Seguridad en Redes de Comunicación

Tema III. Protocolos y Mecanismos de Seguridad

Luis Sánchez González

Departamento de Ingeniería de Comunicaciones
Grupo de Ingeniería Telemática

Contenido

- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Red – IPSec
  - Nivel de Transporte – SSL / TLS
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Contenido

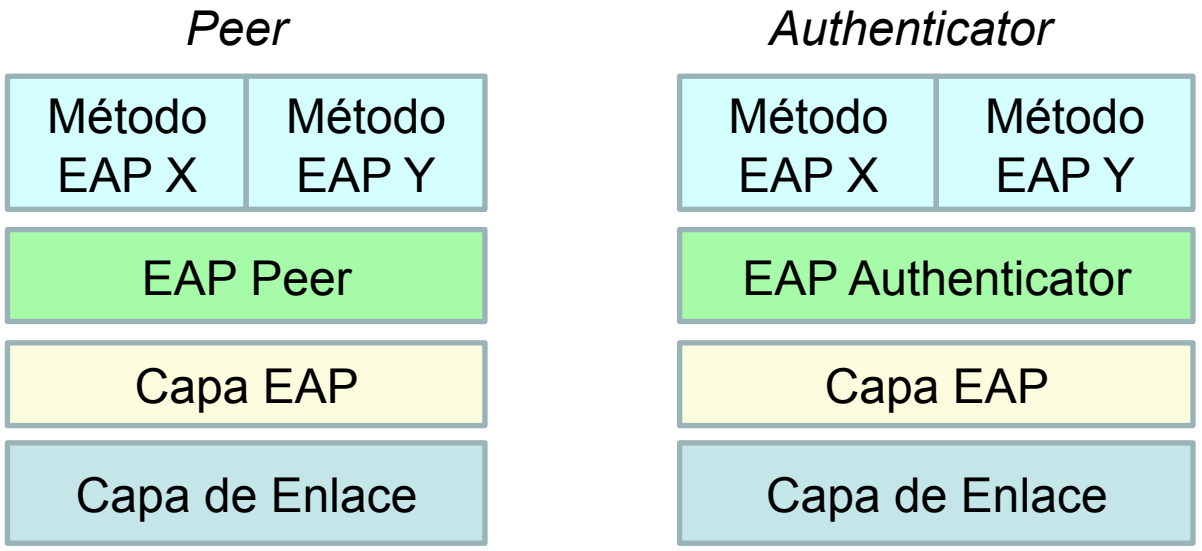
- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Red – IPSec
  - Nivel de Transporte – SSL / TLS
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Protocolos de Autenticación – EAP

- Extensible Authentication Protocol (EAP)
  - RFC 3748
  - Marco genérico de autenticación que soporta diferentes métodos de autenticación
  - Define un formato de trama y unos tipos de mensajes que los distintos métodos de autenticación usan
  - Principalmente se usa para soportar acceso a la red autenticado
    - Originalmente en PPP
    - Hoy en día sobre todo en WLAN combinado con RADIUS e IEEE 802.1x

Protocolos de Autenticación – EAP

- Arquitectura
  - Opera directamente sobre la capa de enlace sin necesidad de IP
  - De manera genérica define dos entidades
    - Peer (Cliente)
    - Authenticator (Servidor)

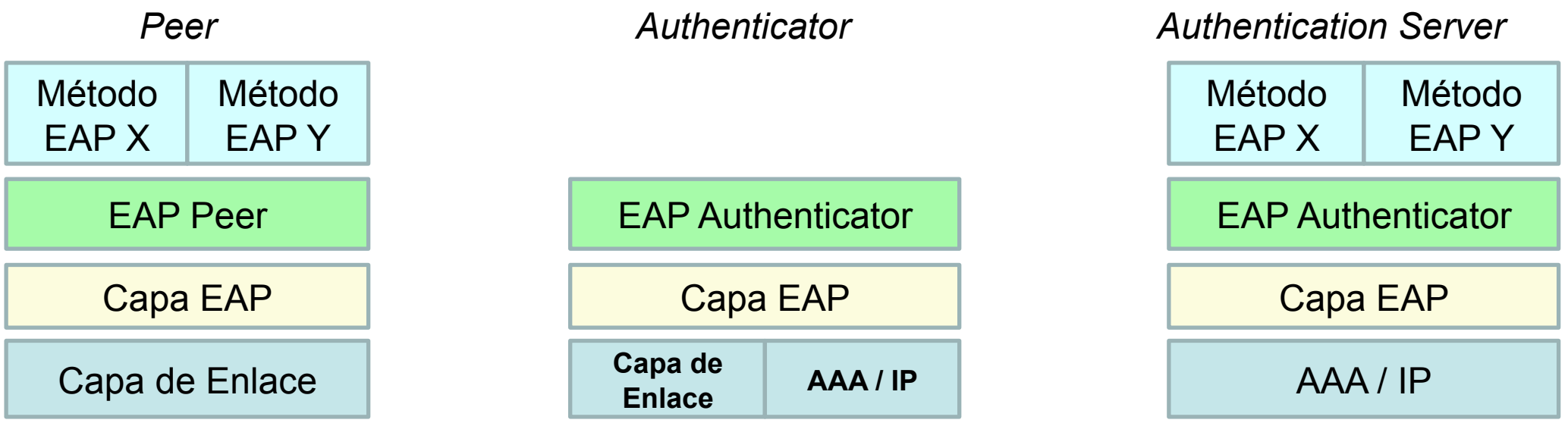


Protocolos de Autenticación – EAP

- Arquitectura
  - Capa de enlace: Transmite y recibe mensajes EAP entre Peer y Authenticator.
  - Capa EAP: Crea los mensajes EAP, hace detección de mensajes duplicados y retransmisión si fuera necesario. Demultiplexa los mensajes recibidos hacia la capa superior (EAP Peer o EAP Authenticator).
  - Capa EAP Peer y EAP Authenticator: Analizan el mensaje EAP y lo demultiplexan hacia el método EAP correspondiente
  - Métodos EAP: EAP es sólo un contenedor, la autenticación se realiza a nivel de método EAP
    - EAP-MD5
    - EAP-TLS
    - EAP-TTLS
    - EAP-SIM
    - …
    - Unos 40 métodos distintos hoy en día

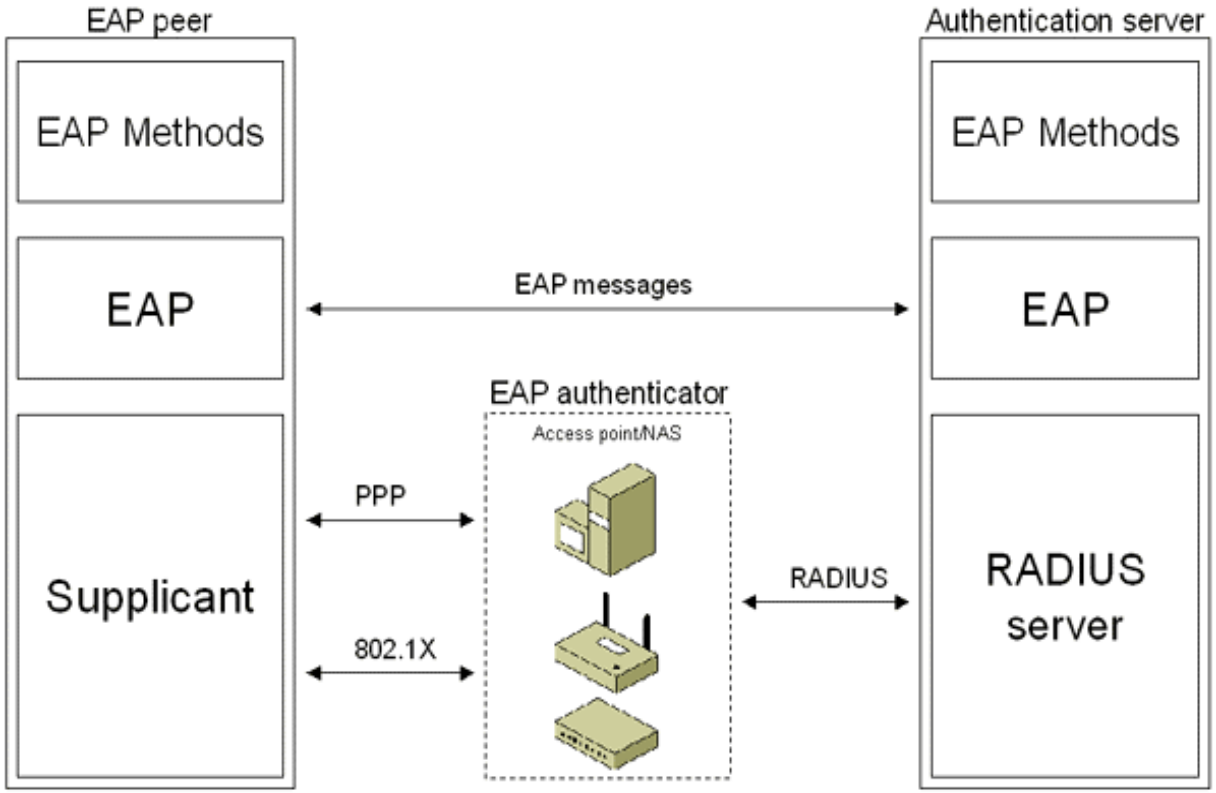
Protocolos de Autenticación – EAP

- Arquitectura
  - Comportamiento Pass-Through
    - Se añade una tercera entidad: Authentication Server



Protocolos de Autenticación – EAP

- Arquitectura
  - Escenario más común en la actualidad



Protocolos de Autenticación – EAP

- Formato del paquete EAP

Código	Identificador	Longitud
Datos …		

  - Código (1 byte): Tipo de paquete EAP
    - Petición (Request)
    - Respuesta (Response)
    - Éxito (Success)
    - Fallo (Failure)
  - Identificador (1 byte): Relaciona Petición y Respuesta
  - Longitud (2 bytes): Tamaño del paquete EAP completo

Protocolos de Autenticación – EAP

- Formato del paquete EAP
  - Código 1 o 2 (Petición o Respuesta)

Código (1 o 2)	Identificador	Longitud
Tipo	Datos …	

  - Código 3 o 4 (Éxito o Fallo)

Código	Identificador	Longitud

Protocolos de Autenticación – EAP

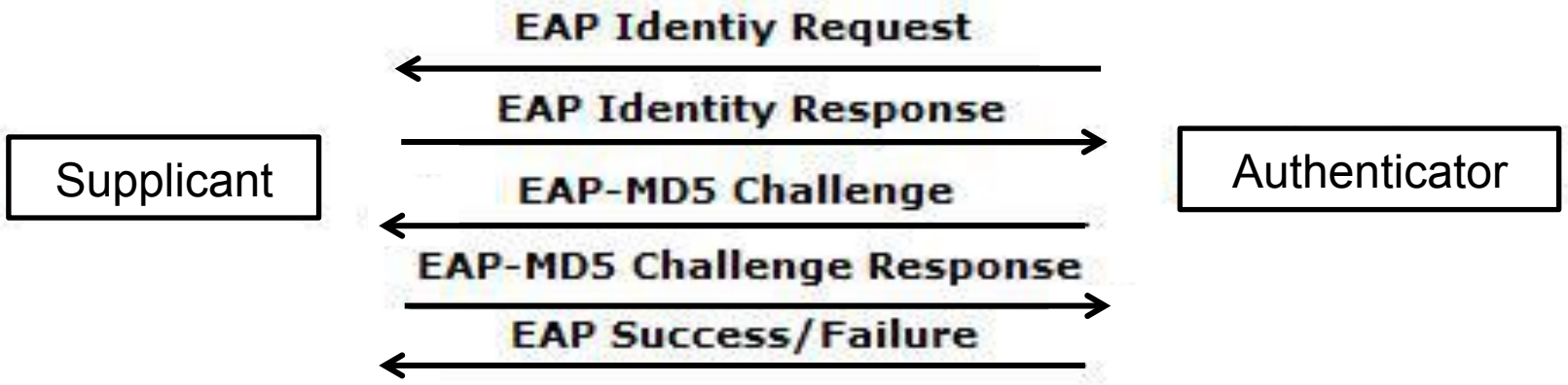
- Protocolo EAP
  - Authenticator envía Petición
  - Peer envía Respuesta
  - Tantas veces como se defina en el método EAP
  - No se envía ninguna petición sin haber recibido una respuesta a la anterior
  - Authenticator envía Éxito o Fallo en función del resultado de la conversación Petición–Respuesta
  - Se permite negociación del método de autenticación
    - Una vez elegido el método no se puede cambiar

Protocolos de Autenticación – EAP

- Protocolo EAP
  - Tipos definidos en RFC 3748
    - 1 → Identity: solicita la identidad del otro extremo
    - 2 → Notification: mensaje a mostrar en el otro extremo
    - 3 → NAK (sólo en Response): tipo de autenticación inaceptable
      - Los datos serán una lista de Tipos de Autenticación alternativos (1 byte por tipo alternativo)
      - Si no se propone alternativa se envía un byte de datos a 0
    - 4 → MD5 Challenge
    - 5 → One time password
    - 6 → Generic Token Card

Protocolos de Autenticación – EAP

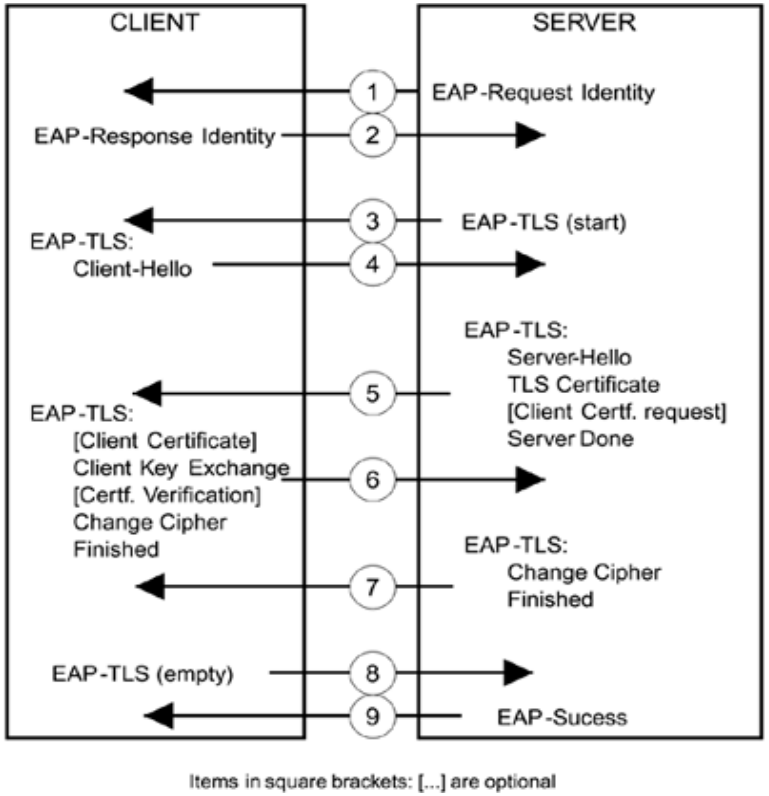
- EAP-MD5
  - Definido en RFC 3748
  - Autenticación básica basada en PSK (password)



  - Challenge Response
    - MD5(EAP Identifier | PSK | Challenge)

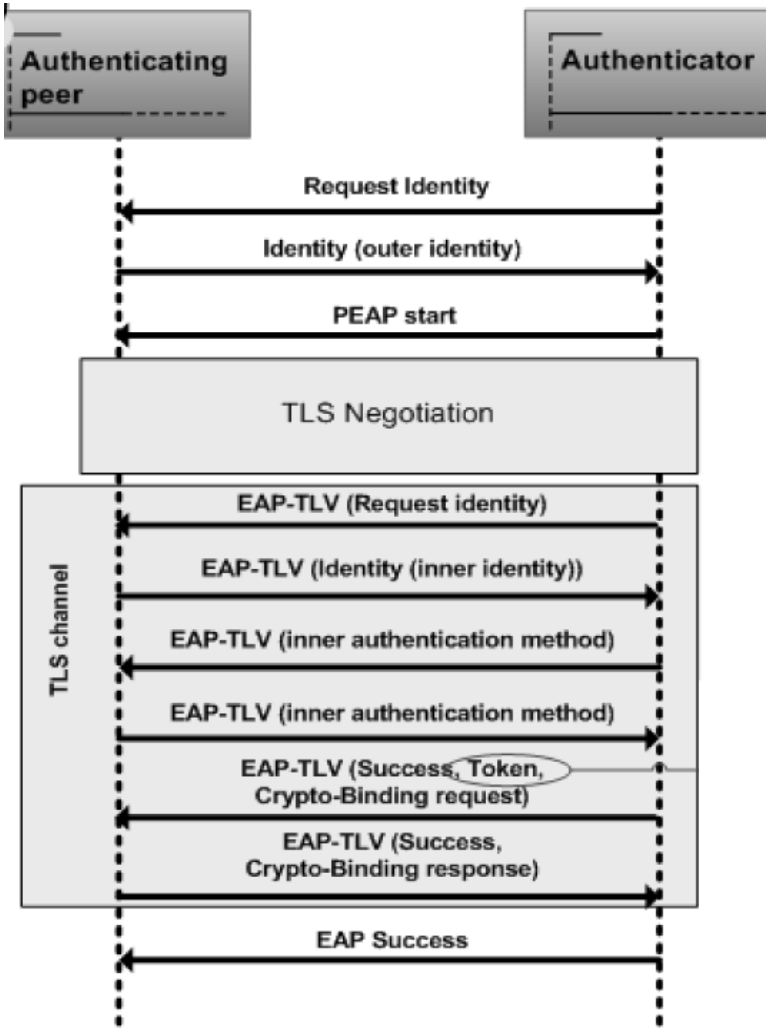
Protocolos de Autenticación – EAP

- EAP-TLS
  - Definido en RFC 5216
  - Usa certificados tanto de cliente como de servidor para autenticación mutua
  - Permite derivación dinámica de claves
    - WEP
    - WPA
    - WPA2



Protocolos de Autenticación – EAP

- Protected Extensible Authentication Protocol (PEAP)
  - Derivado de EAP-TTLS
  - Sólo necesita certificado de servidor
  - Autenticación del cliente dentro del túnel TLS creado con el certificado del servidor
  - Permite derivación dinámica de claves
    - WEP
    - WPA
    - WPA2



Protocolos de Autenticación – EAP

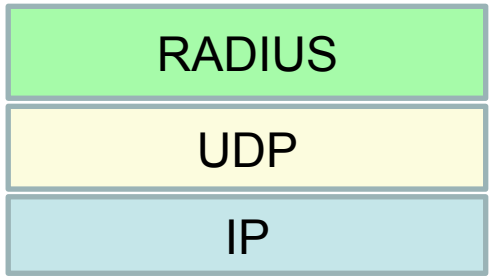
	EAP-MD5	**EAP-TLS**	**EAP-TTLS**	**PEAP**
Autenticación de Servidor	Ninguna	Clave Pública (Certificado)	Clave Pública (Certificado)	Clave Pública (Certificado)
Autenticación de Peer	Hash de Password	Clave Pública (Certificado)	CHAP, PAP, MS-CHAP(v2), EAP-*	Clave Pública, MS-CHAPv2, EAP-*
Derivación dinámica de claves	No	Si	Si	Si

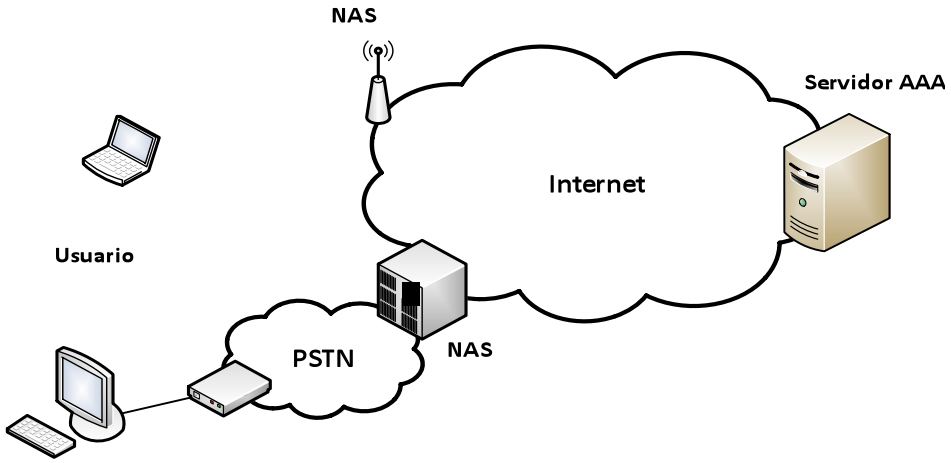
Protocolos de Autenticación – RADIUS

- Remote Authentication Dial In User Service (RADIUS)
  - RFC 2865 (2866, 2868, 3575, 3579, 5080, 6929)
  - Estándar de facto para AAA
    - Autenticación (Authentication): Quién es
    - Autorización (Authorization): Qué puede hacer
    - Contabilidad (Accounting): Qué ha hecho
  - Arquitectura Cliente – Servidor
    - RADIUS es el protocolo para intercambio de información
  - Soporte para otros protocolos de autenticación
    - EAP-*

Protocolos de Autenticación – RADIUS

- Arquitectura
  - Protocolo de nivel de aplicación sobre UDP/IP
  - Tres entidades en la arquitectura de red
    - Usuario
    - Network Access Server (NAS): RADIUS Client
    - Servidor de AAA: RADIUS Server





Protocolos de Autenticación – RADIUS

- ¿Por qué UDP?
  - Protocolo sin estado
    - Los clientes van y vienen
    - Los servidores también
  - Requisitos temporales del protocolo no se adaptan a TCP
    - Fiabilidad basada en retransmisiones
  - Simplifica la implementación del servidor

Protocolos de Autenticación – RADIUS

- Modos de operación
  - Entre usuario y servidor
    - User / Password
    - Challenge / Response
  - Secreto compartido entre NAS y Servidor AAA
    - Cliente y Servidor RADIUS

Protocolos de Autenticación – RADIUS

- Formato de los paquetes RADIUS

Código	Identificador	Longitud
Autenticador		
Atributos …		

  - Código (1 byte): Tipo de paquete RADIUS
    - Access-Request (1)
    - Access-Accept (2)
    - Access-Reject (3)
    - Accounting-Request (4)
    - Accounting-Response (5)
    - Access-Challenge (11)
  - Identificador (1 byte): Relaciona petición y respuesta
  - Longitud (2 bytes): Tamaño del paquete RADIUS completo

Protocolos de Autenticación – RADIUS

- Formato de los paquetes RADIUS
  - Access-Request (1) – (NAS → Servidor) – Petición de Autenticación
  - Access-Accept (2) – (Servidor → NAS) – Respuesta aceptando la sesión del usuario
  - Access-Reject (3) – (Servidor → NAS) – Respuesta rechazando la sesión del usuario
  - Access-Challenge (11) – (Servidor → NAS) – Petición de información adicional del usuario
    - Modo Challenge/Response
    - EAP
  - Account-Request (4) – NAS envía información de Accounting al servidor
  - Account-Response (5) – Reconocimiento de la petición por parte del servidor

Protocolos de Autenticación – RADIUS

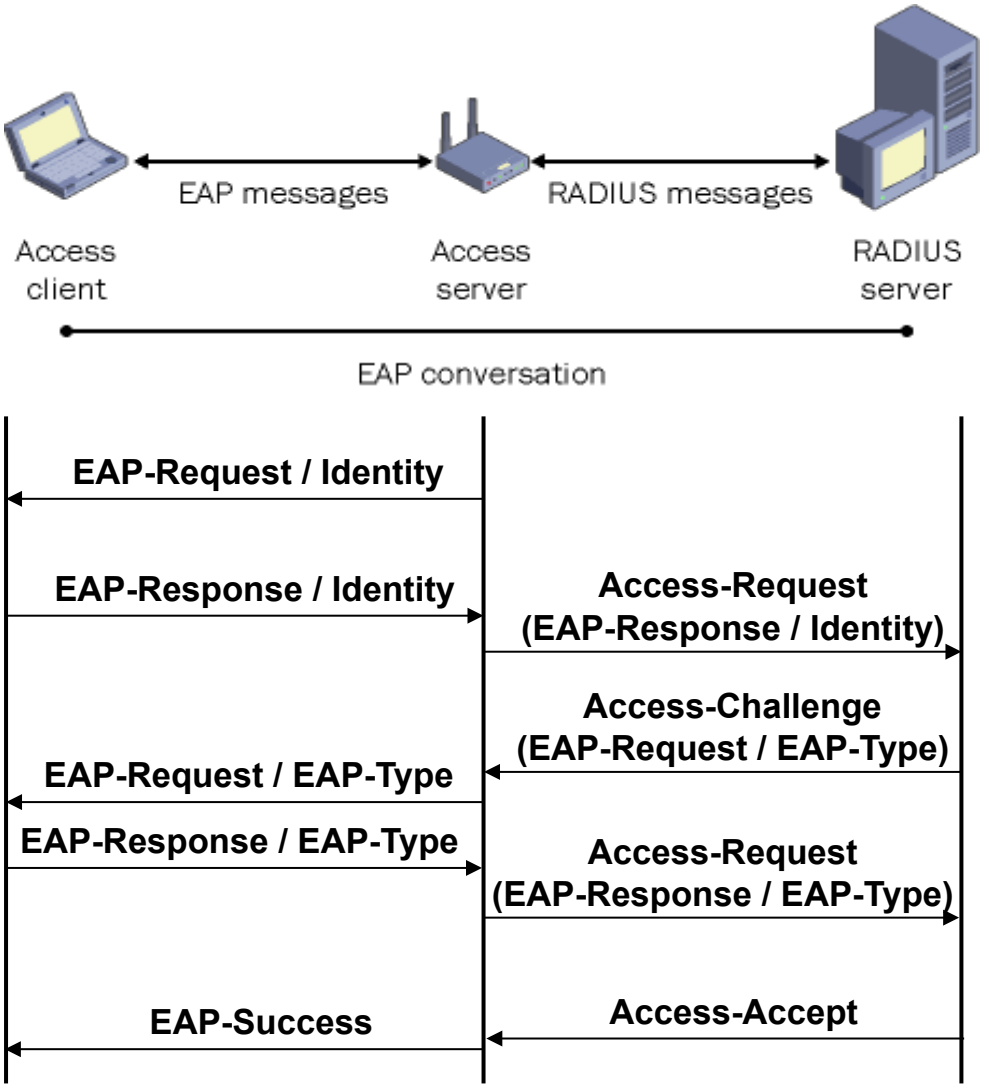
- Formato de los paquetes RADIUS
  - Autenticador (16 bytes)
    - En las peticiones (Tipo Access-Request)
      - Número aleatorio único temporal y geográficamente
      - Oscurece el password del usuario
        - » MD5 (Secreto, RequestAuth) ⊕ Clear Password
    - En las respuestas (Tipos Access-Accept, Access-Reject, Access-Challenge)
      - MD5 (Código | ID | Longitud | RequestAuth | Atributos | Secreto)

Protocolos de Autenticación – RADIUS

- Formato de los paquetes RADIUS
  - Atributos
    - Contienen la información específica para la autenticación, autorización y contabilidad
    - Formato Tipo-Longitud-Valor (TLV)
      - Tipo User-name: 1
      - Tipo User-Password: 2
      - Tipo State: 24
      - Tipo EAP-Message: 79
      - Tipo Message-Authenticator: 80
        - » HMAC-MD5 (Código, Id, Longitud, ReqAuth, Atributos)

Protocolos de Autenticación – RADIUS

- RADIUS / EAP
  - RFC 3579
  - Paquetes EAP encapsulados
    - EAP-Response → Access-Request
    - EAP-Request → Access-Challenge
    - EAP-Success → Access-Accept
    - EAP-Failure → Access-Reject
  - NAS y RADIUS server en segmentos seguros de red
    - VPN
    - Entorno controlado



Protocolos de Autenticación – IEEE 802.1x

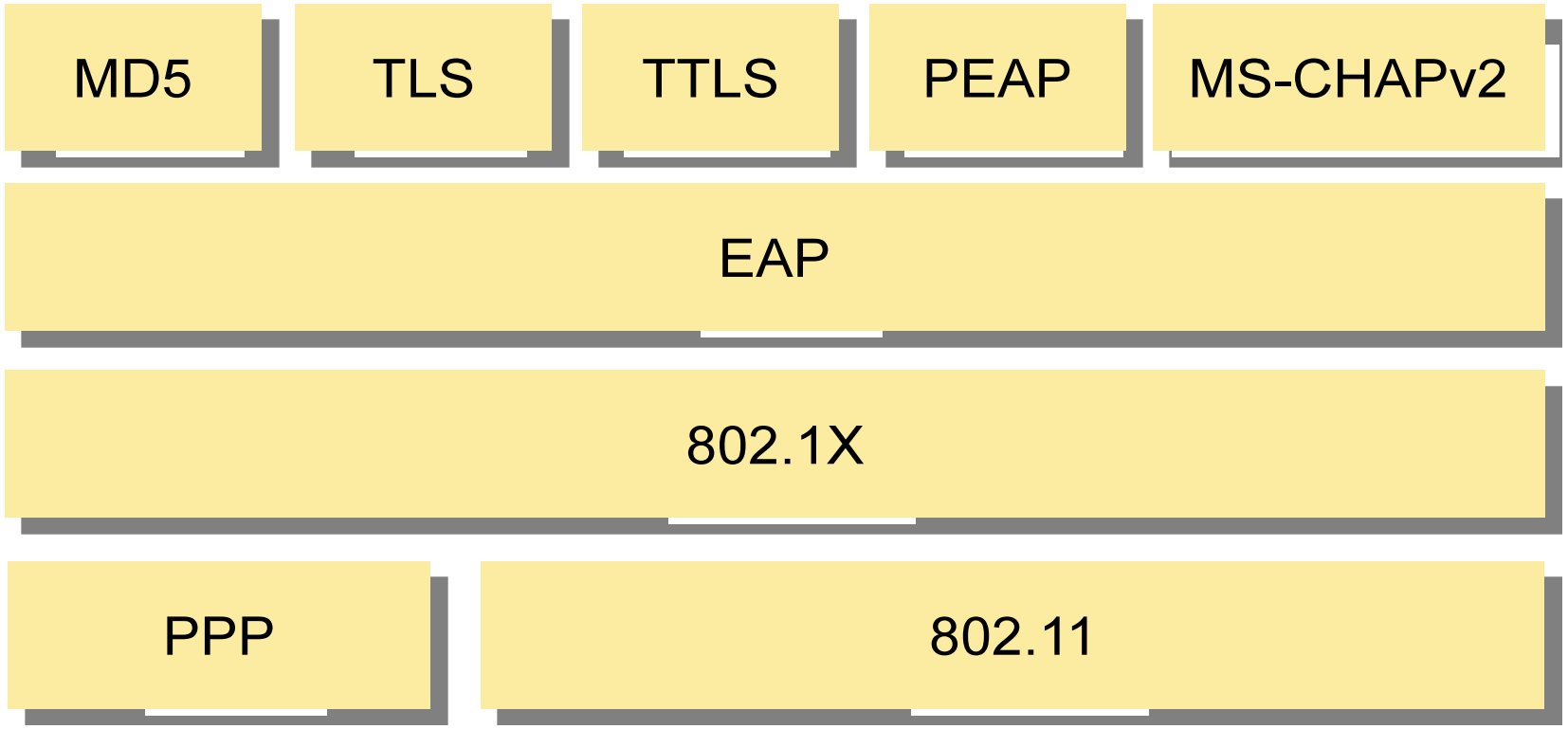
- Definido por el IEEE
  - http://standards.ieee.org/getieee802/download/802.1X-2010.pdf
- Autenticación y Autorización de equipos conectados a LANs IEEE 802
  - Acceso controlado en entornos LAN
  - Autenticación de los dispositivos a nivel 2
    - Antes de permitir que un dispositivo se conecte a un puerto físico o lógico de un switch o AP debe ser autenticado y autorizado.
  - Ejemplos de uso: Ethernet, 802.11 WLAN
- Objetivos
  - Principios de la operativa del Port-based Network Access Control
  - Arquitectura básica de red
  - Uso de EAP como método de autenticación y autorización basada en un servidor AAA externo
  - Formato de encapsulación de EAP sobre la capa MAC
    - EAPOL

Protocolos de Autenticación – IEEE 802.1x

- Arquitectura
  - Se definen tres entidades
    - Supplicant
    - Authenticator
    - Authentication Server
  - Entidades de Autenticación por puerto (Port Authentication Entities, PAEs)

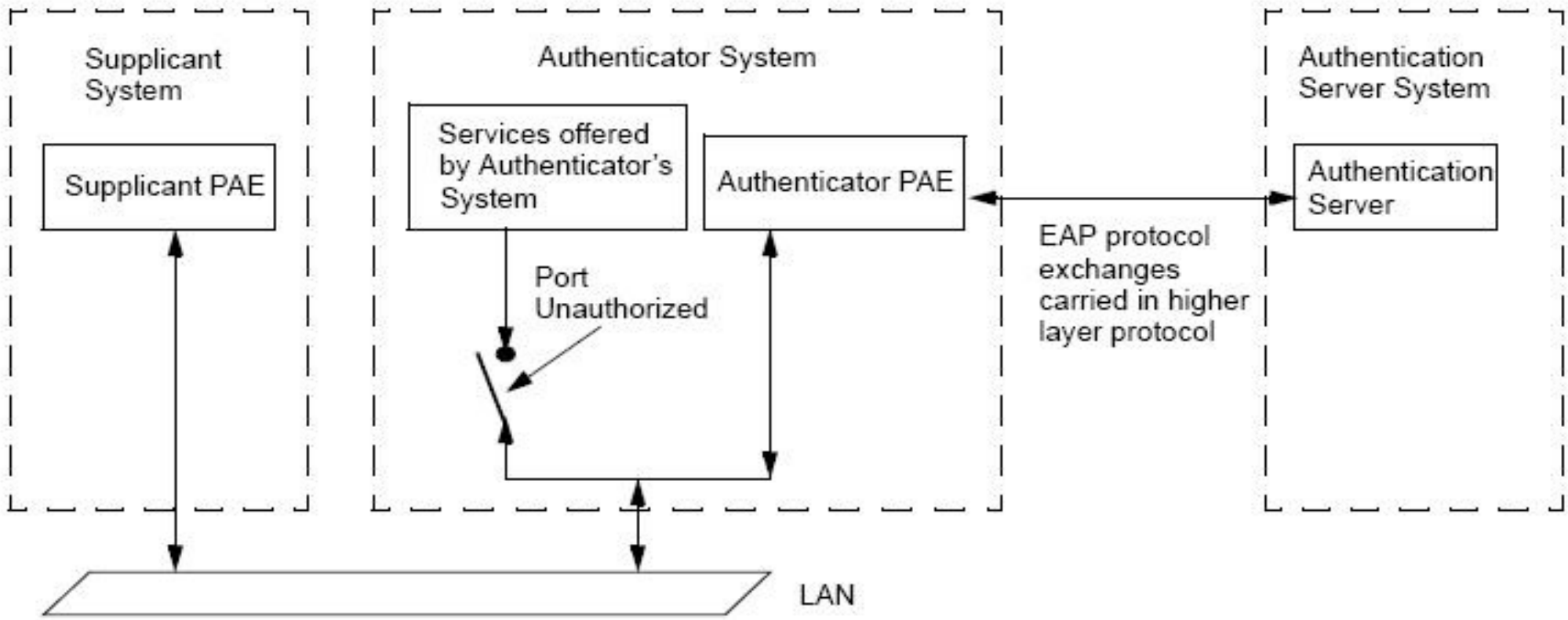
Protocolos de Autenticación – IEEE 802.1x

- Arquitectura
  - IEEE 802.1x es el contenedor
  - EAP es el marco de autenticación



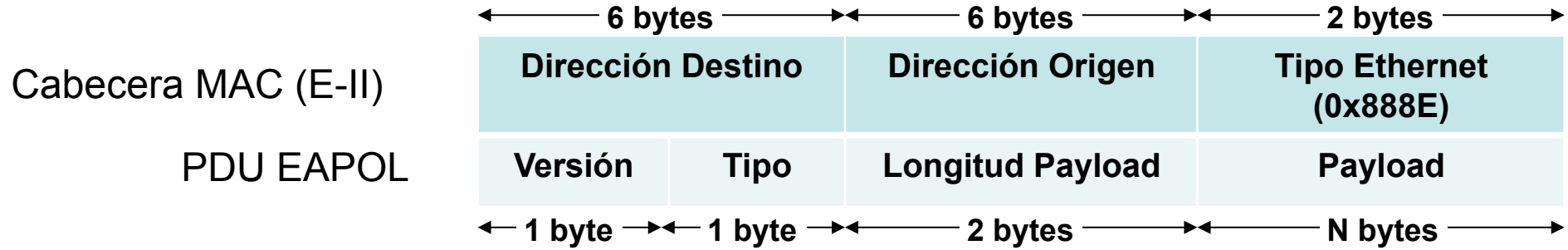
Protocolos de Autenticación – IEEE 802.1x

- Arquitectura
  - Principio básico: Port-based Network Access Control



Protocolos de Autenticación – IEEE 802.1x

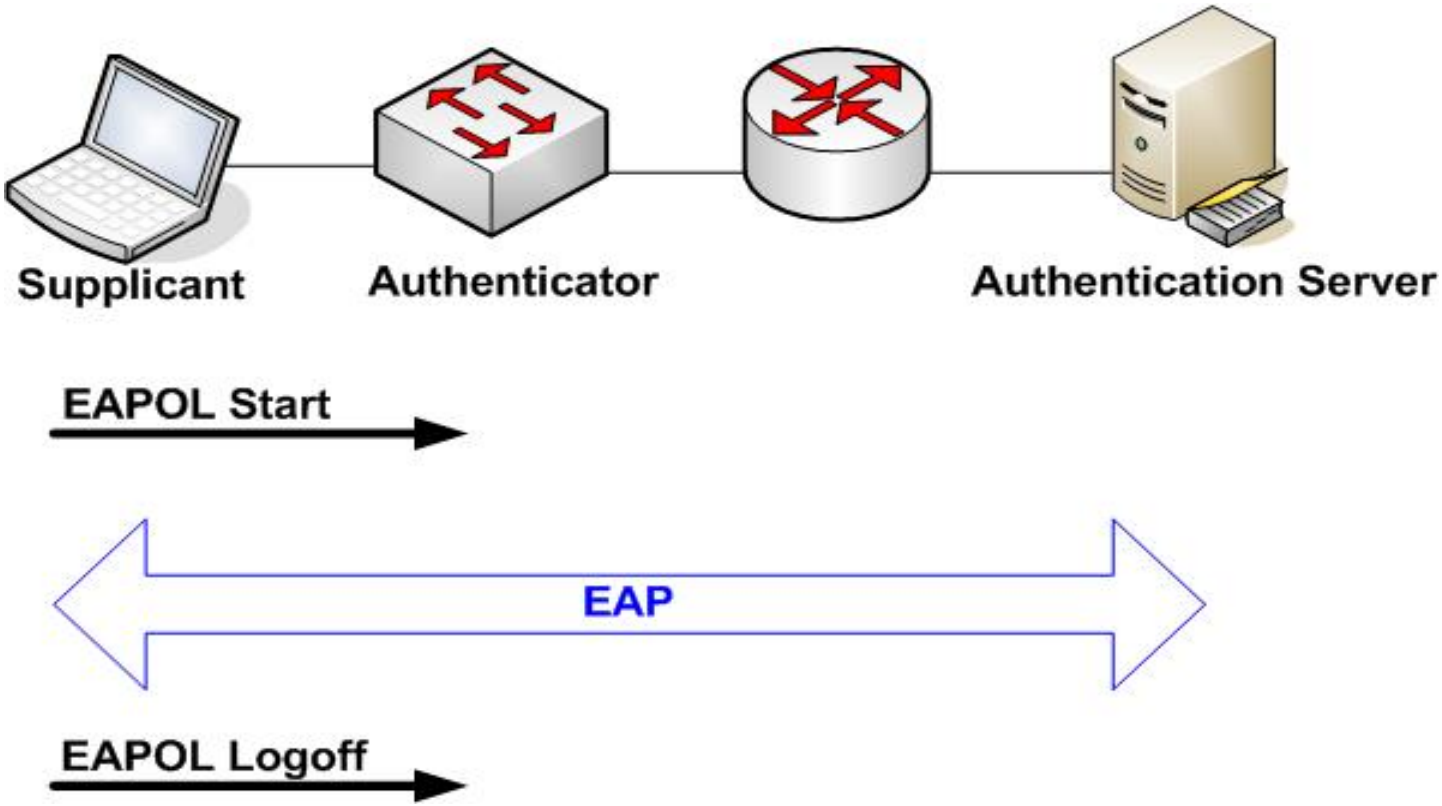
- Formato de la trama EAPOL



  - Versión (1 byte): Dependiente de la especificación
  - Tipo (1 byte): Tipo de paquete EAPOL
    - EAP-Packet: 0
    - EAPOL-Start: 1
    - EAPOL-Logoff: 2
    - EAPOL-Key: 3
  - Longitud Payload (2 bytes): Longitud del payload
  - Payload: Información dependiente de cada tipo

Protocolos de Autenticación – IEEE 802.1x

- Protocolo

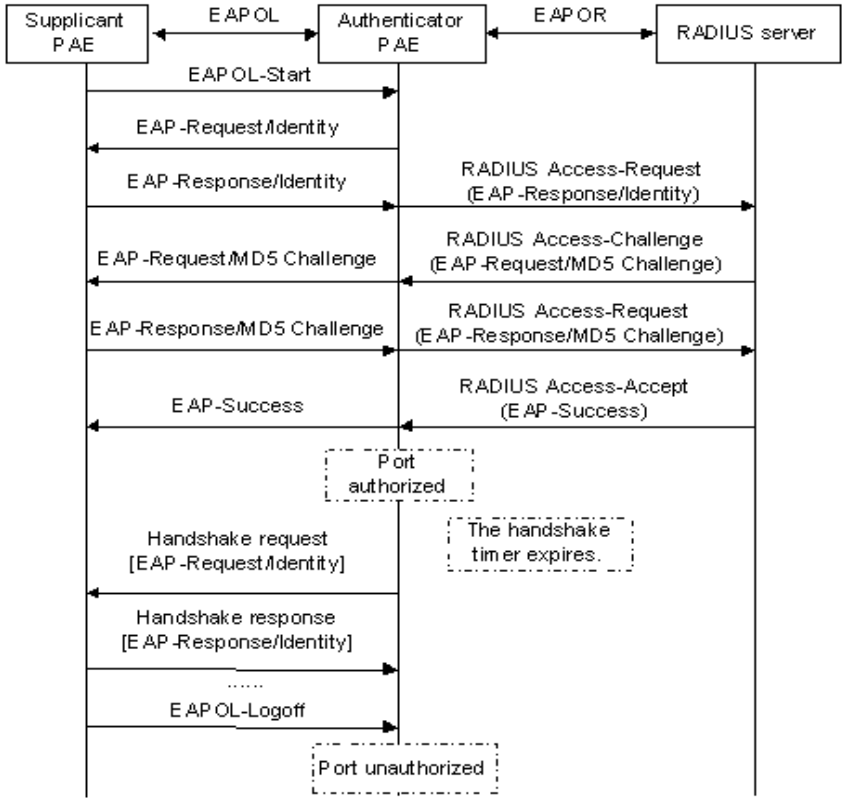


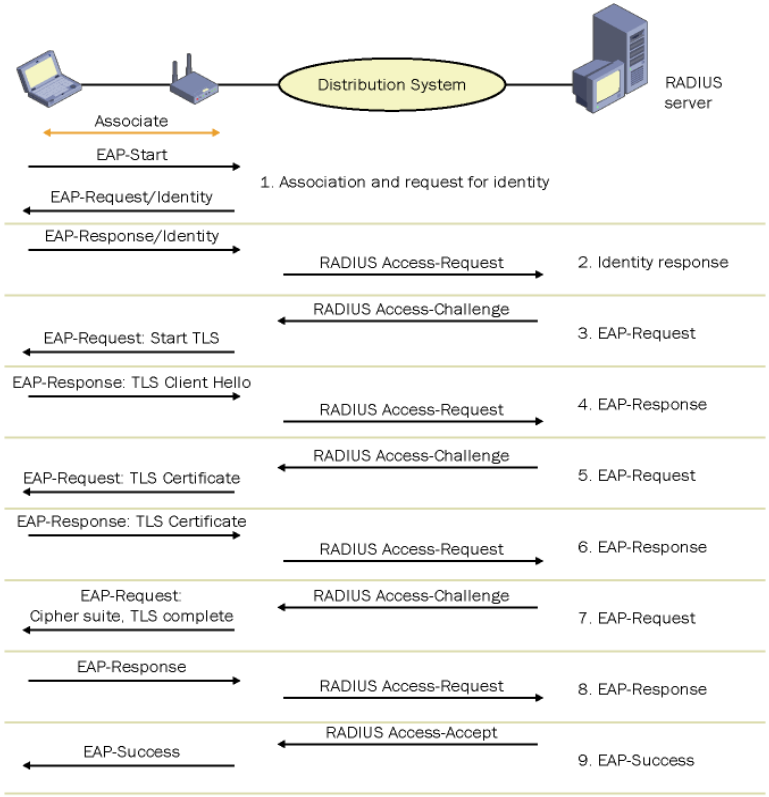
Protocolos de Autenticación – IEEE 802.1x

- Protocolo
  - Autenticación entre Supplicant y Authentication Server, Authenticator hace de intermediario
    - EAPOL (EAP Over LAN) o EAPOW (EAP Over Wireless)
    - RADIUS, DIAMETER
  - Ventajas:
    - cambios en el método de autenticación no requieren hacer cambios en el sistema final ni en la infraestructura
    - flexibilidad en los métodos de autenticación
    - simplicidad para los authenticator

Protocolos de Autenticación – IEEE 802.1x

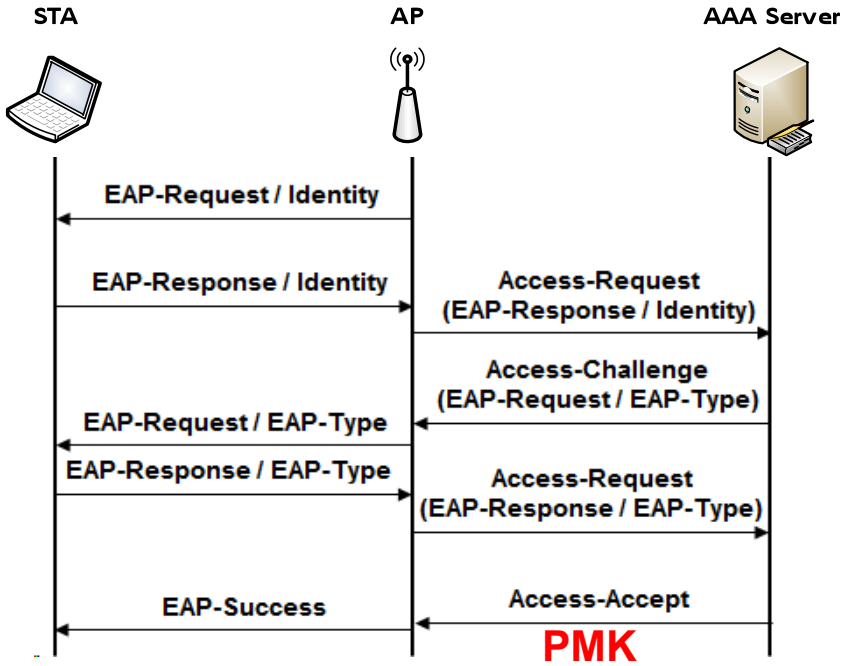
- Protocolo
  - Diversos métodos EAP sobre el mismo sistema

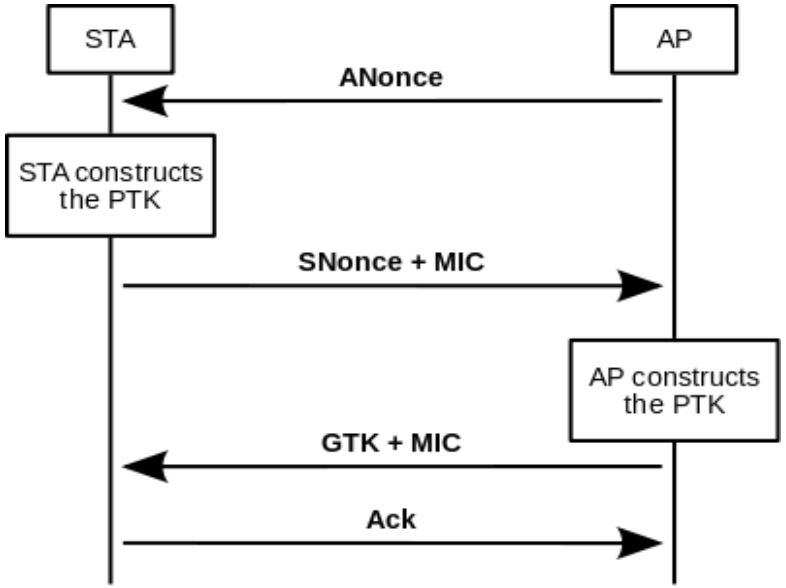




Protocolos de Autenticación – IEEE 802.1x

- Caso práctico – IEEE 802.11i
  - WPA2
    - PTK = PBKDF2-SHA1(PMK | Anonce | Snonce | AP_@MAC | STA @MAC)
  - WPA2-Enterprise
    - PMK derivado dentro del método EAP
      - Ej: Eduroam → PEAP





Contenido

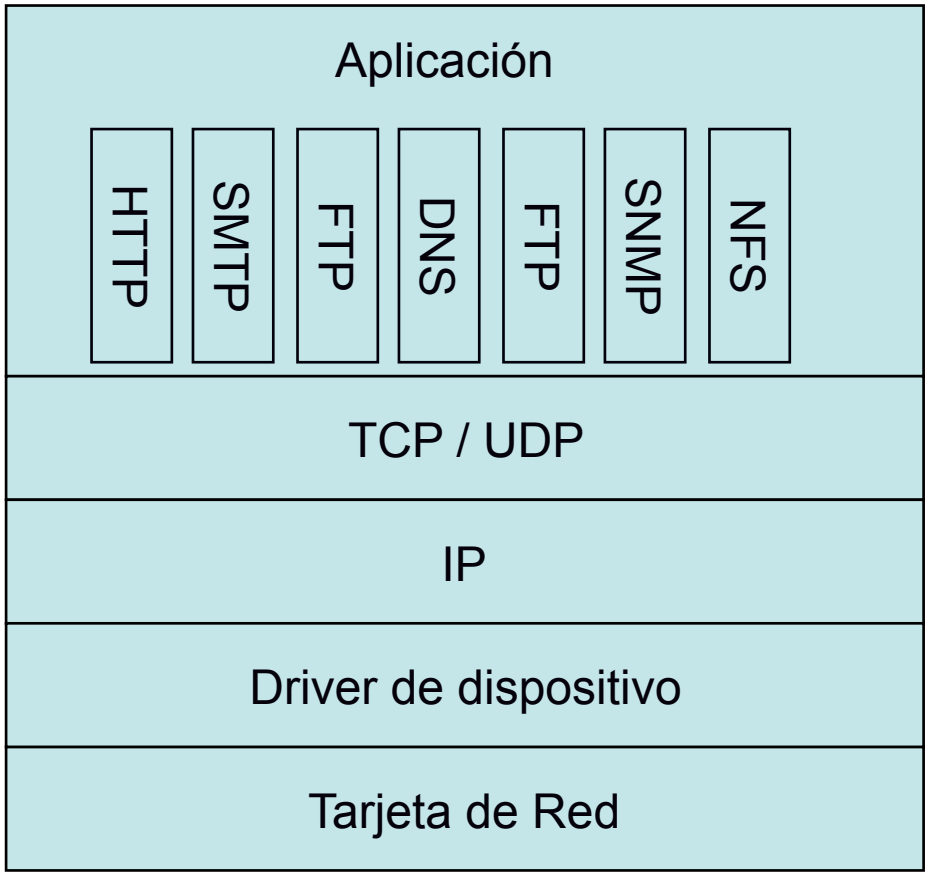
- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Transporte – SSL / TLS
  - Nivel de Red – IPSec
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Seguridad en Internet – Introducción

- Problemas de seguridad en Internet
  - Internet está compuesta por redes:
    - Públicas
    - No confiables
    - No fiables
  - Esta falta de seguridad inherente hace que Internet sea objeto de varios tipos de riesgos …
    - Integridad de los datos
      - El contenido de los paquetes se puede modificar de manera accidental o deliberada
    - Usurpación de la identidad
      - El origen de un paquete se puede modificar
    - Ataques de replicación
      - Paquetes retransmitidos pueden afectar la operativa del sistema
    - Pérdida de privacidad
      - El contenido de un paquete puede ser examinado en su transito a través de la red

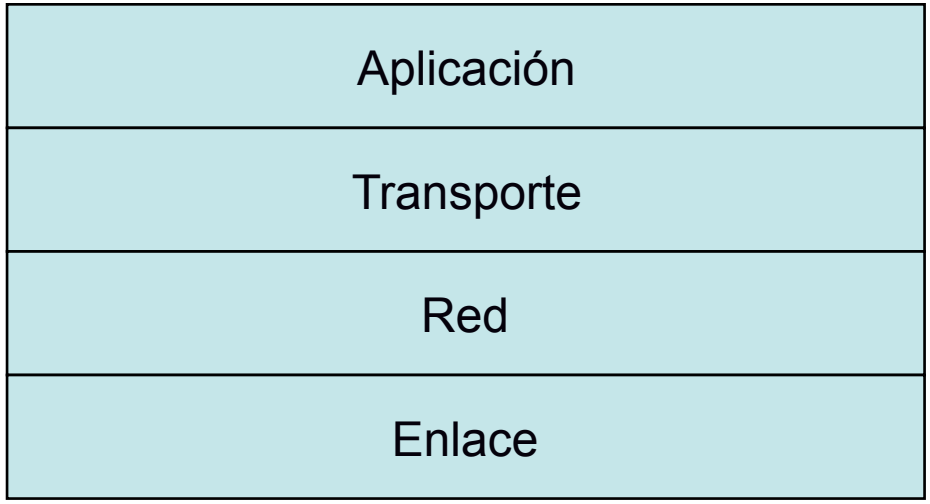
Seguridad en Internet – Introducción

- Modelo TCP/IP



Seguridad en Internet – Introducción

- ¿Dónde ofrecer seguridad?



PGP, Kerberos, SSH, etc.

Transport Layer Security (TLS)

IP Security

Hardware encryption

Seguridad en Internet – Introducción

- A nivel de aplicación
  - (PGP, Kerberos, SSH, etc.)
  - Se implementa en los extremos de la comunicación
  - Ventajas
    - Asegura la aplicación sin involucrar al SO
    - Las aplicaciones entienden la información y ofrecen la seguridad adecuada
  - Desventajas
    - Mecanismos de seguridad específicos para cada aplicación
    - La información sensible no sólo está en el nivel de aplicación

Seguridad en Internet – Introducción

- A nivel de transporte
  - Transport Layer Security (TLS)
  - Se implementa en los extremos de la comunicación
  - Ventajas
    - Las aplicaciones se aseguran de manera transparente
  - Desventajas
    - Específico para cada protocolo

Seguridad en Internet – Introducción

- A nivel de red
  - IP Security (IPSec)
  - Ventajas
    - Seguridad transparente para las capas de aplicación y transporte
    - Seguridad por flujo o por conexión → Control fino
  - Desventajas
    - Más difícil de ofrecer seguridad por usuario en sistemas multi-usuario

Contenido

- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Transporte – SSL / TLS
  - Nivel de Red – IPSec
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Seguridad en Internet – SSL / TLS

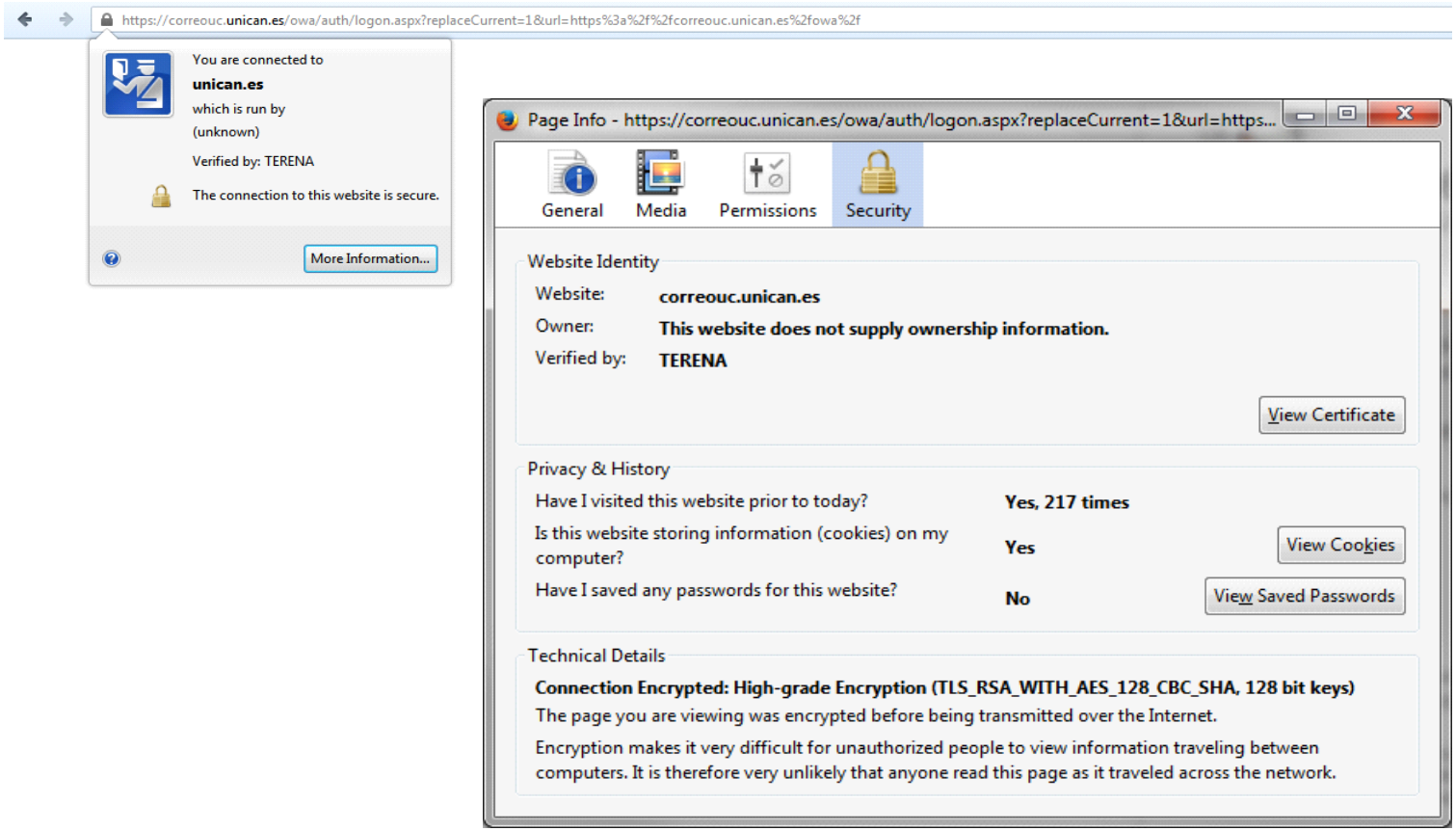
- SSL – Secure Sockets Layer Version 2.0
  - Desarrollado inicialmente por Netscape
  - SSL 2.0 vulnerable a MitM
  - SSL 2.0 no se debe usar
- SSL – Secure Sockets Layer Version 3.0
  - Internet Draft creado por Netscape, Noviembre 1996
  - Soportado por los navegadores
  - Vulnerable al ataque denominado BEAST Cipher-Block-Chaining (CBC)
  - Vulnerable al ataque denominado POODLE
    - https://www.us-cert.gov/ncas/alerts/TA14-290A
- TLS – Transport Layer Security Version 1.0 (SSL 3.1)
  - IETF RFC 2246, Enero 1999
  - TLS 1.0 no es compatible con SSL 3.0
  - Soportado por todos los navegadores
  - Vulnerable al ataque denominado BEAST Cipher-Block-Chaining (CBC)

Seguridad en Internet – SSL / TLS

- TLS – Transport Layer Security Version 1.1 (SSL 3.2)
  - IETF RFC 4346, Abril 2006
  - Protegido contra ataques de CBC
- TLS – Transport Layer Security Version 1.2 (SSL 3.3)
  - IETF RFC 5246, Agosto 2008

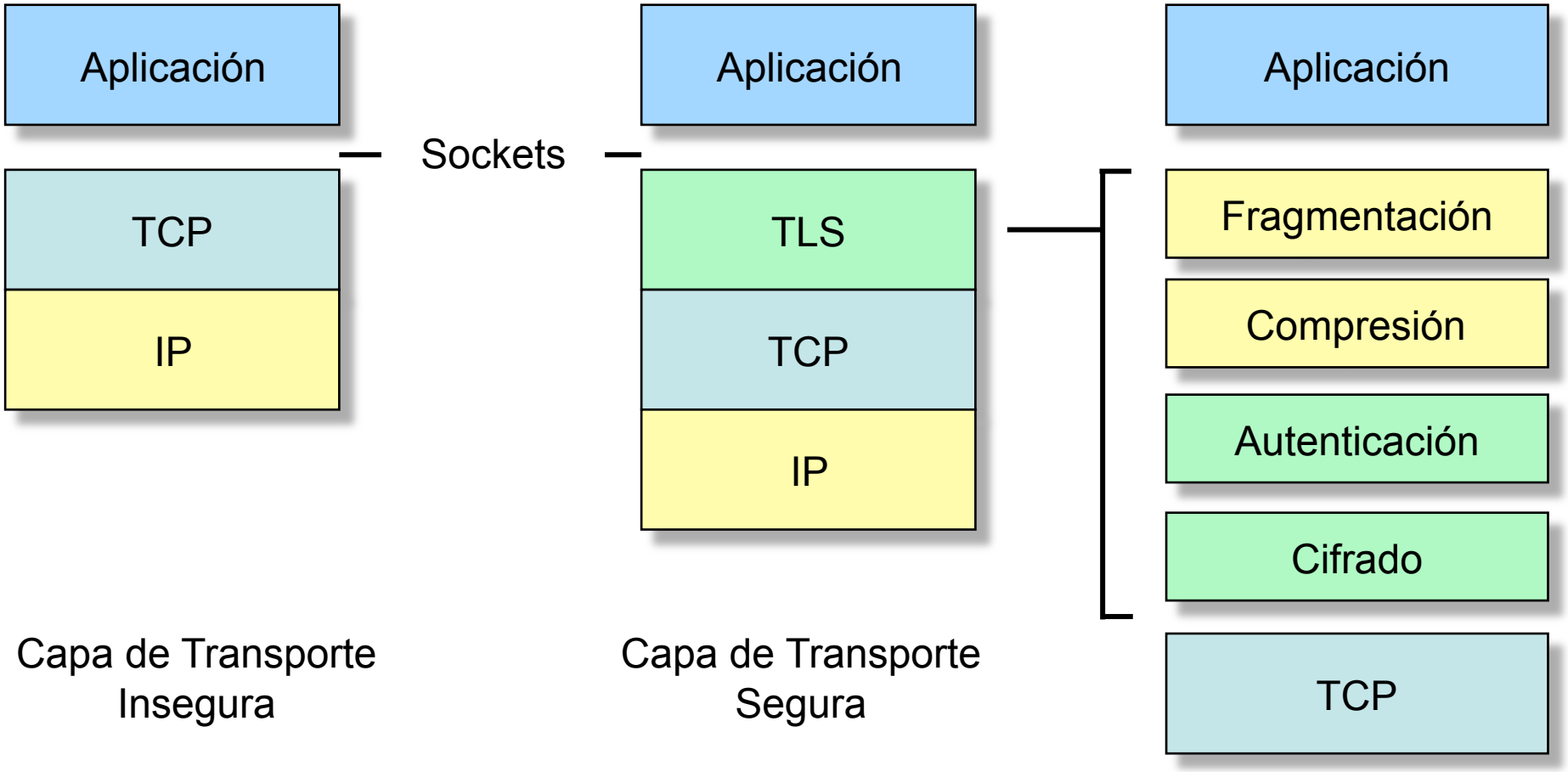
Seguridad en Internet – SSL / TLS

- Secure Sockets Layer / Transport Layer Security



Seguridad en Internet – SSL / TLS

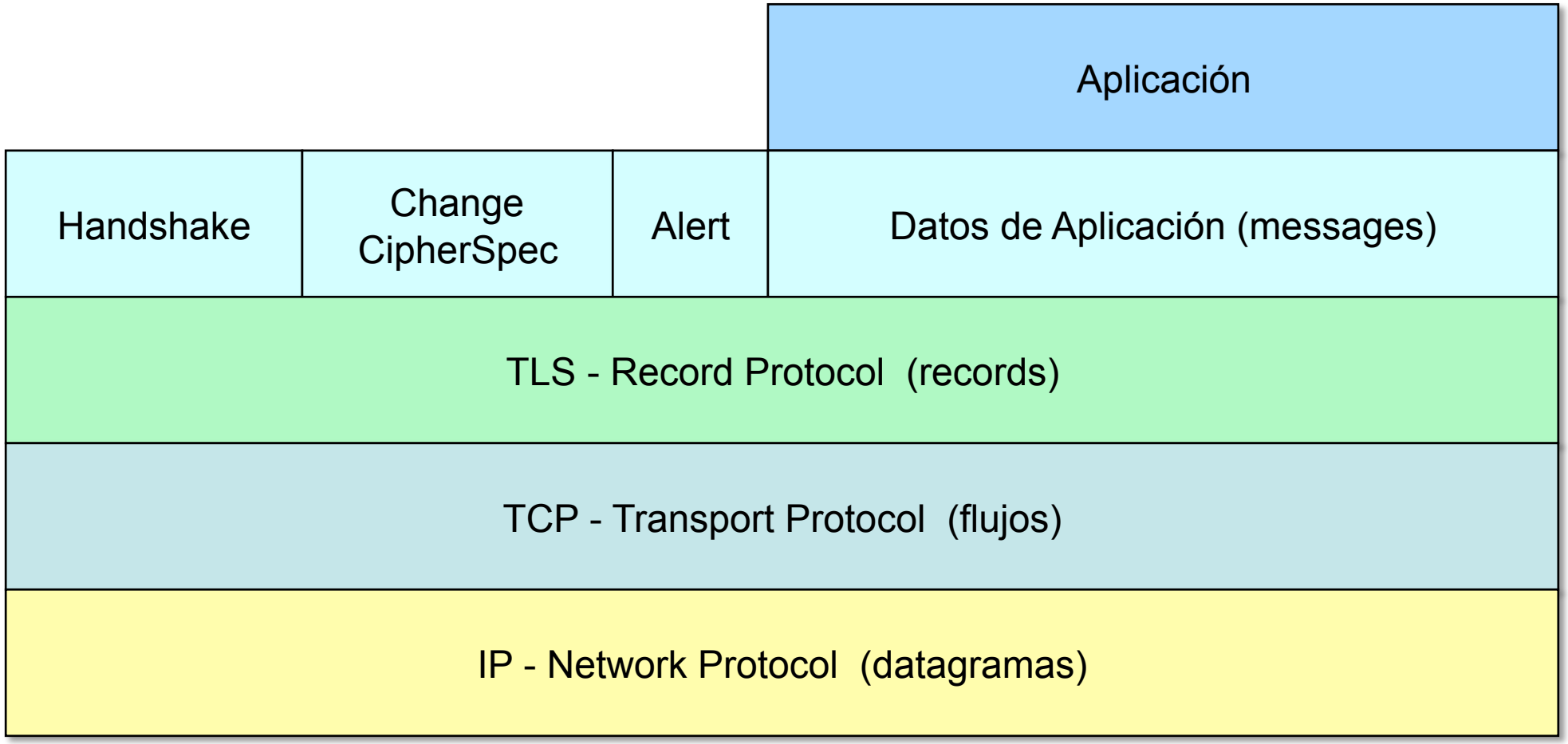
- Arquitectura de protocolos



Seguridad en Internet – SSL / TLS

- Sesiones TLS vs Conexiones TCP
  - Cliente y servidor establecen una sesión TLS
  - Las sesiones son asociaciones con estado:
    - Identificador
    - Algoritmos y parámetros
  - Se pueden establecer múltiples conexiones sobre la misma sesión
    - Comparten el mismo estado

Seguridad en Internet – SSL / TLS



Seguridad en Internet – SSL / TLS

- Protocolo SSL Alert
  - mensajes de error y alertas
- Protocolo SSL Change Cipher Spec
  - un mensaje que indica el final del SSL handshake

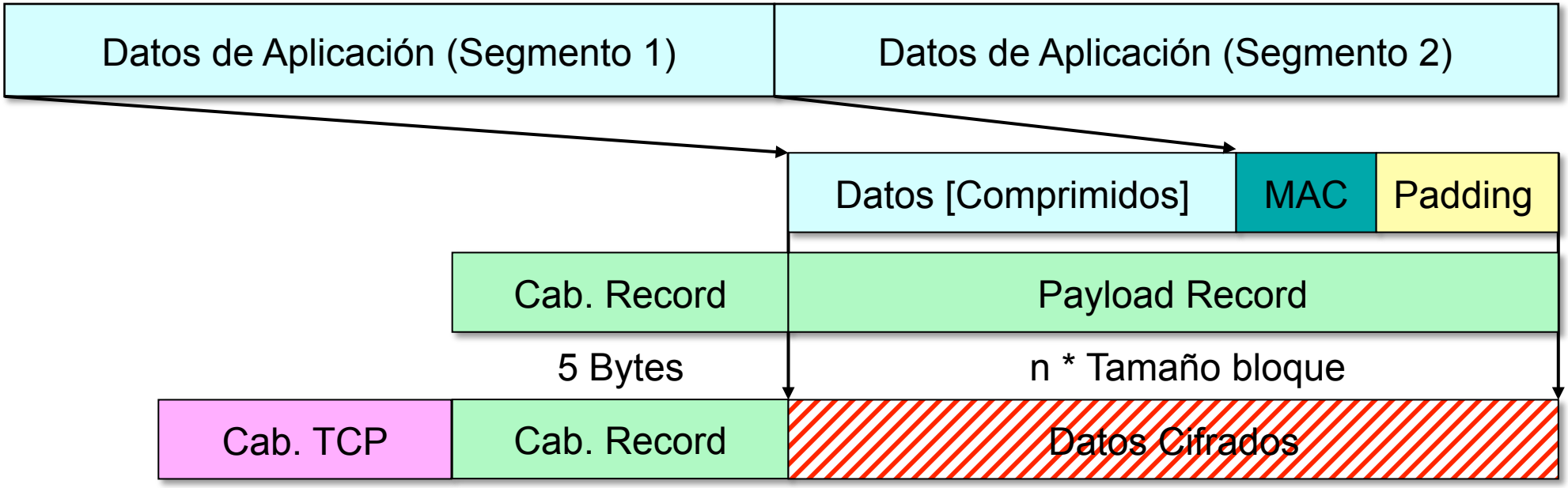
Seguridad en Internet – SSL / TLS

- Protocolo SSL Record
  - fragmentación
  - compresión
  - autenticación de los mensajes e integridad
  - cifrado

Seguridad en Internet – SSL / TLS

- TLS records

```
⊞ Frame 9 (603 bytes on wire, 603 bytes captured)
⊞ Ethernet II, Src: Dell_92:44:9f (00:1a:a0:92:44:9f), Dst: SitecomE_5a:74:5e (00:0c:f6:5a:74:5e)
⊞ Internet Protocol, Src: 192.168.1.198 (192.168.1.198), Dst: hsr.ch (152.96.37.60)
⊞ Transmission Control Protocol, Src Port: 49825 (49825), Dst Port: https (443), Seq: 996, Ack: 1519, Len: 549
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 544
      Encrypted Application Data: C72EA7E35EE5501648FB77E216FCEA6CF62899BBD1ADDDAD...
```



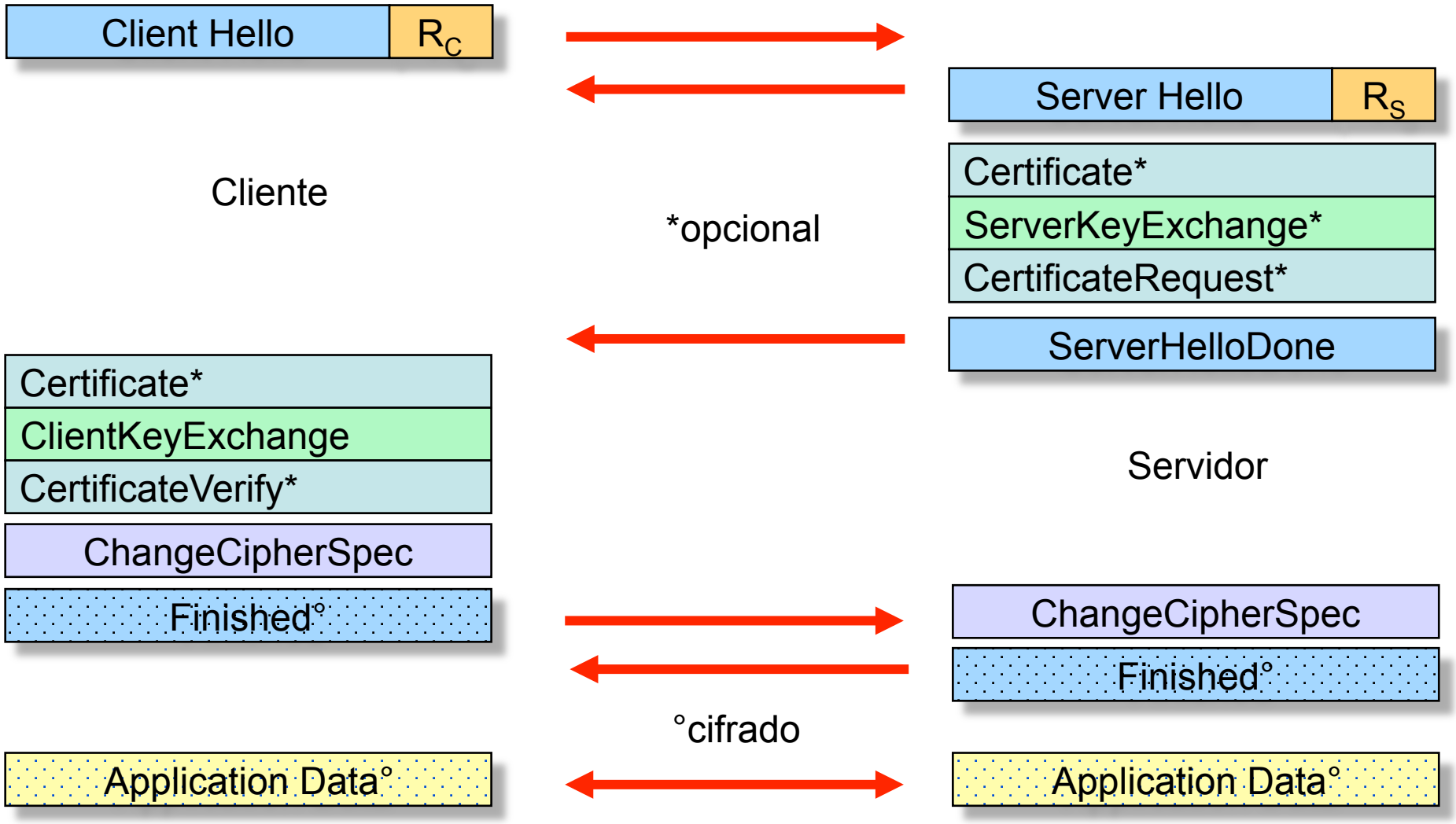
Seguridad en Internet – SSL / TLS

- TLS records
  - Tipo (1 byte)
    - Change Cipher Spec
    - Alert
    - Handshake
    - Datos de aplicación
  - Versión (2 bytes)
    - TLS 1.0 → 0x0301
    - TLS 1.1 → 0x0302
    - TLS 1.2 → 0x0303
  - Longitud (2 bytes)
    - Longitud del segmento

Seguridad en Internet – SSL / TLS

- Protocolo SSL Handshake
  - negociación de la Cipher-Suite
    - Algoritmo de cifrado simétrico
    - Método de intercambio de claves
    - Función de protección de la integridad
  - intercambio de clave maestra y material criptográfico
  - autenticación del servidor y de manera opcional del cliente

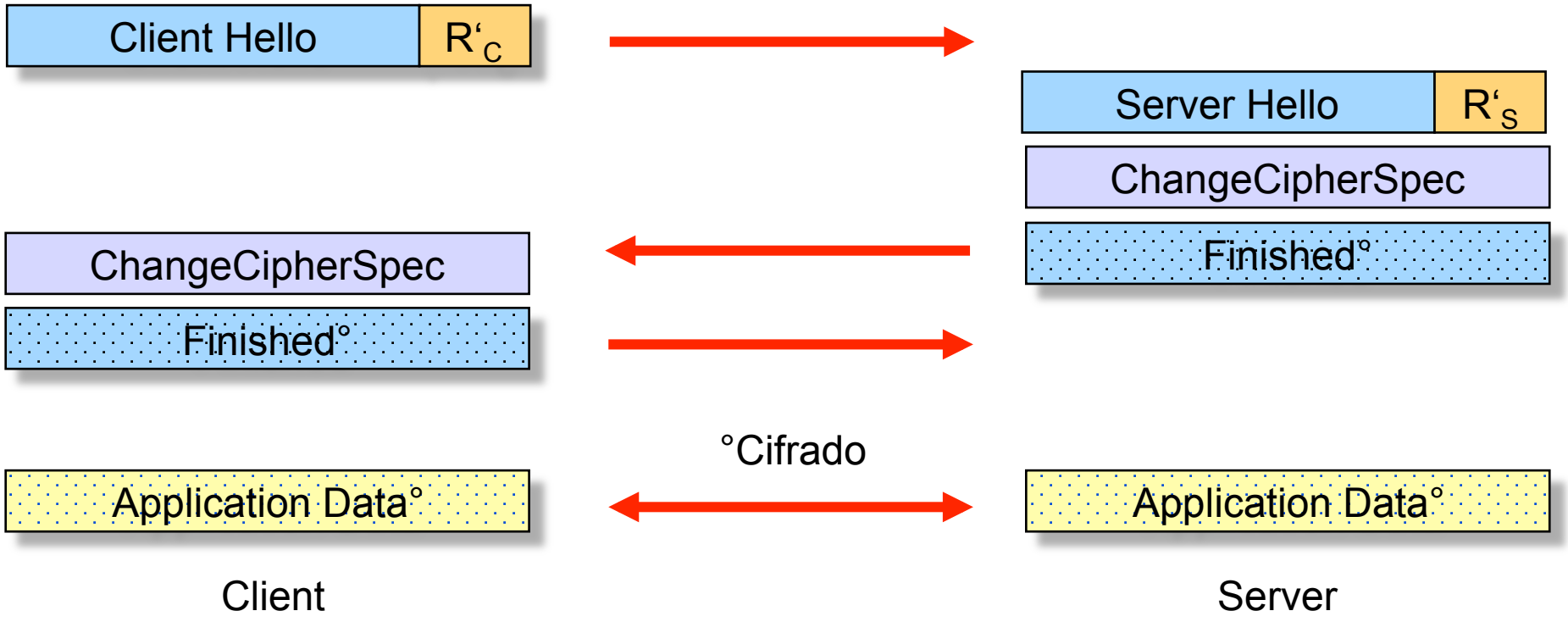
Seguridad en Internet – SSL / TLS



Seguridad en Internet – SSL / TLS

No.	Time	Source	Destination	Protocol	Length	Info
5	1.459095	192.168.9.111	193.144.193.212	TLSv1.2	271	Client Hello
10	1.463413	193.144.193.212	192.168.9.111	TLSv1.2	1280	Server Hello, Certificate, Certificate Status, Server Hello Done
11	1.467343	192.168.9.111	193.144.193.212	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13	1.472621	193.144.193.212	192.168.9.111	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
14	1.498054	192.168.9.111	193.144.193.212	TLSv1.2	763	Application Data
19	1.503620	193.144.193.212	192.168.9.111	TLSv1.2	1059	Application Data

- Re-uso de una sesión TLS



Seguridad en Internet – SSL / TLS

- Cipher Suites
  - **SSL_NULL_WITH_NULL_NULL = { 0, 0 }**

  - SSL_RSA_WITH_NULL_SHA = {0,2}
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA = {0,51}
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA = {0,57}
  - TLS_RSA_WITH_AES_256_CBC_SHA = {0,53}

Seguridad en Internet – SSL / TLS

- Mecanismos de intercambio de claves
  - Basados en RSA (SSL_RSA_with...)
    - el servidor envía su clave pública RSA en su certificado
    - el cliente envía un “pre-master secret” cifrado
    - si se requiere autenticación del cliente este debe mandar tanto su certificado como la firma de todo el handshake
  - Diffie-Hellman estático (SSL_DH_RSA_with… or SSL_DH_DSS_with…)
    - el servidor envía sus parámetros DH en el certificado
    - si se requiere autenticación del cliente, éste enviará sus parámetros DH en su certificado
    - si no se autentica al cliente, éste manda el valor público DH en un mensaje client_key_exchange

Seguridad en Internet – SSL / TLS

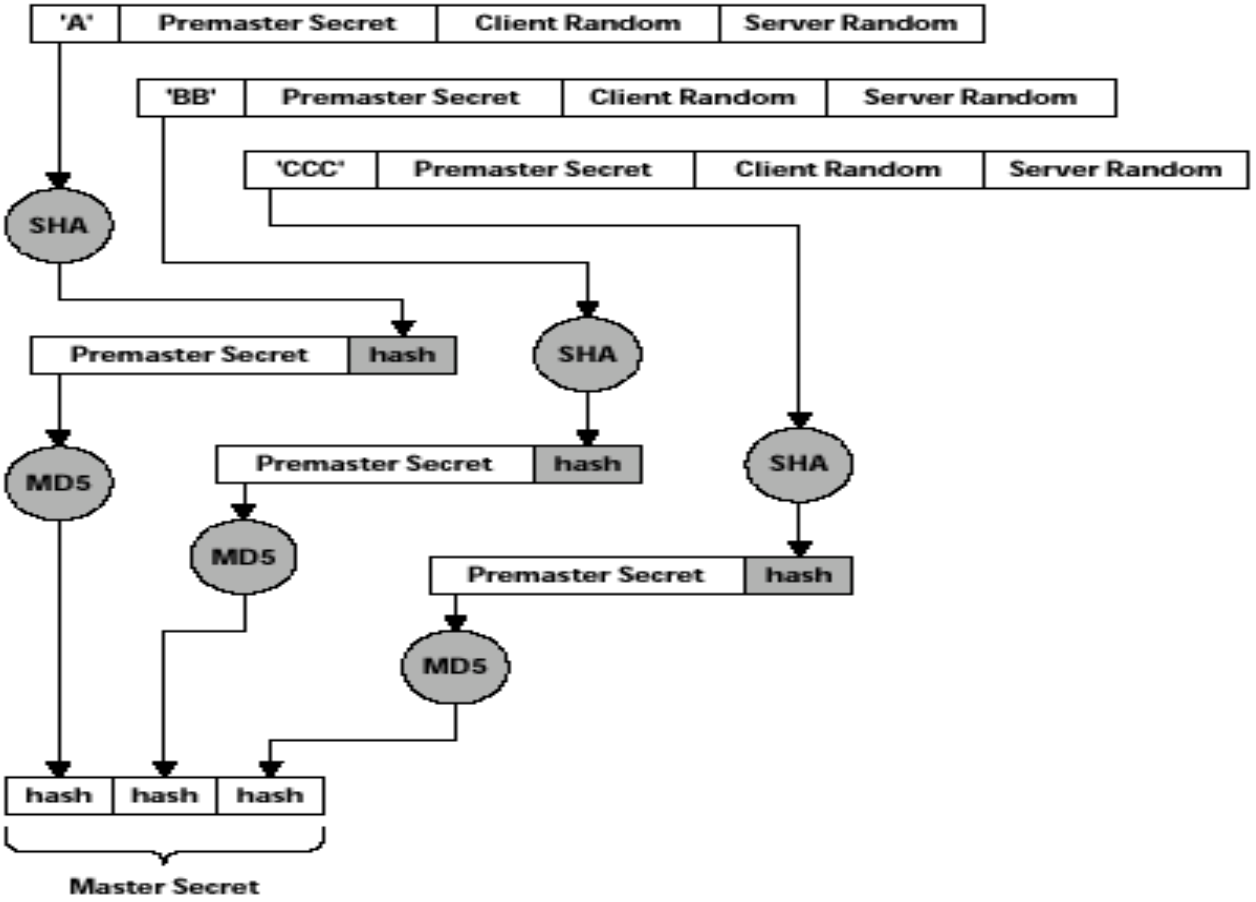
- Mecanismos de intercambio de claves
  - Diffie-Hellman efímero (SSL_DHE_RSA_with… or SSL_DHE_DSS_with…)
    - el servidor envía su certificado y unos parámetros efímeros DH firmados
    - el cliente envía sus parámetros efímeros DH cifrados con la clave pública del servidor
    - si el cliente debe autenticarse enviará su certificado así como la firma de todo el handshake

Seguridad en Internet – SSL / TLS

- Derivación de claves
  - Pre-master secret
    - Si el intercambio se basa en RSA lo genera el cliente
    - Si el intercambio se basa en DH:
      - *pre_master_secret* = g^{xy} *mod p*
  - Clave Maestra (Master secret)
    - Calculada a partir de la Pre-master secret y los Random intercambiados en el handshake
    - 48 bytes
  - Material criptográfico
    - Calculado a partir de la Master secret y los Random intercambiados en el handshake
    - Dependiente de los algoritmos de cifrado y hash
  - Claves de sesión
    - Extraídas del material criptográfico

Seguridad en Internet – SSL / TLS

- Master secret (SSL 3.0)



Seguridad en Internet – SSL / TLS

- Master secret (TLS 1.0, 1.1 y 1.2)

Master_Secret = PRF(Pre-master secret, "master secret", Rc || Rs)

–48 bytes

–PRF(secret, label, seed) = P_MD5(S1, label + seed) XOR
P_SHA-1(S2, label + seed)

- El secreto se divide en dos mitades S1 y S2

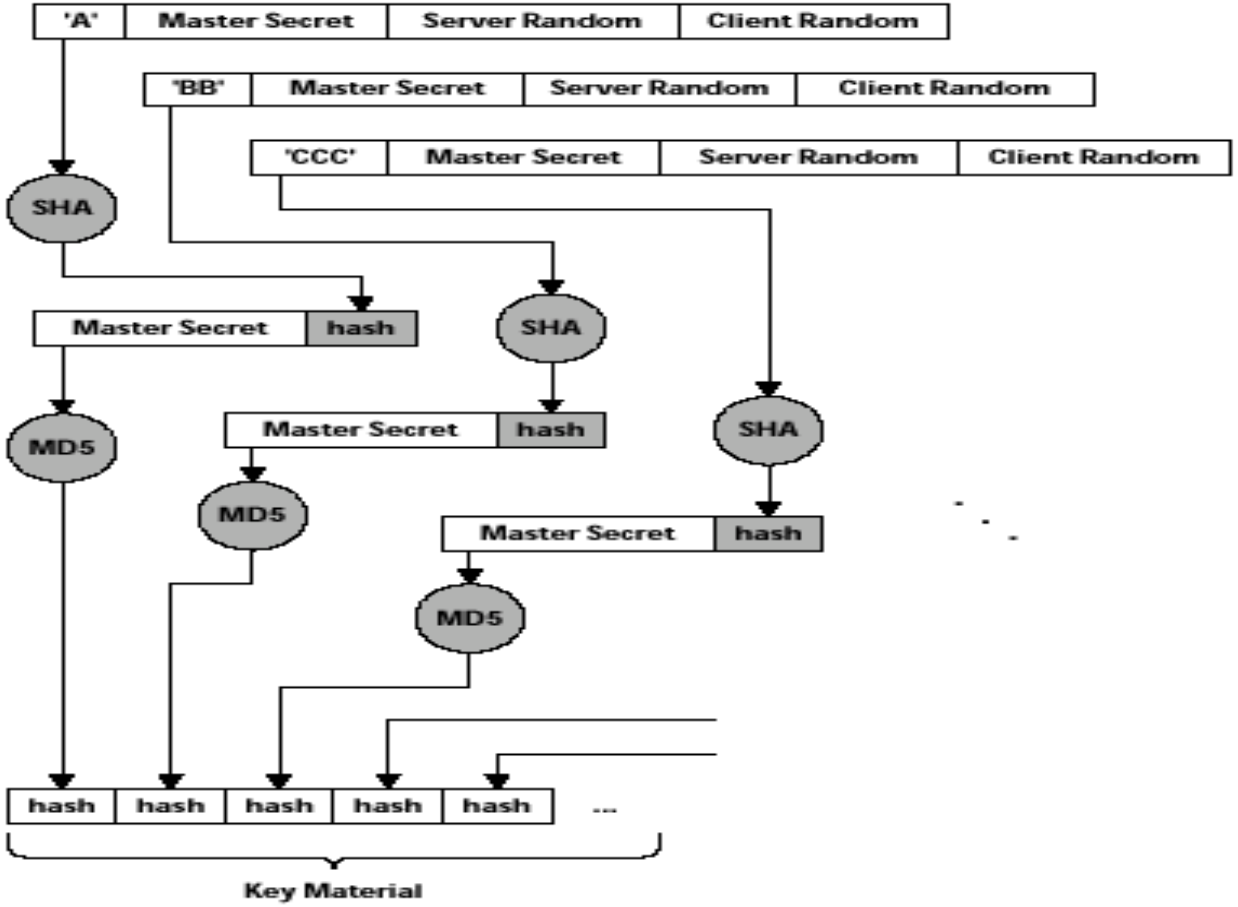
–P_hash(secret, seed) = HMAC_hash(secret, A(1) + seed) +
HMAC_hash(secret, A(2) + seed) +
HMAC_hash(secret, A(3) + seed) + ...

–A():

A(0) = seed
A(i) = HMAC_hash(secret, A(i-1))

Seguridad en Internet – SSL / TLS

- Material criptográfico (SSL 3.0)



Seguridad en Internet – SSL / TLS

- Material criptográfico (TLS 1.0, 1.1 y 1.2)

Key_Material = PRF(Master secret, "key expansion", Rc || Rs)

–Tantos bytes como haga falta por la Cipher-Suite

–PRF(secret, label, seed) = P_MD5(S1, label + seed) XOR
P_SHA-1(S2, label + seed)

- El secreto se divide en dos mitades S1 y S2

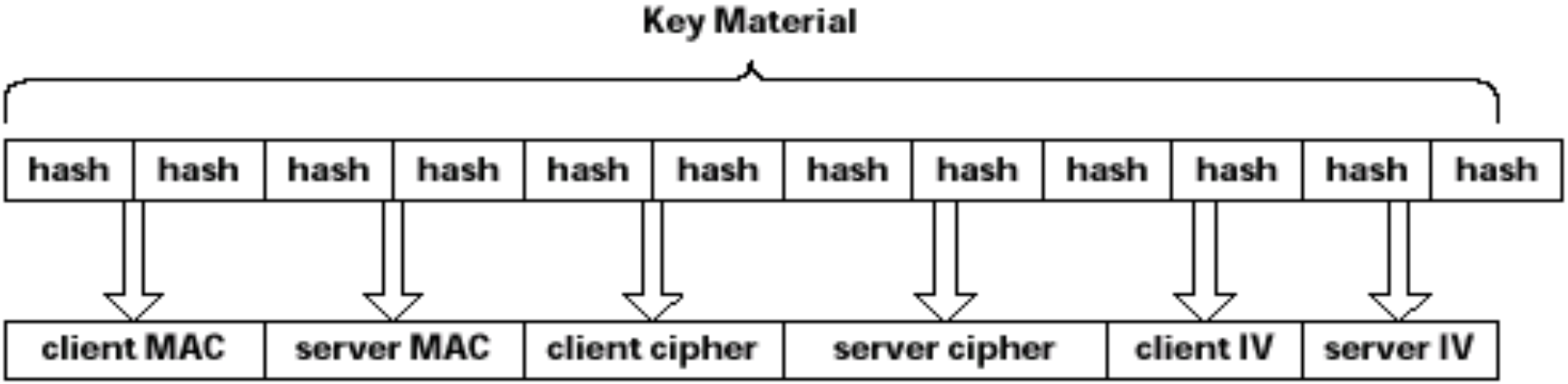
–P_hash(secret, seed) = HMAC_hash(secret, A(1) + seed) +
HMAC_hash(secret, A(2) + seed) +
HMAC_hash(secret, A(3) + seed) + ...

–A():

A(0) = seed
A(i) = HMAC_hash(secret, A(i-1))

Seguridad en Internet – SSL / TLS

- Claves de sesión



Seguridad en Internet – SSL / TLS

- Sobrecarga de TLS
  - 2 a 10 veces más lento que una conexión TCP
  - Donde se pierde rendimiento
    - Handshake
      - Cifrado asimétrico
      - Intercambio de parámetros
    - Intercambio de datos
      - Cifrado simétrico

Contenido

- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Transporte – SSL / TLS
  - Nivel de Red – IPSec
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Seguridad en Internet – IPSec

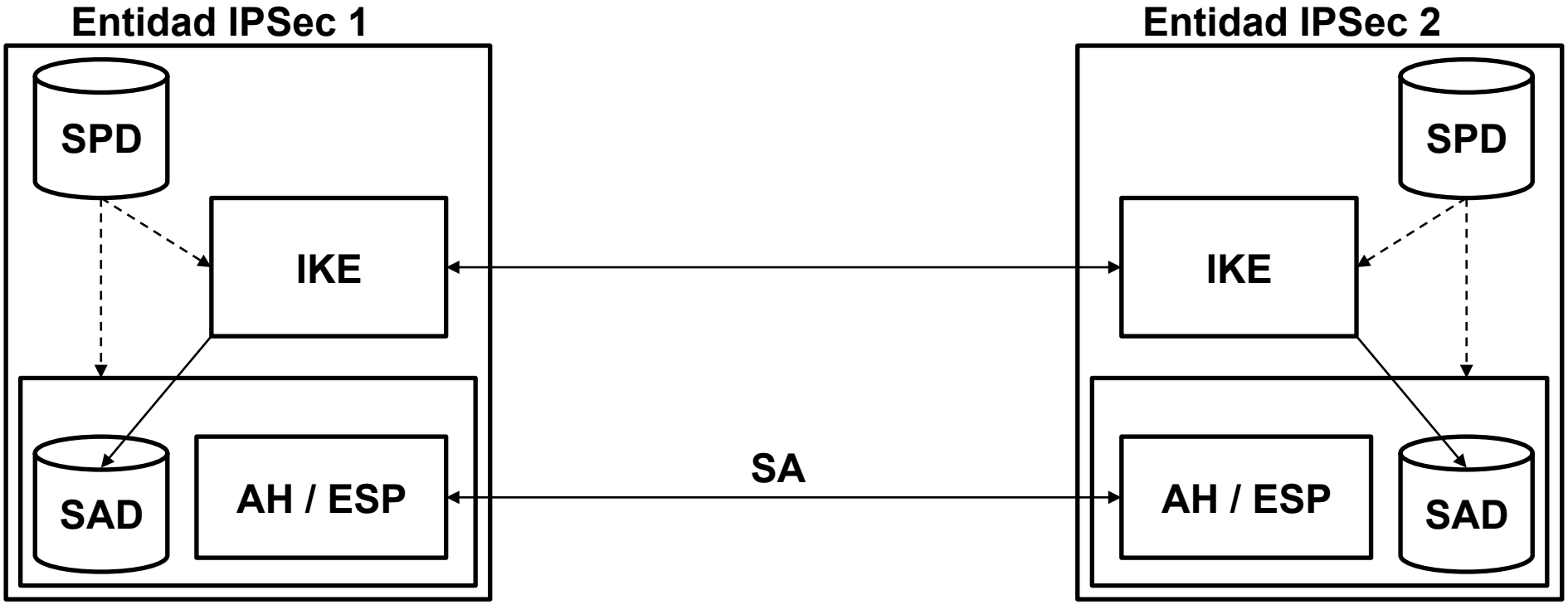
- IP Security Protocol (IPSec)
  - RFC 4301
    - RFC 4302, 4303, 4305, 5996, 4307
  - Conjunto de estándares abiertos que trabajan de forma conjunta para garantizar la comunicación entre entidades a nivel de red:
    - Confidencialidad (cifrado)
    - Integridad (hash)
    - Autenticación (firma)

Seguridad en Internet – IPSec

- Tres conceptos claves en IPSec
  - Dos modos de operación
    - Transporte
    - Túnel
  - Dos protocolos para dar servicios de seguridad
    - Encapsulating Security Payload (ESP)
    - Authentication Header (AH)
  - Asociaciones de Seguridad (SA)
    - Endpoints
    - Algoritmos de autenticación y cifrado
    - Acciones

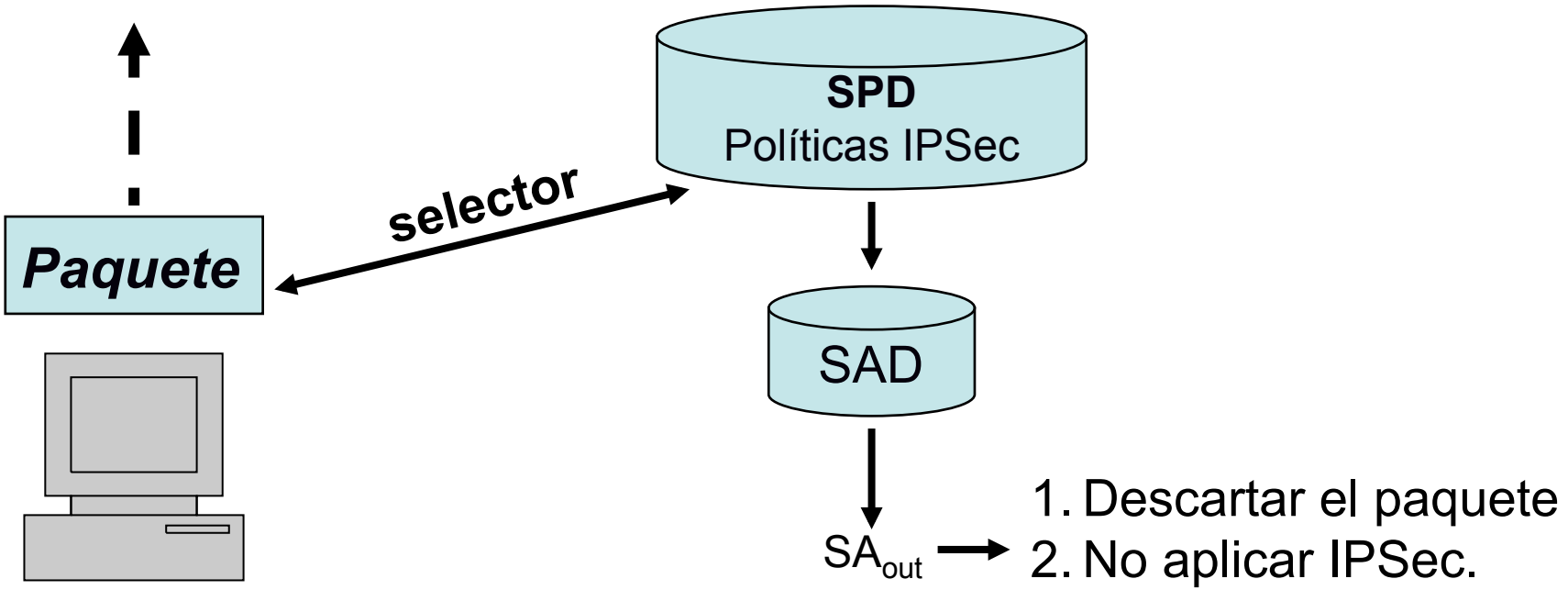
Seguridad en Internet – IPSec

- Arquitectura IPSec
  - SPD Security Policy Database
  - SAD: Security Association Database
  - IKE: Internet Key Exchange



Seguridad en Internet – IPSec

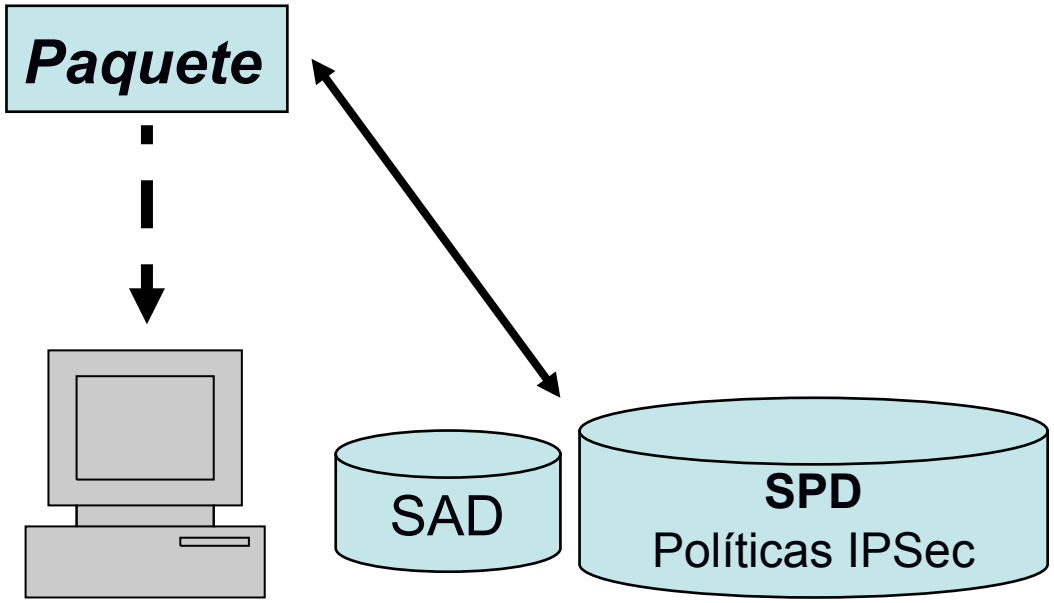
- Arquitectura IPSec – Tráfico Saliente



SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

Seguridad en Internet – IPSec

- Arquitectura IPSec – Tráfico Entrante



Caso 1:

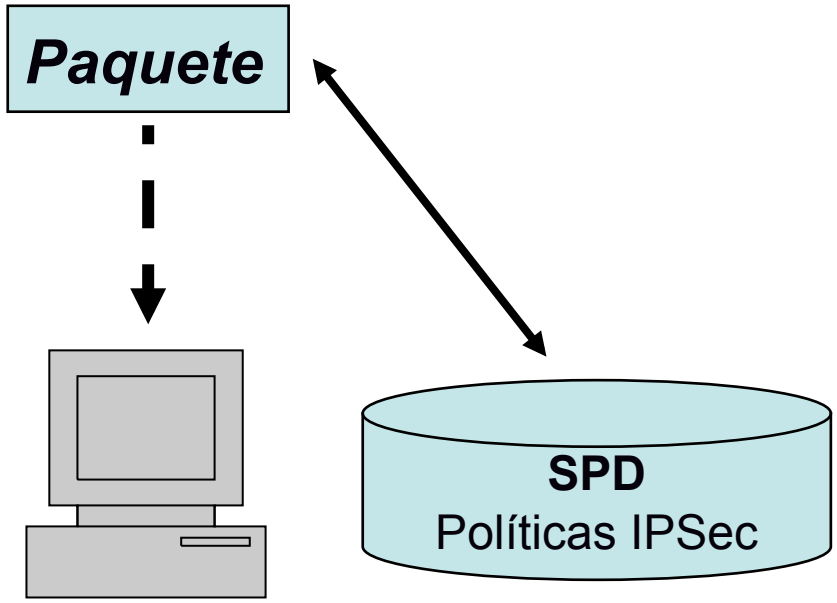
Si hay cabeceras IPSec

1. Se procesa la cabecera usando la información en la SAD.
2. Se consulta la SPD para determinar si el paquete puede ser admitido en base a la SA_{in}.

SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

Seguridad en Internet – IPSec

- Arquitectura IPSec – Tráfico Entrante



Caso 2:

Si no hay cabeceras IPSec

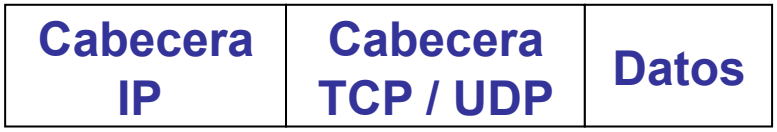
1. Se consulta la SPD para determinar la seguridad requerida para ese paquete.
2. Si necesitara seguridad el paquete se descarta.

SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

Seguridad en Internet – IPSec

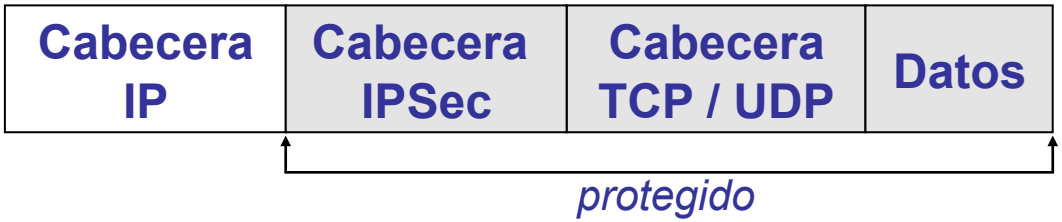
- Modos de operación

Datagrama IP Original



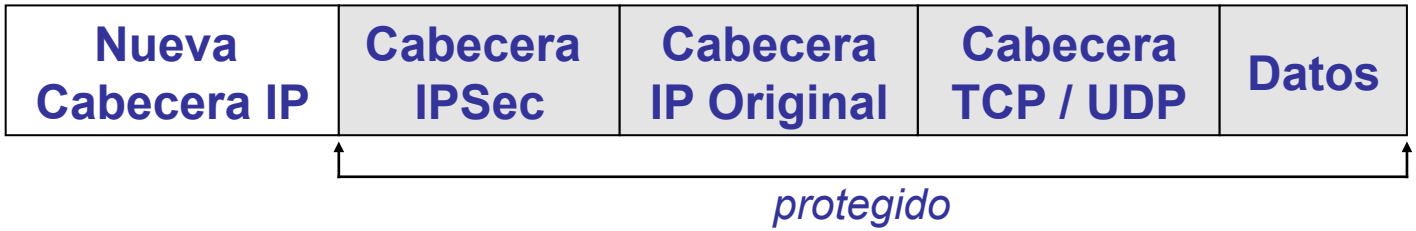
– Modo Transporte: Protege la información de capas superiores

Datagrama protegido en Modo Transporte



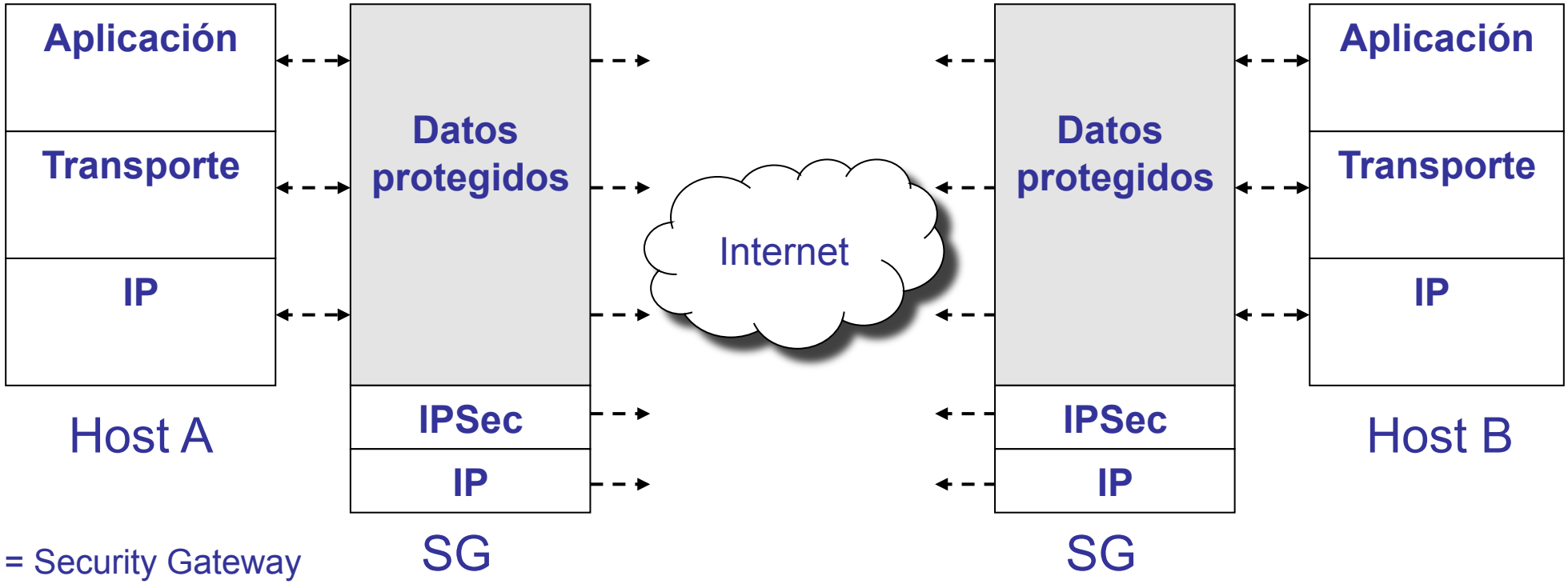
– Modo Túnel: Protege el datagrama IP completo

Datagrama protegido en Modo Túnel



Seguridad en Internet – IPSec

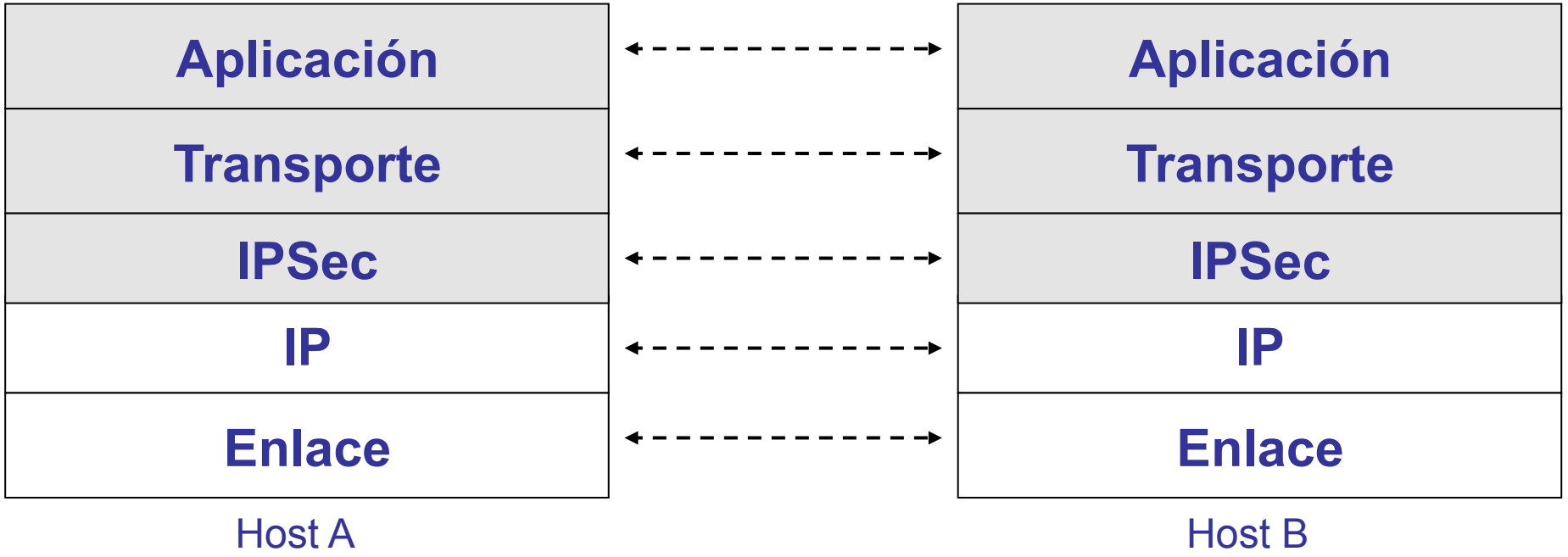
- Modos de operación
  - Modo Túnel
    - Dispositivo-a-Red o Red-a-Red



SG = Security Gateway

Seguridad en Internet – IPSec

- Modos de operación
  - Modo Transporte
    - Dispositivo-a-Dispositivo

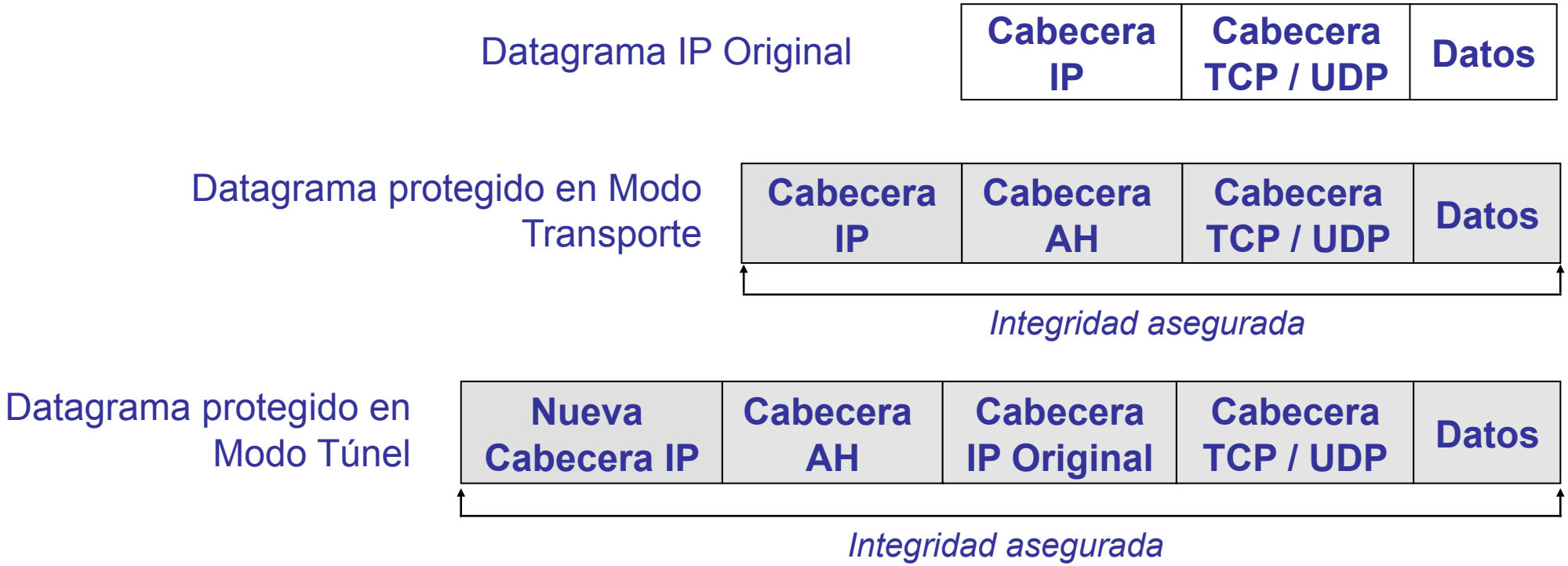


Seguridad en Internet – IPSec

- Protocolos IPSec
  - AH ofrece:
    - Integridad no orientada a la conexión
    - Autenticidad del origen
    - Protección frente a ataques por repetición
  - ESP ofrece:
    - Confidencialidad (cifrado)
    - Integridad no orientada a la conexión
    - Autenticidad del origen
    - Protección frente a ataques por repetición
  - Se pueden usar de manera independiente o conjunta
  - Se pueden usar en modo Transporte o Túnel

Seguridad en Internet – IPSec

- Formato de datagramas protegidos por AH



Seguridad en Internet – IPSec

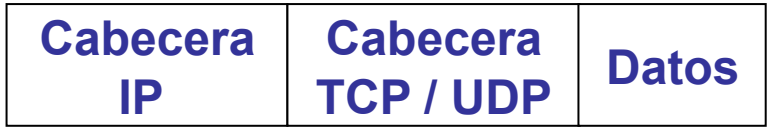
Siguiente Cabecera	Longitud Payload	Reservado
Sequence Paramater Index (SPI)		
Número de Secuencia		
Integrity Check Value (ICV)		

- Cabecera AH
  - Siguiente Cabecera (1 byte)
  - Longitud Payload (1 byte): Longitud de la cabecera (en bloques de 4 bytes) menos 2
  - Reservado (2 bytes)
  - SPI (4 bytes): Identificador de la SA
  - Número de Secuencia (4 u 8 bytes)
    - Comienza en 0 al establecer la SA
    - Número de Secuencia Extendido (ESN) negociado con la SA
  - ICV (variable): HMAC(IP, AH, Todo detrás de AH)
    - Longitud depende del algoritmo definido en la SA
    - Padding si el resultado no es un múltiplo de 4 bytes
    - Mutable vs Inmutable: DSCP, ECN, Flags, Offset, TTL, IP Checksum a 0 para el cálculo

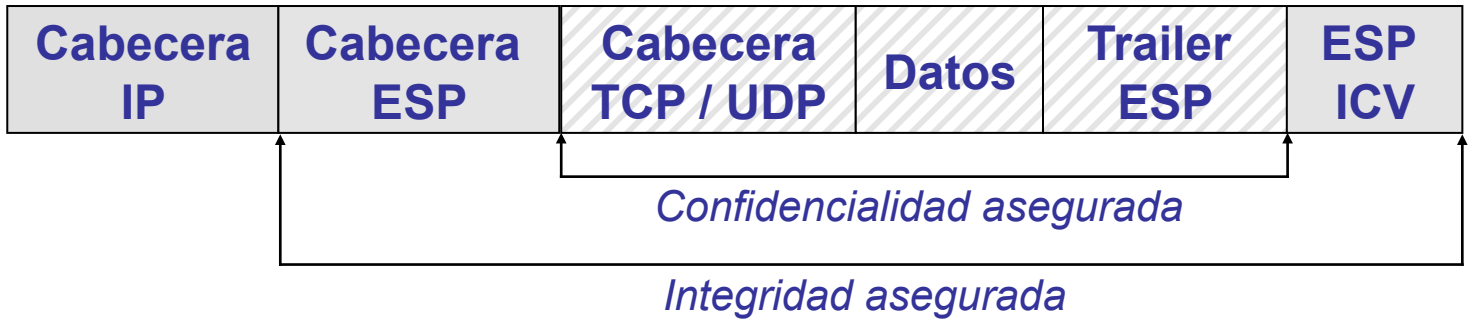
Seguridad en Internet – IPSec

- Formato de datagramas protegidos por ESP

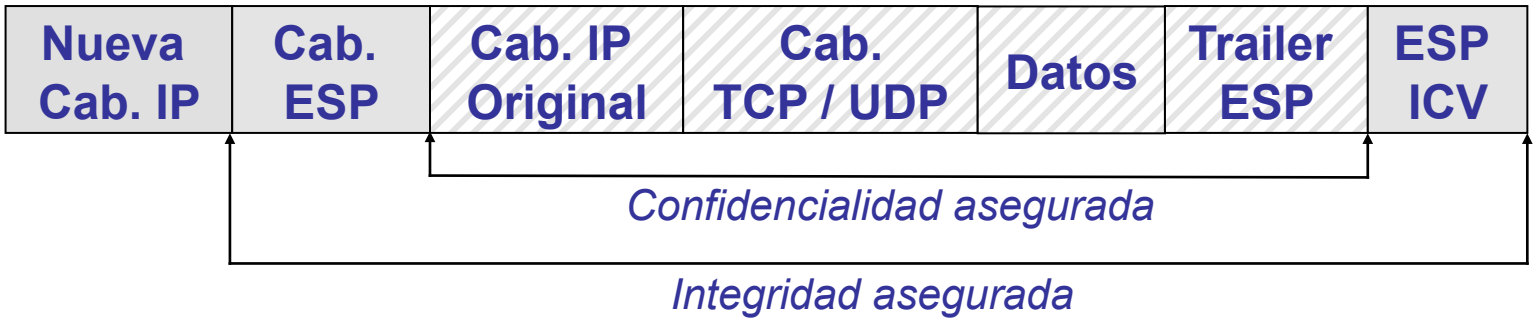
Datagrama IP Original



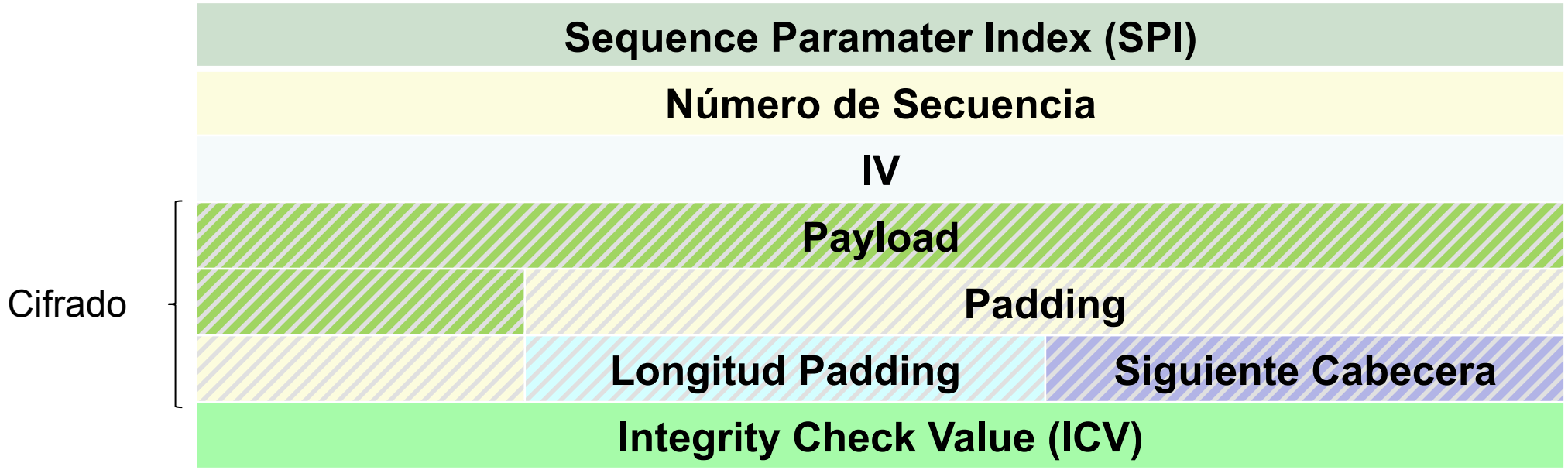
Datagrama protegido en Modo Transporte



Datagrama protegido en Modo Túnel



Seguridad en Internet – IPSec



- Paquete ESP
  - SPI (4 bytes): Identificador de la SA
  - Número de Secuencia (4 u 8 bytes)
    - Comienza en 0 al establecer la SA
    - Número de Secuencia Extendido (ESN) negociado con la SA
  - IV (0 - variable): Depende del algoritmo de cifrado
  - Payload (variable): Depende del modo de operación
  - Padding (variable): Depende del algoritmo de cifrado
    - Ej: Alinear al tamaño de bloque
  - Longitud Padding (1 byte) y Siguiente Cabecera (1 byte)
    - Alineadas a los 4 bytes
  - ICV (variable)
    - Longitud depende del algoritmo definido en la SA
    - HMAC(Paquete ESP)

Seguridad en Internet – IPSec

- Algoritmos criptográficos usados
  - AH
    - HMAC-SHA1-96 [RFC2404] (MUST)
    - AES-XCBC-MAC-96 [RFC3566] (SHOULD+)
    - HMAC-MD5-96 [RFC2403] (MAY)
  - ESP
    - Cifrado
      - TripleDES-CBC [RFC2451] (MUST-)
      - AES-CBC con claves de 128-bits [RFC3602] (SHOULD+)
      - AES-CTR [RFC3686] (SHOULD)
      - DES-CBC [RFC2405] (SHOULD NOT)
    - Integridad
      - HMAC-SHA1-96 [RFC2404] (MUST)
      - AES-XCBC-MAC-96 [RFC3566] (SHOULD+)
      - HMAC-MD5-96 [RFC2403] (MAY)

Seguridad en Internet – IPSec

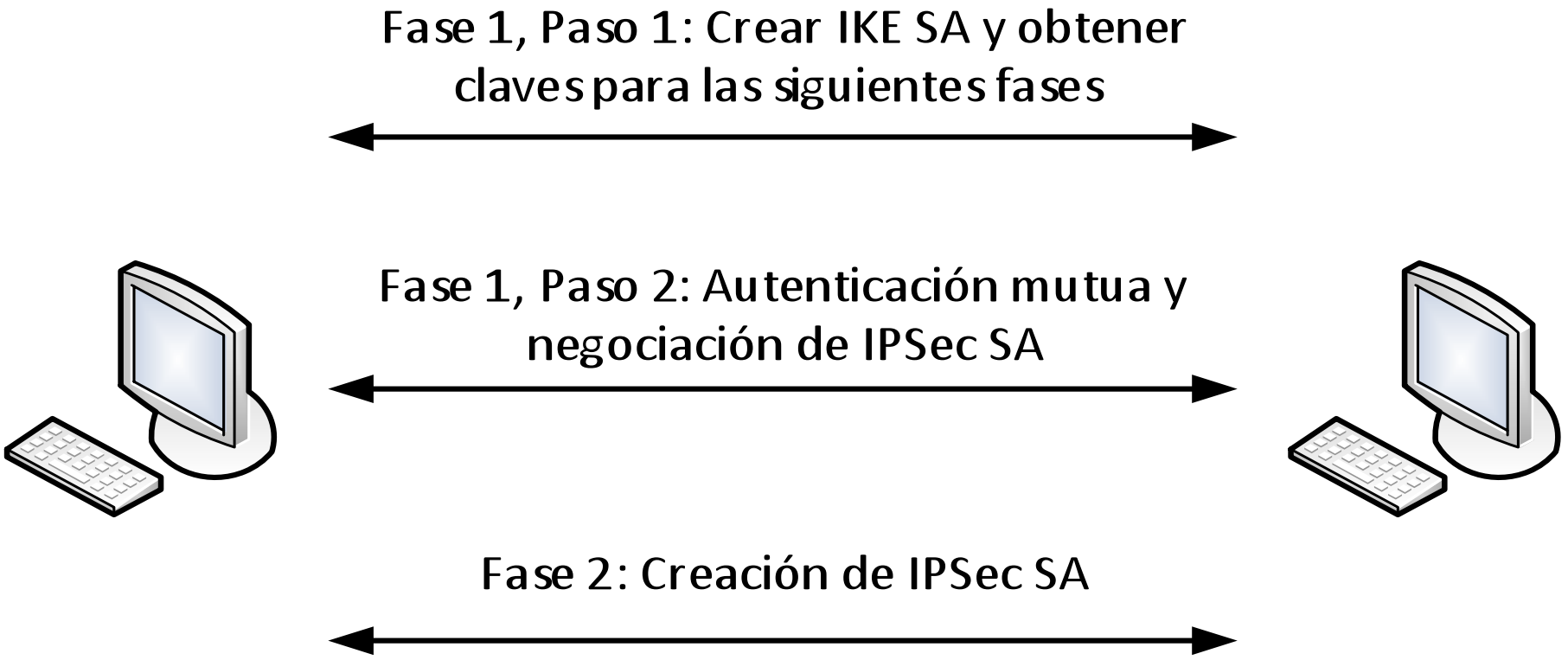
- Establecimiento de SAs
- AH y ESP necesitan claves
  - Gestión manual de claves
    - Sencillo
    - Práctico en entornos pequeños y estáticos
    - Fallos humanos
      - Ej: Add 200.168.1.100 193.68.2.23 esp 0x201 -m tunnel -E 3des-cbc 0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831 -A hmac-md5 0xc0291ff014dccdd03874d9e8e4cdf3e6;
    - Claves estáticas = Claves no seguras
- Gestión dinámica de claves
  - Internet Key Exchange (IKE)

Seguridad en Internet – IPSec

- IKE
  - v1 → RFC 2409
  - v2 → RFC 5996
- Funciones:
  - Autenticación y Generación de claves
  - Negociación de los algoritmos criptográficos (SAs)
  - Re-generación de claves

Seguridad en Internet – IPSec

- IKEv2

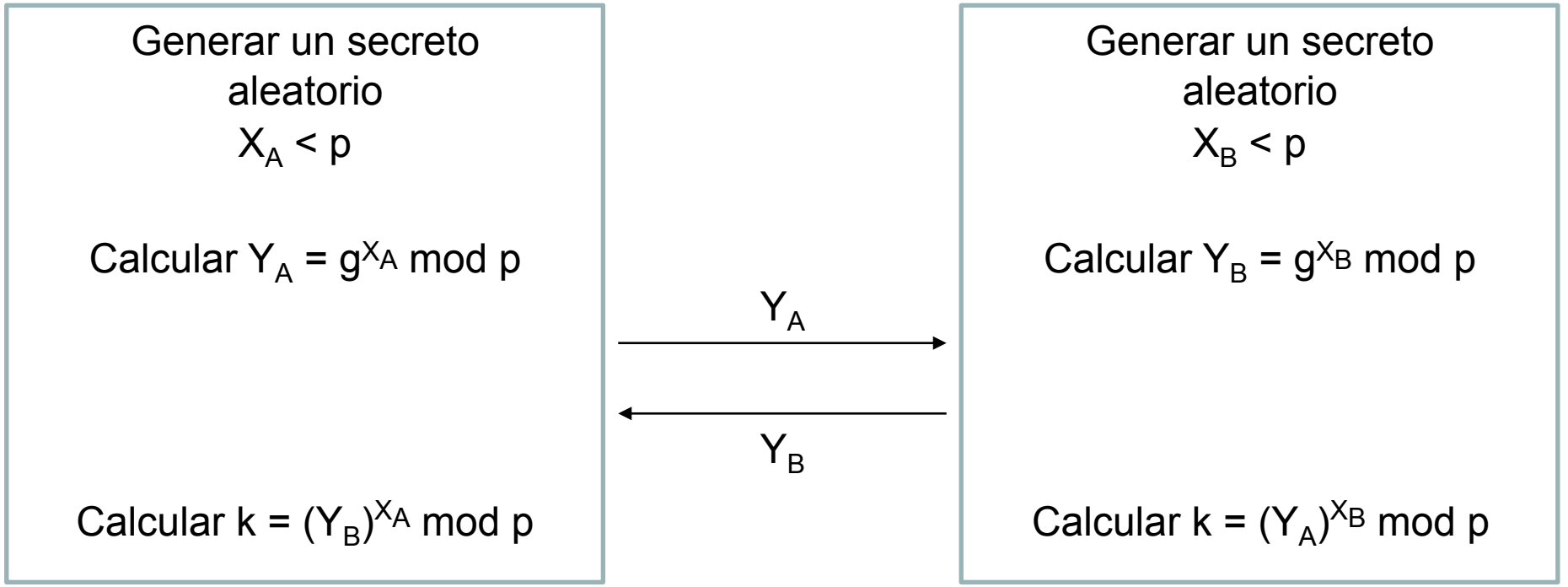


Seguridad en Internet – IPSec

- IKEv2
  - Fase 1, Paso 1: IKE_SA_INIT (Intercambio no seguro)
    - Negociación de los algoritmos que se usarán durante el protocolo IKE
    - Derivación de claves para los algoritmos de IKE
    - Derivación de una clave maestra k_d usada como semilla para las claves de los protocolos ESP y/o AH
  - Fase 1, Paso 2: IKE_AUTH (Intercambio seguro)
    - Autenticación mutua
    - Negociación de los algoritmos usados en IPSec SA
  - Fase 2: CREATE_CHILD_SA (Intercambio seguro)
    - Establecimiento de la IPSec SA
    - Derivación de claves para los protocolos ESP y/o AH

Seguridad en Internet – IPSec

- Diffie-Hellman (repaso)
  - Derivación de claves sin necesidad de secreto previo a través de un canal inseguro



Seguridad en Internet – IPSec

- Función Pseudo Aleatoria (Pseudo-Random Function – PRF)
  - Genera un número de longitud fija en base a una clave y datos de longitud variable
    - Modificación de HMAC
  - Se usa para generar el material criptográfico en IKE
  - Funciones recomendadas por el RFC 4307
    - PRF_HMAC_MD5 (MAY)
    - PRF_HMAC_SHA1 (MUST)
    - PRF_AES128_CBC (SHOULD+)
  - IKE usa PRF+
    - El número generado no es lo bastante largo
    - PRF+(K, S) = T_1, T_2, T_3, T_4, …

      T_1 = PRF(K, S | 0x01)

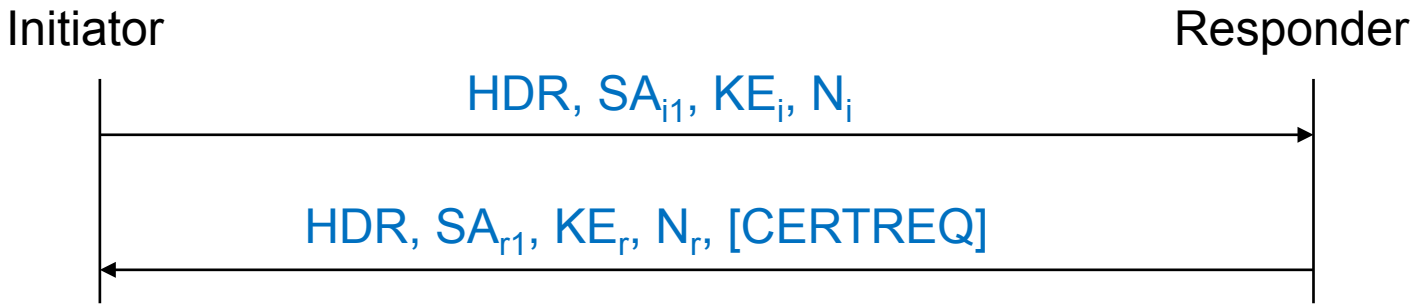
      T_2 = PRF(K, T_1 | S | 0x02)

      T_3 = PRF(K, T_2 | S | 0x03)

      T_4 = PRF(K, T_3 | S | 0x04)

Seguridad en Internet – IPSec

- Fase 1.1: IKE_SA_INIT
  - HDR (Cabecera IKE)
    - Versión del protocolo
    - SPI_i: Identificador de la IKE SA
  - SA_{i1}
    - Propuesta de algoritmos y mecanismos de seguridad para las Fases 1.2 y 2
      - Grupo DH, Algoritmos de cifrado e integridad
  - KE_x
    - Intercambio Diffie-Hellman
  - N_x
    - Nonces de Initiator y Responder
  - SA_{r1}
    - Selección en base a las propuestas en SA_{i1}
  - [CERTREQ]
    - Opcional. Enviado si la autenticación en la Fase 1.2 se basa en certificados



Seguridad en Internet – IPSec

- Fase 1.1: IKE_SA_INIT
  - Cada parte genera SKEYSEED:

$$SKEYSEED = PRF(N_i \mid N_r, K_{DH})$$

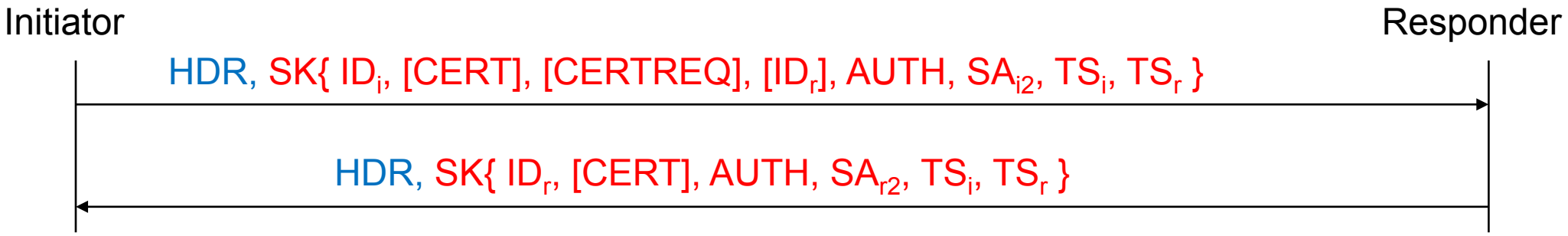
  - SKEYSEED se usa en PRF+ para generar todas las claves necesarias en las Fases 1.2 y 2

$$\{SK\_d \mid SK\_ai \mid SK\_ar \mid SK\_ei \mid SK\_er \mid SK\_pi \mid SK\_pr\} = PRF+(SKEYSEED, N_i \mid N_r \mid SPI_i \mid SPI_r)$$

    - SK_ai y SK_ar para el algoritmo de integridad
    - SK_ei y SK_er para el algoritmo de cifrado
    - SK_pi y SK_pr para autenticación mutua en IKE_AUTH si no se usan certificados
    - SK_d se usará en la Fase 2 para generar las claves IPSec (ESP y/o AH)

Seguridad en Internet – IPSec

- Fase 1.2: IKE_AUTH
  - {…}
    - Contenido protegido por SK_e y SK_a según esté definido en la IKE_SA
  - ID_i, ID_r
    - Identificadores para autenticación mutua
  - AUTH
    - Basada en SK_pi y SK_pr + Idx
  - SA_{i2} / SA_{r2}
    - IPSec SA
  - TS: Traffic Selector
    - @IP y Puerto al que asociar la SA
    - Ej:
      - TS_i = (0, 0-65535, 192.0.2.202-192.0.2.255)
      - TS_r = (0, 0-65535, 192.0.2.202-192.0.2.255)

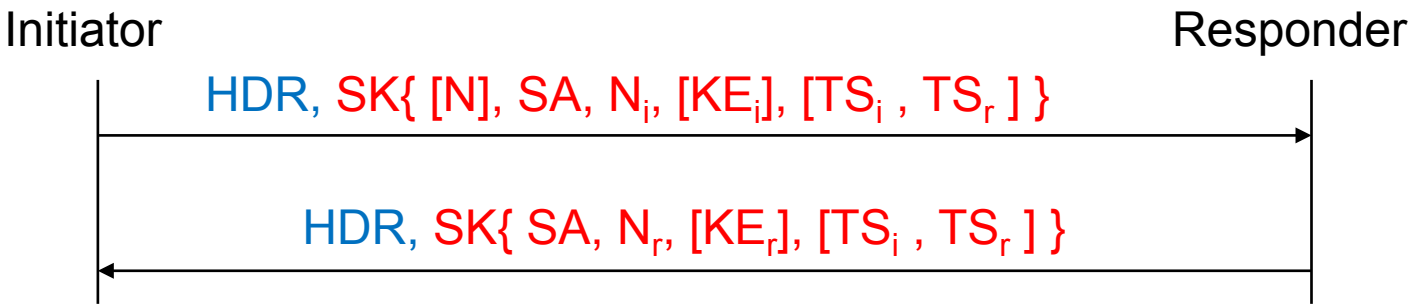


Seguridad en Internet – IPSec

- Fase 1.2: IKE_AUTH
  - Autenticación mutua
    - AUTH basado en dos posibles métodos
      - Firma digital
        - » Firma de clave pública usando los certificados intercambiados
      - Llaves compartidas
        - » SK_pi y SK_pr
        - » AUTH = PRF(PRF(SK_px, “Key Pad for IKEv2”), <mensaje>)
  - Negociación de la IPSec SA
    - SAi2 propuesta de SAs
    - SAr2 selección de entre las propuestas

Seguridad en Internet – IPSec

- Fase 2: CREATE_CHILD_SA
  - [N]: Notificación
    - Presente si se negocia la IPSec SA
  - [KE_x]: Opcionales
    - Intercambio Diffie-Hellman
  - [TS_x]: Opcionales
  - SA
    - Detalles de la IPSec SA negociada
    - Permitido negociar múltiples IPSec SA sobre la misma IKE SA
    - Campos opcionales usados también en Rekeying



Seguridad en Internet – IPSec

- Fase 2: CREATE_CHILD_SA
  - Claves para AH y/o ESP generadas finalmente
  - KEYMAT = PRF+(SK_d, N_i | N_r)
    - N_i y N_r de Fase 2
  - Si KEx están presentes entonces
    - KEYMAT = PRF+(SK_d, K_{DH} | N_i | N_r)

Seguridad en Internet – IPSec

- Formato de propuesta de SAs

```
SA Payload
   |
   +--- Proposal #1 ( Proto ID = ESP(3), SPI size = 4,
   |      |             7 transforms,      SPI = 0x052357bb )
   |      |
   |      +-- Transform ENCR ( Name = ENCR_AES_CBC )
   |      |     +-- Attribute ( Key Length = 128 )
   |      |
   |      +-- Transform ENCR ( Name = ENCR_AES_CBC )
   |      |     +-- Attribute ( Key Length = 192 )
   |      |
   |      +-- Transform ENCR ( Name = ENCR_AES_CBC )
   |      |     +-- Attribute ( Key Length = 256 )
   |      |
   |      +-- Transform INTEG ( Name = AUTH_HMAC_SHA1_96 )
   |      +-- Transform INTEG ( Name = AUTH_AES_XCBC_96 )
   |      +-- Transform ESN ( Name = ESNs )
   |      +-- Transform ESN ( Name = No ESNs )
   |
   +--- Proposal #2 ( Proto ID = ESP(3), SPI size = 4,
          |             4 transforms,      SPI = 0x35a1d6f2 )
          |
          +-- Transform ENCR ( Name = AES-GCM with a 8 octet ICV )
          |     +-- Attribute ( Key Length = 128 )
          |
          +-- Transform ENCR ( Name = AES-GCM with a 8 octet ICV )
          |     +-- Attribute ( Key Length = 256 )
          |
          +-- Transform ESN ( Name = ESNs )
          +-- Transform ESN ( Name = No ESNs )
```

Contenido

- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Red – IPSec
  - Nivel de Transporte – SSL / TLS
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Seguridad en Internet – PGP

- Pretty Good Privacy (RFC 4880)
  - Aplicación de carácter general para proteger (cifrar y/o firmar) archivos
  - Se emplea por lo general para proteger el correo electrónico
  - Se basa en una combinación de criptografía simétrica y asimétrica
    - RSA, DSA, El Gamal, AES, SHA, …
  - Desarrollado en 1991 por Phil Zimmermann
  - En la actualidad soportado por OpenPGP standard
    - Implementación de referencia GnuPG

Seguridad en Internet – PGP

- Servicios PGP
  - Envío de mensajes
    - Autenticación
    - Confidencialidad
    - Compresión
    - Compatibilidad con e-mail
    - Segmentación y ensamblado
  - Gestión de claves
    - Generación, distribución y revocación de claves (pub/priv)
    - Generación y transporte de claves de sesión

Seguridad en Internet – PGP

- PGP define el concepto de *"aro"* (ring) para agrupar las llaves
  - Hay aros tanto para las claves propias (pareja de llaves pública y privada) como para las de los demás usuarios (llave pública del otro).

Private Keyring

ID Usuario	ID Llave	Llave Pública	Llave Privada (cifrada)	Timestamp
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

Public Keyring

ID Usuario	ID Llave	Llave Pública	Confianza en el usuario	Firma	Confianza en la firma	Legitimidad	Tstamp
*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*

Seguridad en Internet – PGP

- Ejemplo Private Keyring
  - Supongamos que Alice tiene dos pares de llaves
    - Una para alice@some.com y otra para alice@anet.net
    - Cada una utiliza un par de llaves distintas.
  - El ID de la llave son los 64 bits menos significativos de la llave pública
    - Únicos para un usuario con altísima probabilidad
  - El cifrado de la llave privada se hace mediante un *passphrase*.

ID Usuario	ID Llave	Llave Pública	Llave Privada (cifrada)	Timestamp
alice@some.com	ABCD1234	FE…ABCD1234	AD1234…894CDE	2014-05-12 08:30
alice@anet.net	5678CDEF	12…5678CDEF	FAC567…1DE3C5	2014-05-12 08:35

Seguridad en Internet – PGP

- PGP no se basa en una estructura PKI con CAs sino que define un concepto denominado Web of Trust (WoT)
  - Confianza en el usuario (owner trust)
    - Asignada por el propio usuario
    - Valores posibles:
      - usuario desconocido
      - no suelo confiar en él
      - suelo confiar en él
      - siempre confío en él
      - confianza total (clave propia presente en el private keyring)
  - Confianza en la firma (signature trust)
    - Asignada automáticamente
    - Si la llave pública correspondiente con la que se ha firmado está en el public keyring se asocia al owner trust de esa llave
    - Si no, se le da un valor de *desconocida*

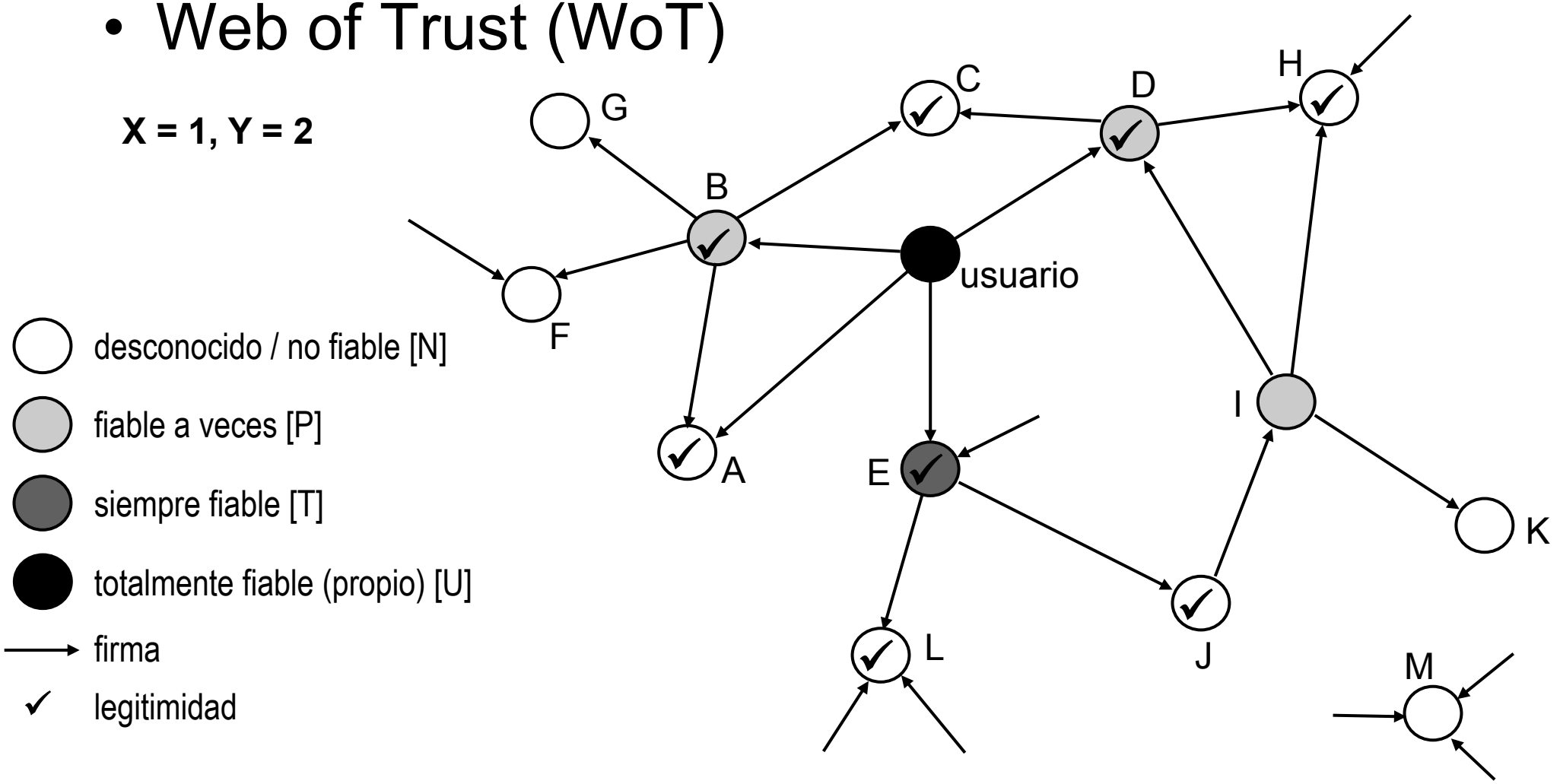
Seguridad en Internet – PGP

- Web of Trust (WoT)
  - Legitimidad
    - Asignada automáticamente
    - Si está firmada por nosotros mismos la legitimidad es total
    - Si no, se hace una suma ponderada de las signature trust de todas las firmas que se tengan
      - firmas de usuarios en los que confío siempre tienen un peso 1/X
      - firmas de usuarios en los que suelo confiar tienen un peso 1/Y
      - X e Y son parámetros configurables
    - Por ejemplo: X = 2, Y = 4
      - 1 firma propia
      - 2 firmas por usuarios fiables
      - 1 firma de un usuario fiable y 2 fiables a menudo
      - 4 firmas de usuarios fiables a menudo

Seguridad en Internet – PGP

- Web of Trust (WoT)

X = 1, Y = 2



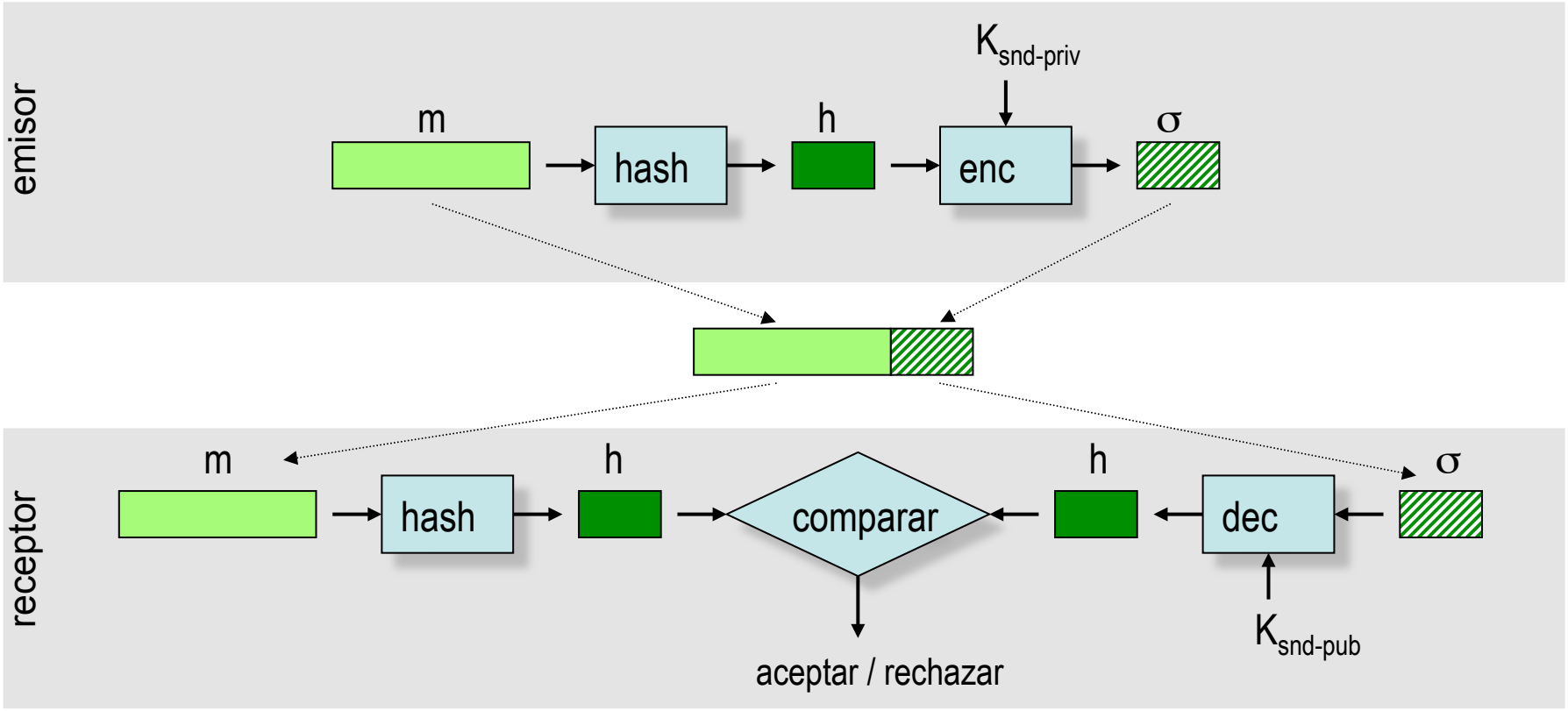
Seguridad en Internet – PGP

- Ejemplo del Aro de Llaves Públicas (Public Ring)

ID Usuario	ID Llave	Llave Pública	Confianza en el usuario	Firma	Confianza en la firma	Legitimidad	Tstamp
alice@some.com	ABCD1234	FE…ABCD1234	[U]			[U]	…
bob@gmail.com	A1B2C3D4	12…A1B2C3D4	[T]			[T]	…
ted@yahoo.com	12345678	AB…12345678	[T]	bob	[T]	[T]	…
joan@msm.com	09876543	CD…09876543	[P]	bob	[T]	[T]	…
john@gmx.net	ABCD6543	FE…ABCD6543	[N]	joan ted	[P] [T]	[T]	…

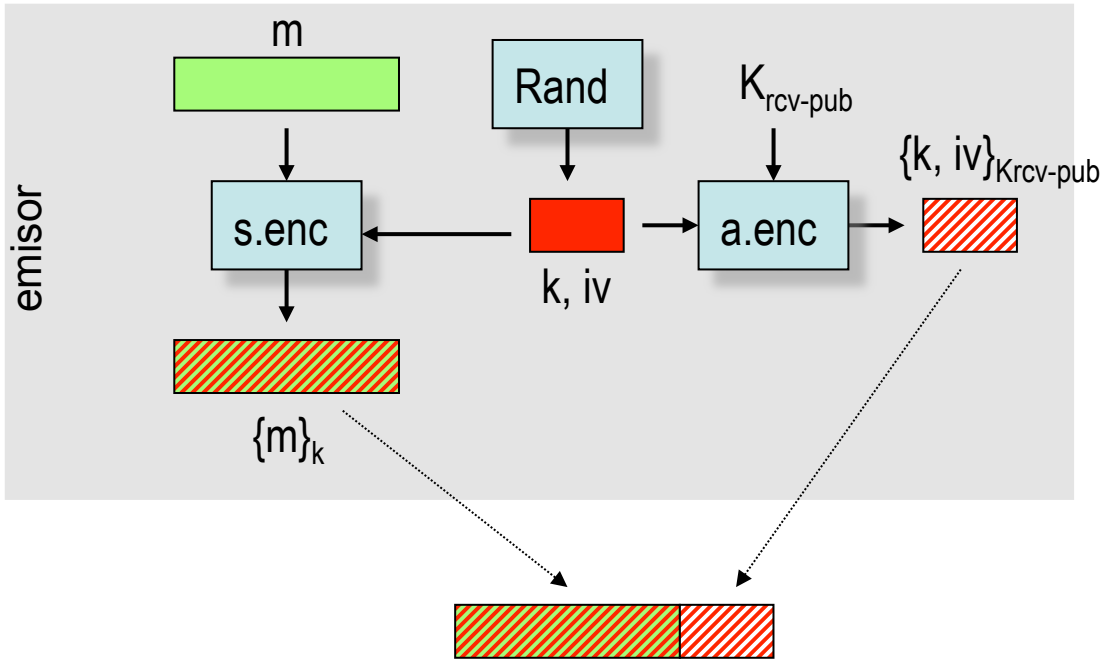
Seguridad en Internet – PGP

- Servicio de autenticación
  - Basado en firma digital



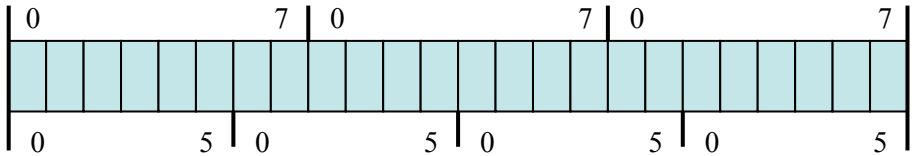
Seguridad en Internet – PGP

- Servicio de confidencialidad



Seguridad en Internet – PGP

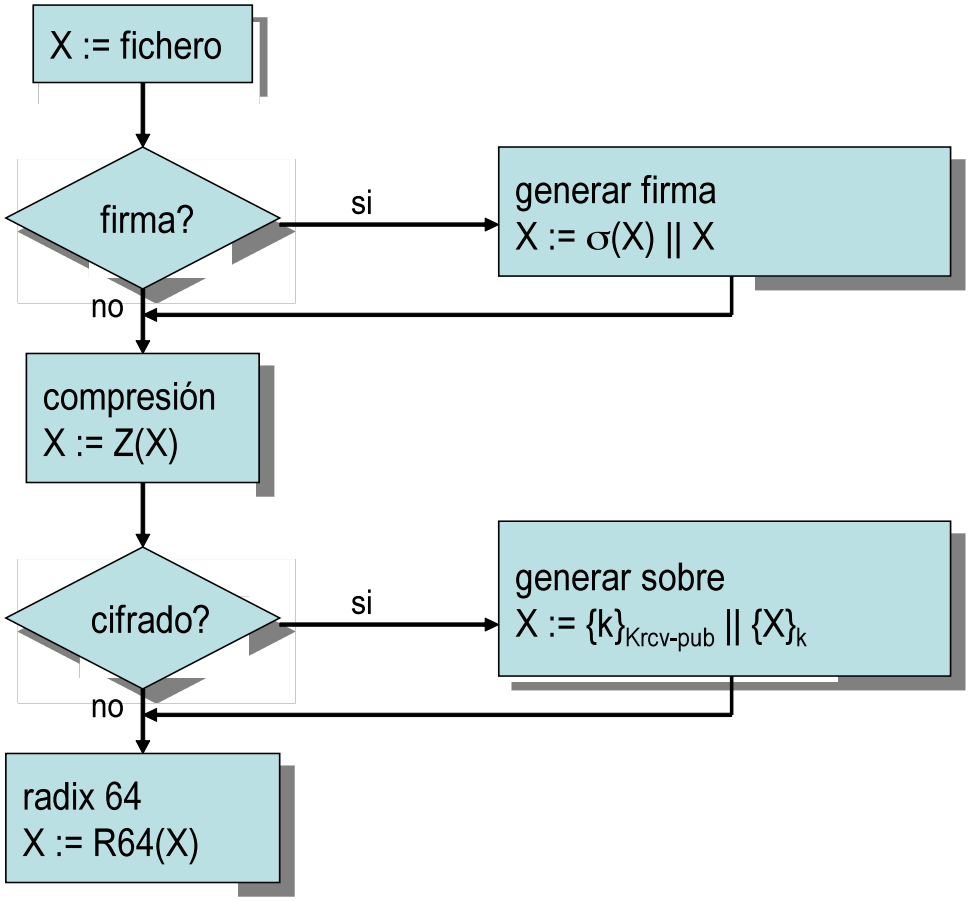
- Servicio de compresión
  - Aplicado después de la firma
    - Permite usar diferentes algoritmos de compresión
  - Aplicado antes del cifrado
    - Reduce la redundancia y hace el cripto-análisis más difícil
  - Algoritmo típico: ZIP
- Compatibilidad con el e-mail
  - Una vez se cifra los octetos son arbitrarios
  - Los clientes de correo están preparados para recibir ASCII
  - Conversión Radix 64
    - 3 bloques de 8-bit binarios → 4 bloques de 6-bit ASCII



6-bit	codificación	6-bit	codificación
0	A	52	0
…	...	…	…
25	Z	61	9
26	a	62	+
…	…	63	/
51	z	(pad)	=

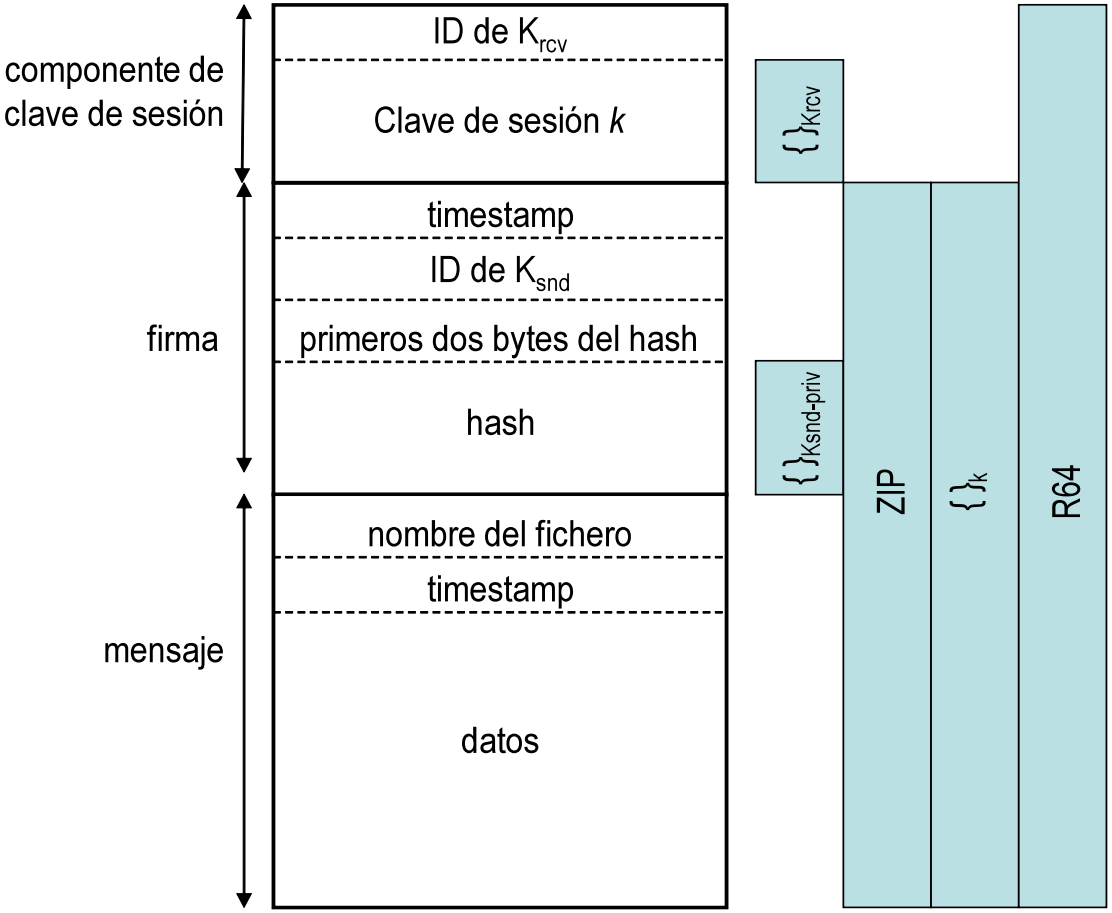
Seguridad en Internet – PGP

- Combinación de servicios



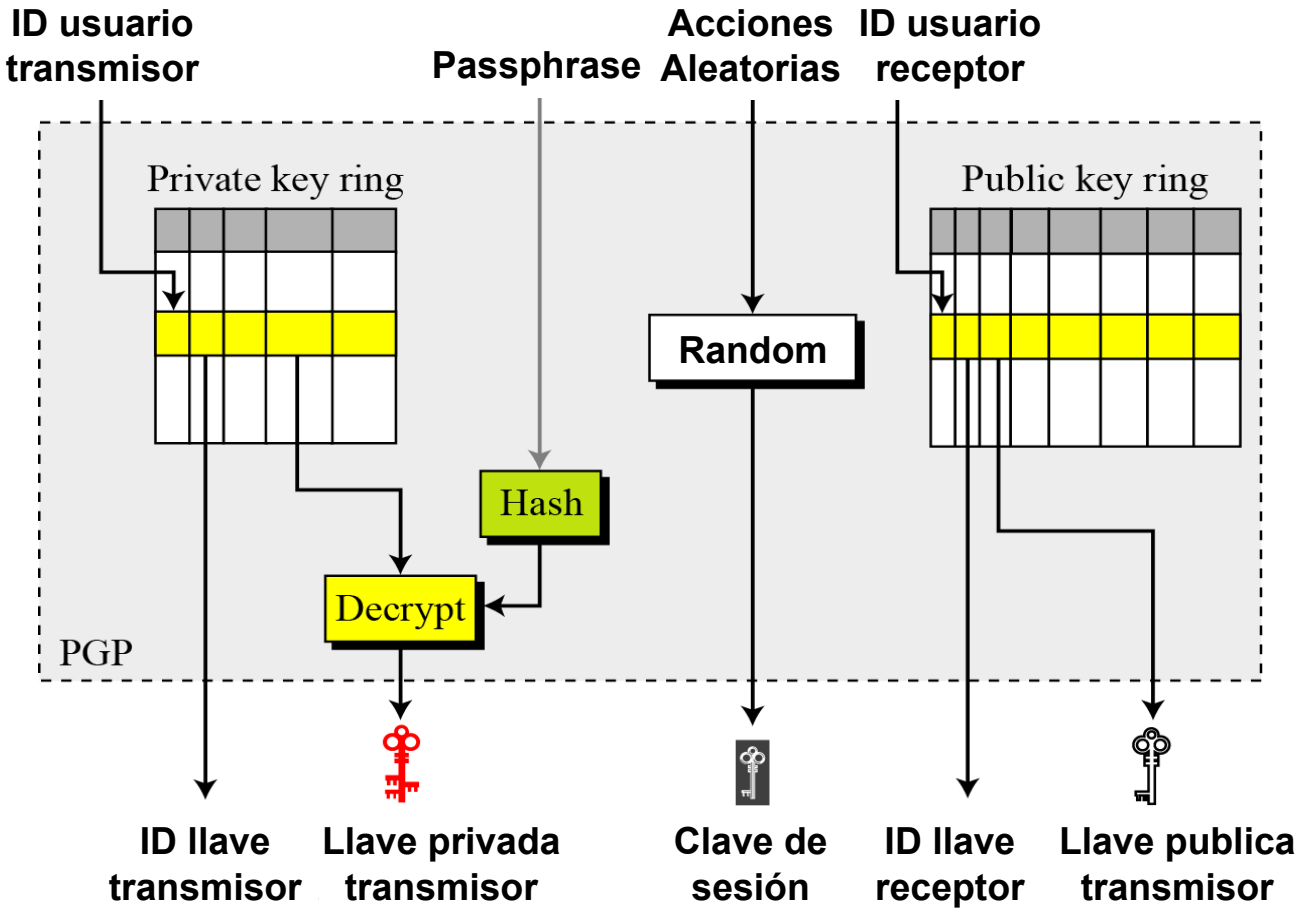
Seguridad en Internet – PGP

- Formato del mensaje PGP



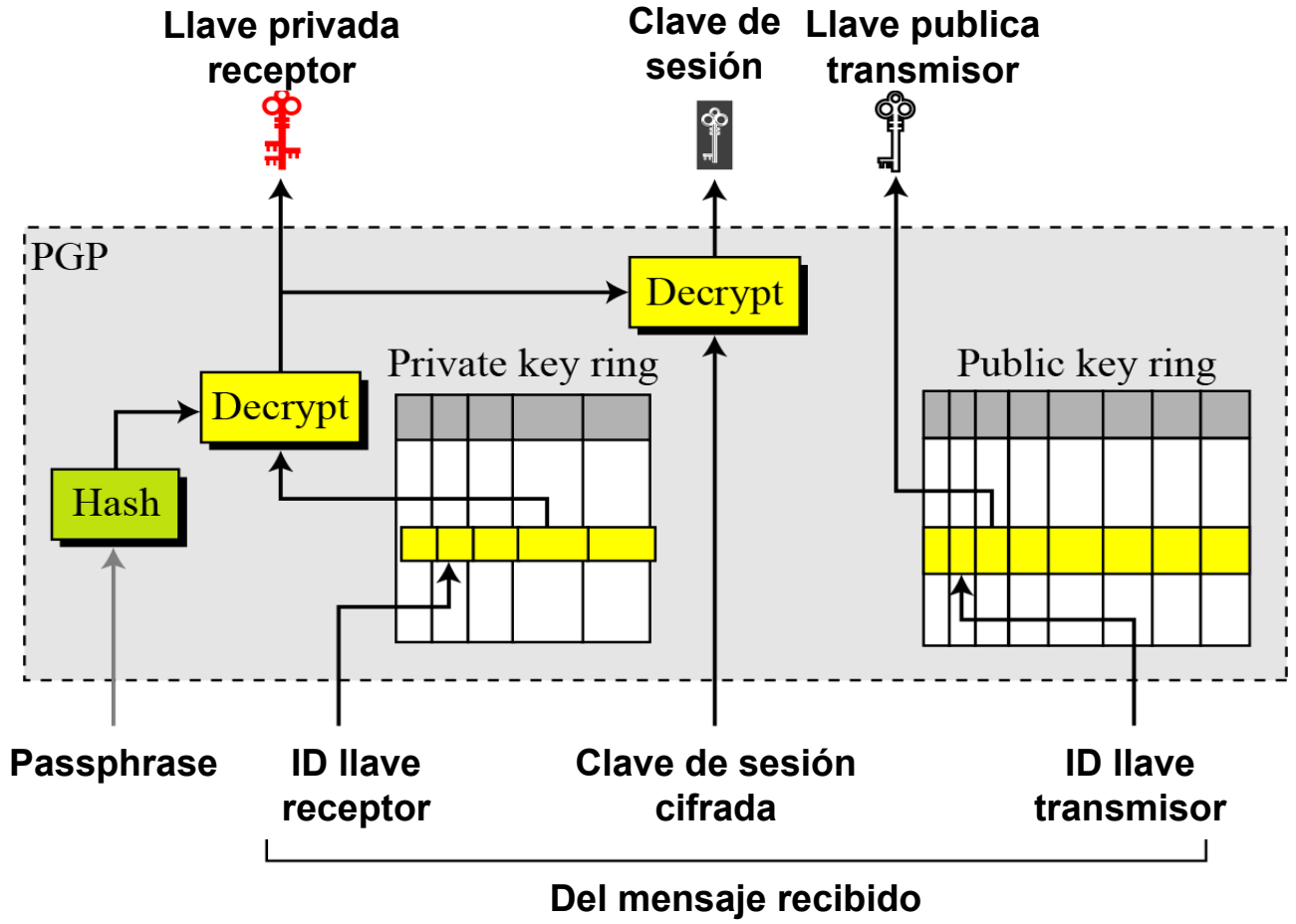
Seguridad en Internet – PGP

- Extracción de información al enviar



Seguridad en Internet – PGP

- Extracción de información al recibir



Contenido

- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Red – IPSec
  - Nivel de Transporte – SSL / TLS
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Control de Acceso – Introducción

- Es necesario proteger redes, sistemas y demás recursos contra ciertos problemas de seguridad:
  - Pérdida de confidencialidad
  - Imposibilidad de garantizar la integridad de la información
  - Pérdida de disponibilidad en servicios críticos
  - Exposición de información que permita realizar ataques a nuestro sistema o a terceros.

Contenido

- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Red – IPSec
  - Nivel de Transporte – SSL / TLS
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Control de Acceso – Cortafuegos

- Un sistema firewall es una combinación de hardware y software usado para implementar la política de seguridad establecida sobre el intercambio de información entre 2 o más redes.
- Es la primera línea de defensa sobre ataques externos
  - También puede ser usado para prevenir ataques internos
- Mejora la seguridad de la red y reduce los riesgos de accesos incontrolados dentro de los sistemas:
  - Concentración de la seguridad
  - Filtrado de servicios / protocolos
  - Ocultación de información
  - Control de accesos detallado (accounting)

Control de Acceso – Cortafuegos

- Criterios de diseño
  - Un firewall se inserta entre redes con distinto nivel de confianza
    - Generalmente entre una Intranet e Internet
  - Todo el tráfico que entra o sale de la red privada pasa a través del firewall
    - Bloqueo físico de cualquier acceso
  - Sólo el tráfico autorizado puede atravesar el firewall
  - El firewall es inmune a los ataques

Control de Acceso – Cortafuegos

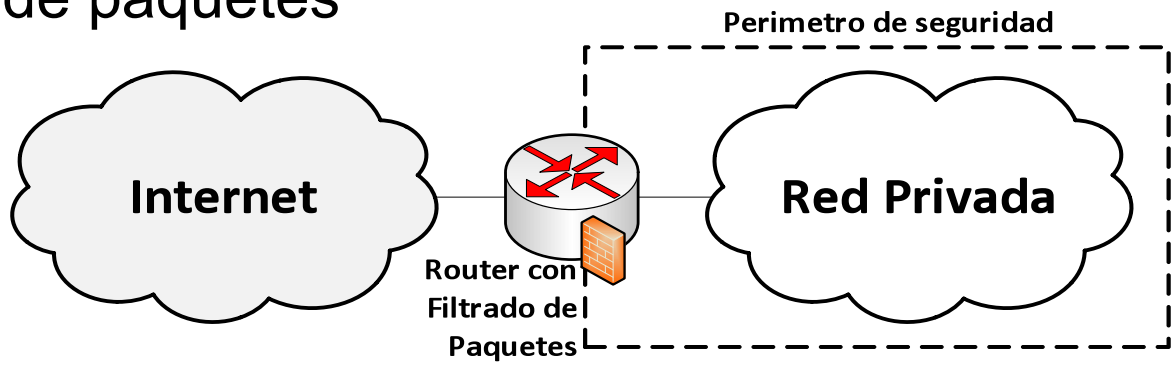
- Cuatro técnicas básicas para implementar el control de acceso
  - Control de servicios
    - Determina el tipo de servicios de Internet a los que se puede acceder (tanto dentro como fuera)
  - Control de sentido
    - Determina el sentido en el que un determinado servicio se puede acceder
  - Control de usuario
    - El control se hace en función de quien accede al servicio
  - Control del comportamiento
    - Limita el modo en el que se accede a un servicio

Control de Acceso – Cortafuegos

- Existen 3 categorías básicas de firewalls dependiendo de en que nivel o niveles dentro del modelo TCP/IP trabaje el sistema firewall:
  - Filtrado de paquetes
  - Servidores Proxy
  - Gateway de circuito
  - Inspección multi-capa (combinación de los anteriores)

Control de Acceso – Cortafuegos

- Filtrado de paquetes



  - Aplica una serie de reglas a cualquier paquete que llegue y después re-envía o descarta el paquete
    - En ambas direcciones
  - Las reglas se definen en base a:
    - Direcciones IP origen y destino
    - Protocolo de nivel superior
      - TCP, UDP, ICMP
    - Puertos origen y destino
    - Flags de TCP
      - SYN para establecimiento de conexión
      - ACK como parte de una conexión ya establecida
    - Interfaz del router por el que llega el paquete

Control de Acceso – Cortafuegos

- Filtrado de paquetes
  - Dos acciones básicas
    - Descartar
    - Re-enviar

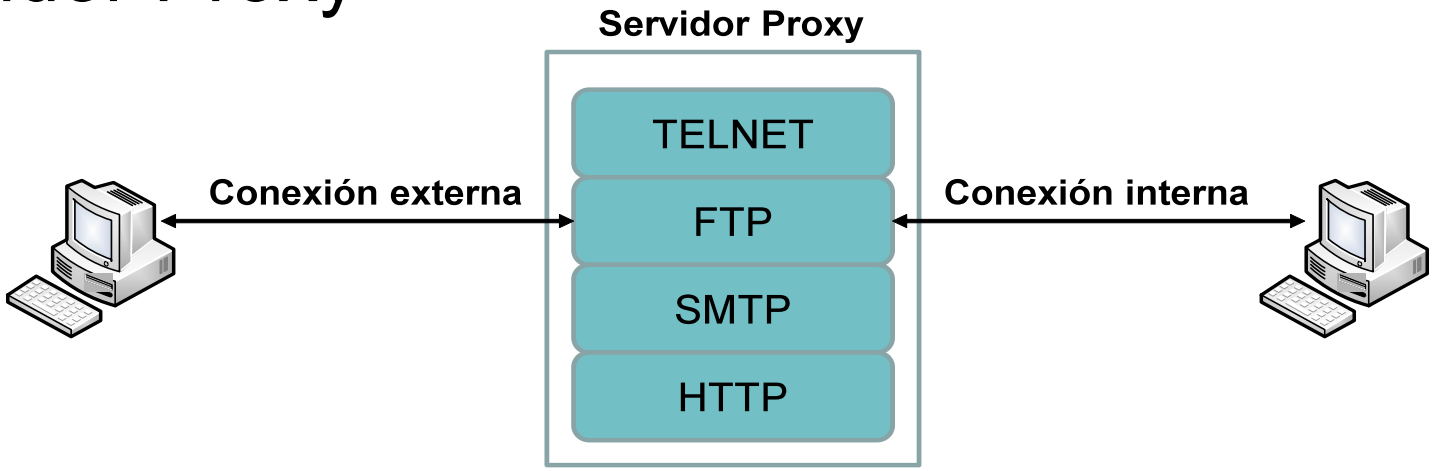
Política	Regla
No se puede acceder a la Web	Descartar cualquier paquete que salga cuyo puerto destino TCP sea 80
Sólo se puede acceder a una web en particular	Descartar cualquier paquete TCP SYN excepto aquellos con destino 1.2.3.4 puerto 80
Evita que se tu red se use para un ataque Smurf DoS	Descarta todos los paquetes ICMP con dirección destino de broadcast (ej. 1.2.255.255)
No permitas que hagan traceroute a la red privada	Descarta todos los paquetes ICMP

Control de Acceso – Cortafuegos

- Filtrado de paquetes
  - Ventajas
    - Simplicidad
    - Transparencia
    - Velocidad
  - Desventajas
    - Sin autenticación (no hay posibilidad de usuarios)
    - Creación de las reglas

Control de Acceso – Cortafuegos

- Servidor Proxy



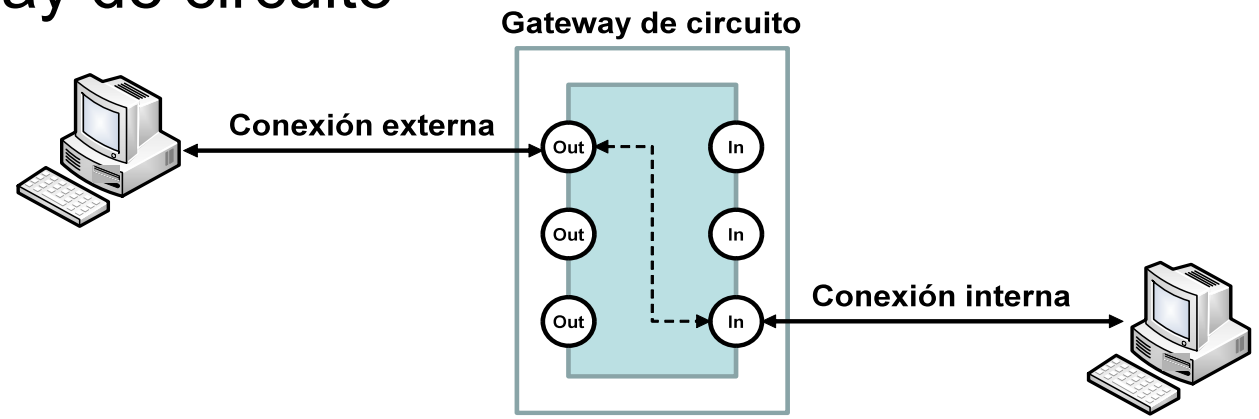
  - Todos los paquetes que entran en la red se dirigen al proxy
  - Todos los paquetes que salen de la red parece que salgan del proxy
  - Un proxy para cada protocolo de nivel de aplicación
    - Filtrado más fino es posible

Control de Acceso – Cortafuegos

- Servidor Proxy
  - Ventajas
    - Mayor seguridad que con el filtrado de paquetes
    - Sólo debe monitorizar una serie de servicios
    - Más fácil de auditar
  - Desventajas
    - Incrementa la sobrecarga de procesamiento

Control de Acceso – Cortafuegos

- Gateway de circuito



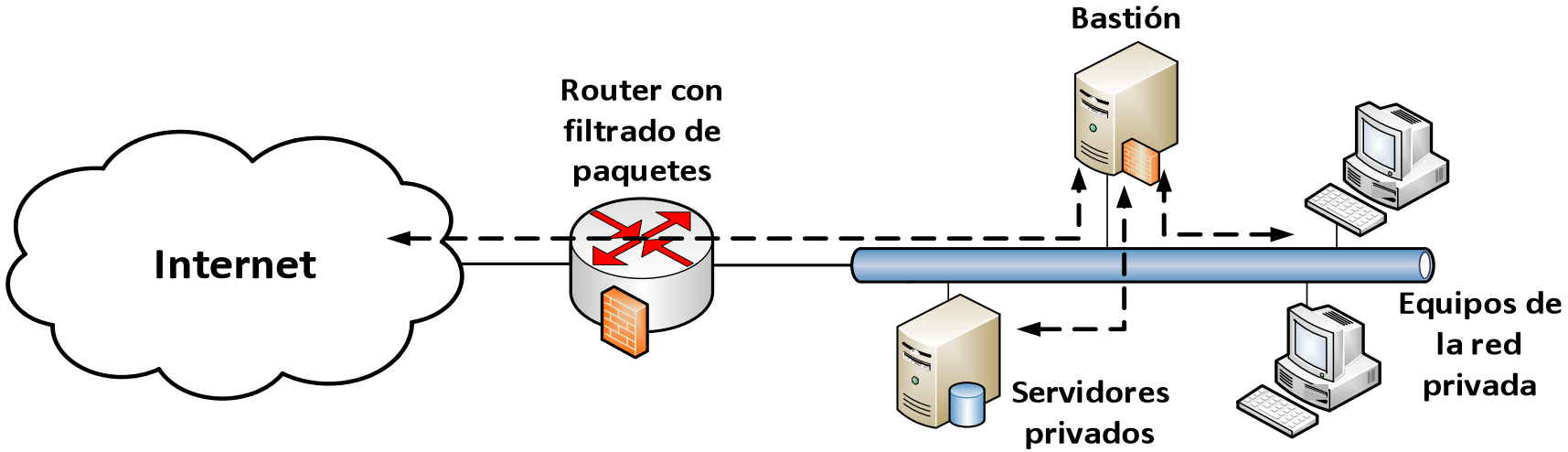
  - Sólo válido para TCP
  - El firewall crea dos conexiones y reenvía los segmentos de una a otra sin escrutinio
  - La seguridad viene dada por la capacidad de determinar que conexiones son permitidas
    - SSL
    - SSH
  - Uso típico actual SOCKS

Control de Acceso – Cortafuegos

- Configuraciones de cortafuegos
  - Bastión (Bastion Host)
    - Equipo que toma el rol de punto fuerte del sistema
    - Plataforma sobre la que se implementan los Servidores Proxy y los Gateway de Circuito
  - Tres configuraciones básicas
    - Bastión con un solo interfaz
    - Bastión con dos interfaces
    - Bastión fuera de la red privada
      - DMZ (DesMilitarized Zone)

Control de Acceso – Cortafuegos

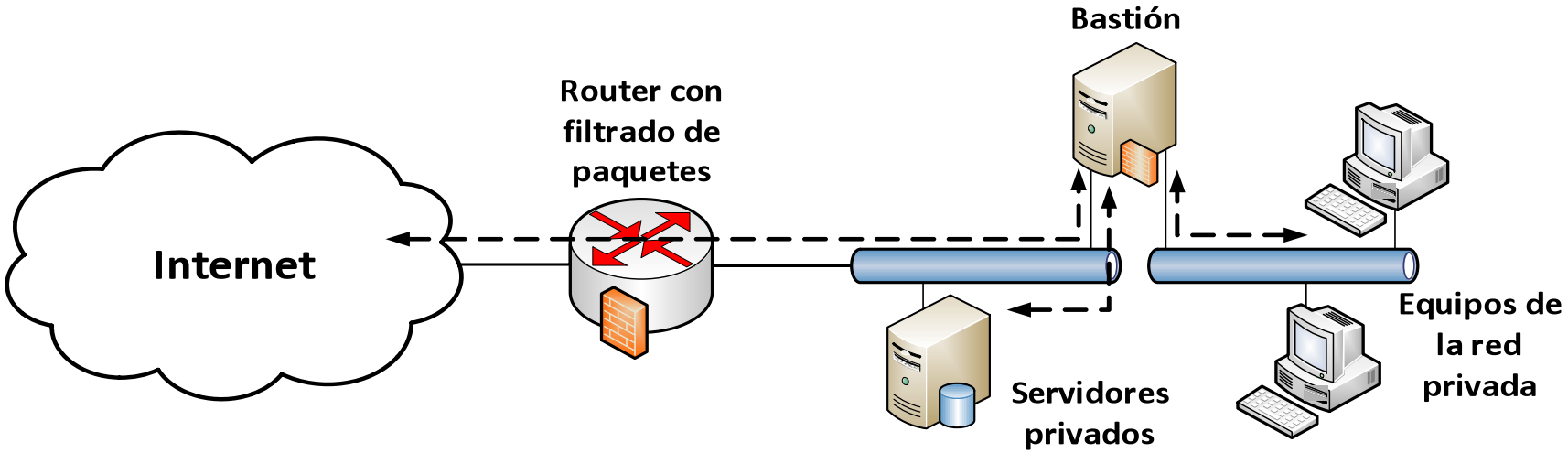
- Bastión con un solo interfaz



  - El cortafuegos consiste en dos equipos
  - El router sólo permite entrar o salir tráfico hacia o desde el Bastión
    - Se puede flexibilizar esta regla (pseudo-DMZ)
  - El Bastión hace de Proxy
  - Un intruso tendría que penetrar en dos sistemas diferentes

Control de Acceso – Cortafuegos

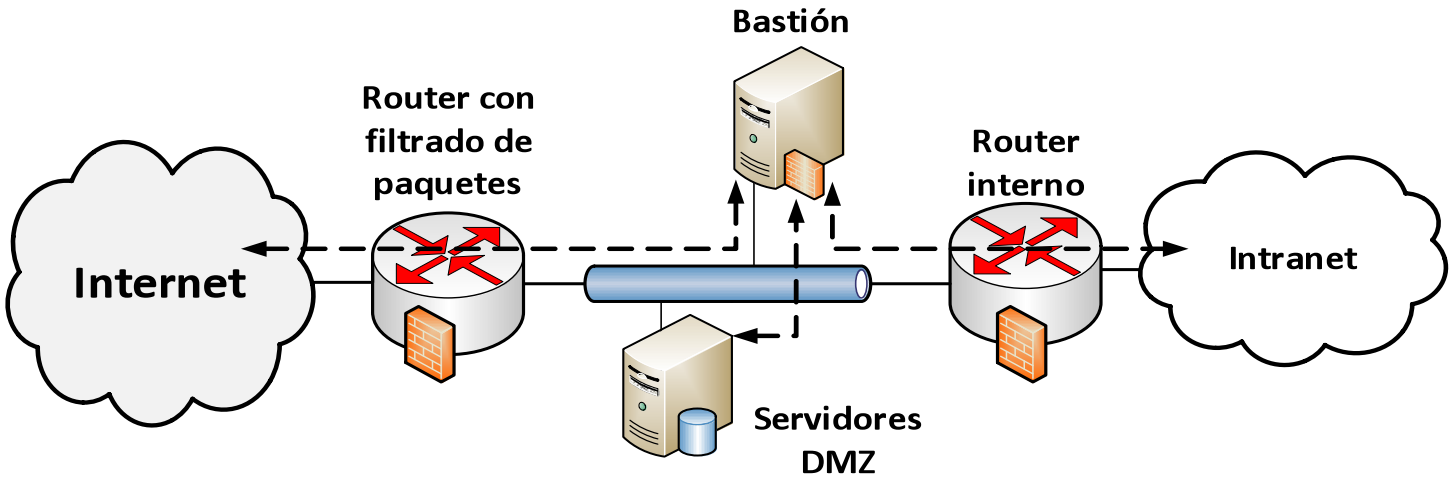
- Bastión con dos interfaces



  - El tráfico entre Internet y los equipos de la red privada pasa por el Bastión

Control de Acceso – Cortafuegos

- Bastión fuera de la red privada



  - Es la configuración más segura
    - Dos routers con posibilidad de filtrado de paquetes
    - Creación de una sub-red aislada: DMZ

Control de Acceso – Cortafuegos

- Bastión fuera de la red privada
  - Ventajas
    - Tres niveles de seguridad
    - El router externo sólo deja ver la DMZ
      - No hay acceso a la Intranet
    - El router interno sólo deja ver la DMZ
      - No hay acceso a Internet

Contenido

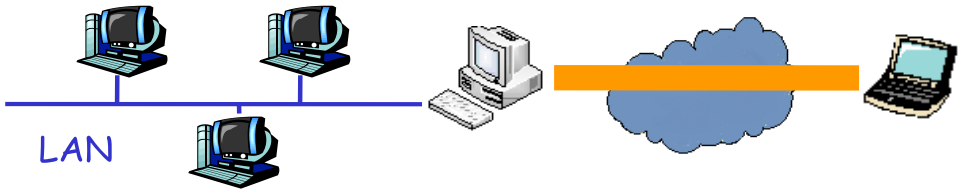
- Protocolos de Autenticación
  - EAP
  - RADIUS
  - IEEE 802.1x
- Seguridad en Internet
  - Nivel de Red – IPSec
  - Nivel de Transporte – SSL / TLS
  - Nivel de Aplicación
- Control de Acceso
  - Cortafuegos
  - VPNs
  - Sistemas IDS

Control de Acceso – VPNs

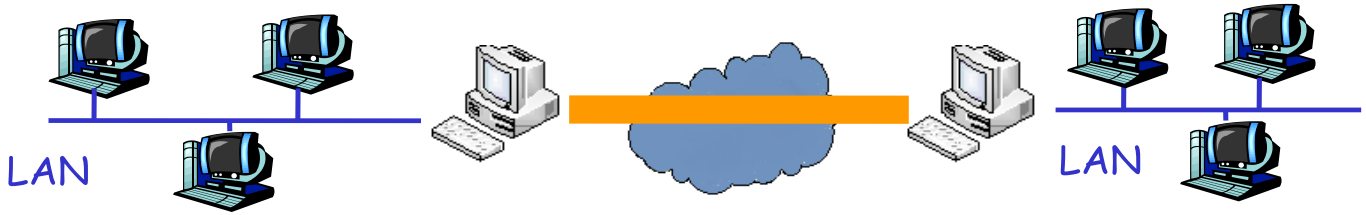
- Virtual Private Network (VPN)
  - Es la extensión de una red privada que incluye enlaces en redes públicas (Internet)
  - Tres clases de VPNs
    - Seguras
      - Se basan en el cifrado de la información
      - Uso de “túneles” a través de la red pública
    - Confiables
      - El proveedor de la red asegura el tráfico
    - Híbridas
      - Uso combinado de las anteriores
  - Requisitos
    - Autenticación y cifrado de la información
    - Gestión del direccionamiento privado
    - Manejo de las claves

Control de Acceso – VPNs

- Escenarios de uso de las VPN
  - Acceso remoto



  - Extensión de la red privada



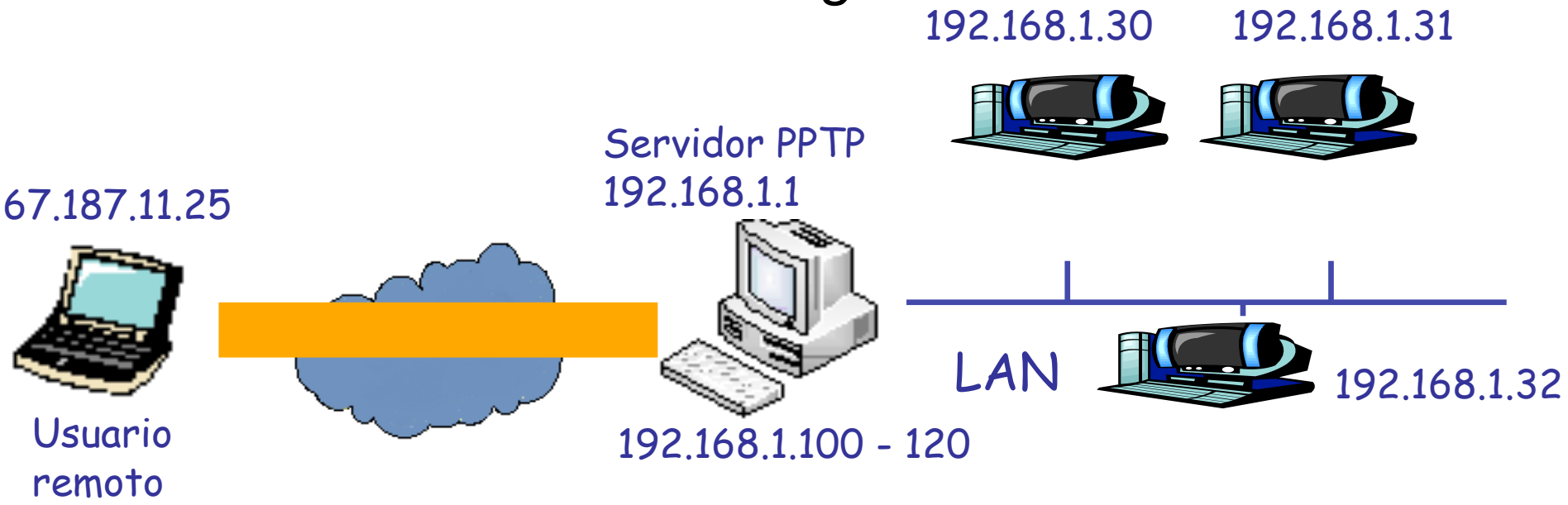
  - Cliente – Servidor (P2P)

Control de Acceso – VPNs

- Protocolos VPN
  - Point-to-Point Tunneling Protocol (PPTP)
    - Acceso remoto
  - Layer 2 Tunneling Protocol (L2TP)
    - Acceso remoto
  - IPSec
    - Acceso remoto
    - LAN-LAN
    - P2P
  - SSL
    - Acceso remoto

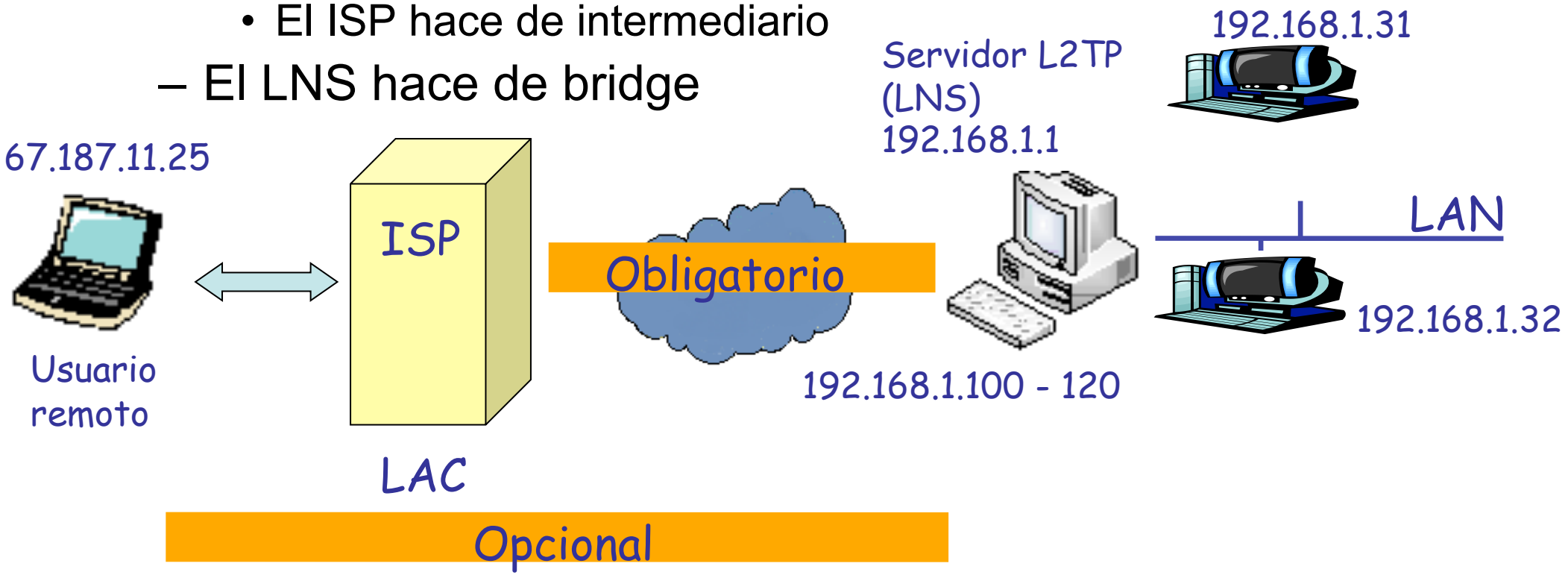
Control de Acceso – VPNs

- PPTP
  - Un servidor PPTP sirve direcciones privadas a los clientes que se conectan a él
  - El servidor actúa como bridge



Control de Acceso – VPNs

- L2TP
  - Usado normalmente junto con IPSec
  - Enlace PPP con el ISP
    - El ISP hace de intermediario
  - El LNS hace de bridge

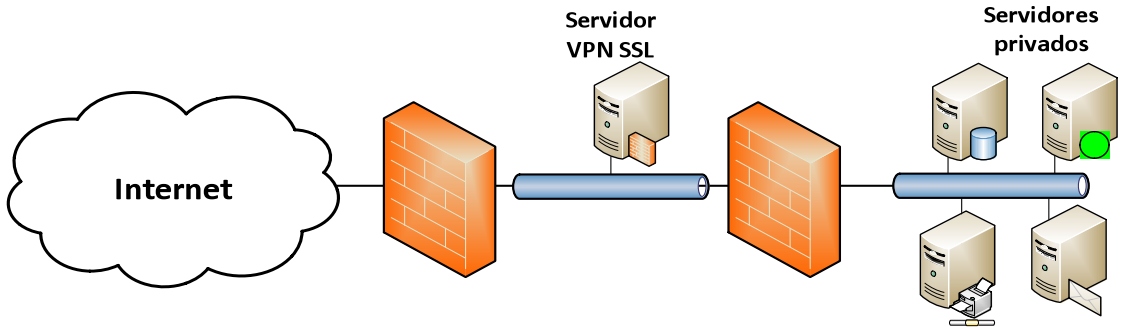


Control de Acceso – VPNs

- IPSec
  - Modo transporte
    - P2P
  - Modo túnel
    - Acceso remoto
    - LAN-LAN
  - Utilizando habitualmente ESP en modo túnel
  - Tiene problemas con los NAT y con los Firewall

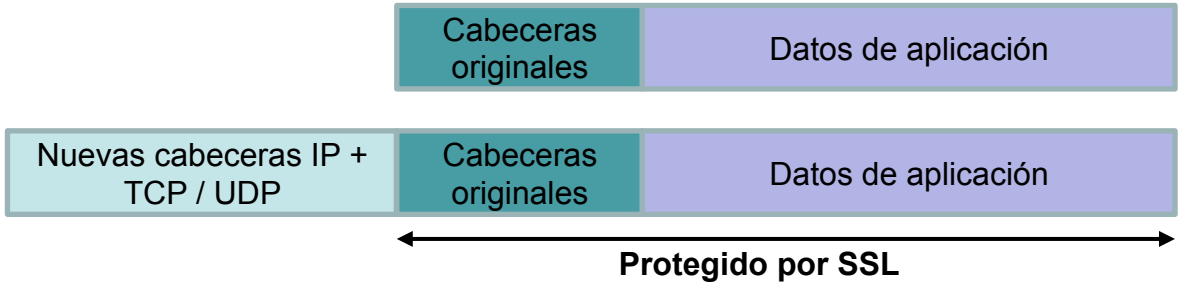
Control de Acceso – VPNs

- SSL
  - Acceso por aplicación no a una red
  - El servidor VPN SSL actúa como proxy
    - Acceso web al servidor VPN SSL
  - Dos modos de acceso
    - Portal VPN SSL
      - Acceso vía servicios web
    - Túnel VPN SSL
      - Generación de un interfaz de red virtual en el cliente



Control de Acceso – VPNs

- SSL



  - OpenVPN
    - Cliente y servidor VPN SSL
    - Multiplataforma
    - Soporta TCP y UDP
    - Cliente
      - Genera el interfaz de red virtual
      - Encapsula / des-encapsula el tráfico
    - Servidor
      - Maneja autenticación y establecimiento de sesión SSL