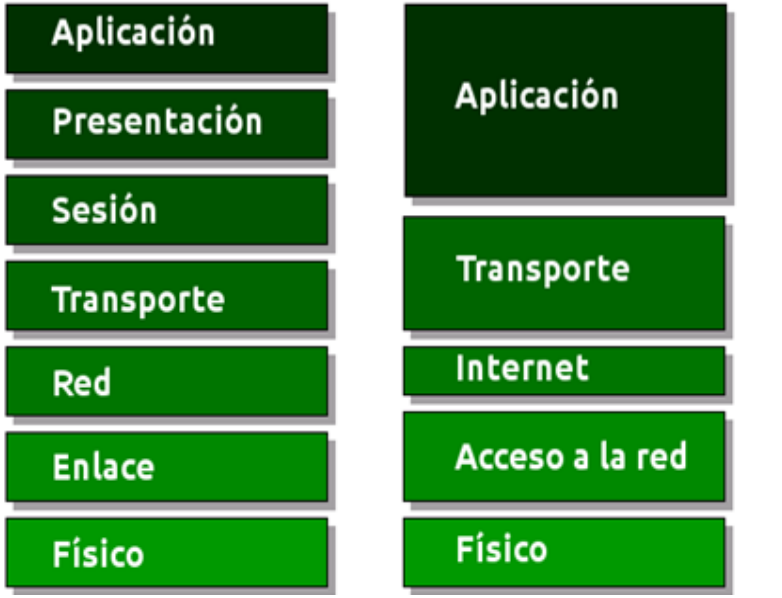
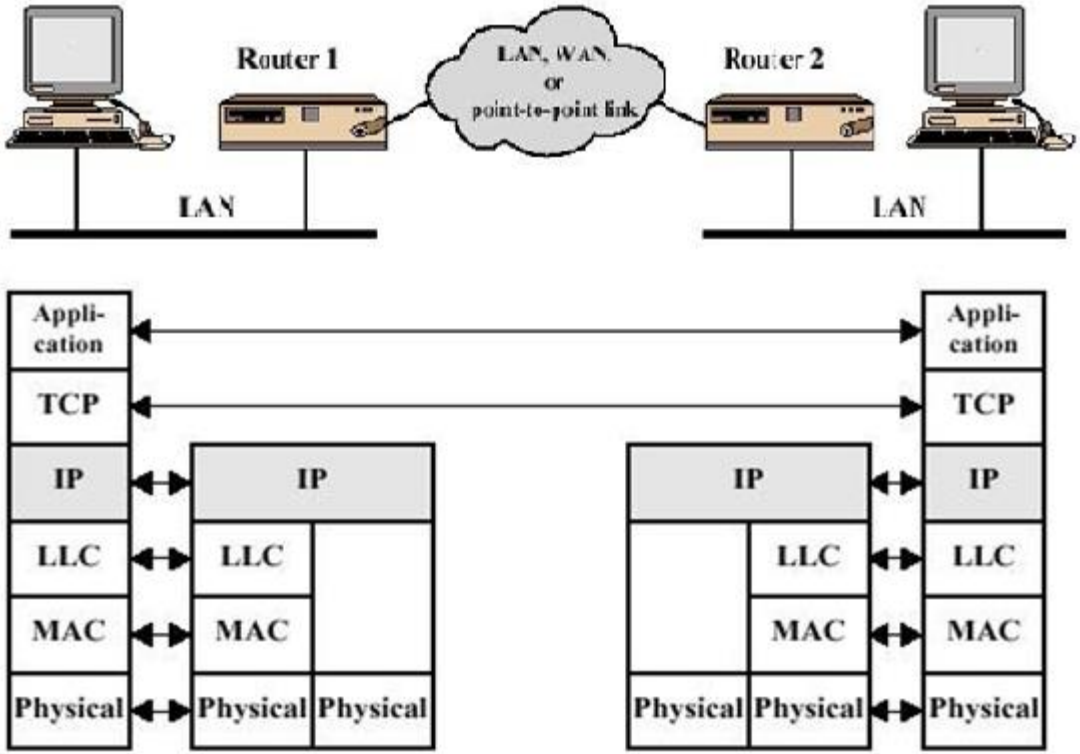
Unidades V y VI: Criptografía en Redes

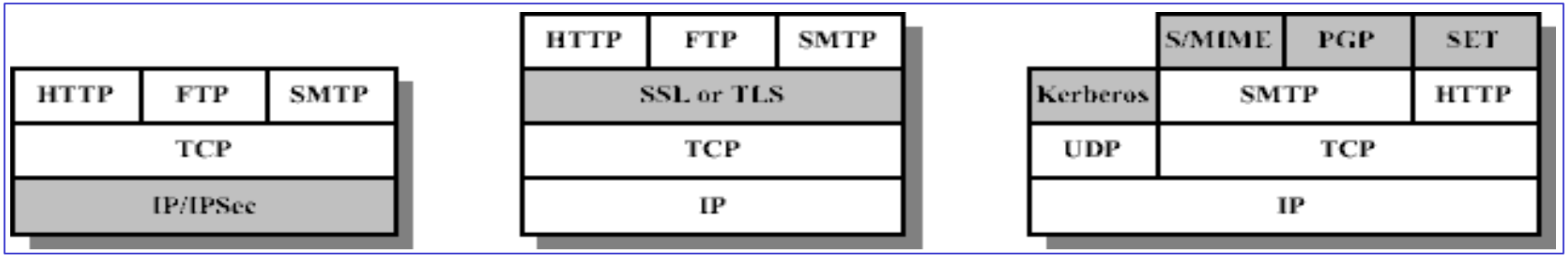
Protocolos TLS/Kerberos/y otros. DSS. PGP. SSH. SSL. TLS. Kerberos. IPSec. Implementación en GNU/Linux y en Windows. Análisis de Técnicas de Intrusión.

El modelo OSI y las redes TCP/IP



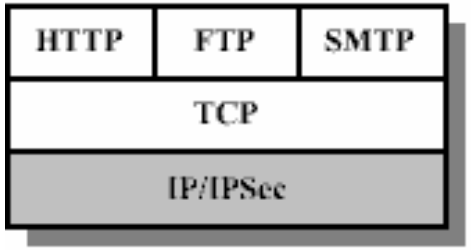


Protocolos de seguridad en TCP/IP



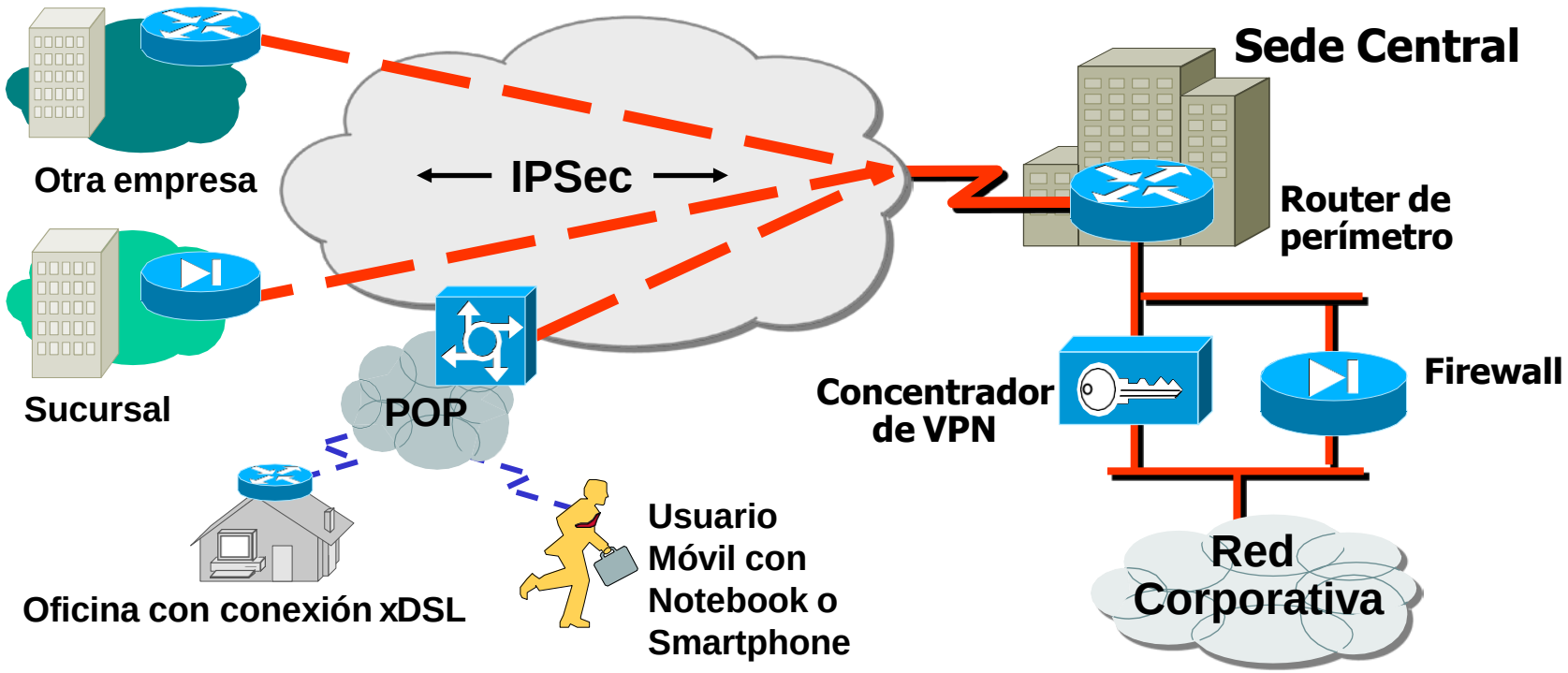
IPSec

- Protocolo específico para IP:
  - Es opcional en IP v4
  - De implementación obligatoria en IP v6



- Puede cifrar y/o autenticar todo el tráfico a nivel IP.
- Permite implementar VPN (Virtual Private Network).
- Permite soportar distintas aplicaciones.
- Es transparente para aplicaciones y usuarios.
- Todas las aplicaciones distribuidas, incluyendo la conexión remota, aplicaciones cliente/servidor, correo electrónico, transferencia de archivos y acceso a la Web se pueden encapsular en IPSec.

IPSec



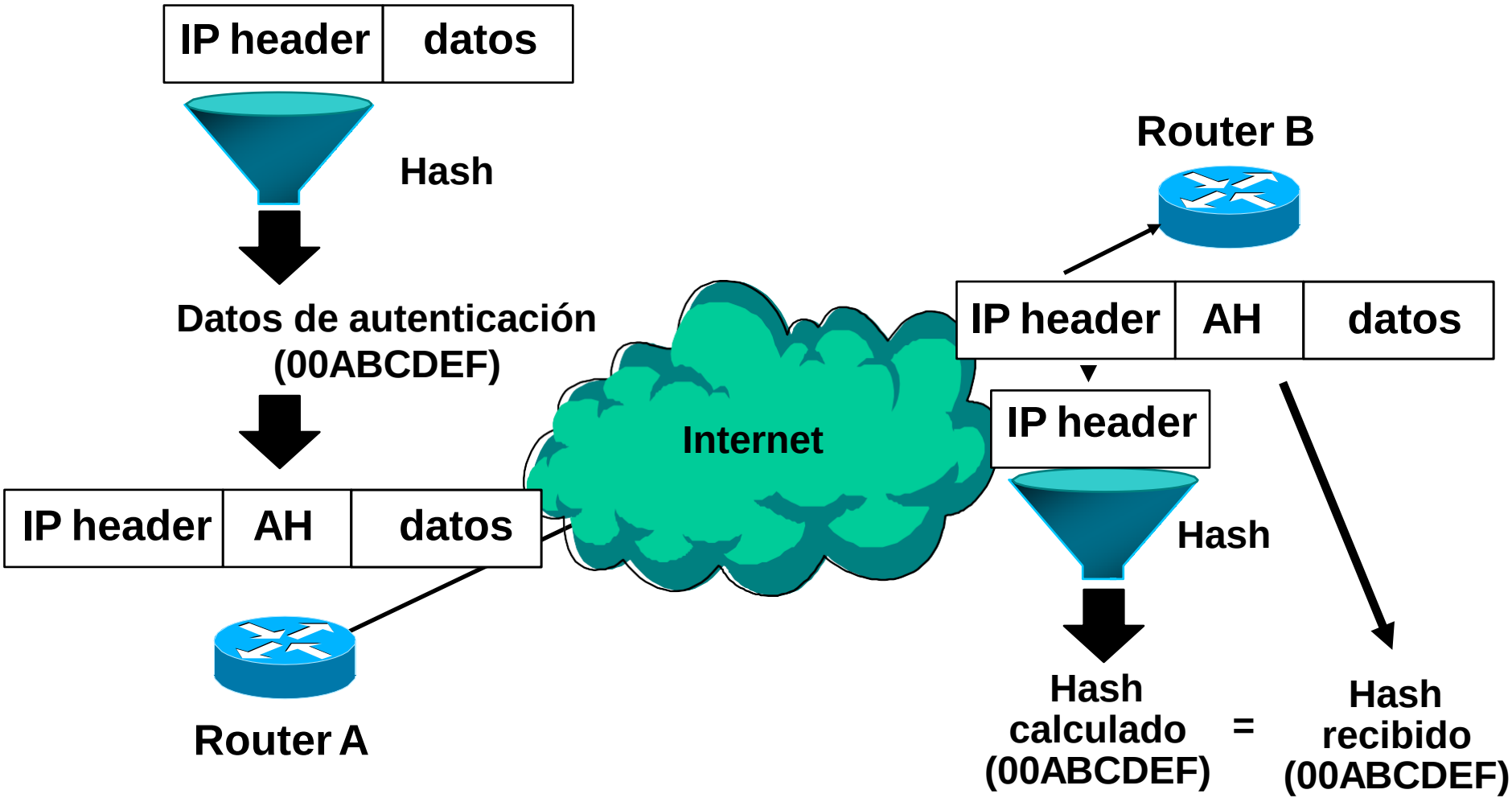
Estándar del IETF: permite comunicaciones seguras entre dos entes de capa 3:

- Estándar abierto que permite asegurar las transmisiones de datos.
- Permite asegurar la confidencialidad, integridad y autenticidad del origen de los datos.

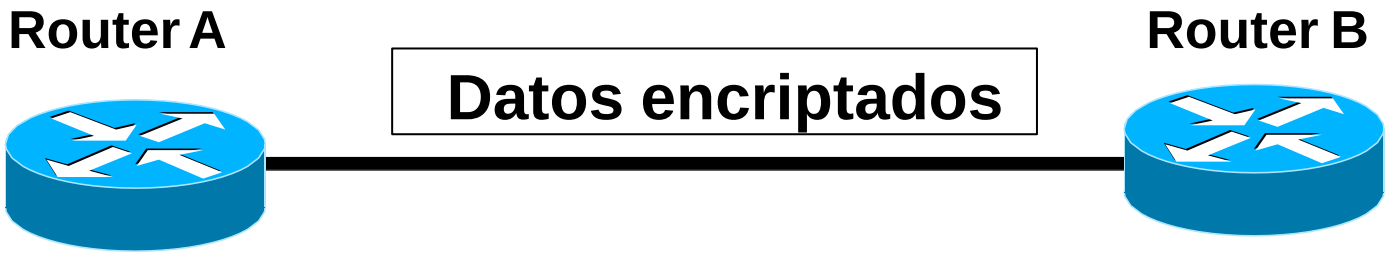
AH – Authentication Header

- Asegura la integridad de los datos
- Provee autenticación de origen (asegura que los datos llegan desde el router origen)
- Usa mecanismos de claves "hasheadas"
- No provee confidencialidad
- Provee en forma opcional servicios anti-replay

AH – Authentication Header

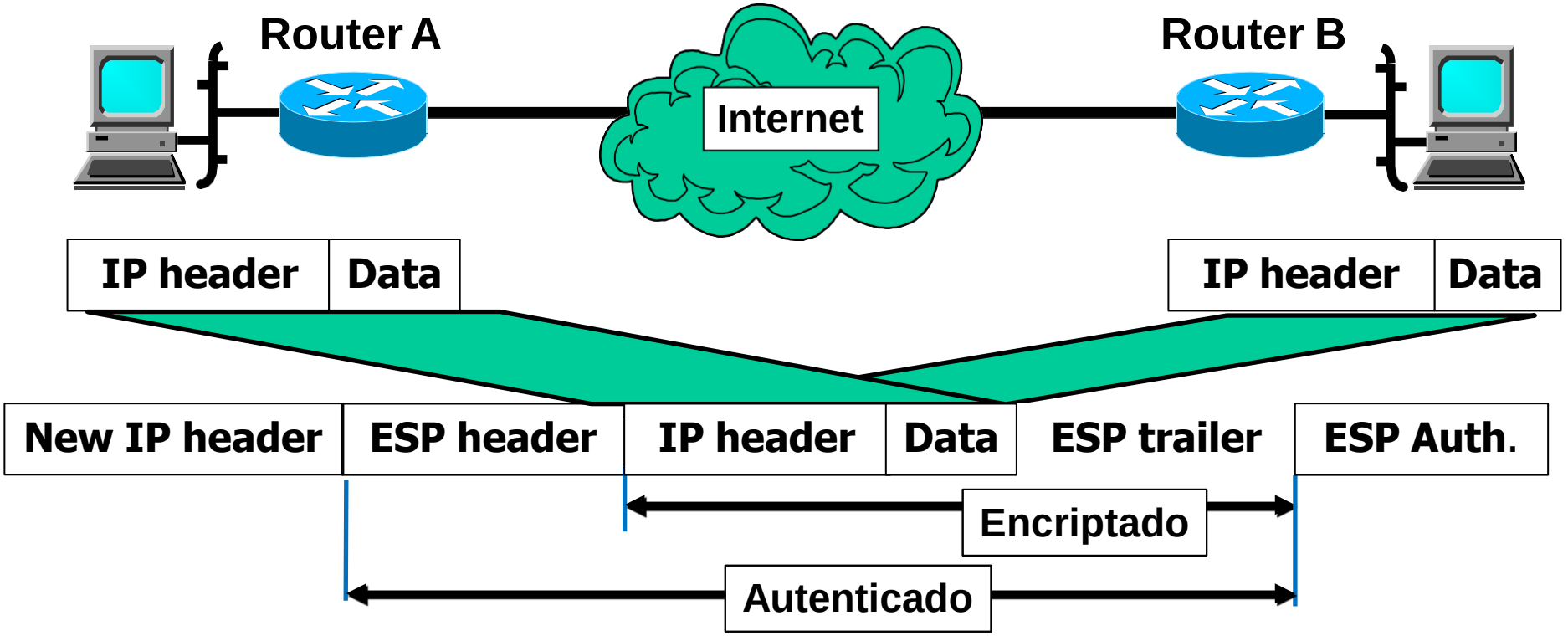


ESP - Encapsulating Security Payload



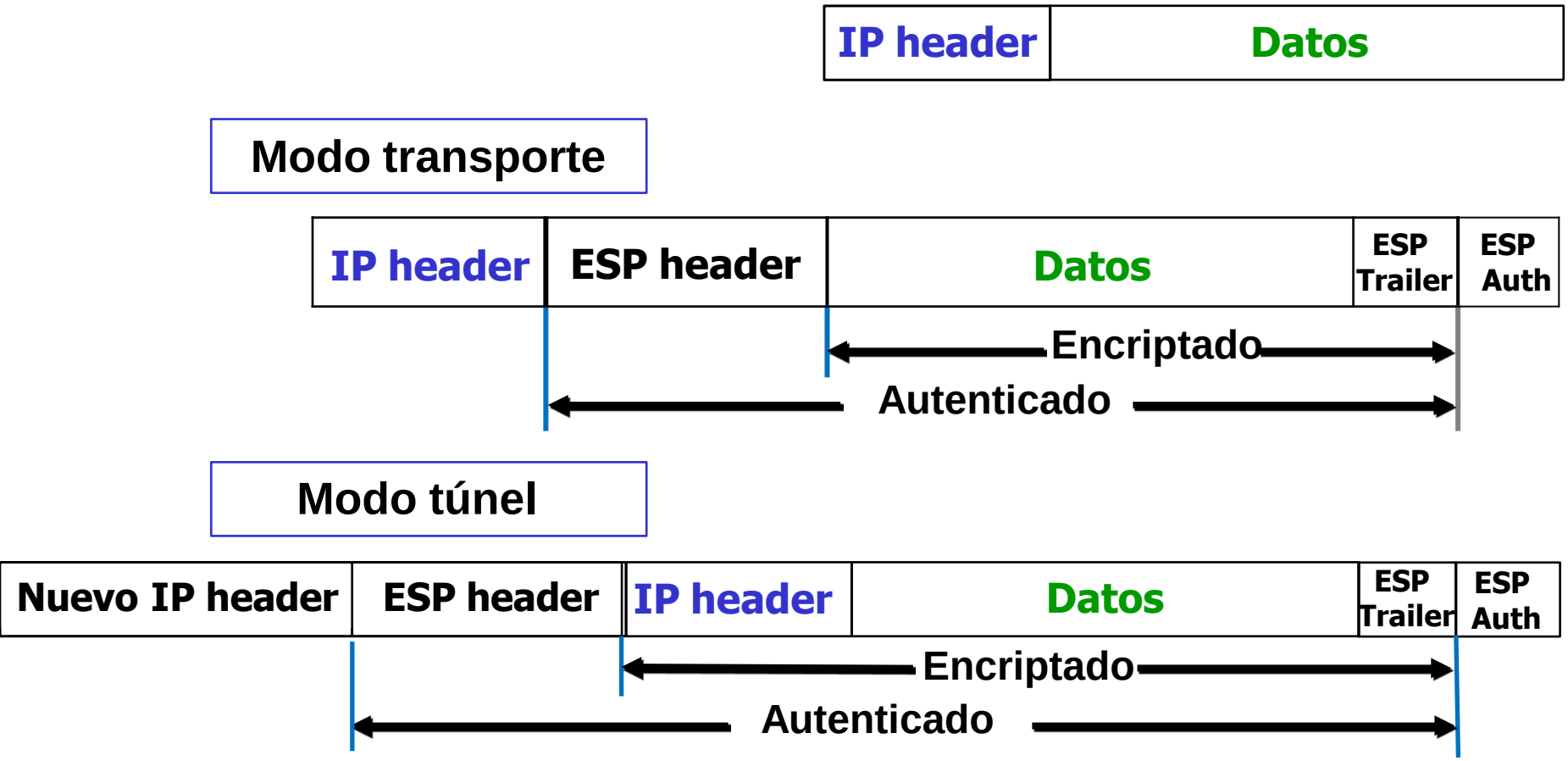
- Confidencialidad de datos → Cifrado
- Integridad de datos
- Aunteticación de origen
- Opcionalmente, protección anti-replay

Protocolo ESP

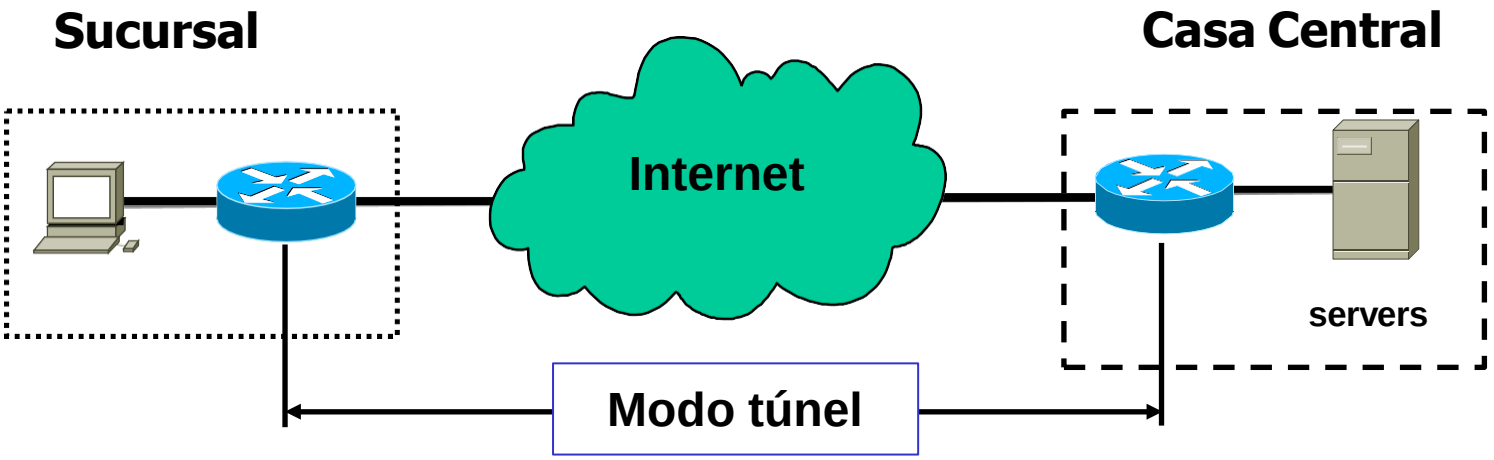


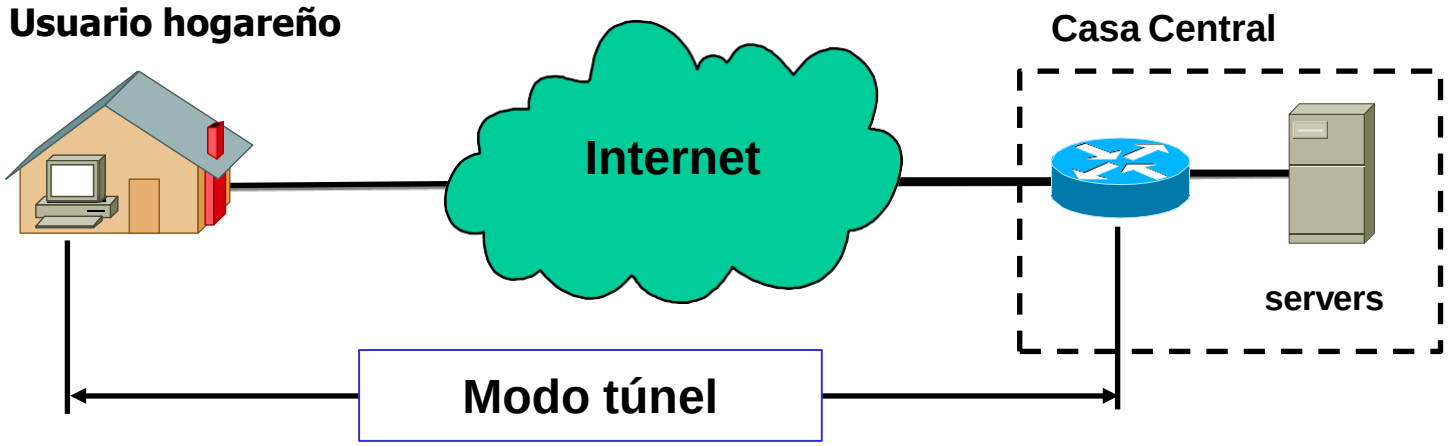
- Provee confidencialidad con cifrado.
- Provee integridad con autenticación.

Modos de uso: túnel vs. transporte



Modo túnel


Sucursal
Casa Central
Internet
servers
Modo túnel


Usuario hogareño
Casa Central
Internet
servers
Modo túnel

Protocolo IPSec: Framework

- Porque es un framework, no hay un único algoritmo para encriptar ni para hacer Hash, ni una única forma de intercambiar las llaves
- Las llaves se pueden administrar manualmente o a través de un Protocolo de Gestión de Llaves
- El estándar de facto es: IKE (Internet Key Exchange)
- IKE es una combinación de los protocolos ISAKMP y OAKLEY
- ISAKMP es un framework que permite negociar los parámetros de conexión (algoritmos, protocolos, modos y llaves)
- El protocolo OAKLEY es el que gestiona el proceso de negociación
- ISAKMP es la infraestructura y OAKLEY ejecuta los pasos

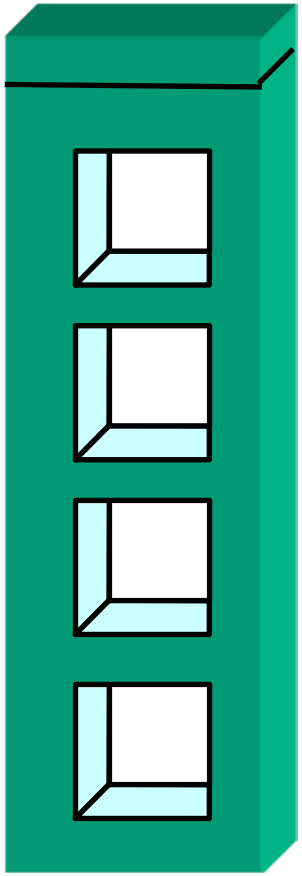
Protocolo IPSec: Framework

ESP

Encripción

Autenticación

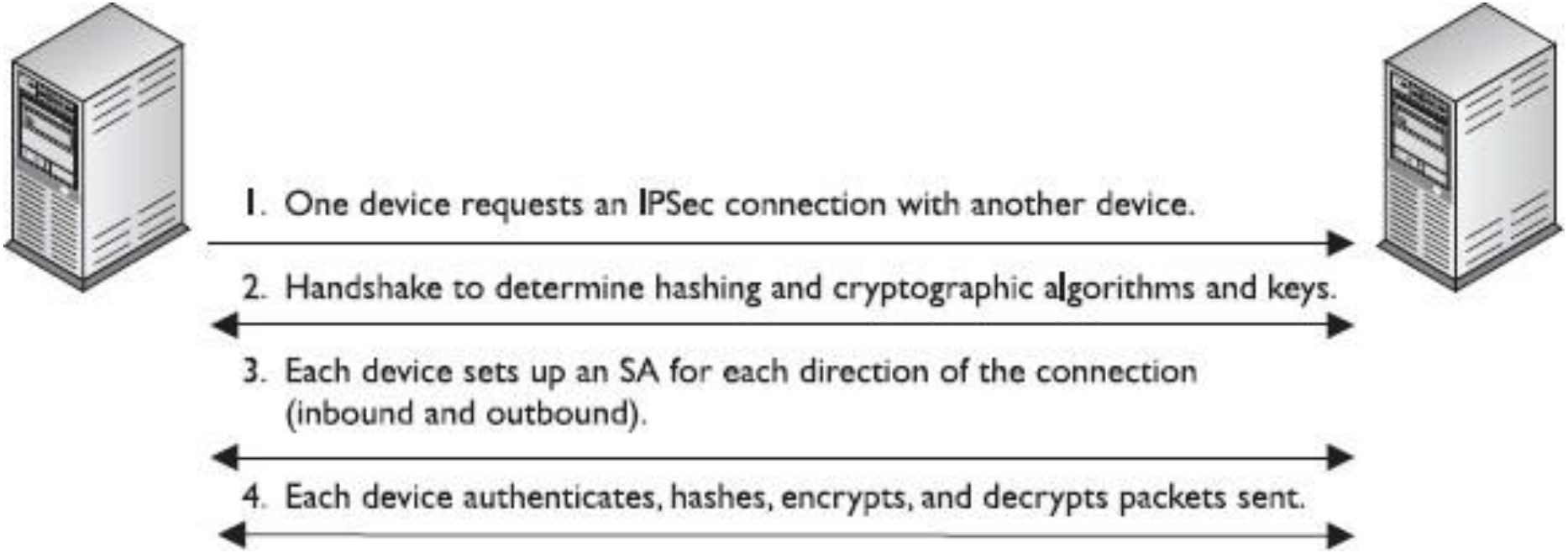
Diffie-Hellman



Posibilidades:

- ESP
- ESP +AH
- DES
- 3 DES
- MD5
- SHA
- DH1
- DH2

Secuencia de una comunicación con IPSec

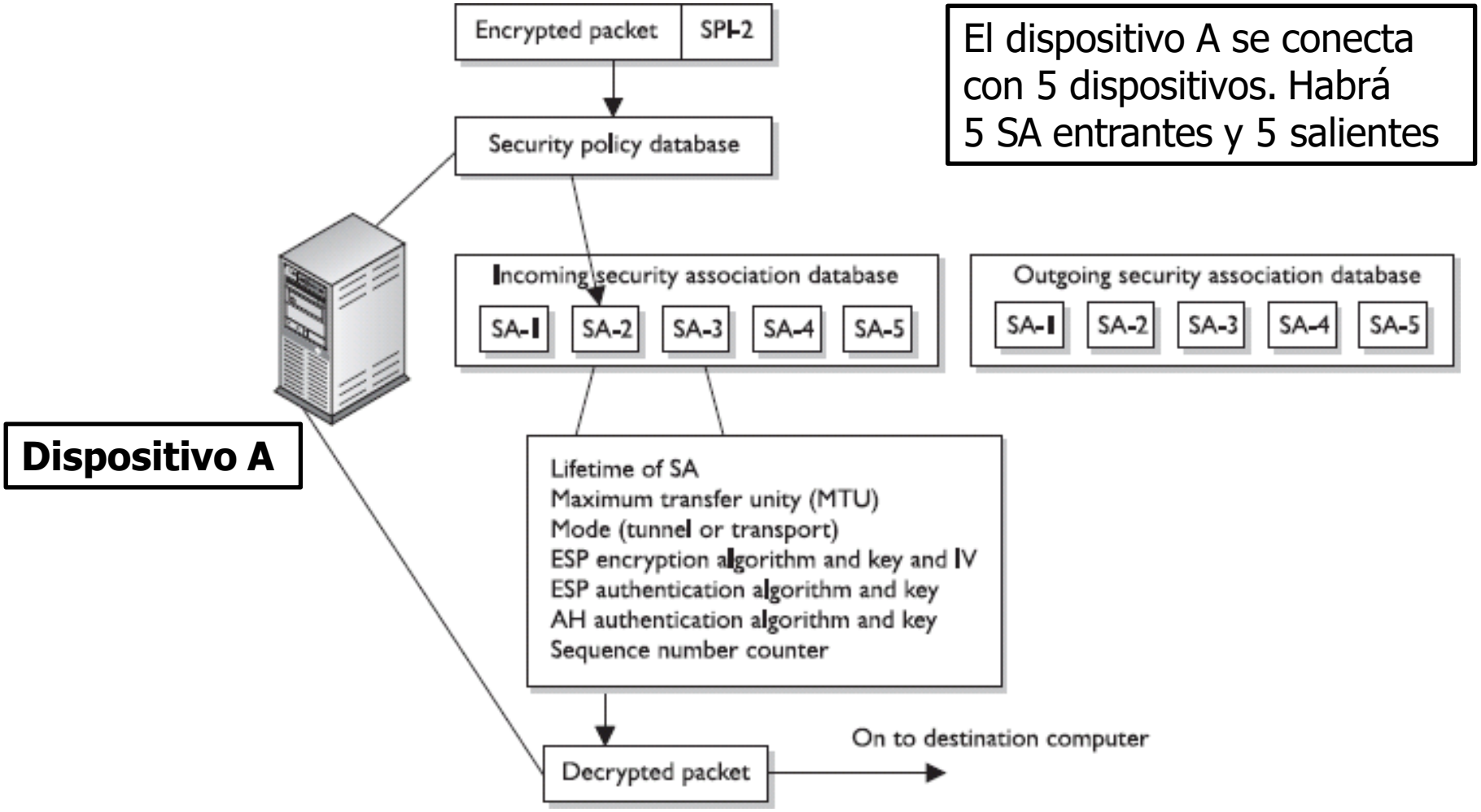


SA: Security Association

SA: ¿cómo funcionan?

- Las SAs son direccionales
- Un dispositivo tiene una SA para el tráfico entrante y otra diferente para el tráfico saliente, para cada canal de comunicaciones
- Además un dispositivo se puede conectar a varios dispositivos
- Para organizar las SAs de las comunicaciones entrantes y salientes con cada uno de los dispositivos a los que se conecta, se utiliza el SPI (Security Parameter Index)
- Cada dispositivo tiene un SPI que guarda el "tracking" de las diferentes SAs y le indica al dispositivo cual SA debe usar cuando transmite o recibe un paquete de datos de otro dispositivo
- El valor del SPI está en el Header del paquete IPSec
- Cuando el dispositivo lee el SPI, sabrá a cual SA consultar

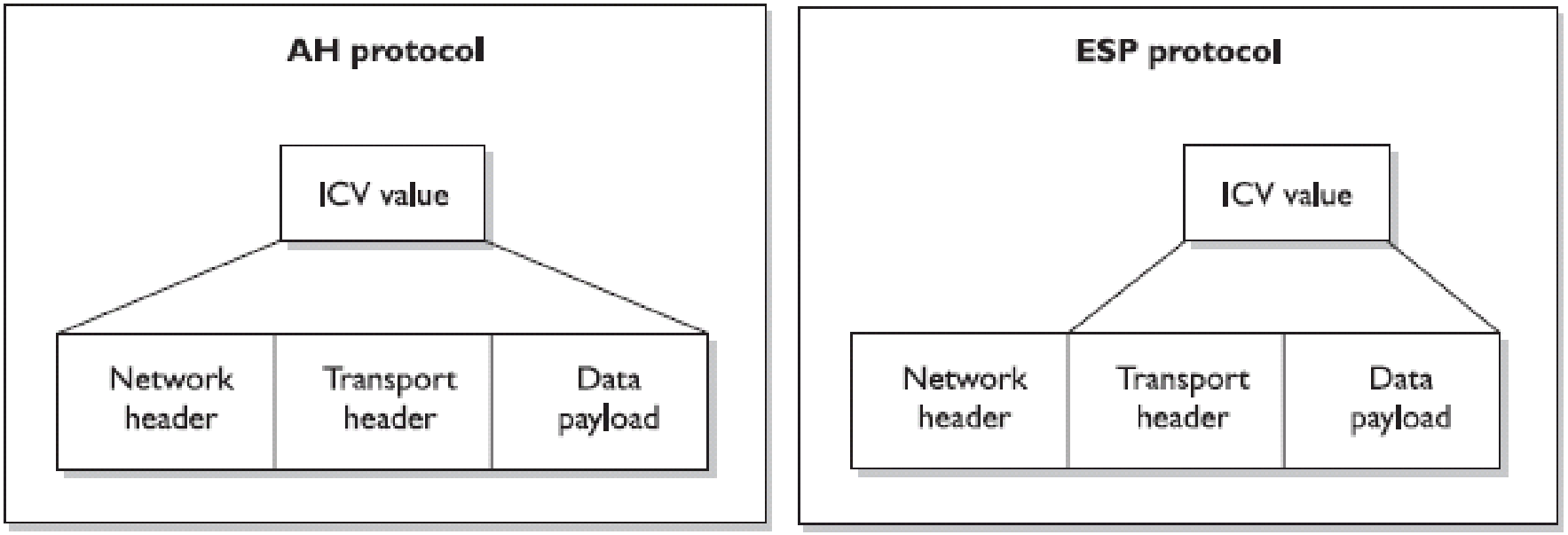
SPI – Security Parameter Index



El dispositivo A se conecta con 5 dispositivos. Habrá 5 SA entrantes y 5 salientes

Dispositivo A

ICV – Integrity Check Value



- IPSec genera un valor de ICV, que es equivalente a un MAC (Message Authentication Code), sobre una parte del paquete de datos.
- El emisor y el receptor generan sus propios valores de ICV.
- Si el valor calculado coincide con el recibido, esto implica que el paquete no ha sido modificado.

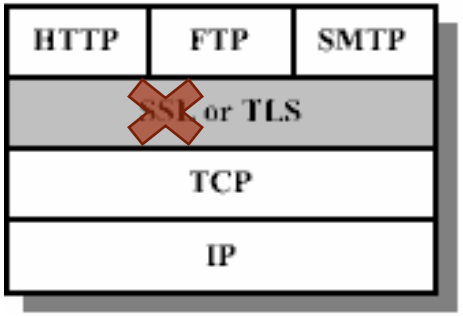
S-HTTP vs. HTTPS

- Secure HTTP (S-HTTP): es una tecnología que protege cada mensaje que es enviado entre 2 computadoras
- HTTPS: protege el canal de comunicaciones entre 2 computadoras
- HTTPS usa TLS y HTTP para proveer un circuito protegido entre un cliente y un servidor. HTTP corre en la capa de Aplicación (OSI) y TLS entre la Sesión y Transporte (OSI)
- Cuando solo tengo que cifrar un mensaje, uso S-HTTP
- Si necesito encriptar toda la información que voy a intercambiar entre 2 computadoras, uso HTTPS

https://https.cio.gov/

TLS (Transport Layer Security)
SSL – Secure Socket Layer

Protocolo de comunicaciones que proporciona integridad, autenticación y privacidad de la información entre extremos.



Las etapas:

- Negociación de algoritmos a utilizar.
- Intercambio de certificados y autenticación.
- Negociación de clave simétrica de sesión.

https://www.incibe.es/protege-tu-empresa/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del

Obsolescencia de SSL – Vigencia de TLS 1.3

- Algoritmos criptográficos que utiliza SSL:
  - Clave pública: RSA, Diffie-Hellman, DSA
  - Clave simétrica: RC2, RC4, IDEA, DES, 3DES o AES
  - Hash: MD5 o alguno de la familia SHA.
- El cliente generaba una llave de sesión y la cifraba con la llave pública del servidor. Se la enviaba al servidor y ambos la usaban para la encripción simétrica de los datos transmitido.
- Utilizado para implementar HTTPS, S-HTTP y canales seguros para otros protocolos como puede ser POP3S.
- Versiones a utilizar: TLSv1.3 (RFC 8446). https://www.ietf.org/blog/tls13/

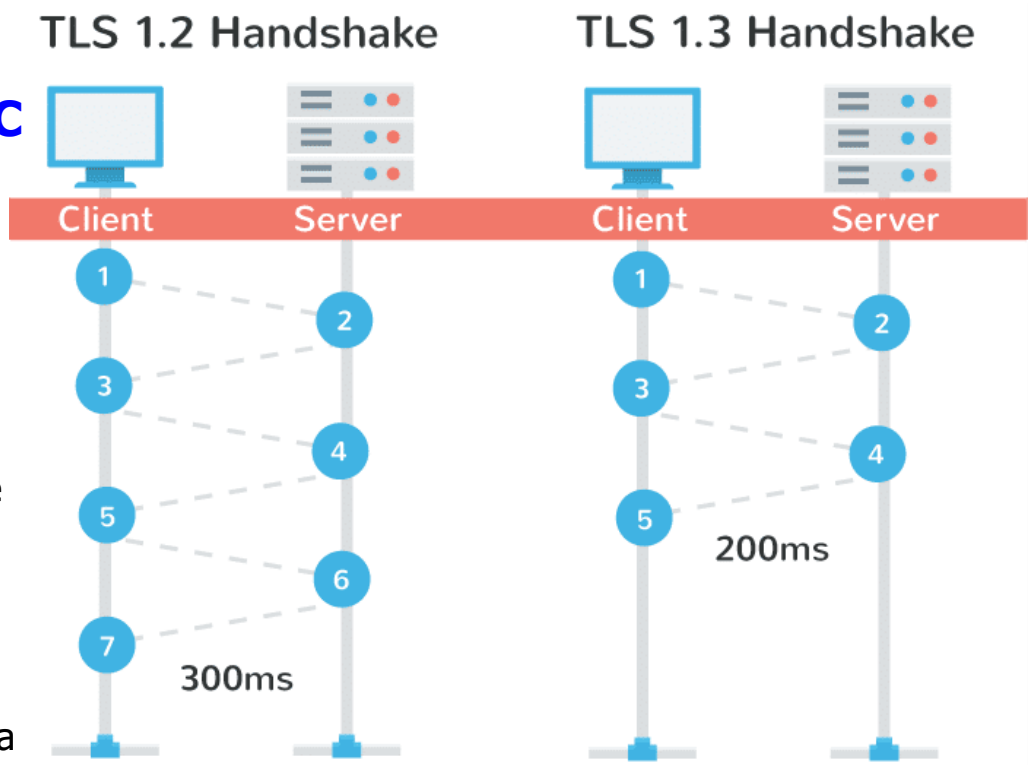
TLS 1.3

- **Privacidad.** El TLS 1.3 encripta la mayor parte del proceso de establecimiento de comunicación (que se conoce como handshake en inglés). Según IETF, esta mejora respecto a TLS 1.2 ayuda a proteger las identidades de los participantes e impide el análisis del tráfico.
- **Mayor seguridad.** Uno de los grandes problemas del TLS 1.2 era la existencia de algoritmos y protocolos obsoletos. Vulnerabilidades como *Logjam* y *Sweet32* que han dado pie a ataques reales. La actualización 1.3 solo trabaja con algoritmos sin vulnerabilidades, al menos, conocidas.
- **Rendimiento.** Para el proceso de handshake, el cliente y el servidor intercambian llaves criptográficas y establecen la comunicación. Este proceso de ida y vuelta se conoce como roundtrip. El TLS 1.3 permite que la mayoría de comunicaciones se establezca en un único roundtrip, lo que reduce mucho los tiempos de la comunicación.

https://hpbn.co/transport-layer-security-tls/

TLS 1.3 – Seguridad y Rendimiento

- Cifrado: **AES**
- Autenticación e integridad: **MAC**
- Proceso de handshake (roundtrip).
  - TLS Change Cipher Spec Protocol (Protocolo de especificación de cifrado de TLS) + Protocolo de alerta TLS + Protocolo de datos de aplicación TLS.
  - Único roundtrip: Zero Round Trip Time (0RTT).
  - Puede combinar TCP Fast Open y la opción TLS False Start, y reducir el retraso de 3-RTT a 1-RTT.

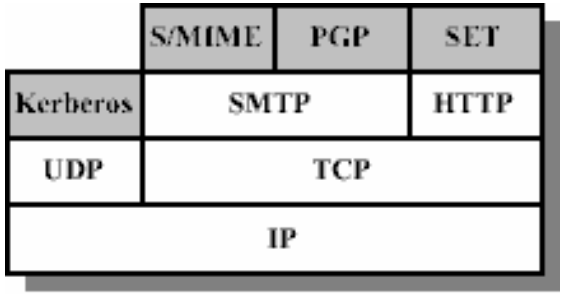


https://blogs.windows.com/msedgedev/2016/06/15/building-a-faster-and-more-secure-web-with-tcp-fast-open-tls-false-start-and-tls-1-3/
https://github.com/tlswg/tls13-spec

E-mail seguro

- **S/MIME: Secure Multipurpose Internet Mail Extensions**
  - Agrega servicios de encripción y firma digital en los clientes de correo en formato MIME, tanto para el texto del mensaje como para los archivos adjuntos (attach).
  - Usa certificados digitales X.509 entregados por una Autoridad Certificante (AC) que los clientes de correo deben reconocer como tal.
  - Crea una especie de sobre en el que se envuelven los datos encriptados y/o firmados digitalmente.
  - Usa plataformas de estándares PKCS, Public-Key Cryptography Standards.
- **SMTP, IMAP, POP3:**
  - Usan TLS para proporcionar seguridad al E-mail.

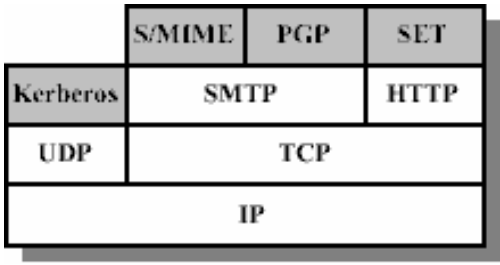
S/MIME: e-mail seguro



S/MIME provee:

- Confidencialidad mediante algoritmos de encripción.
- Integridad mediante algoritmos de Hash.
- Autenticación mediante el uso de certificados X.509.
- No repudio mediante la encripción del Hash con algún algoritmo asimétrico.

SET – Secure Electronic Transaction



- Tecnología de Seguridad desarrollada por Visa y MasterCard para hacer mas seguras las transacciones con tarjetas de crédito.
- Requería que todos los actores instalaran el software:
  - Las entidades emisoras de las tarjetas de crédito
  - Los usuarios de las tarjetas de crédito Los comercios adheridos
  - Los bancos que procesaban las operaciones
- A pesar de ser un sistema muy seguro, no tuvo aceptación por la complejidad de su operación.

SSH – Secure SHell

- Funciona como un tipo de mecanismo de túnel que permite el acceso remoto seguro a otra computadora.
- Es un programa y un set de protocolos que trabajan en conjunto.
- Se usa en reemplazo de FTP, Telnet, rlogin, rexec ó rsh.
- Luego del handshake, se establece un canal seguro que transmite en forma encriptada.

Canal seguro

SSH – Secuencia

Cliente

Servidor

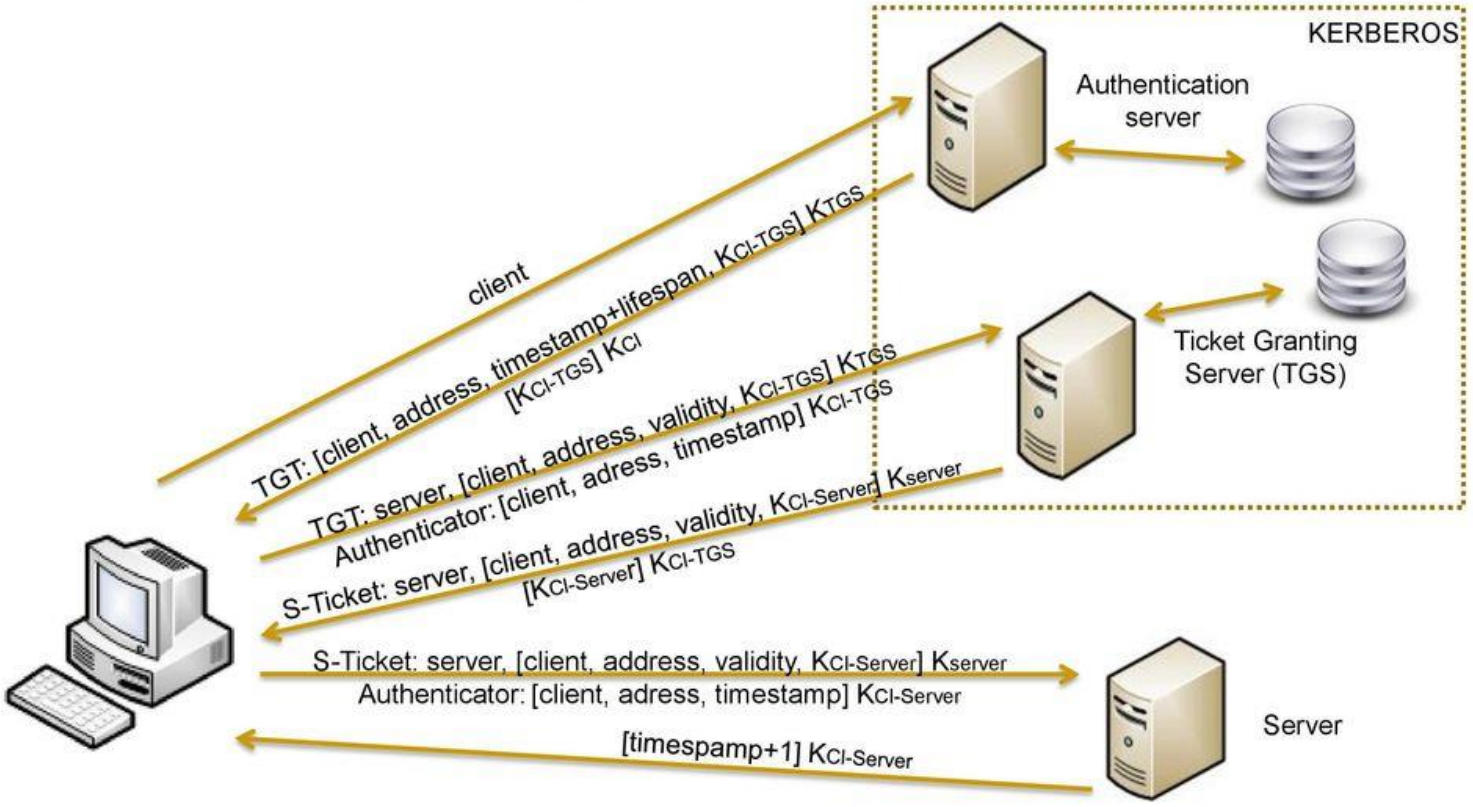
1. Client requests SSH connection
2. Handshake to find out protocol version
3. Algorithm negotiation and key exchange
4. Secure session setup
5. Client runs remote application

Kerberos

- Protocolo de autenticación para cliente-servidor en una red no segura.
- Provee autenticación mutua.
- Basado en criptografía simétrica.
- Existe una tercera parte de confianza (servidor Kerberos).
- Opcionalmente brinda integridad y confidencialidad de los datos.
- Arquitectura basada en:
  - Clave de sesión: clave secreta generada por Kerberos y expedida a un cliente para uso con un servidor durante una sesión.
  - Ticket: token expedido a un cliente por parte del servicio de tickets de Kerberos para solicitar servicios. Garantiza un cliente autenticado.
  - Autenticador: token construido por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación.

Kerberos

Kerberos - Esquema



https://www.tarlogic.com/blog/how-kerberos-works/