IPsec

Seguridad en Redes de Ordenadores

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación (GSyC)

Abril de 2018

Contenidos

1. Introducción
2. Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)
3. AH (Authentication Header)
4. ESP (Encapsulation Security Payload)
5. IKE

Contenidos

1. Introducción
2. Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)
3. AH (Authentication Header)
4. ESP (Encapsulation Security Payload)
5. IKE

Introducción

- IPsec es un protocolo que proporciona confidencialidad, integridad y autenticación.
- Trabaja en el nivel de encaminamiento (a nivel IP), es más flexible que otros protocolos que trabajan a nivel de transporte como TLS ya que permite proporcionar seguridad a los protocolos del nivel de transporte.
- Se encuentra implementado en IPv4 como una extensión a este protocolo, y en IPv6 forma parte de su implementación.
- La especificación de IPsec ha sufrido diversas modificaciones, la última generación de los documentos se encuentra definida en RFC4301 y RFC4309 (del año 2005).

Modos de funcionamiento

- IPsec proporciona una comunicación IP segura entre 2 entidades, **IPsec peers**. Un IPsec peer puede ser un router o una máquina final.
- IPsec establece un **túnel IPsec** entre 2 entidades IPsec peers para proteger los datos. Dos IPsec peer pueden definir varios túneles IPsec.
- IPsec utiliza los siguientes protocolos:
  - **AH** (Authentication Header, código de protocolo=51): protocolo para la autenticación, integridad de datos y no repudio.
  - **ESP** (Encapsulation Security Payload, código de protocolo=50): protocolo que proporciona confidencialidad y/o autenticación.
- IPsec utiliza el protocolo **IKE** (Internet Key Exchange) para gestionar las claves. Durante la fase de negociación, IKE especifica el flujo de tráfico que hará uso de la conexión IPsec: protocolo, direcciones IP, ToS.

Contenidos

1 Introducción

2 Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)

3 AH (Authentication Header)

4 ESP (Encapsulation Security Payload)

5 IKE

Nomenclatura IPsec

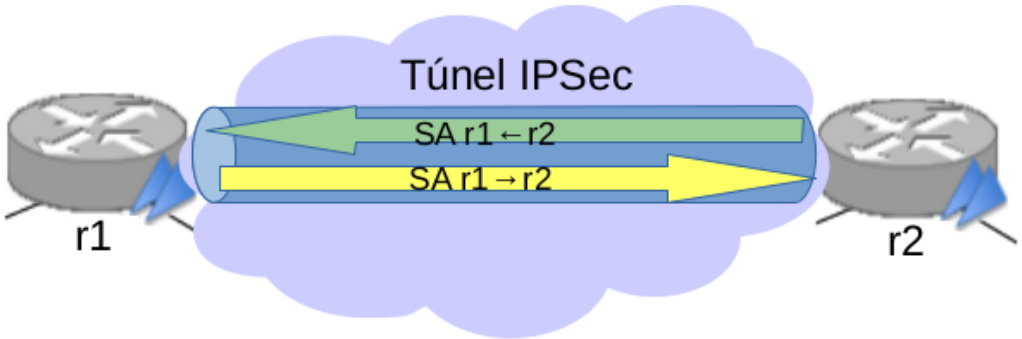
- Una política de seguridad (**Security Policy**, (SP)) es una regla programada en la implementación de IPsec que indica si un paquete debe usar IPsec o directamente la pila TCP/IP. Las SPs se almacenan en la Security Policy Database (SPD).
- Una asociación de seguridad (**Security Associations**, SA) define los parámetros de una comunicación entre dos IPsec peers en un sentido de la comunicación determinado (para la comunicación bidireccional son necesarias 2 SAs):
  - protocolo de seguridad, modo de cifrado de datos, atributos de la comunicación, claves, tiempo de vida, etc.

  IPsec puede establecer el túnel si se acuerdan los mismos parámetros entre los extremos de una SA. Las SAs se almacenan en la Security Association Database (SAD).

Cuando una máquina dispone de un paquete IP en claro para enviar, primero consulta SPD para saber si requiere IPsec. En caso afirmativo, SPD referencia una SA de SAD. La SA indica cómo debe ser cifrado/autenticado dicho paquete.

SA (Security Association)

- Una SA contiene toda la información necesaria para descifrar/autenticar un paquete IPsec: algoritmos y claves, número de secuencia actual, tiempo de vida de SA, etc.
- Una SA queda identificado por 3 parámetros:
  - Security Parameter Index (SPI)
  - Dirección IP destino
  - Protocolo de seguridad (AH o ESP)
- Una SA puede configurarse manualmente o a través del protocolo IKE que negocia las claves y mantiene los SAs.



Dos SAs: r1 $\rightarrow$ r2 y r1 $\leftarrow$ r2

SP (Security Policy)

- Una SP es una regla que indica los valores que debe tener un datagrama para aplicarle una configuración IPsec. Se examina la cabecera IP y la cabecera de nivel de transporte para consultar los siguientes campos
  - Direcciones IP origen/destino
  - Protocolo de nivel de transporte
  - Puertos origen/destino
- Las reglas SP también se denominan selectores de tráfico (TS, Traffic Selectors).
- Las reglas SP se almacenan en SPD.

Envío y recepción de paquetes IPsec

- **Envío**: se consulta SPD para encontrar una política y saber si es necesario aplicar IPsec.
  - Si no es necesario, el paquete se procesa utilizando la pila TCP/IP.
  - Si es necesario, se busca si existe SA, se utiliza la información para construir paquete IPsec. Si no existe, se crea utilizando IKE.
- **Recepción**: se consulta SAD usando la información del paquete <SPI,dirIPDestino,Protocolo>, se descifra/autentica el paquete y se consulta SPD para saber si existía una política asociada a dicho paquete.

Contenidos

1 Introducción

2 Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)

3 AH (Authentication Header)

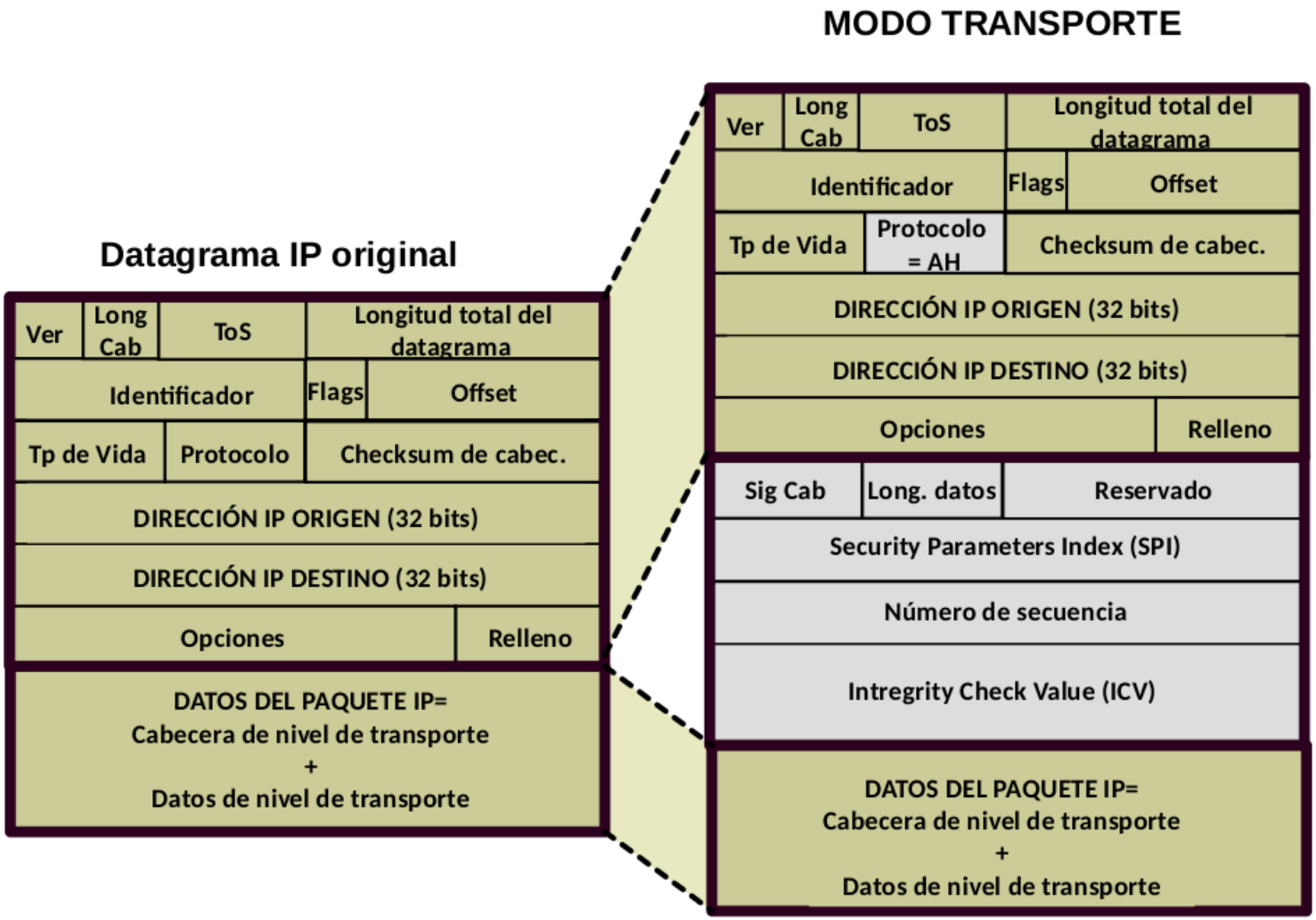
4 ESP (Encapsulation Security Payload)

5 IKE

AH (Authentication Header)

- Garantiza:
  - autenticación de origen y no repudio
  - integridad de la cabecera IP y de los datos.
- El emisor y el receptor del paquete comparten una clave secreta:
  - La clave se utiliza en el cáculo de HMAC.
  - La clave se configura a través de IKE y se guarda en el SA, junto con el algoritmo de hash utilizado: MD5, SHA.
  - El emisor calcula HMAC del paquete IP original y los campos de la cabecera AH y almacena ese valor en la cabecera AH. El receptor también calcula el HMAC y lo compara junto con el valor que recibe en la cabecera AH para ver si los datos se han modificado en el trayecto.
- Dos modos:
  - **Modo transporte**: inserta la cabecera AH entre la cabecera IP y los datos IP del paquete original.
  - **Modo túnel**: no modifica el paquete IP original, construye una nueva cabecera IP junto con la cabecera AH, a continuación adjunta el paquete IP original.

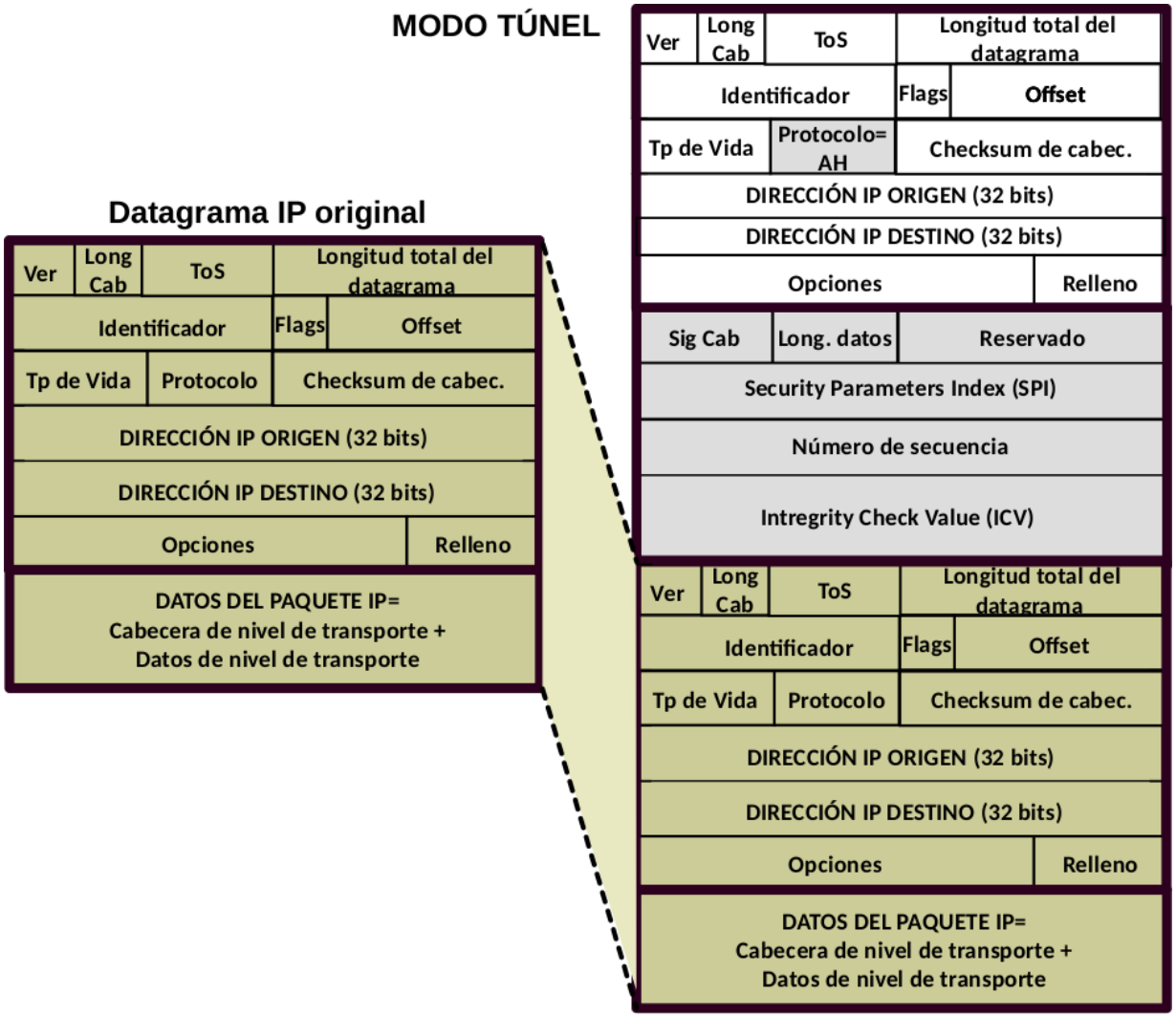
Cabecera AH en modo transporte



Protocolo = AH = 51

Sig. Cab. = Protocolo datagrama IP original

Cabecera AH en modo túnel



Protocolo = AH = 51
Sig. Cab. = IPv4 = 4

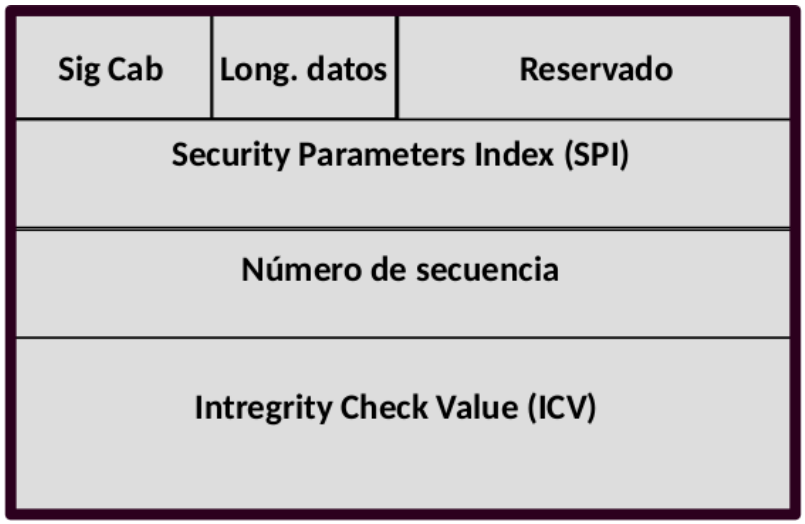
AH: Modo transporte vs túnel

- En **modo transporte**:
  - Los extremos de la comunicación deben soportar IPsec.
  - Quedan protegidos todos los campos inmutables[1] de la cabecera IP original, los datos del paquete IP original y los campos de la cabecera AH.
  - No soporta NAT, hay extensiones.
- En **modo túnel**:
  - Se protege la identidad de los extremos que están comunicándose pues la cabecera externa oculta las direcciones IP de los extremos.
  - Quedan protegidos todos los campos inmutables de la cabecera externa, el datagrama original completo y los campos de la cabecera AH.

[1] Todos son inmutables excepto algunos campos que varían en el trayecto, ToS, TTL, flags de fragmentación, offset fragmentación y checksum

Cabecera AH

- **Sig. Cab.**: Siguiente cabecera o tipo de datos que van a continuación de la cabecera AH. En modo transporte este campo llevará el protocolo de nivel de transporte y en modo túnel llevará el protocolo IP.
- **Long. datos**: Longitud de la cabecera AH.
- **SPI**: junto con dirección IP destino y protocolo AH identifica SA.
- **Número de secuencia**: se incrementa cada vez que se envía un paquete utilizando una determinada SA. Evita ataques de reproducción.
- **ICV**: cálculo de HMAC utilizando el algoritmo fijado.



Contenidos

1 Introducción

2 Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)

3 AH (Authentication Header)

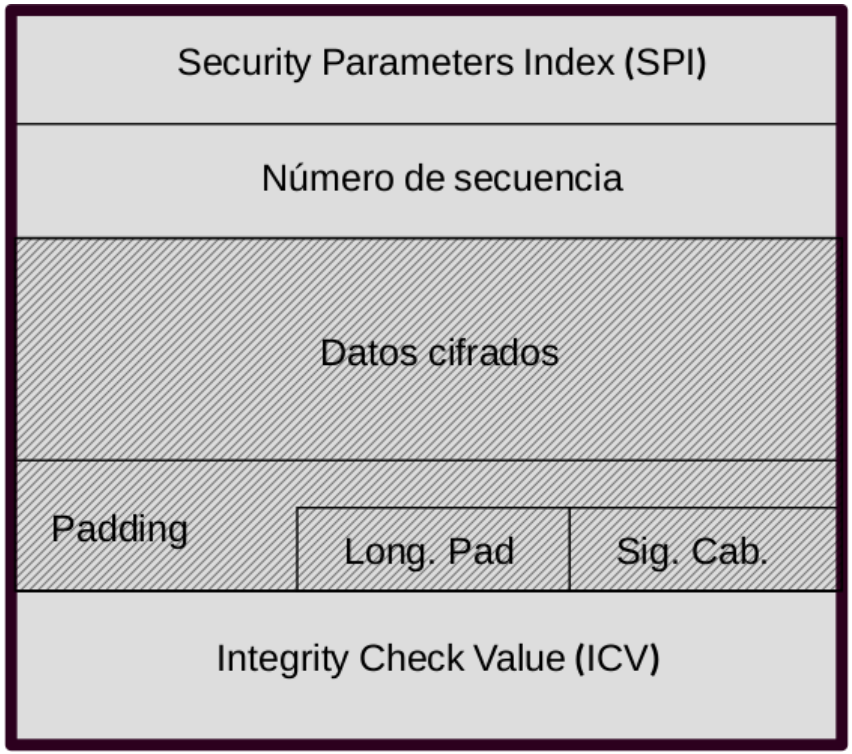
4 ESP (Encapsulation Security Payload)

5 IKE

ESP (Encapsulation Security Payload)

- Garantiza:
  - Confidencialidad a través de cifrado.
  - Integridad del paquete cifrado a través de HMAC, o combinándolo con AH.
- ESP distingue los siguientes componentes en su formato:
  - **ESP Header**: contiene SPI y número de secuencia. Viaja antes que los datos cifrados.
  - **Datos cifrados**.
  - **ESP Trailer**: relleno o padding para alinear los datos cifrados, longitud del relleno y el campo sig. cabecera. Viaja después de los datos cifrados.
  - **ESP Authentication Data**: ICV si ESP ha elegido proporcionar integridad al paquete cifrado.

Formato del mensaje ESP

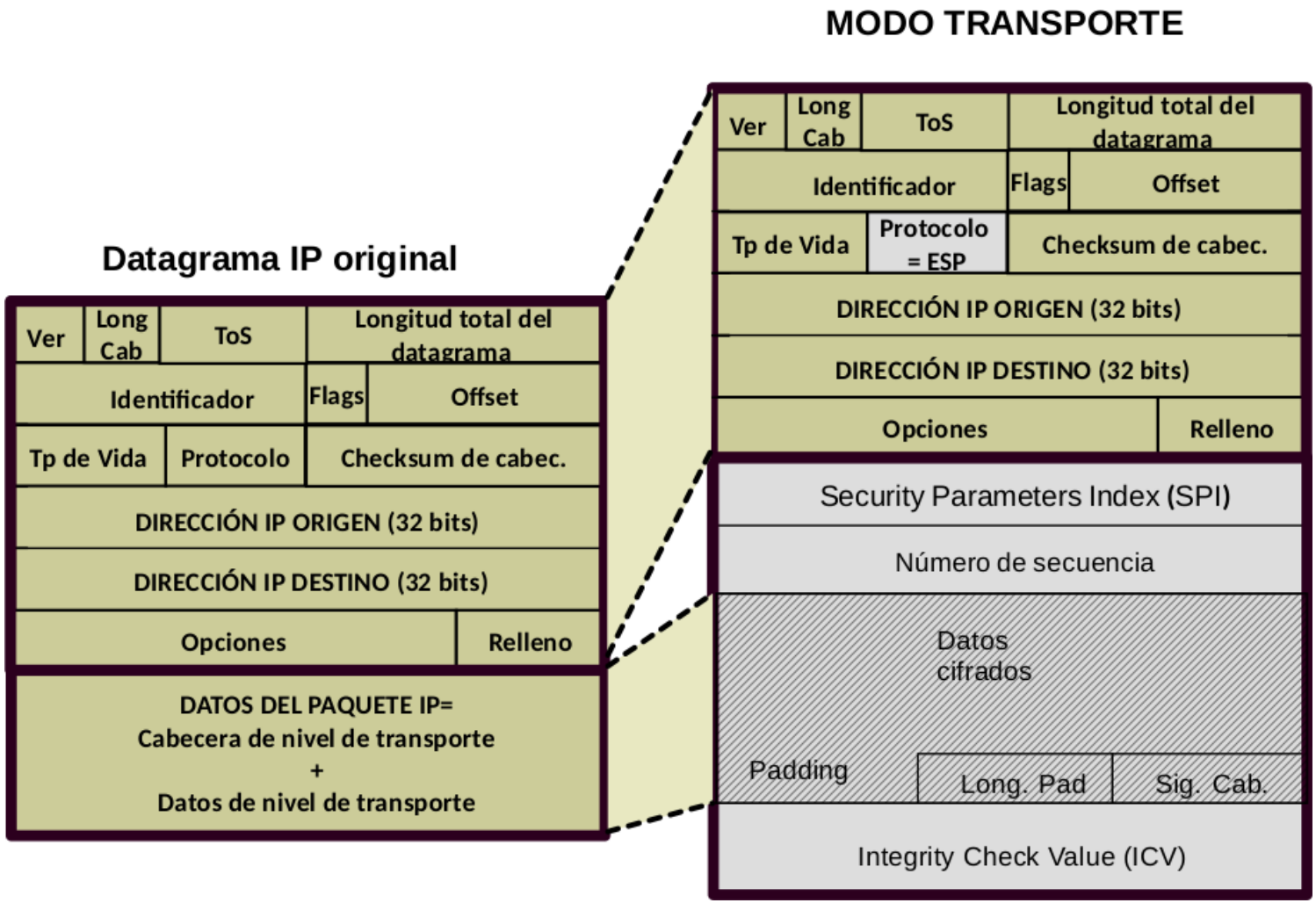


El campo Sig. Cab. va cifrado e indica de qué protocolo son los datos que van cifrados.

ESP: Modo transporte vs túnel

- En **modo transporte**:
  - Los extremos de la comunicación deben soportar IPsec.
  - Sólo se cifran los datos del datagrama IP.
- En **modo túnel**:
  - Se cifra el datagrama IP completo.
  - Se oculta cuáles son las direcciones IP de los extremos que se están comunicando.

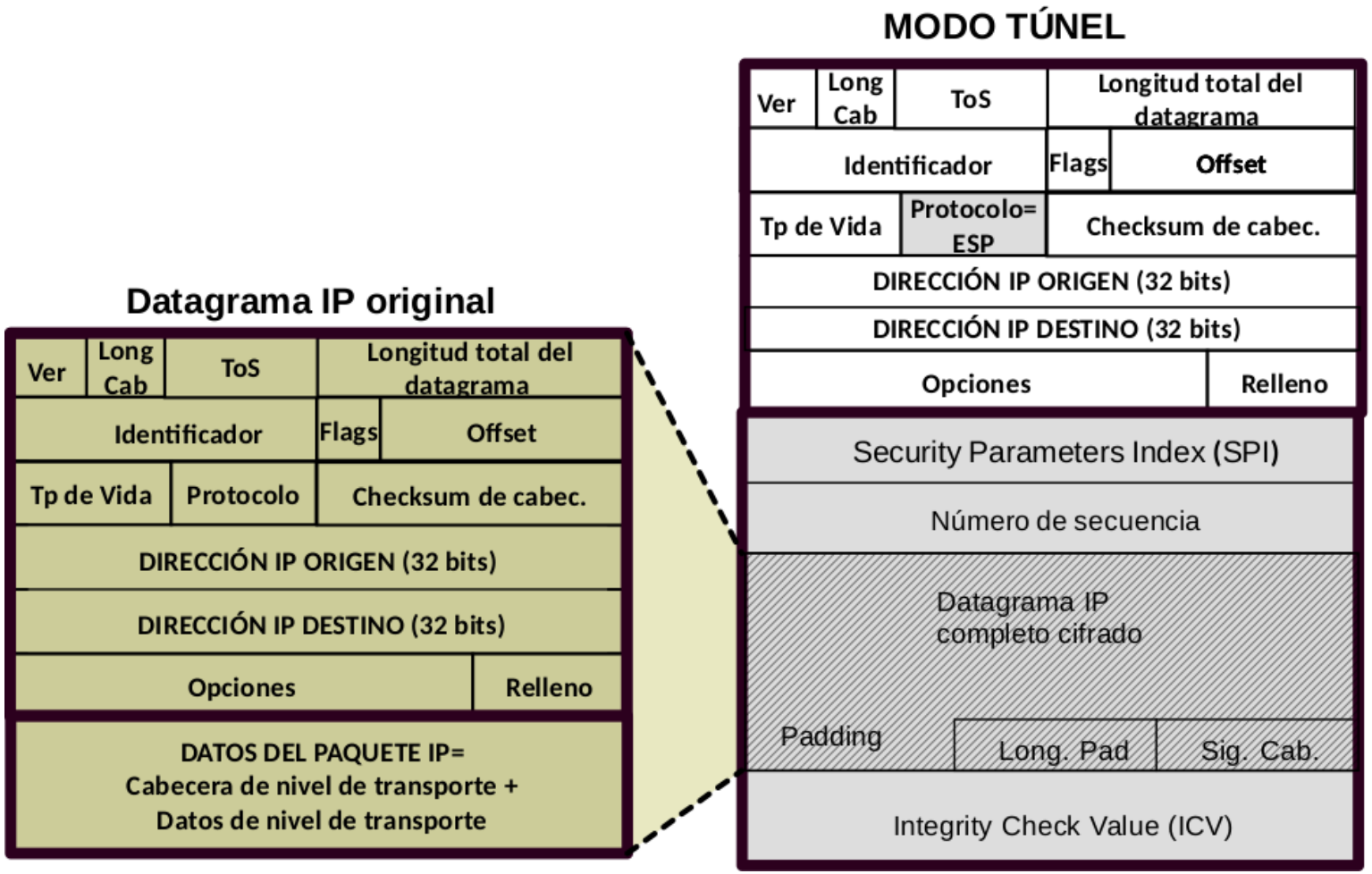
ESP en modo transporte



Protocolo = ESP = 50

Sig. Cab. = Protocolo de nivel de transporte que llevaba el datagrama IP original

ESP en modo túnel



Protocolo = ESP = 50

Sig. Cab. = IPv4 = 4

Contenidos

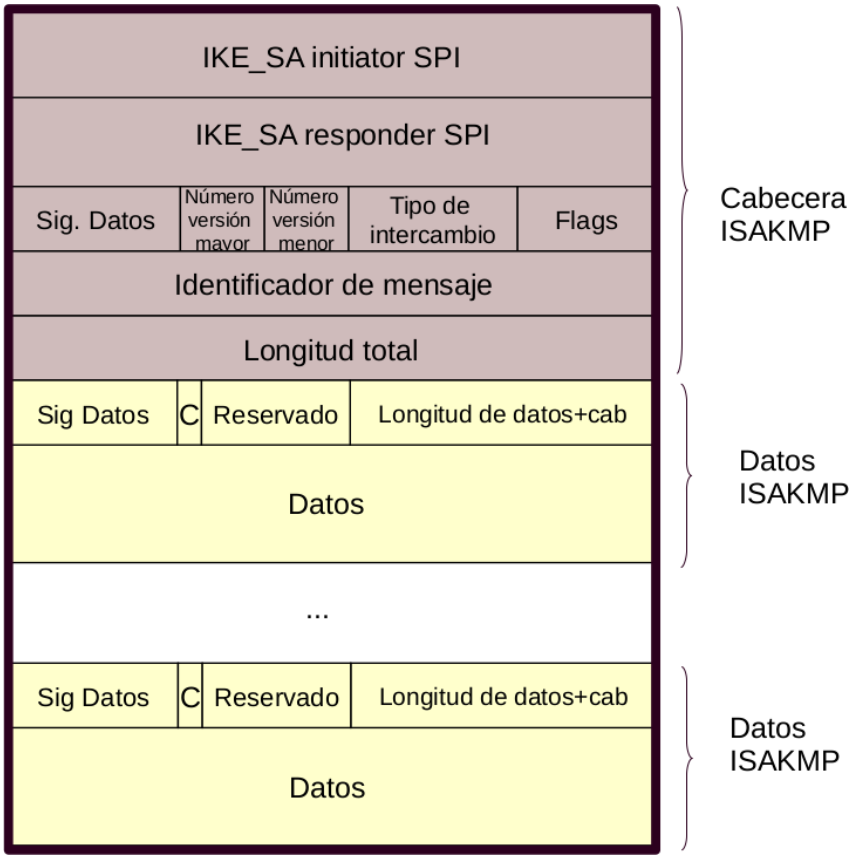
1. Introducción
2. Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)
3. AH (Authentication Header)
4. ESP (Encapsulation Security Payload)
5. IKE

Internet Key Exchange (IKE)

- IKE (RFC-2409), IKEv2 (RFC-7296) es una optimización de la versión anterior con menor número de mensajes y otras funcionalidades como poder atravesar un NAT.
- Simplifica la configuración de IPsec ya que establece una SA en IPsec.
- IKE es un protocolo de nivel de aplicación sobre **UDP** en el puerto 500 y/o 4500. Se construye sobre el protocolo Internet Security Association and Key Management Protocol (ISAKMP).
- Fases IKE:
  - **Primera fase**: establecimiento de canal seguro utilizando claves Diffie-Hellman para generar una clave secreta que se usará para cifrar las comunicaciones IKE. Para ello se establece una `IKE_SA` bidireccional (asociación de seguridad para intercambiar mensajes IKE). La autenticación se puede realizar con diferentes mecanismos: pre-shared-key, PKI.
  - **Segunda fase**: los extremos usan el canal seguro para establecer SA para IPsec, lo que se denomina `CHILD_SA`

Formato de los mensajes ISAKMP

- Los intercambios de mensajes ISAKMP son de tipo solicitud/respuesta.
- Las comunicaciones usando IKE son fiables, IKEv2 implementa un mecanismo de retransmisión si no se recibe respuesta a una solicitud.
- Los mensajes ISAKMP están formados por una primera cabecera seguida de 1 o más campos de datos ISAKMP.

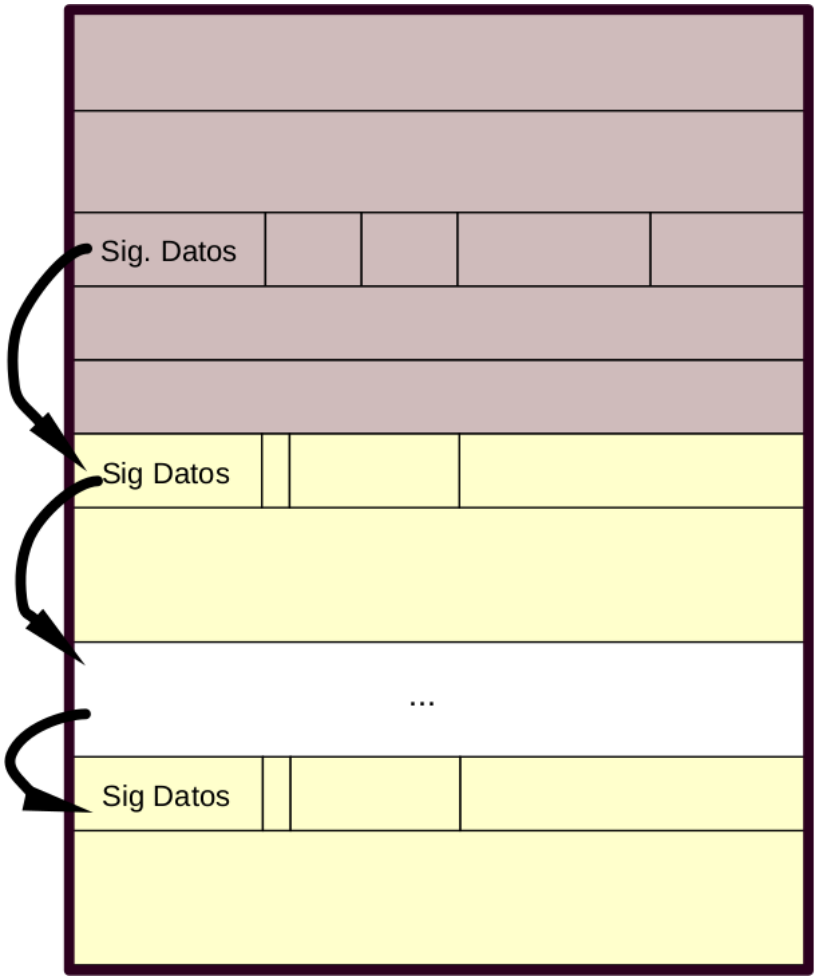


Contenidos

1. Introducción
2. Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)
3. AH (Authentication Header)
4. ESP (Encapsulation Security Payload)
5. IKE
   - Formato de mensajes ISAKMP
   - Intercambio de mensajes ISAKMP

Tipos de datos dentro de un mensaje ISAKMP

- Security Association, SA (33)
- Key Exchange, KE (34)
- Identidades IDi/IDr (35/36)
- Certificate, CERT (37)
- Certificate Request, CERTREQ (38)
- Authentication (39)
- Nonce (40)
- Notify (41)
- Contenido cifrado y autenticado (46)
- ...



Primera cabecera ISAKMP

- `IKE_SA Initiator SPI` (8 bytes): SPI del que inicia la comunicación
- `IKE_SA Responder SPI` (8 bytes): SPI del que responde a la comunicación (inicialmente a cero).
- Campo siguiente tipo de datos ISAKMP: indica qué tipo de datos vienen a continuación.
- Número de versión mayor=2, número de versión menor=0.
- Tipo de intercambio (1 byte):
  - `IKE_SA_INIT`
  - `IKE_AUTH`
  - `CREATE_CHILD_SA`
  - `INFORMATIONAL`
- Flags:
  - R: respuesta=1, solicitud=0
  - I: initiator=1, responder=0
  - V: bit de versión, V=1 implementa versión superior, V=0 no la implementa.
  - C: critical, qué hacer si el receptor no entiende el tipo de cabecera, C=0 lo ignora, C=1 envía mensaje.
- Identificador de mensaje: es un número de sencuencia para identificar solicitud/respuesta. Se utiliza para las retransmisiones.

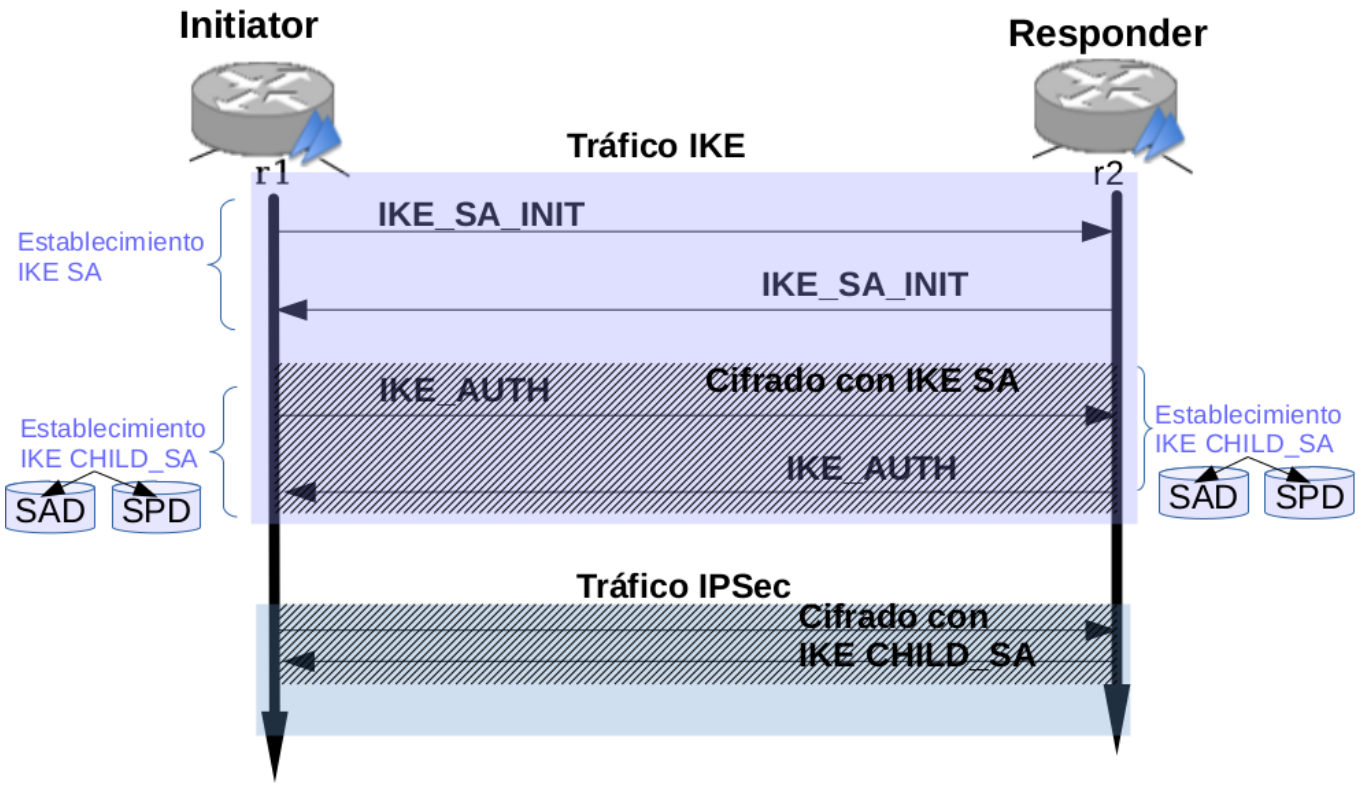
Contenidos

1. Introducción
2. Nomenclatura: políticas de seguridad (SP) y asociaciones de seguridad (SA)
3. AH (Authentication Header)
4. ESP (Encapsulation Security Payload)
5. IKE
   - Formato de mensajes ISAKMP
   - Intercambio de mensajes ISAKMP

Establecimiento IPsec SA (I)

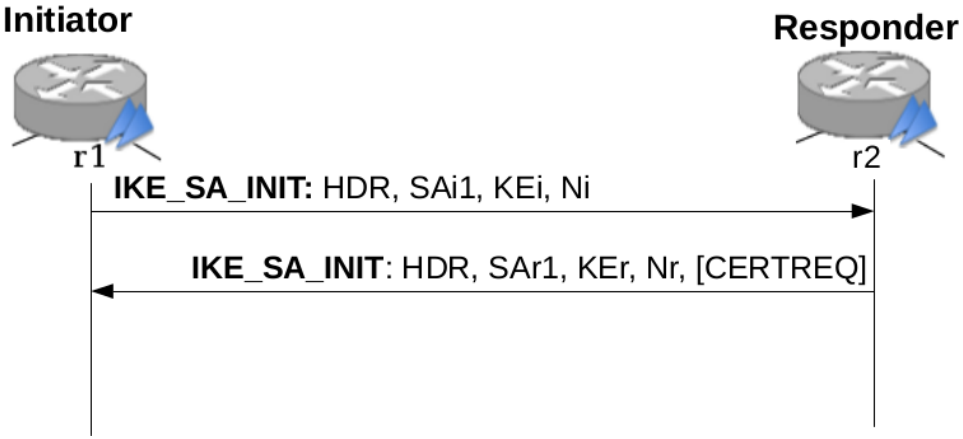
- Para establecer IPsec SA a través de IKEv2 serán necesarios 4 mensajes:
  - **Primera fase**: 2 mensajes para establecer IKE SA, algoritmos y claves para cifrar/autenticar la comunicación que negociará IPsec SA.
    - Initiator $\rightarrow$ Responder: Mensaje de solicitud IKE_SA_INIT
    - Initiator $\leftarrow$ Responder: Mensaje de respuesta IKE_SA_INIT
  - **Segunda fase**: 2 mensajes para establecer IPsec SA, algoritmos y claves para cifrar/autenticar la comunicación IPsec. Estos dos mensajes irán cifrados y autenticados con las claves derivadas del primer intercambio de IKE_SA_INIT.
    - Initiator $\rightarrow$ Responder: Mensaje de solicitud IKE_AUTH
    - Initiator $\leftarrow$ Responder: Mensaje de respuesta IKE_AUTH

Establecimiento IPsec SA (II)



Intercambio IKE_SA_INIT

- Negocia IKE_SA



- SAi1: SA de initiator para enviar una propuesta de los algoritmos que soporta
- SAr1: SA de responder, elige un algoritmo para cada operación: cifrar, integridad, función pseudo-random
- KEi, KEr son los valores Diffie Hellman (DH).
- Ni, Nr: nonces
- Opcionalmente, responder puede solicitar un certificado
- A partir de los mensajes IKE_SA_INIT intercambiados se genera una clave de sesión `SKEYSEED` de la cuál derivarán las claves necesarias para cifrar `SK_e`, para firmar `SK_a` y para obtener el digest `SK_d`.

Mensaje de solicitud IKE_SA_INIT

- Mensaje de solicitud enviado por el lado que inicia la comunicación

```
▶ Frame 1: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits)
▶ Ethernet II, Src: c6:e7:f7:3e:10:e3 (c6:e7:f7:3e:10:e3), Dst: f6:a5:87:28:79:df (f6:a5:87:28:79:df)
▶ Internet Protocol Version 4, Src: 100.0.0.1, Dst: 102.0.0.4
▶ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▼ Internet Security Association and Key Management Protocol
    Initiator SPI: b4331f685c912ab1
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
  ▶ Version: 2.0
    Exchange type: IKE_SA_INIT (34)
  ▶ Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000000
    Length: 560
  ▶ Type Payload: Security Association (33)
  ▶ Type Payload: Key Exchange (34)
  ▶ Type Payload: Nonce (40)
  ▶ Type Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
  ▶ Type Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
```

Mensaje de respuesta IKE_SA_INIT

- Mensaje de respuesta enviado por el lado que responde la comunicación

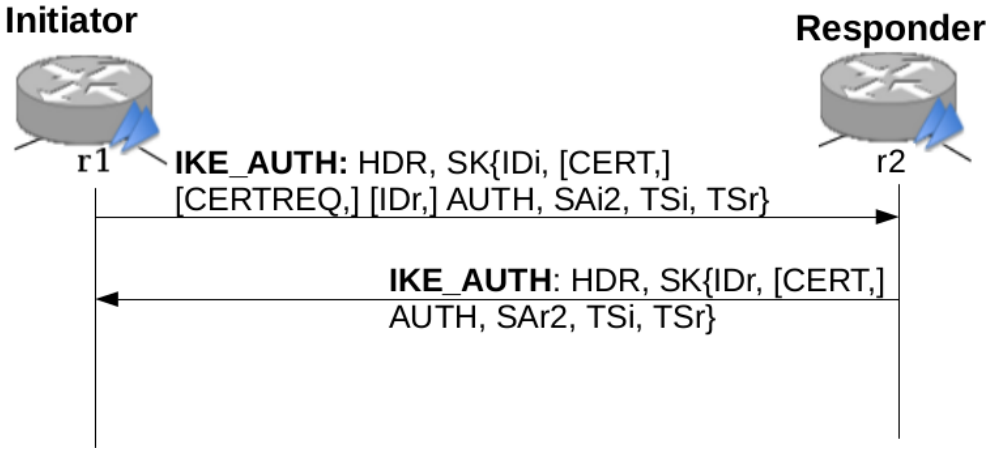
```
▶ Frame 4: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits)
▶ Ethernet II, Src: f6:a5:87:28:79:df (f6:a5:87:28:79:df), Dst: c6:e7:f7:3e:10:e3 (c6:e7:f7:3e:10:e3)
▶ Internet Protocol Version 4, Src: 102.0.0.4, Dst: 100.0.0.1
▶ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▼ Internet Security Association and Key Management Protocol
    Initiator SPI: b4331f685c912ab1
    Responder SPI: 5a81febc2c3a4d12
    Next payload: Security Association (33)
  ▶ Version: 2.0
    Exchange type: IKE_SA_INIT (34)
  ▶ Flags: 0x20 (Responder, No higher version, Response)
    Message ID: 0x00000000
    Length: 593
  ▶ Type Payload: Security Association (33)
  ▶ Type Payload: Key Exchange (34)
  ▶ Type Payload: Nonce (40)
  ▶ Type Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
  ▶ Type Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
  ▶ Type Payload: Certificate Request (38)
  ▶ Type Payload: Notify (41) - MULTIPLE_AUTH_SUPPORTED
```

Secreto compartido a partir de los valores DF: KEi, KEr

- Initiator y Responder pueden calcular el secreto Diffie-Hellman de la siguiente forma: g^{xy} mód p
- En la cabecera Key Exchange se indica el grupo que se está utilizando: 3072 bit MODP group, que especifica el primo y el generador:
  - Primo:
    $p = 2^{3072} - 2^{3008} - 1 + 2^{64} * [(2^{2942} * \pi) + 1690314]$
  - Generador: g=2
- Cada lado generará un número a partir de un secreto individual:
  - Initiator genera x y envía a Responder $X = g^x$ mód p
  - Responder genera y y envía a Initiator $Y = g^y$ mód p
- El secreto Diffie-Hellman compartido por ambos y que ellos pueden calcular es:
  - Initiator calcula Y^x mód $p = (g^y)^x$ mód $p = g^{yx}$ mód p
  - Responder calcula X^y mód $p = (g^x)^y$ mód $p = g^{xy}$ mód p
- `prf(key, msg)`: `prf` es la función pseudo-aleatoria con clave (keyed pseudo-random function), cuya clave se proporciona en el parámetro key, utilizada para generar una salida determinista del mensaje msg y que parece pseudo-aleatoria. `prf` se utilizan para el cálculo de claves y para la autenticación (por ejemplo keyed MAC).

Intercambio IKE_AUTH

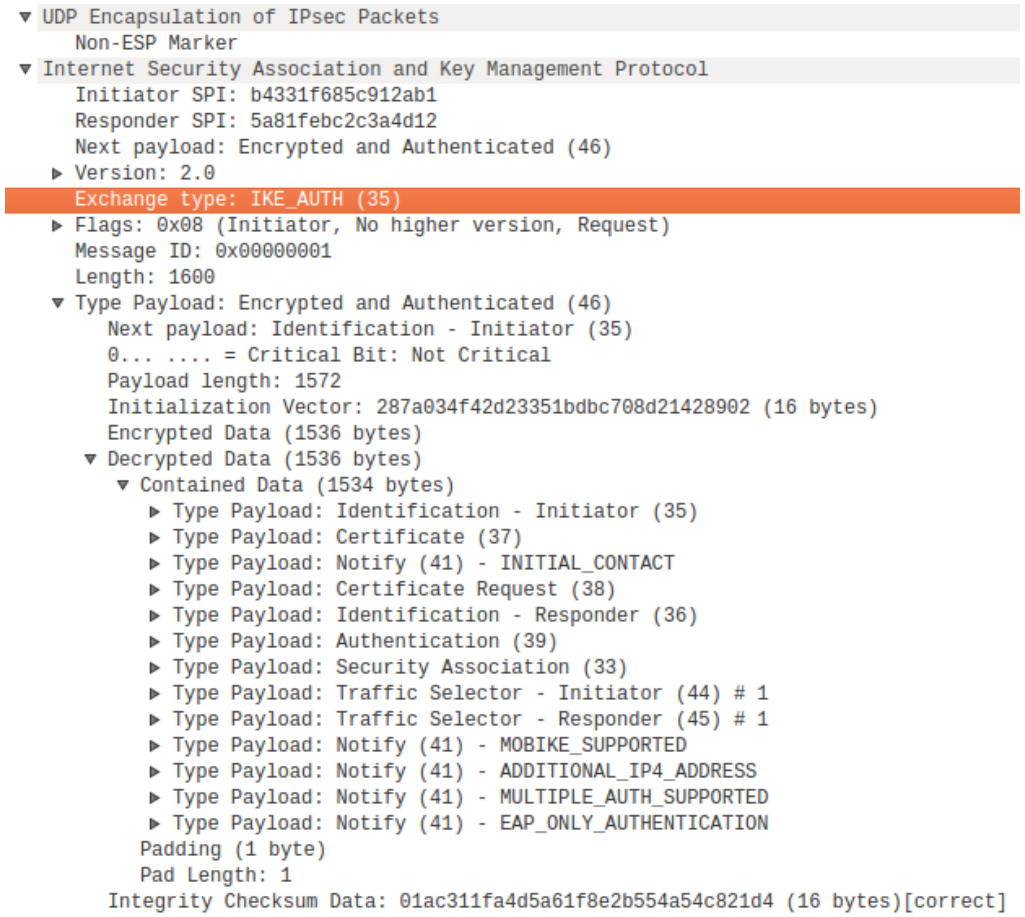
- Autentica los extremos y establece CHILD_SA.
- La notación `SK { ...}` significa que el contenido está cifrado utilizando las claves `SK_e` y `SK_a` de cada sentido de la comunicación.



- Initiator envía su identidad dentro de IDi, puede enviar su certificado y una petición de certificados y puede enviar la identidad del Responder IDr.
- Initiator comienza la negociación de `CHILD_SA` enviando su propuesta SAi2: algoritmos de cifrado/autenticación, SPI, protocolo ESP/AH.
- TSi y TSr son selectores de tráfico: son los rangos de direcciones IP y puertos desde los que se va a aplicar el túnel y hasta los que se va a aplicar el túnel.
- Responder envía su identidad IDr, opcionalmente enviará certificados. La autenticación y la integridad del mensaje se comprueban a través de AUTH.
- Responder completa la negociación de `CHILD_SA` enviando su propuesta SAr2.

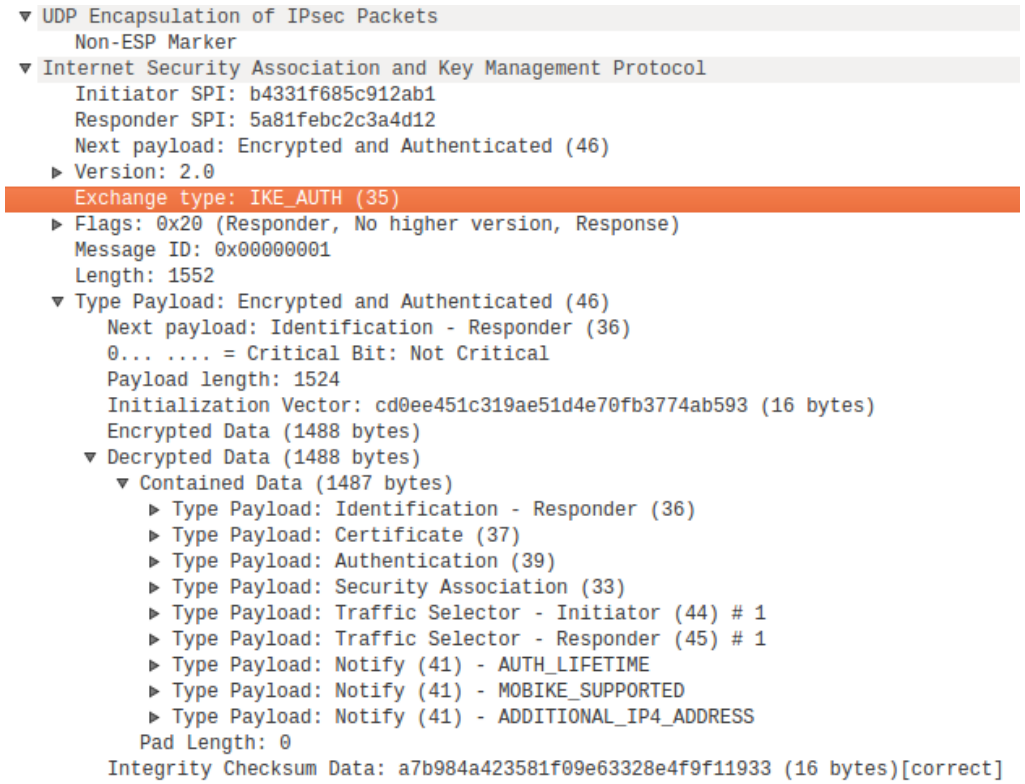
Mensaje de solicitud IKE_AUTH

- Mensaje de solicitud enviado por el lado que inicia la comunicación. Este mensaje va cifrado por la claves que se han derivado de la negociación IKE_SA_INIT (en la figura se muestra descifrado porque se han utilizado las claves para descifrar el contenido).



Mensaje de respuesta IKE_AUTH

- Mensaje de respuesta enviado por el lado que responde la comunicación. Este mensaje va cifrado por la claves que se han derivado de la negociación IKE_SA_INIT (en la figura se muestra descifrado porque se han utilizado las claves para descifrar el contenido).



Recálculo de claves: CREATE_CHILD_SA

- Cada lado puede recalcular sus claves en cualquier momento.
- El recálculo puede afectar a IKE SA o a CHILD_SA.
  - En IKE SA: El nuevo IKE SA hereda todos los CHILD_SA.
  - En CHILD_SA: se genera un nuevo SA y se borra el antiguo.

Intercambio de mensajes INFORMATIONAL

- Se utilizan para el control y la notificación de errores.
- Van cifrados con los parámetros del IKE SA.
- Contienen los siguientes tipos de datos: NOTIFICATION, DELETE, CONFIGURATION.
- Si no contiene datos se utiliza para saber si el otro extremo aún sigue activo.

Bibliografía

- VPNs Illustrated, Tunnels, VPNs and IPsec, Jon C. Snader, Addison-Wesley.
- RFC 4301: Security Architecture for the Internet Protocol, S.Kent, K. Seo, December 2005.
- RFC 4303: IP Encapsulation Security Payload (ESP), S.Kent, December 2005.
- RFC 4302: IP Authentication Header, S. Kent. December 2005
- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2), Oct 2014, C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen.