Seguridad de la Información

TEMA 5 – PARTE B

Seguridad en Redes TCP/IP

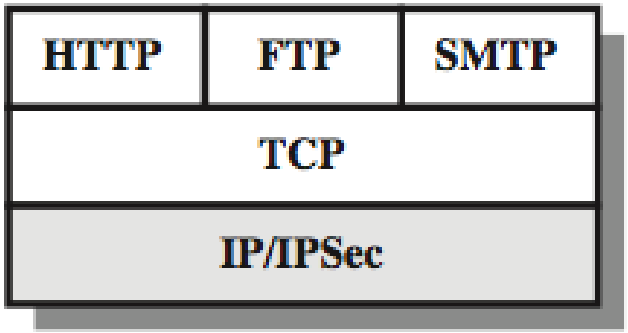
SEGURIDAD EN LA CAPA DE INTERNET

- En 1994, la *Internet Architecture Board (IAB)* publicó un informe titulado “Security in the Internet Architecture” (RFC1636)
  - En este informe se identificaba la necesidad de proporcionar seguridad a la **infraestructura de red**
    - aconsejando la incorporación de mecanismos de
      - cifrado y
      - autenticación

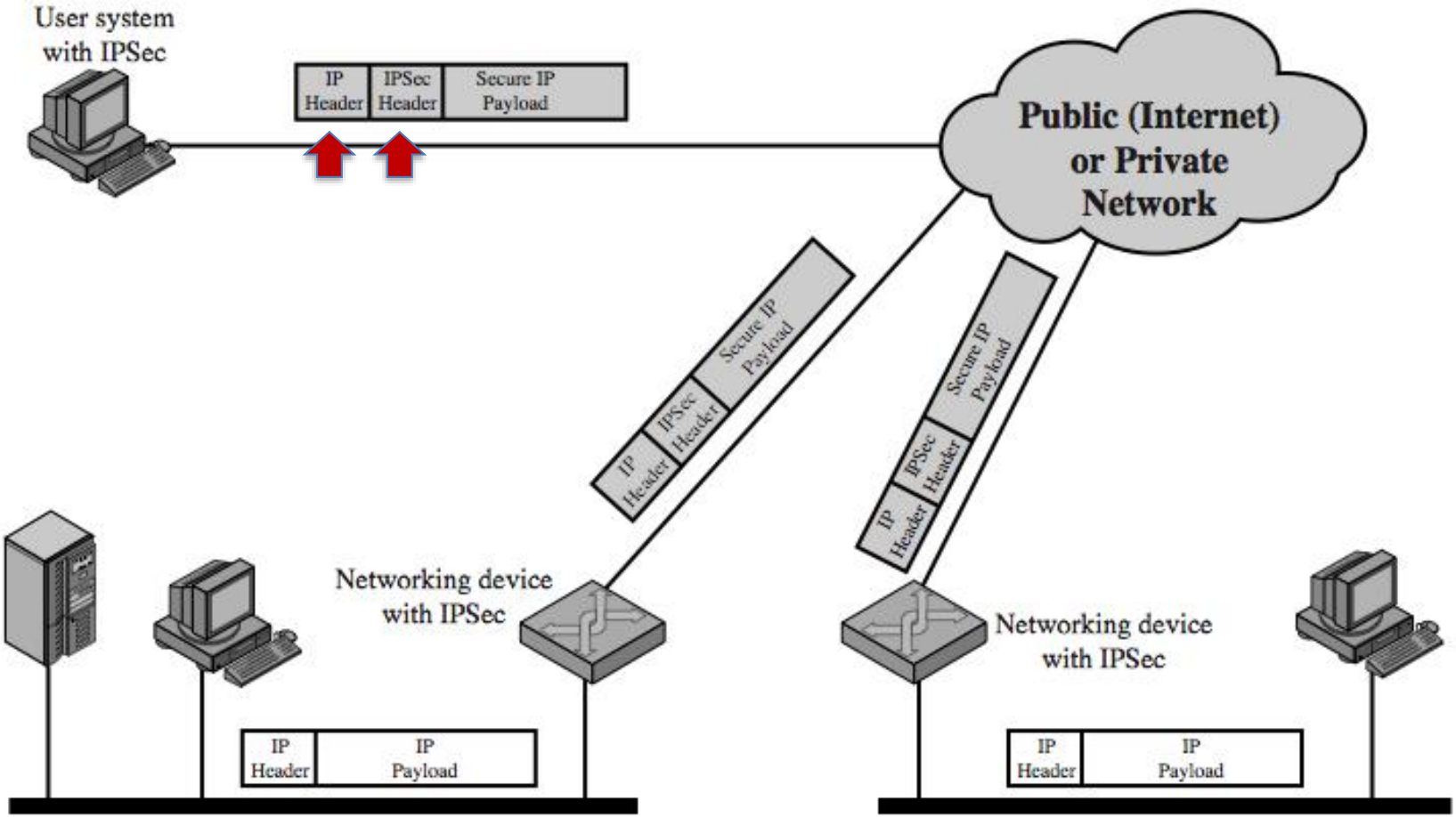
      para la siguiente versión de IP (IPv6)

- A partir de ese momento se elaboraron, bajo el nombre IPSec (RFC 4301), las especificaciones y las funcionalidades de seguridad en la capa de Internet para el modelo TCP/IP
  - no sólo teniendo en cuenta IPv6, sino también para que sirviera para la propia IPv4

- Implementando la seguridad al nivel de IP, una empresa garantiza la protección de **todas sus aplicaciones**, necesiten éstas seguridad o no



- Por ello, se puede usar en muy distintos escenarios:
  - Conectividad segura entre sucursales a través de internet
  - Acceso remoto seguro sobre Internet
  - Establecimiento de conectividad extranet e intranet con socios
  - Aplicaciones de comercio electrónico
  - etc.

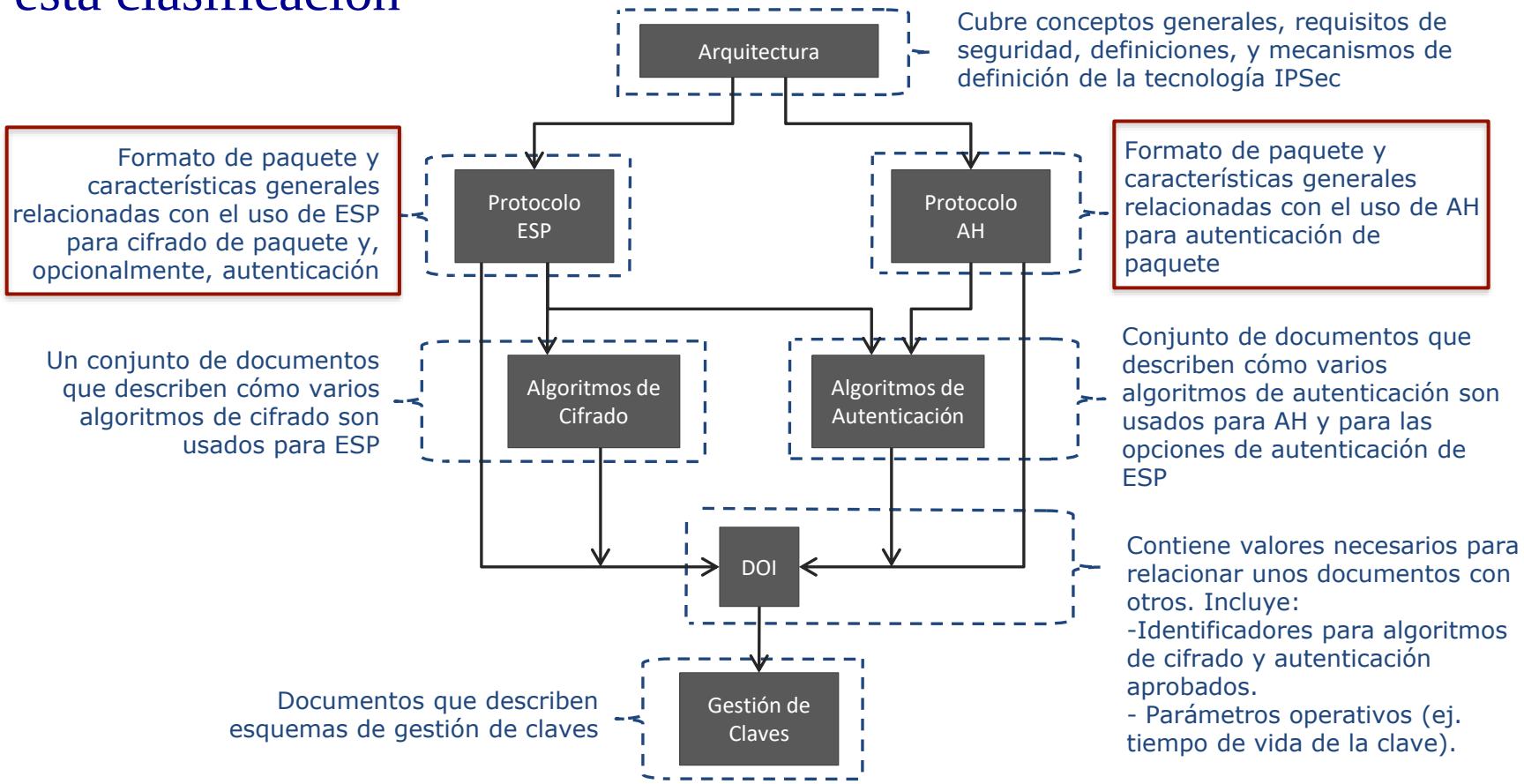

User system
with IPSec
IP
Header
IPSec
Header
Secure IP
Payload
Public (Internet)
or Private
Network
Secure IP
Payload
IPSec
Header
IP
Header
Secure IP
Payload
IPSec
Header
IP
Header
Networking device
with IPSec
Networking device
with IPSec
IP
Header
IP
Payload
IP
Header
IP
Payload

- La seguridad en IPSec se centra en:
  - Autenticación + integridad (MAC),
  - Confidencialidad
  - intercambio de claves entre los puntos que se comunican
- Al funcionar por debajo del nivel de transporte, es transparente a las aplicaciones
  - Por lo tanto, es transparente a los usuarios finales:
    - no es encesario entrenar a los usuarios en el uso de mecanismos de seguridad
    - no hace falta que gestionen claves
- IPSec no proporciona:
  - servicios de no-repudio, como SSL/TLS
  - protección frente a ataques DoS, aunque proporciona una forma de protección ante ataques de repetición

- Para la comunicación segura entre dos puntos, IPSec utiliza los siguientes protocolos:
  - **ESP (Encapsulating Security Payload)**
    - Cabecera para confidencialidad, integridad y autenticación del origen de datos
    - También incluye un número de secuencia que proporciona una forma de protección ante ataques de repetición
    - Además, proporciona una protección parcial ante análisis de tráfico (**sólo en modo túnel)**
  - **AH (Authentication Header)**
    - Cabecera para integridad y autenticación del origen de datos
    - También incluye un número de secuencia que proporciona una forma de protección ante ataques de repetición (mismo motivo que ESP)
  - **IKE (Internet Key Exchange)**
    - Protocolo para generar y distribuir claves criptográficas para ESP y AH
    - También autentica la identidad del sistema remoto

- Antes de que dos puntos se comuniquen de forma segura, tienen que acordar qué parámetros de seguridad se van a aplicar

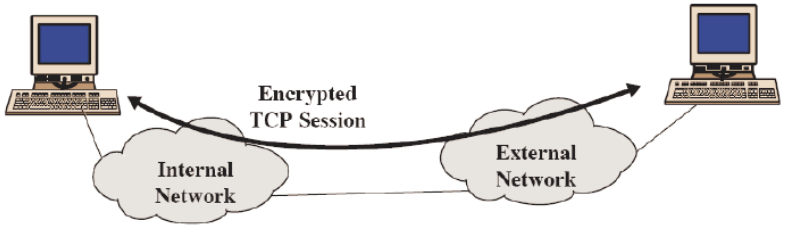
- De hecho, los documentos de IETF al respecto de IPSec siguen esta clasificación



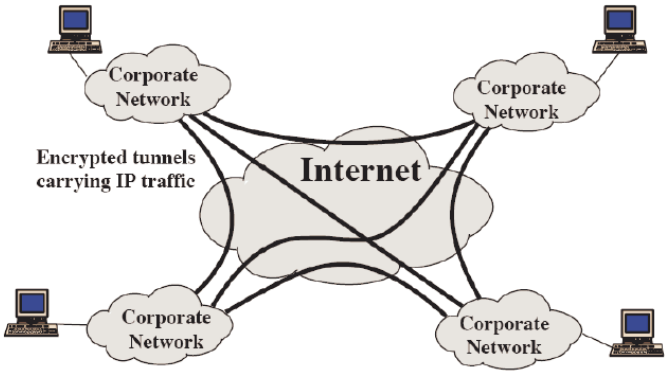
DOI: Domain of Interpretation

Modos de IPSec

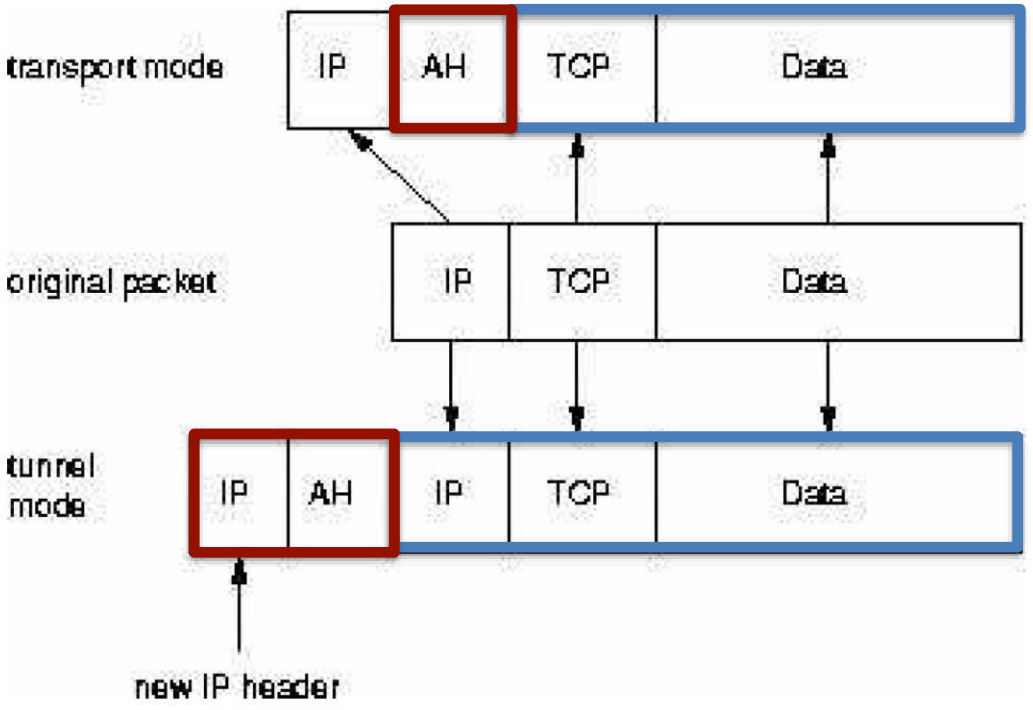
- Modo transporte:
  - Se usa normalmente para comunicaciones punto a punto entre dos hosts
  - Proporciona protección a la carga útil del paquete IP (IP **payload**)
    - es decir, a los protocolos de la capa superior - TCP, UDP, ICMP



- Modo túnel:
  - Se suele usar cuando los puntos a comunicar son gateways de seguridad o bien routers
  - Proporciona **protección a todo el paquete IP**



- Es decir, el modo túnel encapsula el datagrama IP dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En cambio, el modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores



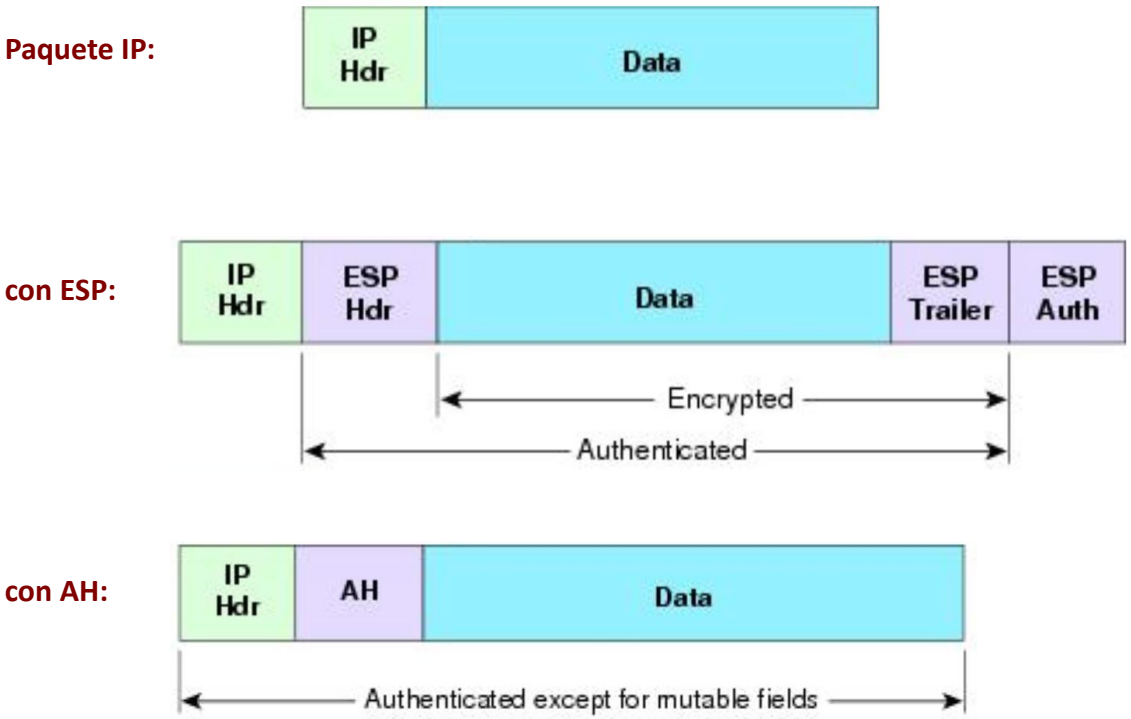
- Como puede verse en la figura anterior, la protección a todo el paquete IP del modo túnel se puede lograr:

    i. añadiendo las cabecera AH o ESP al paquete IP original
    ii. creando una cabecera IP nueva

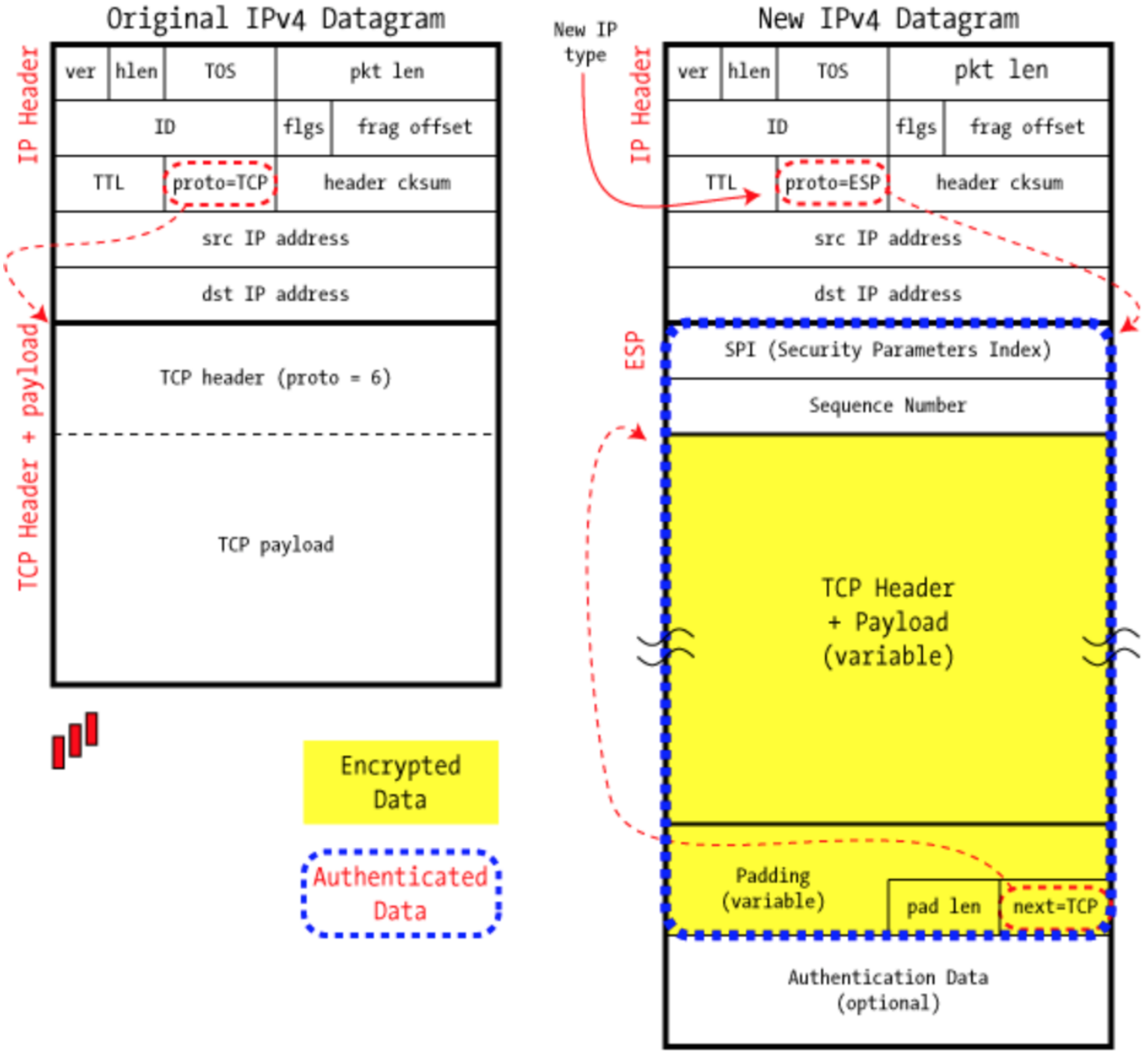
  – De esta forma el paquete IP original (paquete interno) se "**encapsula**" y viaja por el túnel sin que ninguno de los routers intermedios pueda saber **ni el origen ni el destino final de los datos**

Modo transporte

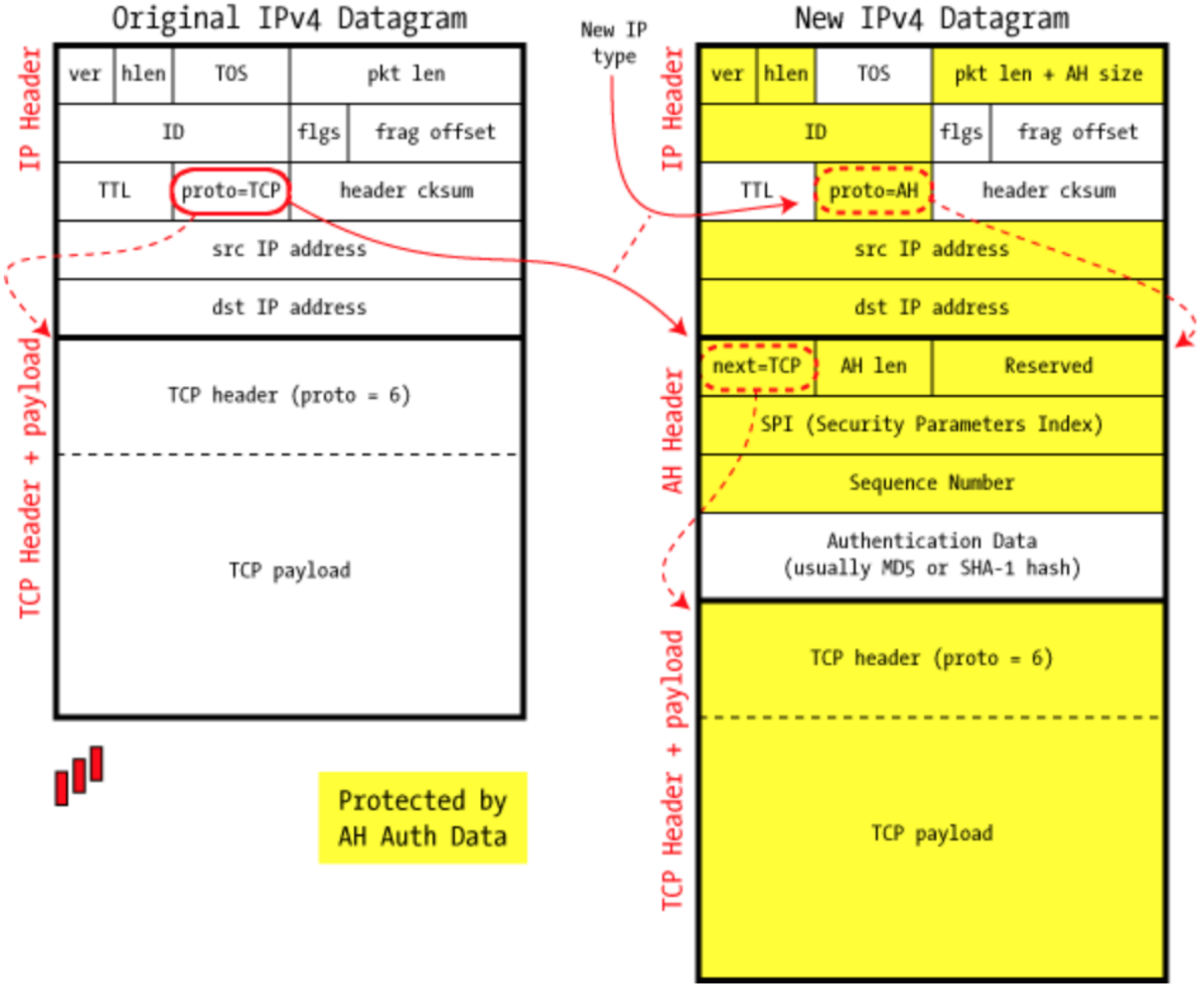
- En este modo de uso:
  - si se utiliza ESP: se cifra y opcionalmente autentica el payload, pero no la cabecera
  - si se utiliza AH: se autentica el payload y algunas porciones de la cabecera



IPSec in ESP Transport Mode



IPSec in AH Transport Mode



- La siguiente tabla muestra algunos de los códigos de protocolos de Internet, asignados por IANA (Internet Assigned Numbers Authority)

Some IP protocol codes

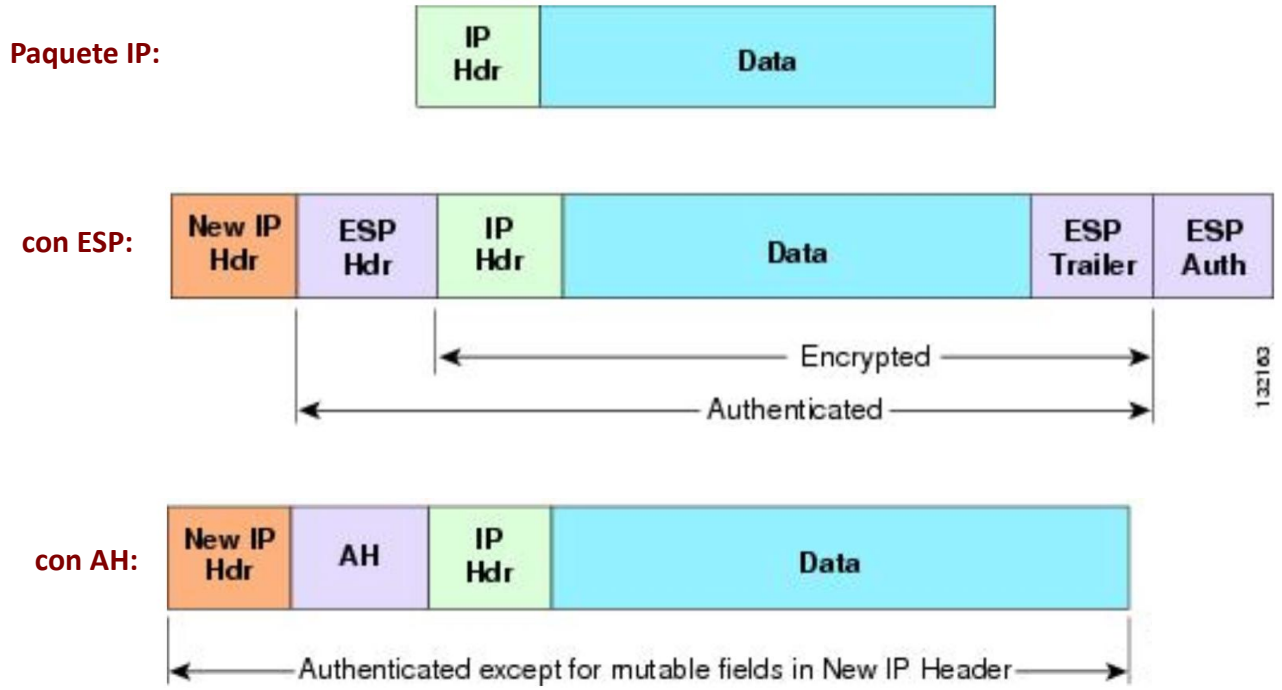
Protocol code	Protocol Description
1	ICMP — Internet Control Message Protocol
2	IGMP — Internet Group Management Protocol
4	IP within IP (a kind of encapsulation)
6	TCP — Transmission Control Protocol
17	UDP — User Datagram Protocol
41	IPv6 — next-generation TCP/IP
47	GRE — Generic Router Encapsulation (used by PPTP)
50	IPsec: ESP — Encapsulating Security Payload
51	IPsec: AH — Authentication Header

- Lista completa en:

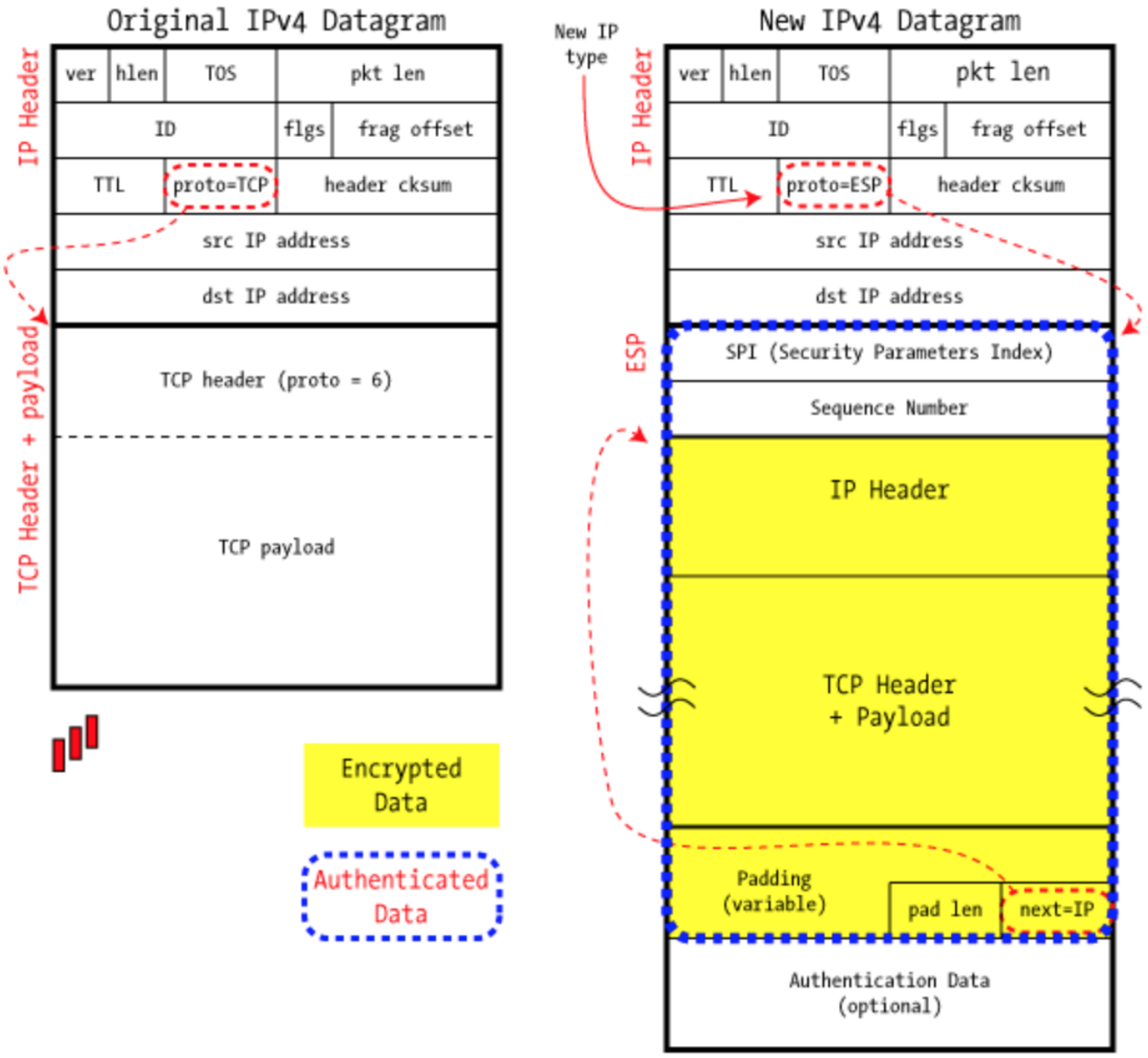
  http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Modo túnel

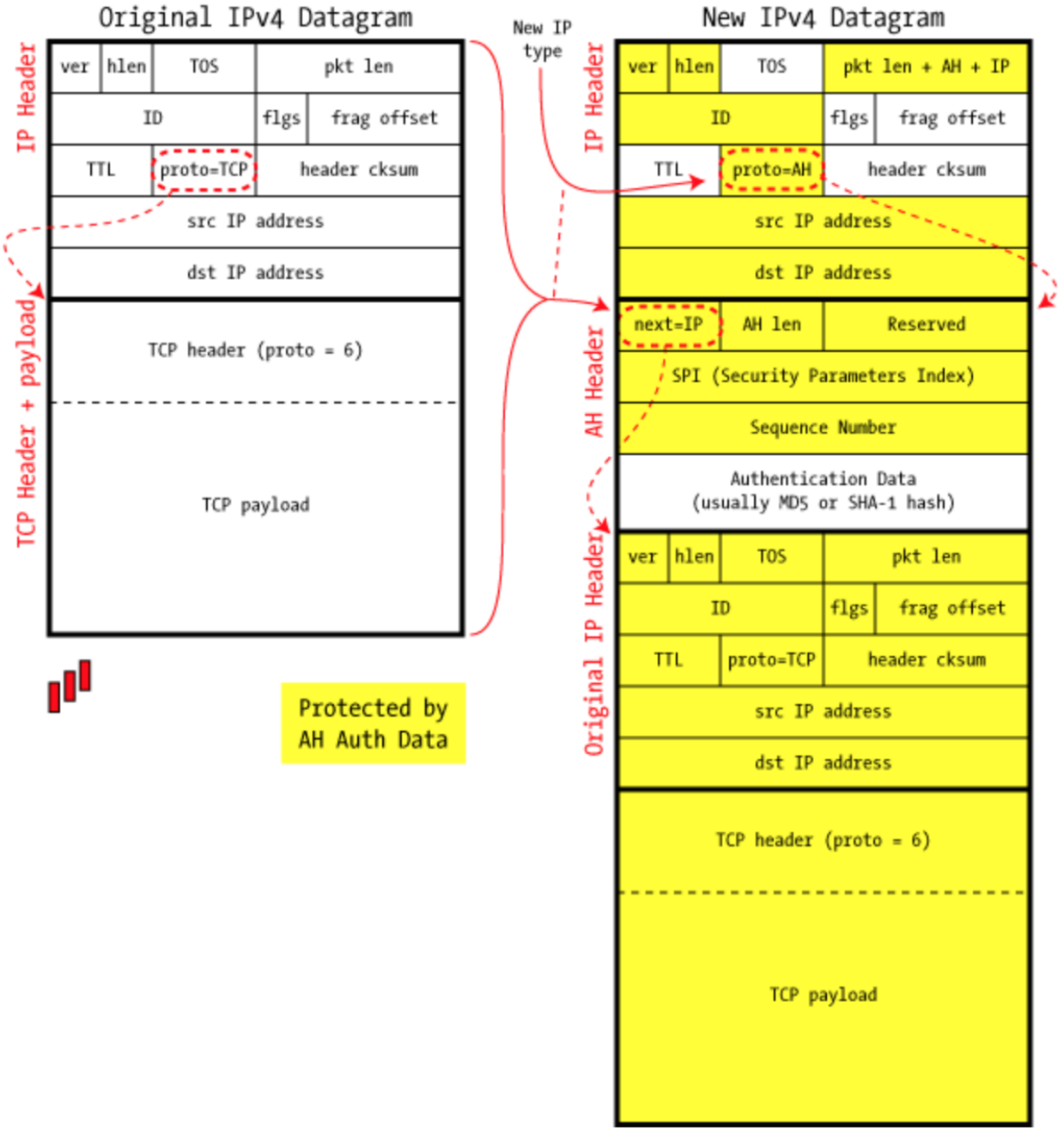
- En este modo de uso:
  - si se usa ESP: se cifra y opcionalmente autentica todo el paquete IP original (paquete interno), incluyendo la cabecera de ese paquete original
  - si se usa AH: se autentica todo el paquete original y algunas partes de la cabecera externa



IPSec in ESP Tunnel Mode



IPSec in AH Tunnel Mode



- Con IPSec se tiene que:
  - Asegurar la integridad de los mensajes por incluir en la cabecera del protocolo IPSec, el HMAC basados en MD5 o SHA
  - Permitir el uso general de algoritmos de cifrados estándar, como DES, 3DES, AES y Blowfish
  - Controlar un tipo de ataque de DoS basado en replay por aplicar un número de secuencia única de paquetes (sólo se aceptan paquetes que tienen un número actual de secuencia o posterior, las anteriores se descartan)
  - Encapsular y desencapsular paquetes IPSec. Para ello, se requiere el uso de algún mecanismo que almacene las claves secretas, los algoritmos de cifrado y autenticación, y las direcciones IP involucradas en la comunicación

Asociaciones de seguridad (SA – Security Associations)

- Por tanto, cada SA define:
  - La dirección IP
    - origen
    - destino
  - Determina el protocolo IPsec (AH o ESP)
    - A veces, se permite compresión de paquetes
  - El algoritmo y la clave secreta empleados por el protocolo IPsec
  - El índice de parámetro de seguridad (**SPI - Security Parameter Index**)
    - Es un número de 32 bits que identifica la asociación de seguridad
  - Sólo se protege un sentido
    - El emisor y el receptor deben aplicar la misma SA pero teniendo en cuenta el destino y el origen

No.	Time	Source	Destination	Protocol	Length	Info
134	215.661944	190.0.0.1	190.0.0.14	ESP	134	ESP (SPI=0x00000070)
135	216.661895	190.0.0.1	190.0.0.14	ESP	134	ESP (SPI=0x00000070)
136	217.663971	190.0.0.1	190.0.0.14	ESP	134	ESP (SPI=0x00000070)
137	218.681817	190.0.0.1	190.0.0.14	ESP	134	ESP (SPI=0x00000070)
138	219.681772	190.0.0.1	190.0.0.14	ESP	134	ESP (SPI=0x00000070)
139	220.681692	190.0.0.1	190.0.0.14	ESP	134	ESP (SPI=0x00000070)
140	230.684156	190.0.0.1	190.0.0.15	ESP	122	ESP (SPI=0x00000071)
141	231.683968	190.0.0.1	190.0.0.15	ESP	122	ESP (SPI=0x00000071)
142	232.683915	190.0.0.1	190.0.0.15	ESP	122	ESP (SPI=0x00000071)
143	233.683761	190.0.0.1	190.0.0.15	ESP	122	ESP (SPI=0x00000071)

```
▶ Frame 143: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
▶ Ethernet II, Src: Dell_4a:d7:0a (00:11:43:4a:d7:0a), Dst: 00:00:00_00:00:15 (00:00:00:00:00:15)
▼ Internet Protocol Version 4, Src: 190.0.0.1, Dst: 190.0.0.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 108
    Identification: 0x0003 (3)
  ▶ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: Encap Security Payload (50)
  ▶ Header checksum: 0xbe4c [validation disabled]
    Source: 190.0.0.1
    Destination: 190.0.0.15
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Encapsulating Security Payload
    ESP SPI: 0x00000071 (113)
    ESP Sequence: 6
```

```
0000  00 00 00 00 00 15 00 11  43 4a d7 0a 08 00 45 00   ........ CJ....E.
0010  00 6c 00 03 40 00 40 32  be 4c be 00 00 01 be 00   .l..@.@2 .L......
0020  00 0f 00 00 00 71 00 00  00 06 08 00 0a 18 7e 64   .....q.. ......~d
0030  00 04 3b a9 f9 43 44 8f  0b 00 08 09 0a 0b 0c 0d   ..;..CD. ........
0040  0e 0f 10 11 12 13 14 15  16 17 18 19 1a 1b 1c 1d   ........ ........
0050  1e 1f 20 21 22 23 24 25  26 27 28 29 2a 2b 2c 2d   .. !"#$% &'()*+,-
0060  2e 2f 30 31 32 33 34 35  36 37 01 02 02 01 ab f8   ./012345 67......
0070  af 87 f4 4f 29 67 2f c4  6c c8                     ...O)g/. l.
```

https://wiki.wireshark.org

- Las SAs se almacenan en una **base de datos de asociaciones de seguridad** (**SAD**). Para cada entrada en la SAD existen varios campos. Entre ellos:
  - *Security Parameter Index (SPI)*: Es un valor de 32 bits para identificar a una SA particular
  - *AH Information*: algoritmo de autenticación, claves y otros parámetros relacionados con AH
  - *ESP Information*: algoritmo de cifrado y autenticación, claves y otros parámetros relacionados con ESP
  - *Lifetime of the SA*: un intervalo o un contador después del cual habrá que reemplazar la SA

- Algunas SAD también definen:
  - El tipo de modo (túnel o transporte)

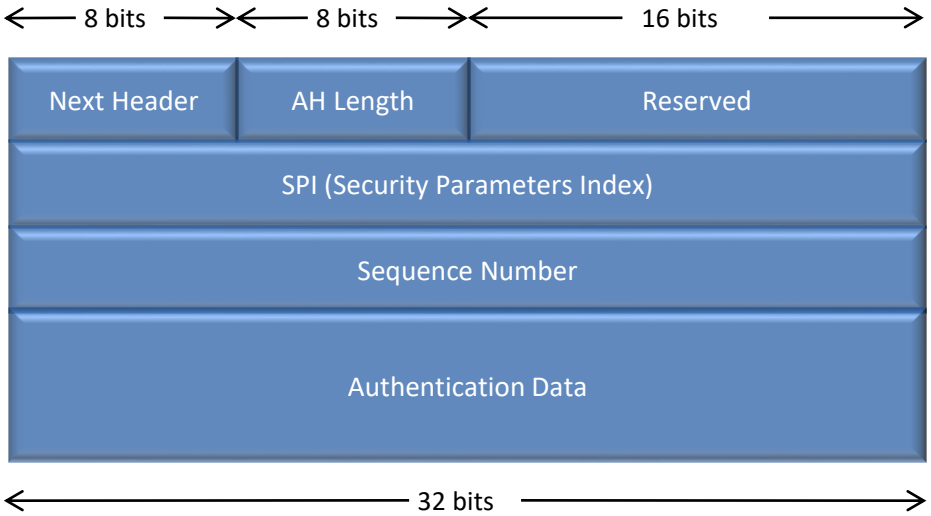
- Sin embargo, **SA sólo especifica "el modo en el que se protegerá el dato IPSec". Para definir "el modo en cómo va a viajar el tráfico entre dos puntos", se requiere de una política de seguridad (SP – Security Policy)** que se almacena en una SPD (Security Policy Database)
- Un SP define:
  - Las direcciones de origen y destino a proteger
    - En modo transporte, éstas serán las mismas direcciones que aquellas definidas en la SA
    - En modo túnel no tienen que ser las mismas
  - Los protocolos y puertos a proteger
    - Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico
  - El modo de protección: túnel o transporte

- Un ejemplo de SPD es el siguiente:

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Cabeceras AH y ESP

- Authentication Header - AH



Next Header (8 bits): Identifica el tipo de cabecera inmediatamente posterior a esta cabecera

AH Length (8 bits): Longitud de la Cabecera de Autenticación en palabras de 32 bits, menos 2 palabras

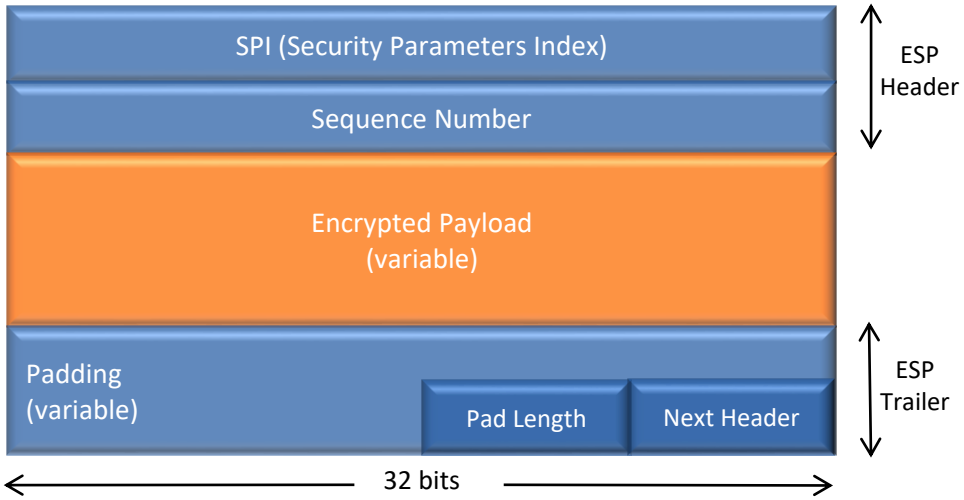
Reserved (16 bits): Para uso futuro

SPI (Security Parameters Index) **(32 bits): Identifica una "asociación de seguridad"**

Sequence Number **(32 bits): contador para evitar ataques de repetición**

Authentication Data (variable): Campo de longitud variable (debe ser un número de palabras de 32 bits) que contiene el valor de comprobación de integridad (valor MAC) para este paquete

• Encapsulating Security Payload – ESP (sólo cifrado)



SPI (Security Parameters Index) (32 bits): Identifica una "asociación de seguridad"

Sequence Number (32 bits): contador para evitar ataques de repetición

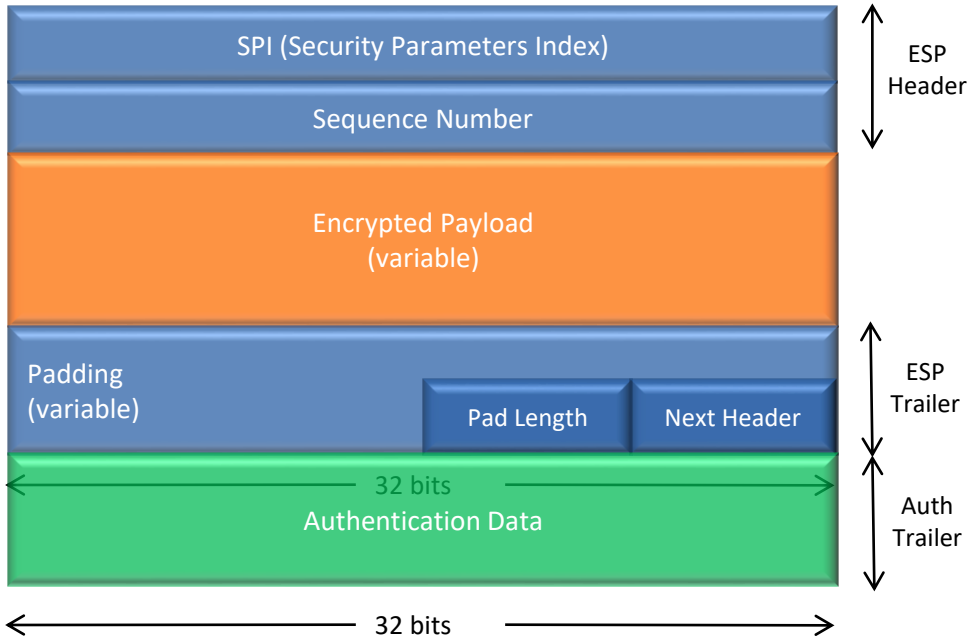
Encrypted Payload (32 bits): Segmento de nivel de transporte (modo transporte) o paquete IP (modo túnel) protegido por medio de cifrado

Padding (0-255 bytes): Espacio adicional incluido porque los algoritmos de encriptación basados en bloque pueden requerir espacios diferentes

Pad Length (8 bits): longitud del "Padding"

Next Header (8 bits): guarda el tipo de la siguiente cabecera (IP, TCP, UDP, etc.)

- Encapsulating Security Payload – ESP (cifrado + autenticación de dato+integridad):



- Las distintas opciones de qué cabeceras usar y qué servicios queramos proporcionar:

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

Ejemplo: modo transporte

- setkey es el comando para establecer la comunicación segura. Concretamente, lee las órdenes asociadas al SA o SAD de un fichero cuando se invoca con:
  - # setkey –f /etc/ipsec.conf (el fichero)
- Se comprueba la viabilidad de la acción setkey por lanzar:
  - # setkey -D
  - # setkey -DP

http://www.ipsec-howto.org/spanish/ipsec-howto.pdf

```
#!/usr/sbin/setkey -f

# Configuración for 192.168.1.100

# Vaciar las SAD y SPD
flush;
spdflush;

# Atención: Emplee estas claves sólo para pruebas
# ¡Debería generar sus propias claves!

# SAs para AH empleando claves largas de 128 bits
add 192.168.1.100 192.168.2.100 ah 0x200 -A hmac-md5 \
0xc0291ff014dccdd03874d9e8e4cdf3e6;
add 192.168.2.100 192.168.1.100 ah 0x300 -A hmac-md5 \
0x96358c90783bbfa3d7b196ceabe0536b;

# SAs para ESP empleando claves largas de 192 bits (168 + 24 paridad)
add 192.168.1.100 192.168.2.100 esp 0x201 -E 3des-cbc \
0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;
add 192.168.2.100 192.168.1.100 esp 0x301 -E 3des-cbc \
0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;

# Políticas de seguridad
spdadd 192.168.1.100 192.168.2.100 any -P out ipsec
           esp/transport//require
           ah/transport//require;

spdadd 192.168.2.100 192.168.1.100 any -P in ipsec
           esp/transport//require
           ah/transport//require;
```

SPI

Se limpia el sistema de SAs y SPs antiguas (el SAD y SPD)

AH

SAs: AH y la clave (en ASCII, “”, hexadecimal) para el HMAC

- -A: alg. de autenticación
- -E: alg. de cifrado
- -C: alg. de comprensión

ESP

SAs: ESP y la clave para el cifrado

SPDs: para ambos lados

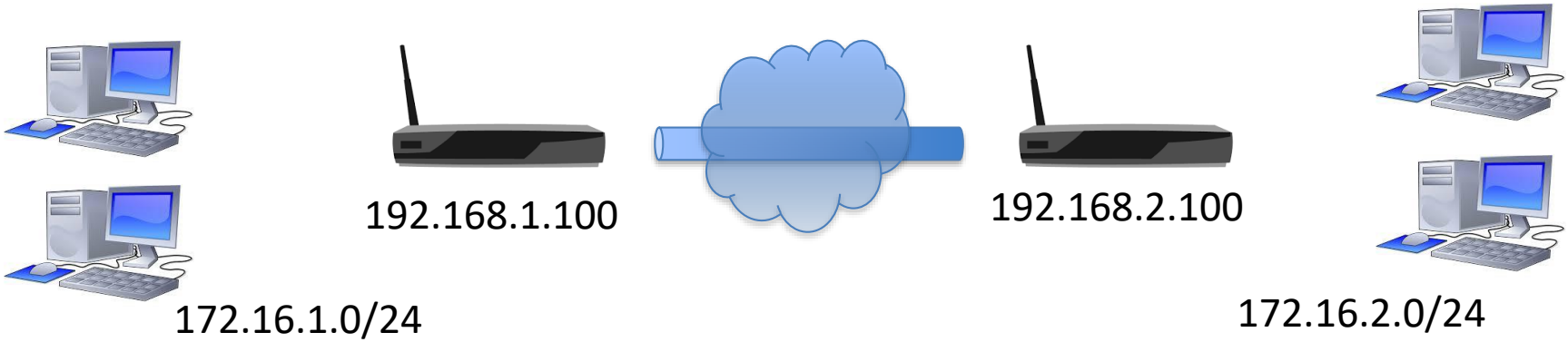
Protocolo y puerto

Dirección de la acción de la política

```
#!/usr/sbin/setkey -f

# Configuración para 192.168.2.100

# Vaciar las SAD y SPD
flush;
spdflush;

# Atención: Emplee estas claves sólo para pruebas
# ¡Debería generar sus propias claves!

# SAs para AH empleando claves largas de 128 bits
add 192.168.1.100 192.168.2.100 ah 0x200 -A hmac-md5 \
0xc0291ff014dccdd03874d9e8e4cdf3e6;
```

```
add 192.168.2.100 192.168.1.100 ah 0x300 -A hmac-md5 \
0x96358c90783bbfa3d7b196ceabe0536b;

# SAs para ESP empleando claves largas de 192 bits (168 + 24 paridad)
add 192.168.1.100 192.168.2.100 esp 0x201 -E 3des-cbc \
0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;
add 192.168.2.100 192.168.1.100 esp 0x301 -E 3des-cbc \
0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;

# Políticas de seguridad
spdadd 192.168.1.100 192.168.2.100 any -P in ipsec
          esp/transport//require
          ah/transport//require;

spdadd 192.168.2.100 192.168.1.100 any -P out ipsec
          esp/transport//require
          ah/transport//require;
```

Ejemplo: modo túnel



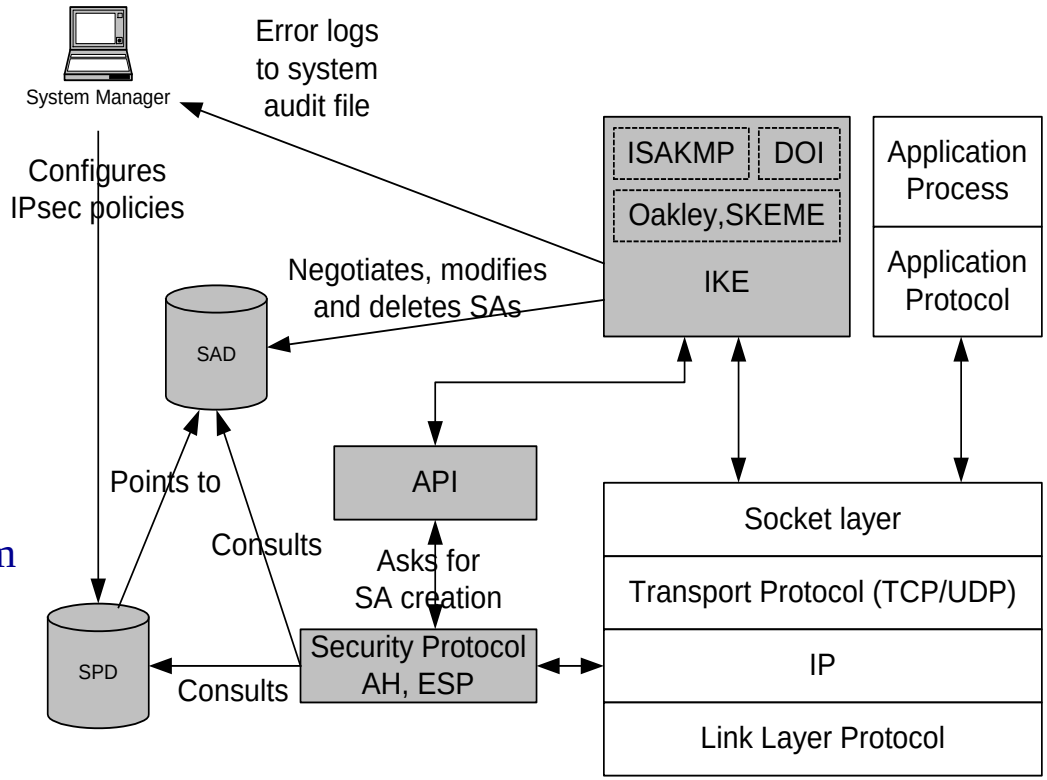

```
#!/usr/sbin/setkey -f

# Vaciar las SAD y SPD
flush;
spdflush;

# SAs para ESP realizando cifrado con claves largas de 192 bit (168 + 24 paridad)
# y autenticación empleando claves largas de 128 bits
add 192.168.1.100 192.168.2.100 esp 0x201 -m tunnel -E 3des-cbc \
0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831 \
-A hmac-md5 0xc0291ff014dccdd03874d9e8e4cdf3e6;

add 192.168.2.100 192.168.1.100 esp 0x301 -m tunnel -E 3des-cbc \
0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df \
-A hmac-md5 0x96358c90783bbfa3d7b196ceabe0536b;

# Políticas de seguridad
spdadd 172.16.1.0/24 172.16.2.0/24 any -P out ipsec
          esp/tunnel/192.168.1.100-192.168.2.100/require;

spdadd 172.16.2.0/24 172.16.1.0/24 any -P in ipsec
          esp/tunnel/192.168.2.100-192.168.1.100/require;
```

IKE

- Como se puede observar en la figura anterior, cuando no existe la SA, hay que negociarla. De eso se encarga el protocolo IKE - Internet Key Exchange
- IKE se encarga de la:
  - autenticación de las partes de la comunicación y
  - el establecimiento de la clave secreta
- IKE utiliza:
  - certificados X.509 para la autenticación, y
  - el algortimo de Diffie-Hellman para establecer la clave secreta
- IKE se basa a su vez en los protocolos:
  - Oakley
  - ISAKMP (Internet Security Association and Key Management Protocol)

Estructura interna de la suite IPSEC:

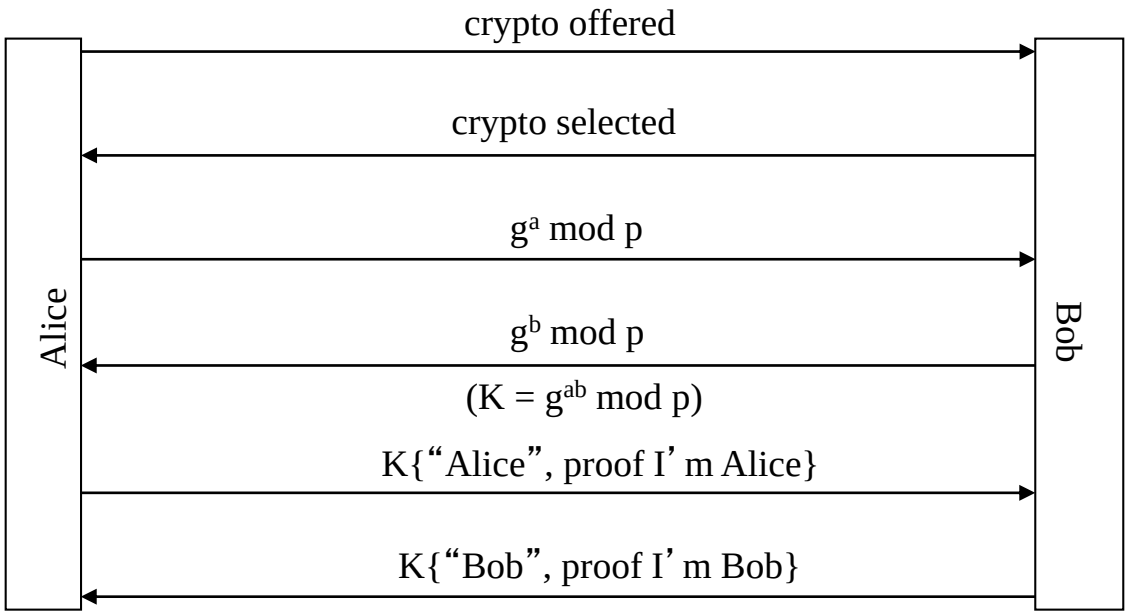
AH = Authentication Header
API = Application Programming Interface
DOI = Domain of Interpretation
ESP = Encapsulated Security Payload
ISAKMP = Internet Security Association and Key Management Protocol
Oakley = Key Exchange Protocol
SA = Security Association
SAD = Security Association Database
SKEME = Secure Key Exchange Mechanism
SPD = Security Policy Database



- Con ISAKMP, IKE funciona de la siguiente forma:
  - Fase 1: establece una SA ISAKMP previa a la SA de IPSec
    - La autenticación de las partes de la comunicación suele basarse en claves compartidas, claves RSA y certificados x.509
    - Esta fase soporta dos modos de autenticación: agresivo y principal
      - El modo agresivo proceso simple y sólo usa la mitad de los mensajes para finalizar el proceso rápidamente. Sin embargo, no soporta la protección completa de las identidades de cada parte de la comunicación y transmite la identidad del cliente en claro
  - Fase 2: el nuevo SA ISAKMP es empleado para negociar y establecer los SAs de IPSec
    - En esta fase el protocolo IKE intercambia propuestas de SAs, negocia asociaciones de seguridad basándose en el ISAKMP SA inicial, y establece la clave de sesión
    - Las claves de las SAs se derivan de las claves de la primera fase, los nonces y los SPI o usando un nuevo DH

Fase 1 a Fase 2: Modo Principal

- El modo principal negocia una ISAKMP SA que se usa para crear las SAs de IPSec
- Tres pasos
  - Negociación de las SA
  - Diffie-Hellman e intercambio de nonce
  - Autenticación



Fase 1 a Fase 2: Modo Agresivo