



1. Introducción
 - 1.1 Contenido de la RFC
 - 1.2 Otros documentos de interés
2. Objetivos de diseño
 - 2.1 Descripción de los objetivos, los requerimientos y los problemas
 - 2.2 Suposiciones y advertencias
3. Apreciación global del sistema IPsec
 - 3.1 Qué es IPsec?
 - 3.2 Cómo trabaja IPsec?
 - 3.3 Dónde se implementa IPsec?
4. Asociaciones de seguridad
 - 4.1 Definición y alcance
 - 4.2 Funcionalidad de las Asociaciones de seguridad
 - 4.3 Asociaciones de Seguridad combinadas
 - 4.4 Bancos de Datos de las Asociaciones de seguridad
 - 4.4.1 Banco de datos de la Política de Seguridad (SPD)
 - 4.4.2 Selectores
 - 4.4.3 Banco de Datos de las Asociación de seguridad (SAD)
 - 4.5 Combinaciones básicas de las Asociaciones de Seguridad
 - 4.6 SA y Manejo de claves
 - 4.6.1 Técnicas manuales
 - 4.6.2 SA automatizadas y el Manejo de claves
 - 4.6.3 Encontrando una pasarela segura
 - 4.7 Asociaciones de seguridad y Multicast
5. Trafico procesado por IP
 - 5.1 Tráfico saliente de IP
 - 5.1.1 Seleccionando y Usando un SA o SA Bundle
 - 5.1.2 Header Construction para el Modo Túnel
 - 5.1.2.1 IPv4--Header Construction para el Modo Túnel
 - 5.1.2.2 IPv6--Header Construction para el Modo Túnel
 - 5.2 Tráfico entrante a IP
 - 5.2.1 Seleccionando y Usando un SA o SA Bundle
6. Procesamiento ICMP relativo a IPsec
 - 6.1 Bit de No Fragmentación (DF)
 - 6.2 Path MTU (PMTU)
 - 6.1.2.1 Propagación de PMTU
 - 6.1.2.2 Cálculo de PMTU
 - 6.1.2.3 Granularidad de PMTU
 - 6.1.2.4 PMTU y el paso del tiempo
7. Uso en Sistemas de seguridad sobre el flujo de información
 - 7.1 Relación entre las Asociaciones de Seguridad y los Datos sensibles
 - 7.2 Comprobación de la sensibilidad de los Datos
 - 7.3 Atributos adicionales de MLS para los Bancos de Datos de Asociaciones de Seguridad

[7.4 Procesamiento del flujo entrante de MLS](#)

[7.5 Procesamiento del flujo saliente a MLS](#)

[7.6 MLS Procedimiento adicionales para las Pasarelas de Seguridad](#)

[8. Referencias](#)

1.Introducción

El presente trabajo ha sido realizado en el marco de la asignatura Sistema de Transporte de Datos de la Universidad de Alicante. Consiste en una descripción de la seguridad ofrecida por IPsec para la pila de protocolos IP. Se ha basado en la RFC 2401 que es la específica para este tema.

1.1 Contenido de la RFC

La RFC especifica la arquitectura a bajo nivel de los protocolos IPsec. La meta de la arquitectura es proporcionar varios servicios de seguridad para el tráfico a la capa de IP, en los entornos IPv4 y IPv6. La RFC describe los objetivos de tales sistemas, sus componentes y cómo ellos encajan entre ellos y en el entorno IP. También describe los servicios de seguridad ofrecidos por los protocolos de IPsec, y cómo estos servicios pueden emplearse en el entorno de IP. La RFC no se ocupa de todos los aspectos de la arquitectura IPsec.

a. Protocolos de seguridad -- Cabecera de autenticación (Authentication Header AH) y Encapsulado de seguridad de carga útil (Encapsulating Security Payload ESP)

b. Asociaciones de seguridad -- Qué son y cómo trabajan, cómo se usan y el procesamiento asociado.

c. Manejo de claves -- Manual y automático (El intercambio de claves en Internet (The Internet Key Exchange IKE))

d. Algoritmos para la autenticación y encriptación

La RFC no trata respecto a una Arquitectura de Seguridad global para Internet; sólo se concentra en la capa de IP, con tal de que a través del uso de una combinación de técnicas criptográficas y protocolos con mecanismos de seguridad.

1.2 Otros documentos de interés

Entre los documentos que se pueden emplear para aumentar los conocimientos respecto a este tema, se pueden destacar los siguientes:

a. "IP Security Document Roadmap" [TDG97] -- En la RFC se explica una guía para la realización de algoritmos de encriptación e identificación usados en este sistema.

b. Security Protocolos -- RFCs que describen la cabecera de autenticación (Authentication Header AH) [KA98a] y Encapsulado de seguridad de carga útil (Encapsulating Security Payload ESP) [KA98b].

c. Algorithms for authentication and encryption -- Existe una RFC explícita para cada algoritmo de encriptación.

d. Automatic Key Management -- RFCs sobre el Intercambio de claves en Internet (The Internet Key Exchange IKE) [HC98], "Internet Security Association and Key Management Protocol (ISAKMP)" [MSST97], "The OAKLEY Key Determination Protocol" [Orm97], y "The Internet IP Security Domain of Interpretation for ISAKMP" [Pip98].

2. Objetivos de diseño

2.1 Descripción de los objetivos, los requerimientos y los problemas

Ipsec se diseñó para proporcionar seguridad de gran calidad empleando técnicas criptográficas para IPv4 y IPv6. La gama de servicios de seguridad ofrecidos incluye control de acceso, fiabilidad de la conexión, autenticación del origen de los datos, protección contra réplicas y confidencialidad dentro de un flujo de tráfico limitado. Estos servicios son proporcionados a la capa IP, ofreciendo protección para IP y los protocolos de capas superiores.

Estos objetivos se resumen en el uso de dos protocolos de seguridad frente al tráfico, la cabecera de autenticación (Authentication Header AH) y Encapsulado de seguridad de carga útil (Encapsulating Security Payload ESP), y a través del uso de procedimientos y protocolos basados en claves criptográficas. El juego de protocolos de IPsec se puede emplear en cualquier contexto, y las formas en las que son empleados, serán determinados por la seguridad y requisitos del sistema, aplicaciones, y/o las organizaciones que lo utilicen.

Cuando estos mecanismos son correctamente implementados y puestos en práctica, los usuarios no deberían verse afectados negativamente al igual que los servidores u otros componentes de Internet para los cuales no han sido desarrollados. Estos mecanismos han sido diseñados para ser algoritmos independientes, por lo que su modularidad permite emplear diferentes algoritmos sin afectar al resto de la implementación.

2.2 Suposiciones y advertencias.

La seguridad ofrecida por IPsec es totalmente dependiente de los posibles aspectos del entorno en el cual IPsec se ejecuta, y todo ello degrada la seguridad que pueda ofrecer IPsec, por ejemplo, poca calidad al generar números aleatorios, una mal manejador de protocolos, ...

3. Apreciación global del sistema IPsec

La implementación de IPsec funciona en servidores o en un entorno seguro ofreciendo protección al tráfico IP. Esta protección está basada en requerimientos definidos por la política de seguridad en Bases de Datos (SPD), establecida y mantenida por el usuario y el administrador, o por las aplicaciones.

Los paquetes se seleccionan por uno de los tres modos de procesamiento basado en la capa de transporte IP, correspondientes a cada entrada en la Base de Datos. Cada paquete recibe los servicios de seguridad ofrecidos por IPsec, de manera que este los deja pasar o los descarta.

3.1 Qué és IPsec?

IPsec proporciona seguridad a la capa IP facilitando un sistema de selección que necesita protocolos de seguridad, que determinen los algoritmos para cada servicio y pongan en su sitio cada clave criptográfica que se necesita para los servicios requeridos.

IPsec puede ser utilizado para proteger uno o mas caminos entre un par de servidores o de pasarelas de seguridad o entre una pasarela y un servidor. La pasarela sobre la que hablamos se refiere a un sistema intermediario que implementa el protocolo IPsec, por ejemplo un router o un cortafuegos.

3.2 Cómo trabaja IPsec?

IPSec utiliza dos protocolos para proveer al tráfico de seguridad:

Authentication Header (AH)-- suministra integridad en la conexión, autenticación de los datos originales y un servicio opcional para repeler los mensajes de respuesta.

Encapsulating Security Payload (ESP)-- puede suministrar confidencialidad de los datos mediante la encriptación de los mismos, y limitar el flujo de tráfico confidencial. También proporciona integridad en la conexión y un servicio anti-repetición de mensajes.

Estos dos protocolos se dedican a controlar el acceso, y son los que distribuyen las claves criptográficas de la seguridad del flujo de tráfico. No pueden ser aplicados conjuntamente. Cada uno de los protocolos antes mencionados soportan dos modalidades de uso: modo transporte (transport mode) y modo túnel (tunnel mode).

IPsec permite al usuario o al sistema administrador controlar la granularidad del servicio que es prestado. Incorpora facilidades para la especificación de qué servicios de seguridad se quieren usar y en qué combinaciones, la granularidad que va a ser aplicada y los algoritmos para la encriptación.

Como estos servicios de seguridad usan claves compartidas, IPsec se vale de mecanismos adicionales para ponerlas en su sitio. Estas claves se usan para la autenticación de la integridad y la encriptación y desencriptación de los paquetes.

3.3 Dónde puede ser implementado IPsec?

Hay varias maneras en las que se puede implementar IPsec, en un servidor o en un router o un cortafuegos para proporcionar una pasarela segura. Las mas comunes son:

a. Integrar IPsec en la implementación nativa de IP --requiere tener acceso al código fuente de IP, y se puede aplicar tanto a servidores como a pasarelas.

b. "Bump In The Stack" (BITS) implementación -- donde IP está implementado oculto junto con una pila (por eso lo de stack), que se da entre los drivers de la máquina y IP.

c. "Bump In The Wire" (BITW) implementación -- utiliza un procesador de encriptación fuera de la máquina. Puede ofrecer servicios tanto a servidores como a pasarelas. Cuando atiente a un solo servidor, resulta igual a la implementación BITS, pero en un router o un cortafuegos se debe operar bajo una pasarela segura.

4. Asociaciones de Seguridad

4.1 Definición y Alcance

Una Asociación de Seguridad (SA) es una conexión unidireccional que aporta servicios de seguridad al tráfico que pasa por ella. Estos servicios de seguridad son ofrecidos a la SA por el uso de AH o ESP, pero nunca ambos juntos. Para obtener una comunicación bidireccional segura entre dos servidores o entre dos pasarelas una SA en cada extremo de la comunicación es imprescindible.

Para identificar una SA, existe un triple parámetro consistente en: una dirección IP, un parámetro índice (Security Parameter Index SPI) y el identificador del protocolo de seguridad (AH o ESP).

Hay dos tipos de SA's definidos:

a. Modo Transporte -- es una asociación de seguridad entre dos servidores. En el caso de utilizar ESP, este modo proporciona servicios de seguridad solo para protocolos de capas superiores, no para la cabecera IP o otras cabeceras que precedan a la cabecera propia de ESP. En el caso de utilizar AH, la protección se extiende sólo a algunas partes de la cabecera IP, alguna parte seleccionada de otras cabeceras y opciones seleccionadas previamente.

b. Modo Túnel -- es esencialmente una SA aplicada a un túnel IP. Una SA entre dos pasarelas de seguridad es siempre un modo túnel, como también una SA entre un servidor y una pasarela de seguridad. El único requisito para cada SA, involucra que la pasarela de seguridad sea un túnel, ya que se presentan problemas con la fragmentación y reagrupación de los paquetes IPsec. En este modo aparecen dos cabeceras IP en cada paquete, la exterior (que especifica la procedencia del paquete) y la interior (que especifica la aparentemente última dirección para el paquete). Si se utiliza AH, partes de la cabecera exterior son protegidas, y las capas de protocolos superiores. Si se utiliza ESP, la protección no afecta a la cabecera exterior, sólo al paquete del túnel.

Un servidor puede soportar juntos los dos modos, pero una pasarela de seguridad requiere sólo modo túnel. Aunque una pasarela si tiene que soportar modo transporte sólo puede ser utilizada cuando la pasarela está actuando como un servidor.

4.2 Funcionalidad de las Asociaciones de seguridad

El conjunto de los servicios de seguridad ofrecidos por una SA dependen de la seguridad del protocolo seleccionado, del modo de SA, de los puntos de terminación de la SA y de la elección de los servicios opcionales del protocolo.

AH ofrece un servicio adicional anti-eco para el receptor, mediante el cual se protege de los ataques. Es un protocolo apropiado cuando la no se necesita confidencialidad (o no está permitida). Al proporcionar autenticación para partes seleccionadas de la cabecera de IP es necesaria en varios contextos.

ESP puede opcionalmente proveer confidencialidad al tráfico de paquetes, que siempre dependerá de lo bueno que sea el algoritmo de encriptación que se utilice. También puede proporcionar autenticación. Si sólo se necesita autenticar los protocolos de capas superiores es más eficiente (en cuanto al espacio) ESP que AH.

Siempre se tiene que elegir uno de estos dos protocolos para la SA.

4.3 Asociaciones de Seguridad combinadas

Los datagramas IP transmitidos por una SA sólo pueden estar protegido por un protocolo, AH o ESP, pero no ambos. El término SA Bundle se aplica a una secuencia de SA's que satisfacen una política de seguridad, y siguen un orden preestablecido por esa política.

Las SA se pueden combinar dentro de SAB's de dos formas:

a. Transporte de Adyacencia (Transport Adjacency) -- aplicar más de un protocolo de seguridad al mismo datagrama IP, sin invocar un túnel. Sólo admite un nivel de combinación.

```
Serv 1 -- Seguridad -- Internet -- Seguridad -- Serv 2
| |           Gwy 1           Gwy 2           | |
```

```

| |
| ----- Asociación de Seguridad 1 (ESP trans)----- |
|
|----- Asociación de Seguridad 2 (AH trans)----- |

```

b. Iterated Tunneling -- es una aplicación para múltiples capas de protocolos de seguridad en el túnel IP. Desde cada túnel se puede originar o terminar en diferentes sitios de IPsec a lo largo del camino.

Hay tres casos de Iterated Tunneling:

1. Los dos puntos terminales de las SA's son el mismo: cada túnel, interior y exterior, puede tener un protocolo diferente (AH o ESP).

```

Serv 1 -- Seguridad -- Internet -- Seguridad -- Serv 2
| |          Gwy 1          Gwy 2          | |
| |
| ----- Asociación de Seguridad 1 (túnel)----- | |
|
|----- Asociación de Seguridad 2 (túnel)-----

```

2. Uno de los dos puntos terminales de las SA's son el mismo: El túnel interior y el exterior pueden tener cualquiera de los dos protocolos AH o ESP.

```

Serv 1 -- Seguridad -- Internet -- Seguridad -- Serv 2
| |          Gwy 1          Gwy 2          |
| |
| ----- Asociación de Seguridad 1 (túnel)--      |
|
|----- Asociación de Seguridad 2 (túnel)-----

```

3. Ninguno de los dos puntos terminales coinciden: Tanto el túnel interior como el exterior pueden tener diferentes protocolos.

```

Serv 1 -- Seguridad -- Internet -- Seguridad -- Serv 2
|          Gwy 1          Gwy 2          |
|          |              |              |
|          ----- Asociación S 1 (túnel)----      |
|
|----- Asociación de Seguridad 2 (túnel)-----

```

4.4 Bancos de Datos de las Asociaciones de seguridad

Alguno de los detalles asociados a el procesamiento del tráfico IP en la implementación de IPsec puede llegar a ser un problema, porque no está sujeto a una estandarización.

Nos encontramos con dos tipos de Bases de Datos, los Bancos de Datos de la Política de Seguridad (Security Policy Database SPD) y las Bases de Datos de las SA's (SAD). Vamos a especificar la política que determina la disposición del tráfico IP (entrante y saliente)de un servidor, de una pasarela de seguridad, o de la implementación BITS o BITW de IPsec a continuación.

4.4.1 Bases de Datos de la Política de Seguridad (SPD)

En el procesamiento de una SA el elemento esencial es la política de seguridad de bases de datos, que especifica qué servicios tienen que ser ofrecidos por los datagramas IP, y en de qué modo. La SPD debe consultar durante el procesamiento de todo el tráfico (entrante y saliente), incluyendo el tráfico que no sea IPsec.

SPD discrimina de entre el tráfico, el que tiene que ser protegido por IPsec, el que se tiene que dejar pasar sin proteger y el que se va a descartar. La protección de IPsec se aplica desde el emisor hasta el destinatario.

Para cada implementación de IPsec debe haber un interfaz administrador que permita al usuario o al sistema administrador manejar la SPD. Específicamente, cada paquete entrante o saliente está sujeto a un procesamiento de IPsec, en el cual la SPD va a especificar qué acción se ha de seguir en cada caso.

En los sistemas servidores, las aplicaciones pueden seleccionar que procesamiento de seguridad va a ser aplicado al tráfico generado y consumido. En cambio, en los sistemas administradores deben de especificar tanto si un usuario o una aplicación pueden sobrescribir los SPD's por defecto.

SPD contiene una lista de políticas de entrada, cada política de entrada está cerrada por uno o más selectores que se definen en el conjunto del tráfico IP abarcado por la misma política de entrada. Cada entrada incluye una indicación de lo que le corresponde entre ser descartado, procesado o dejado pasar. Si se aplica IPsec, la entrada incluirá la especificación de un SA (o SA Bundle), los protocolos, modos, y algoritmos que van a ser implementados.

Si se especifica ESP, puede que la autenticación o la encriptación estén omitidas, puede ser debido a que al configurar los valores de la SPD estos valores estuvieran a NULL. Sin embargo al final uno de estos servicios debe ser seleccionado, porque no es posible configurarlos todos a NULL.

SPD puede ser usada para planificar el tráfico específico de SA's o SA's Bundles. Por ello, SPD requiere que cuando mas de un SA es aplicado a un conjunto de tráfico, en orden específico, la política de entrada debe preservar ese orden establecido.

La SPD se usa para controlar el flujo de todo el tráfico del sistema IPsec, incluyendo la seguridad del manejo de claves del tráfico desde y hasta los extremos de la pasarela de seguridad.

4.4.2 Selectores

La granularidad de una SA o SAB, depende de los selectores que definen el conjunto para el tráfico de SA. Los siguientes parámetros de selección deben soportar el manejo de una SA para facilitar el control de la granularidad de SA.

a. Dirección de Destino IP -- puede ser una única dirección IP (unicast, multicast, broadcast). Se requiere en todas la implementaciones. Este selector es diferente del campo del mismo nombre de la tupla que identifica una SA (<dir Dest IP, IPsec Prot, SPI>).

b. Dirección de Origen IP -- puede ser una única dirección IP (unicast, multicast, broadcast) o un rango de direcciones. Se requiere en todas la implementaciones.

c. Name -- se dan dos casos:

1. ID usuario - puede ser un nombre cualificado (DNS) o un nombre diferenciado de la X.500. Se requiere en el caso de que sea un servidor nativo de implementación, o en las implementaciones de BITS o BITW que sólo tienen un usuario, o en las implementaciones de pasarelas de seguridad par el tráfico entrante.

2. Nombre del Sistema (servidor, pasarela de seguridad,...) - puede ser un nombre cualificado (DNS) o un nombre diferenciado de la X.500, o un nombre general de la X.500. Se requiere para todas las implementaciones.

d. Nivel de Datos Sensibles (Data Sensitivity Level) -- son los campos IPSO/CIPSO, y es opcional para todos los sistemas.

e. Capa de Transporte de Protocolo (Transport Layer Protocol) -- Puede ser un número único de protocolo. Se requiere para todas las implementaciones.

f. Puertos de Origen y Destino -- éstos van pueden ser los mismos que para UDP o TCP. En el caso de que los trate ESP puede que no estén disponibles, por la cabecera ESP.

Si el paquete ha sido fragmentado, el puerto no puede ser accesible en el fragmento actual, por eso de descarta el fragmento.

4.4.3 Bases de Datos de las Asociaciones de Seguridad (SAD)

En cada implementación de IPsec hay una única SAD, que en cada entrada define los parámetros asociados a una SA. Para el tráfico entrante cada entrada en la SAD se identifica por una tupla <dir Dest IP,IPsec Prot, SPI> donde cada campo viene definido por:

1. Dirección de Destino IP -- es la dirección de origen del paquete IP.

2. Protocolo IPsec -- AH o ESP, usado para identificar a la SA en la base de datos. Especifica el protocolo de IPsec que va a ser aplicado en el tráfico de esa SA.

3. SPI -- son 32 bits, que se usan para distinguir diferentes SA's con la misma terminación y que utilizan el mismo protocolo.

Los siguientes parámetros están asociados para cada entrada en la SAD:

a. Contador de Secuencia (Sequence Number Counter) - son 32 bits, que se usan para generar el número de secuencia de la cabecera AH o ESP.

b. Indicador de Desbordamiento (Sequence Counter Overflow) - indica cuando se he producido un desbordamiento en el contador de secuencia.

c. Ventana anti-eco (anti-replay window) - son 32 bits usados para determinar cual de los protocolos es el de respuesta.

d. AH algoritmo de autenticación, claves, ...

e. ESP algoritmo de encriptación, claves, modo, ...

f. Tiempo de vida de la SA - es el intervalo de tiempo en el que se va a mantener la SA actual antes de cambiarla una nueva SA.

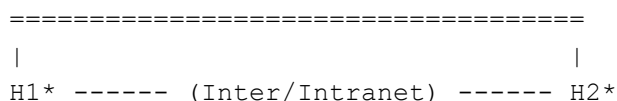
g. Modo del protocolo IPsec - túnel, transporte o wildcard. Indica el modo en que AH o ESP van a ser aplicados al tráfico de la SA. Si el campo es "wildcard", será la aplicación la encargada de especificar el modo de protocolo.

h. Path MTU

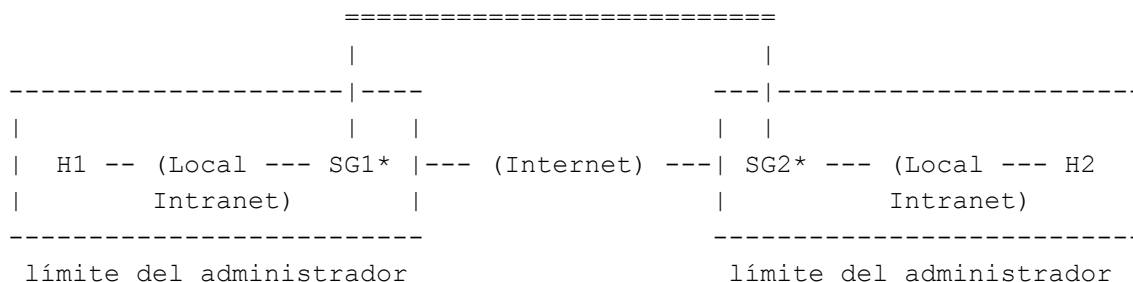
4.5 Combinaciones básicas de las Asociaciones de Seguridad

Los casos básicos son los siguientes:

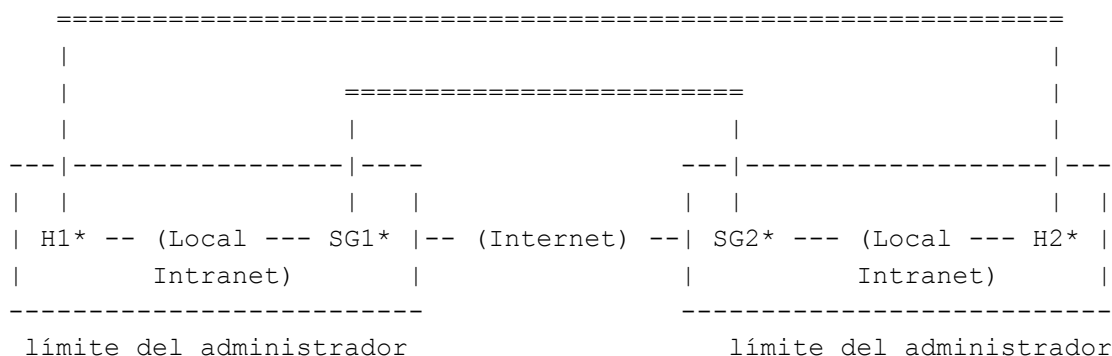
Caso 1. Se provee de seguridad "end-to-end" entre dos servidores através de internet (o una Intranet).



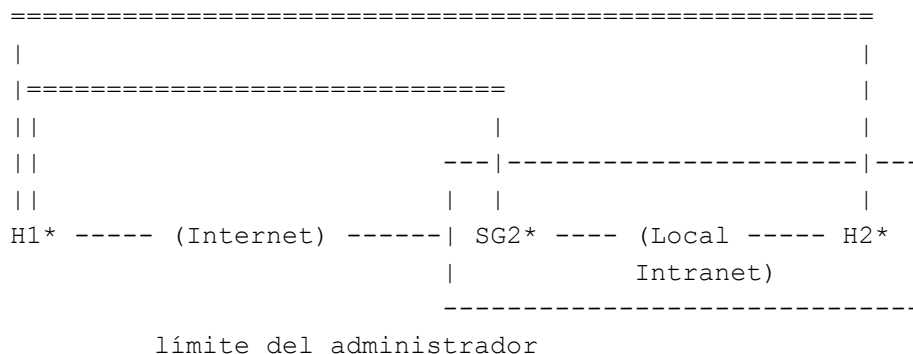
Caso 2. Soporte para una red privada.



Caso 3. Combina el caso 1 y el caso 2, añadiendo seguridad "end-to-end" entre el emisor y el receptor.



Caso 4. Cubre la situación en que un servidor remoto H1, usa internet para alcanzar un cortafuegos (SG2) y tener acceso a otro servidor H2.



La leyenda para todos los casos es la misma:

===== = una o más SA's

---- = conexión

Hx = servidor x

SGx = pasarela de seguridad x
X* = X soporta IPsec

4.6 SA y Manejo de claves

IPsec soporta el manejo de claves automático y manual para SA y su encriptación. Los dos protocolos pertenecientes a IPsec son totalmente independientes de estas técnicas, aunque las técnicas invocadas pueden afectar a la seguridad ofrecida por ambos protocolos. Además, la granularidad de la distribución de claves empleada con IPsec determina la granularidad de la autenticación proporcionada.

En general, la autenticación de los datos originales en AH y ESP está limitada por los secretos del algoritmo de encriptación, y el manejo de claves, que son compartidas por múltiples fuentes.

4.6.1 Técnicas manuales

Es la más simple de las técnicas, en la que una persona configura manualmente cada sistema con claves y SA aplicables para asegurar la seguridad de comunicación con otros sistemas. Estas técnicas manuales se utilizan en entornos pequeños y estáticos.

En estos sistemas, no todo el tráfico se puede proteger, cierto tráfico seleccionado será al que se le proporcione seguridad.

Las técnicas manuales a menudo emplean configuraciones estáticas y claves simétricas.

4.6.2 SA automatizadas y el Manejo de claves

Está muy extendido que para el manejo de IPsec se necesita un Internet estandarizado y automatizado y con protocolos manejadores de SA's. Este soporte se requiere para facilitar el anti-eco, rasgo característico de los protocolos AH y ESP, y la creación de SA's según la demanda.

El protocolo manejador de claves por defecto seleccionado cuando se usa IPsec es IKE, bajo el dominio de IPsec y su interpretación. Otros protocolos manejadores de claves pueden ser también empleados siempre que se ajusten a los requerimientos de IPsec.

Cuando un protocolo automático para manejar claves y SA está trabajando, la salida de este protocolo se suele usar para generar múltiples claves, que se necesitan porque:

- a. los algoritmos de encriptación utilizan múltiples claves.
- b. el algoritmo de autenticación utiliza múltiples claves.
- c. juntos los puntos a y b se benefician de esta generación de múltiples claves.

El sistema de manejo de claves proporciona un vector de bits para cada clave, o puede generar un vector de bits para extraer cada clave. Si se proporciona un solo vector hay que tener cuidado porque también se necesitan las partes en las que se descomponen cada clave para el SA.

Para asegurar que la implementación de IPsec al inicio y al final utiliza los mismos bits para extraer las mismas claves, la clave de encriptación debe ir en los primeros bits y la de autenticación debe ir en los últimos bits. El número de bits para cada clave está definido específicamente en su propia RFC.

En el caso de utilizar múltiples claves de encriptación o múltiples claves de autenticación, el

algoritmo debe especificar en qué orden deben ser seleccionadas del vector de bits proporcionado por el algoritmo generador.

4.6.3 Encontrando una pasarela segura

Considerando la situación en la que un servidor remoto H1, usa internet para acceder a otro servidor H2 en una pasarela segura, nos encontramos frente a varias cuestiones:

- a. ¿Cómo H1 conoce la existencia de una pasarela segura?
- b. ¿Cómo puede autenticarse la pasarela como segura para representar a H2?
- c. ¿Cómo puede autenticar la pasarela a H1 y verificar que H1 está autorizado para contactar con H2?
- d. ¿Cómo puede conocer H1 las pasarelas que le proporcionarán camino hasta H2?

Para responder a estas preguntas, un servidor debe tener un interfaz administrador para configurar la dirección de la pasarela de seguridad para todos los destinos que la requieran. Esto incluye la configuración de:

1. La información para localizar la autenticación de la pasarela segura y verificación de que está autorizado para representar al servidor.
2. La información para localizar la autenticación de cualquier pasarela segura y verificar la autorización de representar el servidor destino para cada pasarela.

Así, asumimos que la SPD está configurada para cubrir toda la información que se requiere para los caminos de pasarelas y servidores.

4.7 Asociaciones de seguridad y Multicast

En el caso de dirección de destino multicast en una SA implica que el valor del SPI configurado manualmente puede resultar conflictivo al encontrarse con otro generado mecánicamente.

Por eso muchos de los sistema necesitan coordinar todos los grupos de multicast para seleccionar un SPI o varios, para asegurar la legitimidad de los miembros de cada grupo multicast, con unos mecanismos que no vamos a definir.

Un multicast emisor debe usar una sola SA para todo su tráfico cuando se utiliza una clave de encriptación simétrica o los algoritmos de autenticación van a ser utilizados. En estas circunstancias el receptor sólo conoce que el mensaje viene de parte de un sistema que posee la clave del multicast único. Normalmente el receptor no puede autenticar qué grupo multicast envió el mensaje.

A estos grupos multicast le suelen pertenecer pocos miembros, así los algoritmos modificados de técnicas manuales de claves para unicast son factibles. Pero para grupos muy grandes estas técnicas se quedan obsoletas.

5. Trafico procesado por IP

Todos los algoritmos criptográficos usados en IPsec transmiten en un riguroso orden, y reciben en un orden estricto. Así todos los paquetes IP son transmitidos a la red en el mismo orden.

5.1 Tráfico saliente de IP

5.1.1 Seleccionando y Usando un SA o SA Bundle

En una pasarela de seguridad o en una implementación BITW (y en algunas implementaciones BITS) cada paquete saliente es comparado por SPD para determinar qué tipo de acción se ha de llevar a cabo sobre él. Si el paquete se deja pasar sin tocar, éste sigue su camino sin que le importe que IPsec esté presente o no. Si IPsec es requerido, el paquete será enviado al SA, o SAB, o se creará un nuevo SA o SAB para el paquete. Desde que el paquete llega y se tiene que procesar, IPsec debe:

1. Hacer coincidir los selectores del paquete con los de la SPD para el tráfico saliente, para localizar la política apropiada.
2. Hacer coincidir los campos de los selectores del paquete con los del SAB, para saber a qué clase de SAB se corresponde. Si no corresponde a ninguno, se crea un SAB apropiado para él, y se introduce junto con las otras entradas en la SAD. Si no se encuentra un manejador de claves apropiado el paquete se desecha.
3. Usar el SAB encontrado o creado para procesar el paquete.

En un servidor implementado basado en sockets, la SPD se consulta cuando se crea un nuevo socket para determinar el proceso de IPsec que se le tendrá que aplicar al tráfico que fluirá por dicho socket.

5.1.2 Header Construction para el Modo Túnel

La idea general es IP encapsulado con IP, que viene de la RFC 2003:

1. La cabecera exterior identifica los puntos de terminación del túnel. La cabecera interior identifica los originales emisores y receptores del datagrama.
2. La cabecera interior no cambia ningún valor excepto el campo TTL, y permanece intacto mientras viaja por el túnel.
3. Las opciones de IP o extensiones de la cabecera en la cabecera interior no cambian durante el procesamiento del paquete en el túnel.
4. Si se necesita, otra cabecera de protocolo como la de IP de autenticación puede ser insertada entre las cabeceras exterior e interior IP.

5.1.2.1 IPv4--Header Construction para el Modo Túnel

Cab Ext	Cab Int	
	Encapsulación	Decapsulación
Campos Cabecera:	-----	-----
version	4 (1)	no cambia
header length	construido	no cambia
TOS	copied from inner hdr (5)	no cambia
total length	construido	no cambia
ID	construido	no cambia
flags (DF, MF)	construido, DF (4)	no cambia
fragmt offset	construido	no cambia

TTL	construido (2)	decrementa (2)
protocolo	AH, ESP, routing hdr	no cambia
checksum	construido	construido (2)
src address	construido (3)	no cambia
dest address	construido (3)	no cambia
Opciones	nunca copiadas	no cambia

1. La versión IP en la cabeza encapsulada puede ser diferente del valor existente en la cabecera interna.

2. El campo TTL en la cabecera interna se va decrementando por la encapsulación y por la decapsulación si reenvía el paquete.

3. Las direcciones de destino y origen dependen del SA, y se usan para determinar el destino en caso de que haya que reenviar el paquete.

4. La configuración determina cómo copiar de la cabecera interior (sólo en IPv4), o cómo poner a cero o a uno el bit DF.

5. Si la cabecera interior es IPv4 (protocolo 4), copia el campo TOS. Si la cabecera interior es IPv6 (protocolo 41) planifica el campo Class con el campo TOS.

5.1.2.2 IPv6--Header Construction para el Modo Túnel

Cab Ext	Cab Int	
	Encapsulación	Decapsulación
Campos Cabecera:	-----	-----
version	6 (1)	no cambia
class	copiado o configurado (6)	no cambia
flow id	copiado o configurado	no cambia
len	construido	no cambia
next header	AH,ESP,routing hdr	no cambia
hop limit	construido (2)	decrementa (2)
src address	construido (3)	no cambia
dest address	construido (3)	no cambia
ón Cab	nunca copiado	no cambia

6. Si la cabecera interior es IPv4 (protocolo 4), planifica el campo TOS con el campo Class. Si la cabecera interior es IPv6 (protocolo 41) copia el campo Class.

5.2 Tráfico entrante a IP

Antes de ejecutar AH o ESP, se reagrupan todos los fragmentos del paquete IP. Cada datagrama IP entrante que necesita procesamiento IPsec, se identifica porque aparecen los valores de AH o ESP en el campo "IP Next Protocol" .

5.2.1 Seleccionando y Usando un SA o SA Bundle

Planificando el datagrama IP para la apropiada SA se simplifica por la presencia del SPI dentro de la cabecera AH o ESP. Este selector está en la cabecera interior.

Los pasos seguidos son:

1. Usar la dirección de destino del paquete ubicada en la cabecera exterior del protocolo IPsec, y el SPI para buscar el SA de la SAD. Si la búsqueda falla, el paquete se deshecha y se devuelve un error.
2. Usar la SA encontrada en el 1 para empezar a procesar con IPsec. Este paso incluye hacer corresponder los selectores del paquete con los de la SA. En general, la dirección de destino debe corresponder con un selector de la SA.
3. Encontrar la política de entrada en la SPD que le corresponda al paquete.
4. Comprobar el procesamiento indicado por el paquete que tiene que ser aplicado por IPsec.

Después de estos pasos, se pasa el paquete resultado a la capa de transporte para enviar el paquete.

6. Procesamiento ICMP relativo a IPsec

El tráfico ICMP no relativo a seguridad se debe tratar exactamente igual a como se hacía anteriormente y puede ser protegido en una base “end-to-end” usando SAs como se ha ido haciendo hasta ahora.

Un mensaje de error ICMP protegido por AH o ESP generado por un router debe ser procesado y dirigido a un túnel tipo SA. La política local debe determinar si va a ser subordinado a la dirección fuente detectada por el router. Cabe resaltar que si el router del fin del túnel que se está generando está conduciendo un mensaje ICMP de error de otro router, la comprobación de dirección fuente fallará.

Un mensaje ICMP generado por un host debe ser comprobada en los “source IP address selectors” unidos al SA cuando el mensaje llega. Esto es así porque aunque se haya autenticando el origen del mensaje de error ICMP, la cabecera IP devuelta puede ser no válida. Por ello se comprueba.

Un mensaje ICMP no protegido por AH o ESP no es autenticado y su procesamiento y/o direccionamiento resulta en una negación del servicio. A pesar de ello, es posible que algunos routers no tengan implementado Ipsec, conllevando esta contingencia en el descarte de varios mensajes. El resultado es que varias funciones críticas de IP se pierdan. Por ello debe ser posible configurar Ipsec para aceptar o rechazar el tráfico de estos routers siguiendo una política local determinada.

6.1 Bit de No Fragmentación (DF)

En algunos casos cuando un sistema (host o gateway) añade una cabecera encapsulada (túnel ESP o AH), debe permitir la opción de copiar el bit DF del paquete original a la cabecera encapsulada (y procesar los mensajes ICMP PMTU). Esto significa que debe ser posible configurar el tratamiento que ofrece el sistema del bit DF en cada uno de las interfaces.

6.2 Path MTU (PMTU)

ICMP PMTU se emplea aquí para referirnos a un mensaje ICMP para:

Ipv4 (RFC 792)

- Type=3 (Destino inalcanzable)
- Code=4 (Se necesita fragmentación y DF a ‘1’)
- El próximo salto MTU en los bits de menor peso de la segunda palabra, con los 16 bits de mayor

pesos son puestos a '0'

Ipv6 (RFC 1885)

- Type=2 (Paquete demasiado grande)
- Code=0 (Se necesita fragmentación)
- El próximo salto MTU en los 32 bits del campo MTU en el mensaje ICMP6.

6.1.2.1 Propagación de PMTU

La cantidad de la información devuelta con el mensaje ICMP PMTU está limitada y esto afecta a la cantidad de selectores que están disponibles en la posterior propagación de información PMTU.

-Mensajes PMTU con cabecer Ipv6 de 64 bits. Si el mensaje ICMP PMTU contiene solo 64 bits de cabecera Ipv6 (mínimo para Ipv4), entonces un gateway de seguridad debe soportar las siguientes opciones en su base SPI/SA.

a. Si el host generador puede ser determinado (o las posibles fuentes englobadas en un número que se pueda tratar), hay que enviar la información PM a todos los posibles hosts generadores.

b. Si el host generador no puede ser identificado, se debe almacenar la PMTU con el SA y esperar hasta que el próximo paquete llegue para llegar a la asociación de seguridad. Si el paquete es más grande que la PMTU, deja el paquete y compone un(os) mensaje(s) ICMP PMTU con el(los) nuevo(s) paquete(s) y la actualizada PMTU, y envía el(los) mensaje(s) ICMP sobre el problema al mensaje generador. Retiene la información PMTU para cualquier mensaje que pueda llegar después.

-Mensajes PMTU con más de 64 bits de cabecera IPsec. Si el mensaje ICMP contiene más información del paquete original, entonces debe haber suficiente información no opaca como para determinar que host propagó el mensaje ICMP/PMTU y proporcionar qué sistema necesita almacenar y actualizar la PMTU. Se deben suministrar los cinco campos (direcciones origen y destino, puertos origen y destino y el protocolo empleado). Algunas veces, un gateway de seguridad debe generar un mensaje ICMP PMTU inmediatamente para asentar la ruta.

-Distribuyendo la PMTU a la capa de transporte. El mecanismo que emplea el host para proporcionar la PMTU actualizada no ha sido cambiada como está especificado en la RFC 1191 (Path MTU Discovery).

6.1.2.2 Cálculo de la PMTU

El cálculo de la PMTU desde un mensaje ICMP PMTU debe tener en cuenta la adición de la cabecera Ipv6.

En algunos casos, esta adición, puede resultar en una PMTU efectiva demasiado pequeña. Para evitar este problema, la implementación debe establecer que se aplique Ipv6 y después se fragmente el paquete resultante de acuerdo con la PMTU. De este modo se aprovecha mejor el ancho de banda.

6.1.2.3 Granularidad en el proceso de PMTU

En un host se pueden dar las siguientes situaciones respecto a PMTU:

- a. Integración de Ipv6 en la implementación IP nativa.
- b. Bump-in-the-stack. Cuando Ipv6 ha sido implementado por debajo de una implementación existente de una pila de protocolos TCP/IP.
- c. Sin implementación Ipv6.

Solo en el caso a. se puede mantener la misma granularidad en las asociaciones de comunicación. En b y c, la capa IP solo puede mantener los datos PMTU en la granularidad de las direcciones IP de origen y destino como se describe en la RFC 1191.

La implementación del calculo de la PMTU y el soporte de PMTUs en la granularidad del asociación de comunicación individual es un problema local. Además, una implementación basada en sockets de Ipsec en un host debería mantener la información en la base del socket.

6.1.2.4 PMTU y el paso del tiempo

En todos los sistemas (host o gateway) que implementen Ipsec y que mantengan la información PMTU, la PMTU asociada a una asociación de seguridad (transporte o túnel) debe ser fechada y algún mecanismo debe actualizar la PMTU cada cierto tiempo. La PMTU debe permanecer el tiempo suficiente como para que el paquete llegue al destino y que se puedan tratar los mensajes ICMP de error.

Los sistemas deben seguir las directrices descritas en la RFC 1191 (Path MTU Discovery) en su sección 6.3, que sugieren la reanudación de la PMTU en el primer salto.

7. Uso en Sistemas de seguridad sobre el flujo de información

La información de diferentes niveles de importancia puede ser transportada a través de una red. El uso de etiquetas facilita la segregación de la información, para ayudar a los sistemas de seguridad de flujos de datos. Los modelos, y su correspondiente tecnología de soporte, son diseñados para prevenir flujos no autorizados de información de sensibilidad, como podría ser el caso de los ataques de caballos de Troya. Los mecanismos convencionales DAC (Discretionary Access Control) no son suficientes para mantener estas políticas y estas características.

En un contexto militar, la tecnología que permite estos modelos es conocida como Multi-Level Security (MLS). Computadores y redes son a veces clasificados como "seguros a multi-nivel" y se soportan la separación de datos etiquetados en consonancia con las políticas de seguridad de flujos de información.

Los mecanismos Ipsec pueden soportar las redes MLS. Este tipo de redes requiere el uso de fuertes Mandatory Access Controls (MAC), que usuarios no privilegiados o procesos no pueden violar.

AH puede usarse para proveer de fuerte autenticación para ayudar a las decisiones MAC. Si información explícitamente sensible se usa confidencialmente no se considera necesario en el entorno operativo, AH puede usarse para relacionar las etiquetas en la cabecera IP y los datos. Toda la información explícitamente de sensibilidad debe ser autenticada usando ESP, AH o los dos.

La encriptación es útil y puede ser deseable cuando todos los host se encuentran en entorno protegido. ESP puede usarse junto con un manejo correcto de las claves y algoritmos de encriptación para soportar tanto DAC como MAC.

El manejo de claves puede hacer uso de información de sensibilidad para proveer MAC. La implementación de sistemas que demanden MLS deben ser capaces de usar Ipsec para proporcionar MAC en comunicaciones basadas en IP.

7.1 Relación entre las Asociaciones de Seguridad y los Datos sensibles

Ambas, ESP y AH pueden ser combinadas con apropiadas asociaciones de seguridad para proveer redes MLS. En este caso cada asociación se usa normalmente para una sola instancia de información

de sensibilidad.

7.2 Comprobación de la sensibilidad de los Datos

Una implementación MLS (host o router) debe asociar información de sensibilidad, o un rango de información de sensibilidad con una interface, o una dirección IP configurada con su prefijo asociado. Si tales propiedades existen, una implementación debe comparar la información de sensibilidad asociada con el paquete con la información de sensibilidad asociada a la interface o la dirección/prefijo desde la que el paquete ha llegado o desde el paquete puede ser suministrado. Esta comprobación debe verificar que las sensibilidades concuerdan o que esta sensibilidad concuerda con el rango de la interface o dirección/prefijo.

7.3 Atributos adicionales de MLS para los Bancos de Datos de Asociaciones de Seguridad

La información de sensibilidad ayuda a la selección de algoritmos apropiados y a claves fuertes, por ello el tráfico consigue un nivel de protección apropiado para su importancia y sensibilidad.

7.4 Procesamiento del flujo entrante de MLS

Después de que un paquete de entrada ha pasado por el procesamiento Ipsec, una implementación MLS debe primero comprobar la sensibilidad del paquete con la interface o la dirección/prefijo antes de enviar el datagrama al protocolo superior o el mecanismo de direccionamiento.

El sistema MLS debe retener la unión entre los datos recibidos en el paquete protegido por Ipsec y la información de sensibilidad en la SA o las SAs usadas para el procesamiento, para ello se deben emplear políticas apropiadas dependientes de la implementación.

7.5 Procesamiento del flujo saliente a MLS

Una implementación MLS de Ipsec debe realizar dos comprobaciones adicionales además de los pasos habituales. Cuando se consulte SPD o la SAD para encontrar la SA de salida, la implementación MLS debe usar la sensibilidad de los datos para seleccionar una SA o SAs de salida. La segunda comprobación viene antes del direccionamiento del paquete a su destino, y es la comprobación de la consistencia de la sensibilidad descrita en la sección 8.2

7.6 MLS Procedimiento adicionales para las Pasarelas de Seguridad

Una pasarela MLS debe seguir los procesamientos de entrada y salida anteriores y algunos mecanismos adicionales.

Estas pasarelas deben actuar como un proxy de entrada, creando SAs para sistemas MLS que generan paquetes dirigidos por la pasarela. Estos sistemas MLS deben etiquetar explícitamente los paquetes para ser direccionados o la globalidad del sistema debe tener características relativas a la sensibilidad que permitan este direccionamiento. La pasarela debe crear y usar SAs apropiadas para AH, ESP o los dos, para proteger el tráfico que direcciona.

De forma similar, esta pasarela de seguridad acepta y procesa paquetes de AH y/o ESP de entrada y los direcciona apropiadamente, usando un etiquetado de paquetes explícito o debe confiar en las características de sensibilidad que posea la red de destino.

8. Referencias

[HC98] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, Noviembre 1998.

[KA98a] Kent, S., y R. Atkinson, "IP Authentication Header", RFC 2402, Noviembre 1998.

[KA98b] Kent, S., y R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, Noviembre 1998.

[MSST97] Maughan, D., Schertler, M., Schneider, M., y J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, Noviembre 1998.

[Orm97] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, Noviembre 1998.

[Pip98] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, Noviembre 1998.

[TDG97] Thayer, R., Doraswamy, N., y R. Glenn, "IP Security Document Roadmap", RFC 2411, Noviembre 1998.