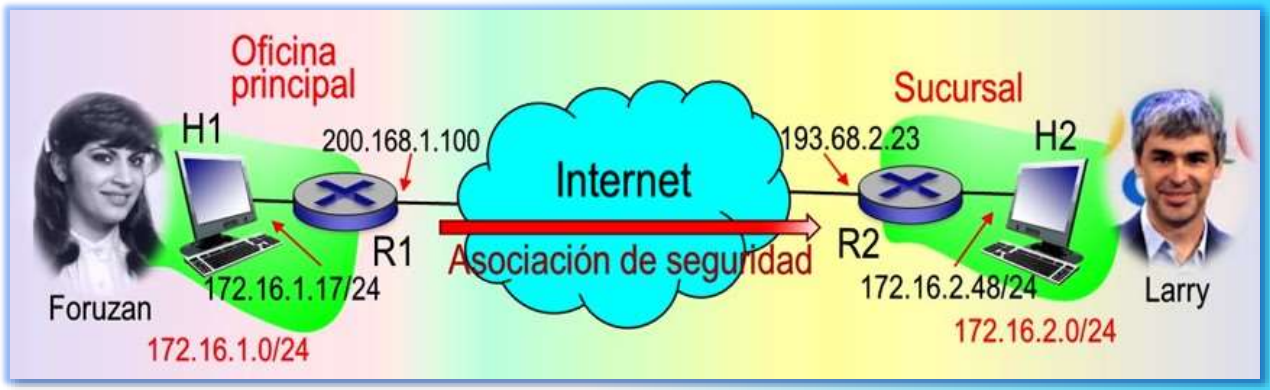
Gestión de claves en IPsec

VPN CON PROTOCOLO IPsec

Fase 2 de IKE para el intercambio de claves

(Kurose, 2017)

- ▶**Fase 2**. Durante el segundo intercambio de mensajes ambos lados se revelan mutuamente su identidad, firmando sus mensajes.
  - ✉ Sin embargo, las identidades no son reveladas a nadie que esté husmeando pasivamente el canal de comunicación, ya que los mensajes se envían a través del canal IKE SA seguro.

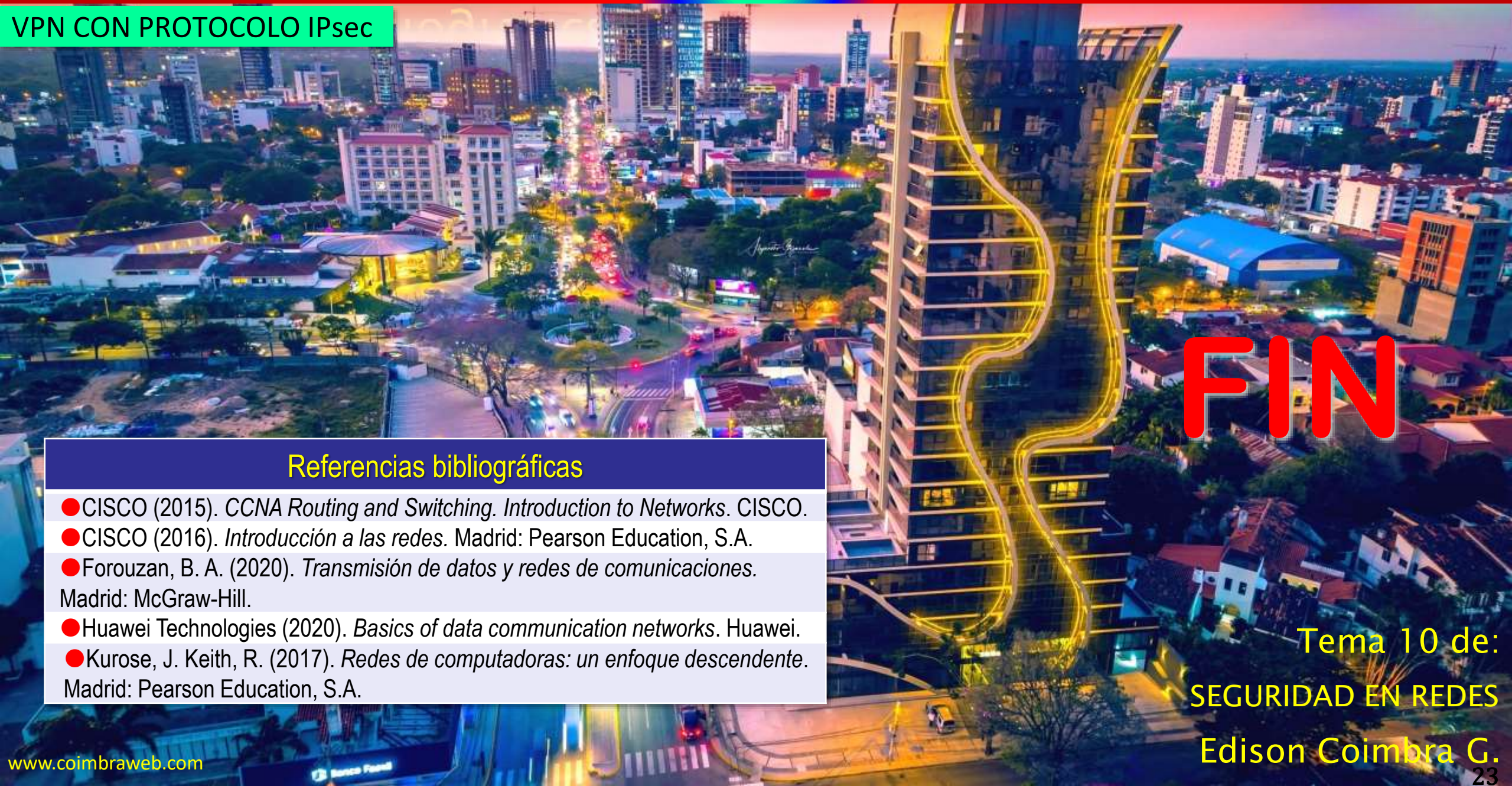


  - ✉ También durante esta fase los dos lados negocian los algoritmos de cifrado y autenticación IPsec que serán empleados por las asociaciones de seguridad IPsec.

- **En esta Fase 2 de IKE,** los dos lados crean una asociación de seguridad en cada dirección. Al final, las claves de sesión para cifrado y autenticación habrán sido establecidas en ambos terminales para las dos asociación de seguridad. Los dos lados pueden emplear entonces las asociaciones de seguridad para enviar datagramas seguros.

- **La principal motivación** para que existan dos fases IKE es el costo computacional, puesto que la Fase 2 no implica ningún tipo de criptografía de clave pública, IKE puede generar un gran número de asociaciones de seguridad entre las dos entidades IPsec con un costo de computación relativamente bajo.

Referencias bibliográficas



Referencias bibliográficas

- CISCO (2015). *CCNA Routing and Switching. Introduction to Networks*. CISCO.
- CISCO (2016). *Introducción a las redes.* Madrid: Pearson Education, S.A.
- Forouzan, B. A. (2020). *Transmisión de datos y redes de comunicaciones.* Madrid: McGraw-Hill.
- Huawei Technologies (2020). *Basics of data communication networks*. Huawei.
- Kurose, J. Keith, R. (2017). *Redes de computadoras: un enfoque descendente*. Madrid: Pearson Education, S.A.

FIN

Tema 10 de:

SEGURIDAD EN REDES

Edison Coimbra G.