Grupo de Trabajo en Red — S. Kent
Request for Comments: 2401 — BBN Corp
Obsoleto: 1825 — R. Atkinson
Categoría: Pila de estándares — @Home Network
Noviembre 1998

Traducción al castellano: Agosto 2005
Hugo Adrian Francisconi <adrianfrancisconi@yahoo.com.ar>

Arquitectura de Seguridad para el Protocolo Internet

Status de este memorándum

Este documento especifica un protocolo de Internet en vías de estandarización para la comunidad de Internet y solicita debate y sugerencias para mejorarlo. Por favor, remítase a la edición actual de "Estándares de Protocolos Oficiales de Internet" (STD 1) para conocer el estado de estandarización y status de este protocolo. La distribución de este memorándum es ilimitada.

Aviso De Copyright

1 Introducción

1.1 Contenido del documento

Este documento especifica la estructura fundamental de IPsec. La meta de la arquitectura es proporcionar diversos servicios de seguridad para el tráfico en la capa IP, en ambientes IPv4 e IPv6. Este documento describe las metas de tales sistemas, sus componentes y cómo estos se adaptan en el ámbito IP. Este documento también describe el servicio de seguridad proporcionado por los protocolos IPsec, y como estos servicios se pueden emplear en ambientes IP. Este documento no trata todos los aspectos de la arquitectura IPsec. Documentos siguientes se ocuparán de detalles arquitectónicos adicionales de naturaleza más avanzada, por ejemplo, uso de IPsec en ambientes NAT y soporte más completo para multicast. Los siguientes componentes fundamentales de la arquitectura de IPsec se discuten en términos de la funcionalidad subyacente requerida. RFCs adicionales (véase la Sección 1.3 que comenta otros documentos) definen los protocolos (a), (c), y (d).

a. Protocolos de seguridad: Cabecera de Autentificación AH (Authentication Header) y Carga de Seguridad Encapsulada, ESP (Encapsulating Security Payload).
b. Asociaciones de Seguridad SA: que son, como funcionan, como se administran, y como se procesan.
c. Manejo de claves: en forma manual y automática (Intercambio de Claves en Internet, IKE).
d. Algoritmos para autentificación y encriptación.

Este documento no es una arquitectura global de seguridad para Internet, solo se ocupa de la seguridad en la capa IP, proporcionando un uso combinado de mecanismos criptográficos y de protocolos de seguridad.

1.2 Audiencia

La audiencia de este documento incluye a implementadores de esta tecnología de seguridad IP y a los interesados que quieran un conocimiento profundo del sistema. En particular, los usuarios

potenciales de esta tecnología (los usuarios finales o los administradores de sistema) son parte de la audiencia. Un glosario es proporcionado como apéndice para comprender el vocabulario. Este documento asume que el lector esta familiarizado con el Protocolo Internet (IP), la tecnología relacionada a redes, los términos y conceptos generales de seguridad.

Las palabras DEBE, NO DEBE, REQUERIDO, PODER, NO PODER, DEBERÍA, NO DEBERÍA, RECOMENDADO, PUEDE y OPCIONAL, cuando aparezcan en este documento, deben interpretarse como se describe en [Bra97].

1.3 Documentos Relacionados

Otros documentos proporcionan definiciones detalladas de algunos de los componentes de IPsec y de su interrelación. Los siguientes temas se incluyen en los RFCs siguientes:

a. Documento de Guía para IPsec (IP Security Document Roadmap) [TDG97]: un documento que proporciona las pautas para las especificaciones que se describen, los algoritmos de cifrado y de autentificación usados en este sistema.
b. Protocolos de seguridad: RFCs que describen la Cabecera de Autentificación (AH) [KA98a] y la Carga de Seguridad Encapsulada (ESP) [KA98b].
c. Algoritmos para autentificación y encriptación: un RFC separado para cada algoritmo.
d. Gestión automática de claves -- RFCs en "Intercambio de Clave en Internet (IKE)" [HC98], " Protocolo de Manejo de Claves y Asociaciones de Seguridad en Internet (ISAKMP)" [MSST97], "Protocolo de Determinación de Claves OAKLEY" [Orm97], y El Dominio de Interpretación de Seguridad IP en Internet para ISAKMP [Pip98].

2 Objetivos de Diseño

2.1 Metas/Objetivos/Requisitos/Problemas

IPsec está diseñado para proporcionar seguridad ínter-operable, de alta calidad, basada en criptografía tanto para IPv4 como para IPv6. El conjunto de servicios de seguridad ofrecidos incluye: control de acceso, integridad sin conexión, autenticación del origen de los datos, protección antireplay (una forma de integrabilidad parcial de la secuencia), confidencialidad (encriptación), y confidencialidad limitada del flujo de tráfico. Estos servicios se implementan en la capa IP, y ofrecen protección para este nivel y/o los niveles superiores.

Estos objetivos se llevan a cabo haciendo uso de dos protocolos de seguridad, la Cabecera de Autentificación (AH) y Carga de Seguridad Encapsulada (ESP), a través de procedimientos de manejo de claves criptográficas y protocolos. El conjunto de protocolos IPsec empleados en cualquier conexión, y la forma en que se emplean, serán determinados por la seguridad, y los requerimientos del sistema del usuario, aplicaciones y/o sitios o organizaciones.

Cuando estos mecanismos se implementan correctamente y se ejecutan, no afectan negativamente a los usuarios, hosts, y otros componentes de Internet que no empleen estos mecanismos de seguridad para la protección de su tráfico. Estos mecanismos están diseñados para ser independientes del algoritmo. Esta modularidad permite seleccionar diferentes conjuntos de algoritmos sin afectar a las otras partes de la implementación. Por ejemplo, grupos diferentes de usuarios pueden seleccionar grupos diferentes de algoritmos si se necesita.

Un conjunto de algoritmos se especifica para facilitar la interoperatibilidad en la Internet global. El uso de estos algoritmos, en conjunto con la protección del tráfico de IPsec, y los protocolos de manejo de claves, están constituidos para permitir el desarrollo de aplicaciones, sistemas y tecnología de seguridad criptográfica de alta calidad en la capa IP.

2.2 Observaciones y Advertencias

El grupo de protocolos IPsec y demás algoritmos asociados permiten proporcionar seguridad de alta calidad para el flujo de tráfico de Internet. Sin embargo, la seguridad ofrecida por estos protocolos depende en ultima instancia de la calidad de su implementación, que esta fuera del alcance de estos estándares. Además, la seguridad de un sistema informático o en una red es una función de muchos factores. IPsec solo es una parte de un sistema global de seguridad.

Por último, la seguridad proporcionada por el uso de IPsec dependerá bastante de diversos aspectos del ambiente operativo en el cual la implementación de IPsec se ejecuta. Por ejemplo, los defectos en la seguridad del sistema operativo, negligencia en la práctica de manejo de protocolos, etc., todo esto puede degradar la seguridad proporcionada por IPsec. Como se mencionó anteriormente, ninguna de estas características están dentro del alcance de estos o de otros estándares de IPsec.

3 Descripción del Sistema

Esta sección proporciona una descripción de cómo trabaja IPsec, los componentes del sistema, y como se adapta para proporcionar los servicios de seguridad descriptos anteriormente. La meta de esta

descripción es permitirle al lector "comprender" el proceso global del sistema, ver como se adaptan en el ambiente IP, y proporcionar el contexto para secciones posteriores de este documento, que describen cada uno de los componentes más detalladamente.

Una implementación de IPsec funciona en un host o en un security gateway (SG), proporcionando protección al tráfico IP. La protección ofrecida se basa en requerimientos definidos en el establecimiento de una "Base de Datos de Políticas de Seguridad" (SPD) y mantenidas por un usuario o administrador del sistema o por una aplicación funcionando dentro de las restricciones ya establecidas. En general, los paquetes se seleccionan para uno de tres modos de procesamiento basados en IP y la información de la cabecera de la capa de transporte (selectores, Sección 4.4.2) comparándolas con las entradas en la Base de Datos de Políticas de Seguridad (SPD). Cada paquete es un servicio de seguridad, descartado, desviado, o procesado, de acuerdo con las políticas aplicables en la base de datos identificadas por los selectores.

3.1 Que hace IPsec

IPsec proporciona servicios de seguridad en la capa IP permitiendo a un sistema seleccionar los protocolos de seguridad, determinar el/los algoritmo/s a utilizar para el/los servicio/s, y instaurar cualquier criptografía de clave requerida para proporcionar los servicios solicitados. IPsec se puede utilizar para proteger una o más "trayectorias" entre un par de hosts, o entre un par de security gateway, o entre un security gateway y un host. El término security gateway se utiliza a través de los documentos de IPsec para referirse a un sistema intermedio que implementa los protocolos IPsec. Por ejemplo, un router o un firewall implementando IPsec es un security gateway.

El conjunto de servicios de seguridad que puede proporcionar IPsec incluye: control de acceso, integridad sin conexión, autenticación del origen de los datos, protección antireplay (una forma de integridad parcial de la secuencia), Confidencialidad (encriptación), y confidencialidad limitada del flujo de tráfico. Estos servicios se proporcionan en la capa IP, y pueden ser utilizados por cualquier protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, BGP, etc.

El IPsec DOI también soporta negociación de compresión IP [SMPT98], motivado en parte por la observación de que cuando se emplea encriptación en IPsec, esta impide la compresión eficiente de los datos en los protocolos inferiores.

3.2 Como Trabaja IPsec

IPsec utiliza dos protocolos para proporcionar seguridad al tráfico: la Cabecera de Autentificación (AH) y la Carga de Seguridad Encapsulada (ESP). Ambos protocolos se describen más detalladamente en su RFCs respectivos [KA98a, KA98b].

- La Cabecera de Autentificación (AH) [KA98a]: Proporciona integridad sin conexión, autentificación del origen de datos, y un servicio opcional de protección antireplay.
- La Carga de Seguridad Encapsulada (ESP) [KA98b]: Puede proporcionar confidencialidad (encriptación), y confidencialidad limitada de flujo de tráfico. También puede proporcionar integridad sin conexión, autentificación del origen de datos, y un servicio de protección antireplay. (Uno u otro de estos servicios de seguridad debe ser aplicado siempre que se use ESP.)
- AH y ESP son instrumentos para el control de acceso, basados en la distribución de claves criptográficas y en el manejo de flujo de tráfico concerniente a estos protocolos de seguridad.

Estos protocolos pueden aplicarse solos o en conjunto con otros para proporcionar un conjunto de servicios de seguridad en IPv4 e IPv6. Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En modo transporte los protocolos proporcionan protección sobre todo a los protocolos de capa superiores; en modo túnel, los protocolos son aplicados a paquetes (a los que se hizo un túnel a través de IP). Las diferencias entre los dos modos se discuten en la Sección 4.

IPsec permite que el usuario (o el administrador de sistema) controle la granularidad [grado de modularidad de un sistema, cuanto mayor sea la granularidad, más personalizadle o flexible será el sistema] en la cual un servicio de seguridad es ofrecido. Por ejemplo, uno puede crear un único túnel encriptado y llevar todo el tráfico entre dos security gateway o un túnel encriptado separado se puede crear para cada conexión TCP entre cada par de hosts que se comunican a través de un gateways. La gestión de IPsec debe incorporar facilidades para especificar:

- Que servicios de seguridad se utilizar y en que combinaciones.
- La granularidad con la que se debe aplicar una determinada protección de seguridad.
- Los algoritmos usados para efectuar la seguridad basada en criptografía.

Debido a que estos servicios de seguridad usan valores secretos compartidos (claves criptográficas), IPsec se basa en un conjunto de mecanismos separados para que pongan estas claves en su sitio (las claves se utilizan para autentificación/integrabilidad y los servicios de encriptación). Este documento requiere soporte para la distribución manual y automática de claves. Especifica un acercamiento basado en clave publica (IKE -- [MSST97, Orm97, HC98]) para la gestión automática de claves, pero otras técnicas de distribución automatizada de claves pueden ser utilizadas. Por ejemplo, los sistemas basados en KDC tales como Kerberos y otros sistemas de clave pública tales como SKIP podrían ser empleados.

3.3 Donde Puede ser Implementado IPsec

Hay varias formas en las cuales se puede implementar IPsec, en un host o en conjunto con un router o un firewall (creando un security gateway). Algunos ejemplos frecuentes son:

a. Integrar IPsec en una implementación nativa IP. Requiere tener acceso al código fuente IP, y se puede aplicar tanto a host como a un security gateway.

b. "Puesto-en-la-Pila" (BITS), IPsec se implementa "por debajo" de una implementación existente de una pila IP, entre el IP nativo y los drivers locales de la red. El acceso al código fuente para la pila IP no es requerido en este contexto, este contexto es apropiado para los sistemas antiguos. Este método, cuando se adopta, se emplea generalmente en hosts.

c. El uso de un procesador criptográfico externo es una característica de diseño común de los sistemas de seguridad de red usados por los militares, y en algunos sistemas comerciales. A estos sistemas algunas veces se los refiere como implementaciones "Puesto-en-el-cable" (BITW). Tales implementaciones se pueden diseñar para asistir a un host o un gateway (o a ambos). El dispositivo BITW generalmente tiene una IP direccionable. Cuando asiste a un único host, puede resultar análogo a una implementación BITS, pero en un router o en un firewall debe funcionar como un security gateway.

4 Asociaciones de Seguridad

Esta sección define los requisitos para administrar Asociaciones de Seguridad (SAs) para toda implementación IPv6 y para implementaciones IPv4 que implemente AH, ESP, o ambos. El concepto de Asociación de Seguridad (SA) es fundamental para IPsec. AH y ESP hacen uso de SAs y

una función importante de IKE es el establecimiento y el mantenimiento de SAs. Toda implementación de AH o ESP DEBE soportar el concepto de SA como se describe abajo. El resto de esta sección describe los diversos aspectos del manejo de SA, definiendo las características requeridas para la gestión de políticas de SA, procesamiento de tráfico, y las técnicas de gestión de SA.

4.1 Definiciones y Ámbito

Una Asociación de Seguridad (SA) es una "conexión" unidireccional (simplex) que ofrece servicios de seguridad al tráfico transportado por este. Los servicios de seguridad ofrecidos en una SA son usados por AH o ESP, pero no por ambos. Si ambos (AH y ESP) se aplican a un flujo de tráfico, dos (o más) SAs se crearán para generar la protección de flujo de tráfico. Para asegurar la comunicación bidireccional entre dos hosts, o entre dos security gateway, se requieren dos Asociaciones de Seguridad (uno en cada sentido).

Una SA es identificada unívocamente por un trío que consiste en: un Índice de Parámetros de Seguridad (SPI), una Dirección IP de Destino, y un identificador de protocolo de seguridad (AH o ESP). En principio, la Dirección de Destino puede ser una dirección unicast, una dirección de difusión IP, o una dirección de grupo multicast. Sin embargo, los mecanismos IPsec para la gestión de SA se definen solamente para unicast. Por lo tanto, publicaciones siguientes, describirán el contexto de comunicaciones punto-a-punto, aun cuando el concepto también es aplicable a conexiones punto-a-multipuntos.

Según lo observado arriba, se definen dos tipos de SAs: modo transporte y modo túnel. Una SA en modo trasporte es una SA entre dos hosts. En IPv4, una cabecera de protocolo de seguridad en modo transporte aparece inmediatamente después de la cabecera IP y de algunas opciones, y antes que cualquier protocolo de capas superior (por ejemplo, TCP o UDP). En IPv6 las cabeceras del protocolo de seguridad se situarán después de la cabecera IP y de extensiones pero deben aparecer antes o después de la cabecera de opciones de dirección y antes de los protocolos de capas superiores. En el caso de ESP, una SA en modo transporte proporciona servicios de seguridad solamente para los protocolos de las capas superiores, no para la cabecera IP o cualquier cabecera de extensión precedente a la cabecera ESP. En el caso de AH la protección se extiende a las partes seleccionadas de la cabecera IP, a las partes seleccionadas de las cabeceras de extensión y a las opciones seleccionadas (contenidas en la cabecera de IPv4, la cabecera de extensión Salto-por-Salto de IPv6, o la cabecera de extensión de destino de IPv6). Para más detalles de la cobertura proporcionada por AH, vea la especificación de AH [KA98a].

Una SA en modo túnel es en esencia una SA aplicada a un túnel IP. Siempre que un extremo de la SA sea un security gateway, la SA DEBE estar en modo túnel. Una SA entre dos security gateway, es siempre una SA en modo túnel, al igual que una SA entre un host y un security gateway. Nótese que para el caso donde el tráfico es destinado para el security gateway, por ejemplo, comandos SNMP, la security gateway actúa como un host y el modo trasporte es permitido. Pero en este caso, la security gateway, no esta actuando como un gateway, es decir, no esta trasportando tráfico. Dos host pueden establecer una SA en modo túnel entre ellos. El requisito para cualquier SA que involucre a una security gateway (trasporte de tráfico) es un túnel SA debido a la necesidad de evitar problemas potenciales con la fragmentación y reensamblaje de paquetes IPsec y en circunstancias donde existan múltiples trayectorias (por ejemplo vía diferentes security gateway) para el mismo destino detrás de un security gateway.

Para una SA en modo túnel, hay una cabecera IP "externa" que especifica el destinatario del proceso IPsec, más una cabecera IP "interna" que especifica el último destinatario (aparente) del paquete. La cabecera del protocolo de seguridad aparece después de otras cabeceras IP externas y antes de las cabeceras IP internas. Si se emplea AH en modo túnel, a otras partes de la cabecera IP se les ofrecen protección así como también a todo el paquete IP al cual se le hizo el túnel (es decir, toda la cabecera IP interna es protegida, como así también protocolos de capas superiores). Si se emplea ESP, la protección es proporcionada únicamente al paquete IP al cual se le hizo el túnel (al paquete "tunelizado"), no a las cabeceras externas.

En resumen:

a) Un host DEBE soportar modo trasporte y túnel.
b) Una security gateway solo debe soportar el modo túnel. Si soporta modo trasporte este debería ser usado únicamente cuando la security gateway actúa como host, por ejemplo para la administración de la red.

4.2 Funcionalidad de las asociaciones de seguridad

El conjunto de servicios de seguridad ofrecido por una SA depende del protocolo de seguridad seleccionado, del modo de la SA, de los extremos de la SA, y de la elección de los servicios opcionales seleccionados dentro del protocolo. Por ejemplo, AH proporciona autentificación del origen de los datos e integridad sin conexión para datagramas IP (a partir de ahora equivale a "autentificación"). La "precisión" de estos servicios de autentificación estará en función de la granularidad de la SA con la que se emplea AH. Esto se describe en la sección 4.4.2 "selectores"

AH ofrece además un servicio de anti-replay (integridad parcial de la secuencia) según el deseo del receptor, esto ayudará a prevenir ataques contra denegación de servicios. AH es un protocolo apropiado para emplearse cuando la confidencialidad no es requerida (o no se permite, por ejemplo, debido a las restricciones gubernamentales en el uso criptográfico). AH también proporciona autentificación para las partes seleccionadas de la cabecera IP, que puede ser necesaria en algunos contextos. Por ejemplo, si la integridad de una opción de IPv4 o una cabecera de extensión de IPv6 se debe proteger en el camino entre el emisor y el receptor, AH puede proporcionar este servicio (a excepción de las partes mutables no predecibles de la cabecera IP).

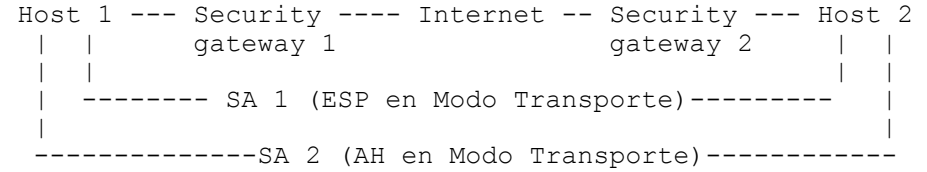
ESP proporciona de forma opcional confidencialidad para el tráfico. (La robustez del servicio de confidencialidad depende en parte, del algoritmo de encriptación utilizado). ESP también proporciona de forma opcional, autenticación como en el caso anterior. Si la autentificación es negociada por una SA ESP, el receptor también puede elegir implementar el servicio de anti-replay con las mismas características que el servicio de anti-replay de AH. La autentificación ofrecida por ESP abarca menos que la ofrecida por AH, es decir las cabeceras que quedan por fuera de la cabecera ESP no están protegidas. Si solo los protocolos de capas superiores necesitan ser autentificados, entonces la autentificación de ESP es una elección apropiada y es más eficiente en tamaño que usar ESP encapsulado con AH. Note que aunque la confidencialidad y la autenticación son opcionales, no se pueden omitir ambas, al menos una DEBE ser escogida.

Si se elige el servicio de confidencialidad, entonces una SA ESP (en modo túnel) entre dos security gateway pueden ofrecer confidencialidad parcial al flujo de tráfico. El uso del modo túnel permite encriptar las cabeceras IP internas, ocultando las identidades del origen del tráfico y del (último) destino. También, se puede usar el "relleno en la carga útil" (payload padding) de ESP para ocultar el tamaño de los paquetes, consiguiendo ocultar las características externas del tráfico. Similares servicios de confidencialidad del flujo de tráfico pueden ser ofrecidos cuando un usuario móvil está asignado a una dirección IP dinámica en un contexto de dialup, y establecer una SA ESP (en modo túnel) en un firewall corporativo (actuando como un security gateway). Observe que SAs con poca granularidad generalmente son más vulnerables al análisis de tráfico que unos con mucha granularidad en el cual se esta llevando el tráfico de muchos suscriptores.

4.3 Combinación de Asociaciones de Seguridad

Los datagramas IP trasmitidos por una SA individual permiten la protección de un protocolo de seguridad, AH o ESP, pero no ambos. En ocasiones una política de seguridad puede determinar una combinación de servicios para un flujo de tráfico especifico que no se puede realizar por una única SA. En estos casos será necesario emplear múltiples SAs para implementar la política de seguridad requerida. El termino "grupo de asociaciones de seguridad" o "grupo de SA" se aplica a una secuencia de SAs las cuales deben procesar el tráfico para satisfacer una política de seguridad. El orden de la secuencia se define en la política de seguridad. (Note que las SAs que comprenden un grupo pueden terminar en diferentes extremos. Por ejemplo, una SA puede extenderse entre un host móvil y un security gateway y una segunda, SA puede extenderse a una host detrás de un gateway.)
Las SAs pueden combinarse entre grupos de dos formas: transporte adyacente (transport adjacency) y entre túneles (iterated tunneling).

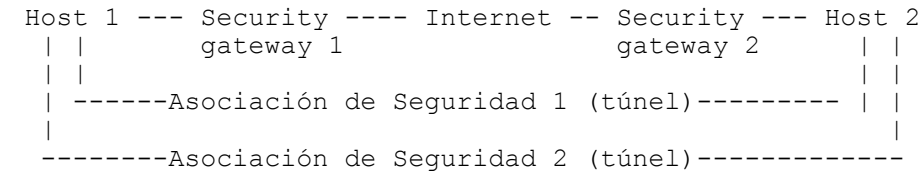
- Transporte adyacente: se aplica más de un protocolo de seguridad sobre el mismo datagrama IP, sin utilizar túneles. Este método combina a AH y a ESP permitiendo solamente un nivel de combinación, el anidado adicional no produce un beneficio adicional (asumiendo el uso de algoritmos adecuados en cada protocolo) puesto que el proceso se realiza en una instancia de IPsec en el (último) destino.

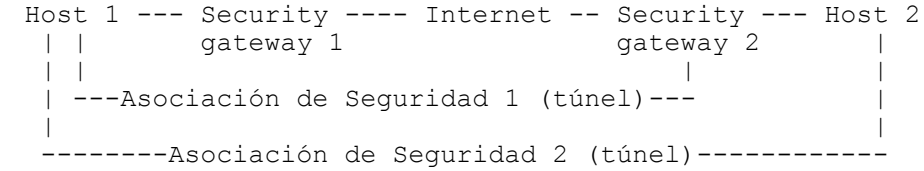
- Entre túneles: se refiere a la aplicación de múltiples capas del protocolo de seguridad efectuando múltiples túneles IP. Este método permite múltiples niveles de anidado, puesto que cada túnel se puede originar o terminar en nodos diferentes a lo largo de la trayectoria. No se espera ningún tratamiento especial para el tráfico de ISAKMP en las security gateway intermedias con excepción de que se puede especificar a través de que SPD asignada entrar (véase el caso 3 en la Sección 4.5).

  Hay tres casos básicos de entre túneles -- se requiere soporte solo para el caso 2 y 3:

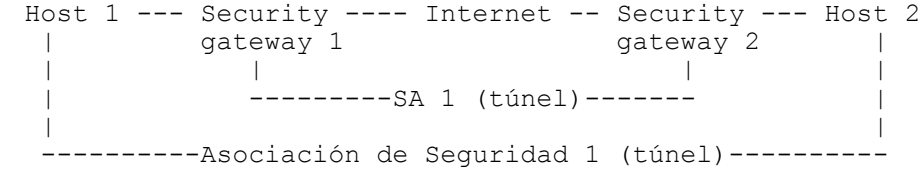
1. Ambos extremos de las SAs son los mismos: Los túneles (interno o externo) pueden ser AH o ESP, aunque es improbable que el host 1 especifique ambos túneles iguales, es decir, AH a dentro de AH, o ESP dentro de ESP.



2. Un extremo de las SAs es igual: Los túneles (interno o externo) pueden ser AH o ESP.



3. Ninguno de los extremos es igual: Los túneles (interno o externo) pueden ser AH o ESP



Estos dos métodos podrían ser combinados, por ejemplo, un grupo de SAs se podría construir a partir de un modo túnel SA y uno o dos modo trasporte SAs, aplicados en secuencia (ver Sección 4.5 "Combinaciones Básicas de Asociaciones de Seguridad"). Observe que los túneles anidados también pueden existir donde ni el origen ni los extremos destinatarios de cualquiera de los túneles son los mismos. En este caso no habría host o security gateway con un grupo que corresponda para los túneles anidados.

Para SAs en modo trasporte, sólo una estructura de protocolos de seguridad parece apropiada. AH es aplicado tanto a los protocolos de capas superiores como a las partes de la cabecera IP. Así si AH es usado en modo trasporte, en conjunto con ESP, AH DEBERÍA aparecer como la primera cabecera después de la cabecera IP, antes de la cabecera ESP. En este caso, AH se aplica a la salida del texto

cifrado de ESP. En cambio, para SAs en modo túnel, uno puede usar varias estructuras (ordenamientos) de AH y de ESP. El conjunto requerido de tipos de grupos de SA DEBE ser soportado por una implementación compatible IPsec como se describe en la Sección 4.5

4.4 Bases de Datos de Asociaciones de Seguridad (SAD)

Muchos de los detalles relacionados al procesamiento de tráfico IP en una implementación IPsec son en gran parte tema local, no sujetos a estandarización. Sin embargo algunos aspectos externos del proceso deben ser estandarizados para asegurar interoperatibilidad y proporcionar una capacidad de gestión mínima que es esencial para el uso productivo de IPsec. Esta sección describe un modelo general para procesar el tráfico IP referente a asociaciones de seguridad, el soporte de esta interoperatibilidad y el funcionamiento global. El modelo descripto debajo es nominal; las implementaciones obtenidas no necesitan igualar los detalles de este modelo según lo presentado, pero el comportamiento externo de tales implementaciones debe ser manejado por las características externas observadas de este modelo.

Hay 2 bases de datos nominales en este modelo: la Base de Datos de Políticas de Seguridad (SPD) y la Base de Datos de Asociaciones de seguridad (SAD). SPD especifica las políticas que determinan el tratamiento de todo el tráfico IP entrante o saliente en un host, security gateway, o en implementaciones IPsec BITS o BITW. SAD contiene los parámetros que se asocian con cada SA (activa). Esta sección también define el concepto de Selector, que es un conjunto de campos con valores de protocolos de capas superiores y de la capa IP que son usados por la SPD para asignar el tráfico a una política, es decir, a una SA (o grupo de SA).

Cada interfaz para la cual se habilite IPsec normalmente requiere, entradas y salidas de la base de datos separadas (SAD y SPD), debido a que la direccionalidad de varios de los campos son usados como selectores. Típicamente hay solo una interfaz, para un host o security gateway. Observe que un security gateway podría tener 2 interfaces, pero una red corporativa interna, usualmente no tendría habilitado IPsec y tan sólo un par de SADs y un par de SPDs sería necesarios. Por otra parte, si un host tiene múltiples interfaces o un security gateway tiene múltiples interfaces externas, puede que sea necesario tener una SAD y una SPD separadas para cada interfase.

4.4.1 Base de Datos de Políticas de Seguridad (SPD)

En última instancia, una SA es generada por la gestión usada para implementar una política de seguridad en el ambiente IPsec. De esta manera un elemento esencial del proceso de la SA es una SPD subyacente que especifica qué servicios deben ser ofrecidos a los

datagramas IP y de qué forma. La forma de la base de datos y su interfaz están fuera del alcance de esta especificación. Sin embargo, esta sección especifica ciertas funciones mínimas de gestión que deben ser proporcionadas, para permitir que un usuario o administrador del sistema controle cómo se aplica IPsec al tráfico enviado o recibido por un host o una transmisión a un security gateway.

El SPD se debe consultar durante todo el procesamiento del tráfico (entrante y saliente), incluyendo tráfico no IPsec. Para soportar esto, la SPD requiere entradas distintas para el tráfico de entrada y de salida. Uno puede pensar en esto como SPDs separadas (una de entrada y otra de salida). Una SPD nominal separada se debe proporcionar para cada interfaz IPsec habilitada.

Una SPD debe diferenciar entre el tráfico al que debe ofrecer protección IPsec de al que le esta permitido evitar IPsec. Esto implica que la protección IPsec a ser empleada debe estar presente tanto en el receptor como en el emisor. Para cualquier datagrama de entrada o de salida, hay tres opciones de procesamiento posibles: descartar, evitar IPsec (no IPsec), y que se aplique IPsec. La primera opción se refiere al tráfico que no se permite salir del host, atravesar una security gateway, o que se entregue a una aplicación. La segunda opción se refiere al tráfico que se le permite pasar sin la protección de IPsec. La tercera opción se refiere al tráfico que es protección producida por IPsec, y para tal tráfico la SPD debe especificar los servicios de seguridad que se proporcionarán, los protocolos que se emplearán, los algoritmos que se utilizarán, etc.

Para cada implementación IPsec, DEBE haber una interfaz administrativa que permita a un usuario o administrador del sistema manejar la SPD. Específicamente, cada paquete de entrada o de salida esta sujeto al procesamiento de IPsec, SPD debe especificar qué acción será tomada en cada caso. La interfaz administrativa debe permitir que el usuario (o el administrador del sistema) especifique que proceso de seguridad a de ser aplicado a cualquier paquete entrante o saliente del sistema, o a un paquete por paquete básico. (En una implementación IPsec el host utiliza una interfaz socket, la SPD puede no necesitar ser consultado sobre bases de paquetes, pero el efecto sigue siendo igual.) La interfaz de gestión para el SPD DEBE permitir la creación de entradas consistentes con los selectores definidos en la sección 4.4.2, y DEBE soportar el ordenamiento (total) de esas entradas. Se espera que con el uso de comodines en varios campos del selector, y puesto que todos los paquetes en una sola conexión UDP o TCP tenderán correspondencia con una sola entrada SPD, este requisito no impondrá un nivel irracionalmente detallado de la especificación de SPD. Los selectores son análogos a los que se

encuentran en un firewall o en un filtrado de router los cuáles son actualmente manejados de esa forma.

En un sistema host, las aplicaciones se PUEDEN permitir seleccionar que proceso de seguridad debe ser aplicado al tráfico que generan y consumen. (Los medios para señalar tales peticiones para la implementación IPsec están fuera del alcance de este estándar.) Sin embargo, el administrador de sistema DEBE poder especificar si una aplicación puede o no reemplazar la política del sistema (por defecto). Observe que la aplicación especificó políticas que pueden satisfacer requisitos del sistema, de modo que el sistema puede no necesitar un proceso IPsec adicional que procese más allá de este para resolver los requisitos de una aplicación. La forma de la interfaz administrativa no es especificada por este documento y puede diferir entre un host y un security gateway, y en interior del host la interfaz puede diferir entre socket-base o implementación BITS. Sin embargo, este documento especifica un conjunto de estándares de SPD, elemento que toda implementación de IPsec DEBE soportar.

El SPD contiene una lista ordenada de políticas de entrada. Cada política de entrada es introducida [keyed] por uno o más selectores que definen el conjunto de tráfico IP comprendido por esta política de entrada. (Los tipos de selectores se definen en la sección 4.4.2.) Estos definen la granularidad de las políticas o SAs. Cada entrada incluye un indicador para el tráfico coincidente con esta política, si será desviado, desechado, o procesado por IPsec. Si el procesamiento IPsec es aplicado, la entrada incluirá una especificación de SA (o grupo de SA), listado de Protocolos IPsec, los modos, y algoritmos que se emplearán, y incluirán cualquier requisito relacionado. Por ejemplo, una entrada puede demandar proteger todo el tráfico coincidente por ESP en modo trasporte usando 3DES-CBC con un IV explicito, anidado adentro de AH en modo túnel usando HMAC/SHA-1. Para cada selector, la política de entrada especifica cómo obtener los valores correspondientes para una nueva entrada SAD (SAD, ver sección 4.4.3) en la SPD y el paquete (Note que actualmente, los rangos son sólo soportados para direcciones IP, pero por medio del comodín puede ser expresado cualquier selector):

a. Usar el valor en el mismo paquete: Esto limita el uso de las SA a paquetes que tienen esos valores en el paquete para el selector, incluso si en selector tiene una política de entrada en un rango de valores de entrada permitidos o en comodín para este selector.
b. Usar el valor asociado con la política de entrada: Si este fuera un solo valor, no habría diferencia entre (a) y (b). Sin embargo si los valores permitidos para el selector son un rango (de direcciones IP) o un comodín, entonces en el caso de un rango, (b) se habilitaría el uso de SA para

cualquier paquete con un valor del selector dentro de un rango no exacto pero los paquetes con el valor del selector en el paquete provocarán la creación de SA. En el caso de un comodín, (b) podría usarse en la SA para paquetes con cualquier valor para ese selector.

Por ejemplo suponga que hay una SPD de entrada donde el valor permitido para una dirección de origen es cualquiera de un rango de host (192.168.2.1 a 192.168.2.10). Y suponga que un paquete es enviado a una dirección 192.168.2.3. El valor que se utiliza para la SA podría ser cualquiera de los que esta debajo de ejemplo, dependiendo de la política de entrada para este selector, es decir el origen del valor del selector.

	Origen del valor a ser usado en la SA	Ejemplo de un nuevo valor de selector SAD
a.	Paquete	192.168.2.3 (un host)
b.	Entrada SPD	192.168.2.1 a 192.168.2.10 (rango de host)

Note que si la entrada de SPD tenía un valor permitido de comodín para la dirección de origen, entonces el valor del selector de la SAD podría ser un comodín (cualquier host). Caso (a) se puede utilizar la prohibición de compartir, aun entre paquetes que correspondan a la misma entrada de SPD.

Como se describe en la Sección 4.4.3, los selectores pueden incluir entradas "comodín" y por lo tanto selectores de dos entradas pueden superponerse. (Esto es análogo a la superposición que se presenta con ACLs o filtro de entradas en routers o firewalls de filtrado de paquetes). De esta manera se asegura consistencia, procesamiento predecible, las entradas SPD DEBEN ser ordenadas y el SPD DEBE buscar siempre en el mismo orden, para que la primera entrada coincidente sea seleccionada consistentemente. Este requisito es necesario a los efectos del procesamiento del tráfico entre las entradas SPD que debe ser deterministas, pero no hay posibilidad de que las entradas canónicas de SPD soporten el uso de comodines para algunos selectores). Para más detalles sobre la correspondencia de paquetes entre entradas de la SPD ver la Sección 5.

Note que si ESP es especificado, la autentificación o encriptación pueden ser omitidas (pero no ambos). También DEBE ser posible configurar el valor de la SPD para que los algoritmos de autentificación o encriptación sean "NULL". Sin embargo, por lo menos uno de estos servicios debe ser seleccionado, es decir, no debe ser posible configurar a los dos como "NULL".

La SPD puede utilizarse para asignar tráfico especifico de SAs o grupos de SA. Así puede funcionar como base de datos de referencia para la política de seguridad y como asignador de SA (o grupos de SA). (Para organizar el desvió y el descarte de las políticas citadas arriba, la SPD también puede proporcionar un medio para asociar tráfico de estas funciones, aunque no son, de por si, procesamiento IPsec). La forma en la cual funcionan las SPD es diferente para el tráfico de entrada que para el tráfico de salida y también puede ser diferente para implementaciones en un host, un security gateway, BITS o un BITW. En la Sección 5.1 y 5.2 se describe el uso de la SPD para el procesamiento de salida y de entrada respectivamente.

Para que una política de seguridad pueda requerir que más de una SA se aplique a un grupo especifico de tráfico, en un orden especifico, la política de entrada en la SPD debe preservar el orden requerido. Así debe ser posible para una implementación IPsec determinar que paquete de entrada o de salida debe ser completamente procesado por una secuencia de SAs. Conceptualmente para el procesamiento de salida, uno puede imaginar vínculos (hacia la SAD) desde una entrada SPD para la cual hay SA activas y cada entrada consistirá de una sola SA o de una lista ordenada de SA que corresponden a un grupo de SA. Cuando un paquete es coincidente con una entrada en la SPD y hay una SA (o grupo de SA) activas que se pueden usar para trasportar el tráfico, el procesamiento del paquete es controlado por la SA (o grupo de SA) de entrada de la lista. Para un paquete IPsec de entrada para el cual múltiples SAs IPsec se aplican, las operaciones de búsqueda se basan en la dirección de destino, protocolo IPsec, y el SPI, los cuales deberían identificar una SA.

La SPD se utiliza para controlar todo el flujo de tráfico en IPsec incluyendo seguridad y manejo de claves (por ejemplo ISAKMP) tráfico entrante y saliente de entidades detrás de un security gateway. Esto significa que el tráfico ISAKMP se debe referenciar explícitamente en la SPD, sino será descartado. Note que un security gateway podría prohibir la encriptación de paquetes de barias formas, por ejemplo: con una entrada de descarte en la SPD para paquetes con ESP o proporcionando claves en proxys. En este último caso el tráfico estaría internamente ruteado por el módulo manejador de claves en la security gateway.

4.4.2 Selectores

Una SA (o grupo de SA) puede tener mayor o menor modularidad dependiendo de los selectores usados para definir el grupo de tráfico para la SA. Por ejemplo todo el tráfico entre dos host puede ser trasportado por una SA simple, y ofrecer un conjunto uniforme de servicios de seguridad. Alternativamente, el tráfico entre un par de host puede ser extendido a múltiples SAs, dependiendo de la

aplicación donde será usada (definido por el campos Siguiente Protocolo y el Puerto), cuando diferentes servicios de seguridad se ofrecen por diferentes SAs. Similarmente, todo el tráfico entre un par de security gateway puede ser trasportado por una SA simple, o una SA podría ser asignada para cada par de host que se comunican. Los siguientes parámetros del selector deben ser soportados por la gestión de SA para facilitar el control de la granularidad de SA. Note que en el caso de recibir un paquete con una cabecera ESP, por ejemplo en un security gateway o en una implementación BITW, el protocolo de la capa de trasporte, puerto de origen/destino y nombres (si están presente) pueden estar "ocultos", es decir inaccesibles debido a la encriptación o fragmentación. Note también que la Dirección de Origen y de Destino deben ser IPv4 o IPv6.

- Dirección IP de Destino (IPv4 o IPv6): Esta puede ser una dirección IP simple (unicast, anycast, broadcast (únicamente para IPv4), o de grupo multicast) o un rango de direcciones (valores altos y bajos (inclusive), dirección + mascara, o una dirección comodín). Estas ultimas tres se usan para soportar más de un destino que comparten la misma SA (por ejemplo detrás de un security gateway). Note que estos selectores se conceptualizan diferente del campo "Dirección IP de Destino" en la tupla <Dirección IP de destino, Protocolo IPsec, SPI> usada para identificar unívocamente a una SA. Cuando llega un paquete tuneliado, la SPI/Dirección de destino/Protocolo se usa para buscar la SA para ese paquete en la SAD. Esta dirección de destino viene desde la cabecera IP encapsulada. Una vez que el paquete se a procesado según el túnel SA y se a llegado a la salida del túnel, este selector busca en la SPD de entrada. La SPD de entrada tiene un selector denominado, dirección de destino. Esta dirección IP de destino es la que esta en el interior (encapsulada) de la cabecera IP. En el caso de un paquete en modo trasporte, habrá una sola cabecera IP y esta ambigüedad no existirá. -- Requerido por toda implementación --

- Dirección IP de Origen (IPv4 o IPv6): Esta puede ser una dirección IP simple (unicast, anycast, broadcast (únicamente para IPv4), o de grupo multicast) o un rango de direcciones (valores altos y bajos (inclusive), dirección + mascara, o una dirección comodín). Estas ultimas tres se usan para soportar mas de un origen que comparten la misma SA (por ejemplo detrás de un security gateway o en un host multihomed) -- Requerido por toda implementación --

- Nombre: Hay dos casos (note que esta forma de nombre es soportada en el IPsec DOI):

1. Identificación de usuario (User ID)
   a. Una secuencia de nombre de usuario completamente cuantificada (DNS), por ejemplo: mozart@foo.bar.com
   b. Nombre característico X.500, por ejemplo: C = US, SP = MA, O = GTE Internetworking, CN = Pepe Lopez
2. Nombre del sistema (host, security gateway, etc.)
   a. Un nombre completamente cuantificado DNS, por ejemplo: foo.bar.com
   b. Nombre característico X.500
   c. Nombre genérico X.500

Nota: un uso de los valores de este selector es "oculto" ("OPAQUE")

-- Requerido para los siguientes casos. Observe que el soporte para formas de nombres con excepción de la dirección no es requerido para las claves administrativas manuales en las SA.:

- o Identificación de usuario
  - implementación en un host nativo
  - Implementación BITW y BITS activas como HOST cuando solamente hay un usuario
  - Implementación en un security gateway para el procesamiento de entrada
- o Nombres de sistemas: todas las implementaciones --

- Nivel de sensibilidad de los datos: (etiquetas IPSO/CIPSO) --Requerido por los sistemas que proporcionan información de flujo de seguridad según la Sección 8, opcional para el resto de los sistemas --

- Protocolo de la Capa de Trasporte: obtenido del campo "Protocolo" en IPv4 o del campo "Siguiente Cabecera" en IPv6. Este puede ser un número de protocolo individual. Estos campos del paquete pueden no contener el Protocolo de Trasporte debido a la presencia de cabeceras de extensión, por ejemplo: una cabecera de enrutamiento, AH, ESP, fragmentación, opciones de destino, opciones salto-por-salto, etc. Note que el protocolo de trasporte puede no estar disponible en el caso de recibir un paquete con un encabezado ESP, en este caso un valor de "oculto" ("OPAQUE") debería ser soportado. --Requerido por toda implementación. --

  Observe que: La localización del protocolo de trasporte, en un sistema que tiene encadenamientos la cabecera del paquete controla el campo "protocolo" o "Siguiente Cabecera" hasta que encuentra y reconoce el protocolo de trasporte, o hasta que

alcanza uno que no este en la lista de encabezados de extensión, o hasta que encuentra un encabezado ESP que haga al protocolo de trasporte "oculto".

- Puertos de Origen y Destino (por ejemplo, puertos TCP o UDP): Estos pueden ser valores de puertos TCP o UDP individuales o un puerto comodín. (El uso del campo Siguiente Protocolo y el campo Puerto de Origen y/o Destino (en conjunto con el campo Dirección de Origen y/o Destino), como un selector de SA a veces se especifican como "claves orientadas a sesión"). Note que el puerto origen y destino pueden no estar disponibles en el caso de recibir un paquete con un encabezado ESP, en este caso un valor de "oculto" debería ser soportado.

  La tabla siguiente resume la relación entre el valor "Siguiente Cabecera" en el paquete y la SPD y el valor obtenido del Puerto del Selector para la SPD y SAD.

Siguiente Cabecera en el Paquete	Protocolo de la Capa de Trasporte en la SPD	Valor Derivado del Campo Puerto del Selector en la SPD Y SAD.
ESP	ESP o cualquiera	cualquiera (es decir, no busca aquí)
no importa	cualquiera	cualquiera (es decir, no busca aquí)
fragmento valor especifico	cualquiera	no cualquiera (es decir, parte del paquete)
no fragmento valor especifico	valor especifico	campo del puerto del selector actual

  Si el paquete ha sido fragmentado, la información del puerto puede no estar disponible en el fragmento actual. Si es así entonces se descarta el fragmento. Un ICMP PMTU debería ser enviado para el primer fragmento, el cual contendrá la información del puerto. --Puede ser soportado--

El contexto de una implementación IPsec determinará que selector se debe utilizar. Por ejemplo una implementación integrada en un host dentro de la pila puede hacer uso de una interfaz socket. Cuando una nueva conexión es establecida la SPD puede ser consultada y una SA (o grupo de SA) unirá al socket. Así el tráfico enviado vía ese socket no necesitará operaciones de búsqueda adicionales en la SPD/SAD. En contraste implementaciones, BITS, BITW o security gateway necesitan mirar cada paquete y realizar operaciones de búsqueda en SPD/SAD basados en los selectores. Los valores permitidos para los campos del

selector difieren entre el flujo de tráfico, la SA y la política de seguridad.

La siguiente tabla suministra los tipos de entradas que uno necesitan poder expresar en la SPD y en la SAD. Muestra como se relacionan los campos en el tráfico de datos filtrados de IPsec. (Nota: La entrada "carácter comodín" ("wild") o "comodín" ("wildcard") para direcciones de origen (src) y destino (dst) incluyen una máscara, un rango, etc.)

Campo	Valor del tráfico	Entrada SAD	Entrada SPD
Direc. de origen	Direc. IP única	Único,rango,wild	Único,rango,comodín
Direc. de dest.	Direc. IP única	Único,rango,wild	Único,rango,comodín
Protocolo xpt*	Protocolo xpt	único,comodín	único,comodín
Puer. de origen*	single src port	único,comodín	único,comodín
Puer. de dest.*	single dst port	único,comodín	único,comodín
ID de usuario*	single user id	único,comodín	único,comodín
Segunda etiqueta	Valor único	único,comodín	único,comodín

N.T.:single src port= Puer de origen único, single dst port= Puerto de destino único, single user id= ID de usuario único.

* Las entradas SAD y SPD para estos campos podrían ser "ocultas" debido a que el valor del tráfico esta encriptado.

Nota: En principio, uno puede tener selectores y/o valores de selectores en la SPD que no pueden ser negociados por una SA o grupos de SA. Por ejemplo se puede incluir valores de selectores usados para seleccionar el tráfico para descartar o listas enumeradas que causen que SA separadas puedan ser creadas para cada ítem de la lista. Por ahora esto se deja para versiones futuras de este documento y la lista de selectores requeridos y valores de selectores es el mismo para la SPD y la SAD. Sin embargo es aceptable tener una interfaz administrativa que soporte el uso de valores de selectores que no pueden ser negociados a condición de que ello no confunda al usuario en la creencia de que está creando una SA con estos valores del selector. Por ejemplo, la interfaz puede permitir que el usuario especifique una lista enumerada de valores pero daría lugar a la creación de una política separada y a una SA para cada ítem de la lista. Un vendedor puede soportar tal interfaz para hacérselo más fácil a sus clientes específicos y para especificar políticas.

4.4.3 Base de Datos de Asociaciones de Seguridad (SAD)

En cada implementación de IPsec hay una SAD, en la cual cada entrada define los parámetros asociados con una SA. Cada SA tiene una entrad en la SAD. Para el procesamiento saliente, las entradas están señaladas por entradas en la SPD. Note que si una entrada SPD

actualmente no señala (apunta) a una SA que es apropiada para el paquete, la implementación creará una SA (o grupo de SA) y vínculos a las entradas SPD para la entrada SAD (ver Sección 5.1.1). Para el procesamiento de entrada, cada entrada en la SAD es indexada por, una dirección IP de destino, tipo de protocolo IPsec y SPI. Los siguientes parámetros se asocian con cada entrada en la SAD. Esta descripción no se propone ser una Base de Información de Gestión (MIB MIB-Management Information Base), sino solamente una especificación de los ítem de datos mininos requeridos que debe soportar una SA en una implementación IPsec.

Para el procesamiento de entrada: Los siguientes campos del paquete se usan para buscar la SA en la SAD:

- Dirección IP de Destino, otras cabeceras: La dirección de destino IPv4 o IPv6. --Requerido por toda implementación--
- Protocolo IPsec: AH o ESP, usado como un índice para buscar la SA en esta base de datos. Especifica el protocolo IPsec aplicado al tráfico en esta SA -Requerido por toda implementación---
- SPI: es un valor de 32 bits que se usa para diferenciar SAs diferentes que tienen el mismo destino (la misma dirección IP de destino) y que usan el mismo protocolo IPsec. --Requerido por toda implementación--

Para cada uno de los selectores definidos en la Sección 4.4.2, la entrada de la SA en la SAD debe contener el valor o los valores que fueron negociados para esa SA cuando fue creada. Para el emisor, estos valores se utilizan para decidir si una SA dada es apropiada para usarse con un paquete de salida. Esto es parte de la comprobación para saber si una SA existente puede ser utilizada. Para el receptor, este valor es utilizado para comprobar que los valores de los selectores en un paquete de entrada concuerdan con aquellos para la SA (y así indirectamente aquellos para la política coincidente). Para el receptor esta es parte de la verificación de que la SA fue la correcta para el paquete (véase la Sección 6 para las reglas para los paquetes ICMP). Estos campos pueden contener valores específicos, un rango, comodines, o "oculto" según lo descripto en la Sección 4.4.2 "selectores". Note que para una SA ESP, el algoritmo de encriptación o el algoritmo de autentificación podrían ser "NULL". Sin embargo no deben ser ambos "NULL".

Los siguientes campos de la SAD son usados en el procesamiento IPsec:

- Contador de Número de Secuencia: Un valor de 32 bit usado para generar el campo Número de Secuencia de la cabecera AH o ESP. -- Requerido por toda implementación, pero es usado solamente para el tráfico saliente --

- o Desbordamiento del Contador de Secuencia: Una bandera (flan) que indica si el desbordamiento del Contador del Número de Secuencia debería generar un acontecimiento auditadle y prevenir la transmisión de los paquetes adicionales en la SA. -- Requerido por toda implementación, pero es usado solamente para el tráfico saliente --
- o Ventana de Anti-Replay: un contador de 32 bits y un asignador de bits [bit-map] (o equivalente) usado para determinar si un paquete AH o ESP es un paquete duplicado. -- Requerido por toda implementación, pero es usado solamente para el tráfico entrante. Nota: Si el anti-replay ha sido desactivado por el receptor, por ejemplo en el caso de una clave [keyed] SA manual, la ventana de anti-replay no se utilizará. --
- o Algoritmo de Autenticación AH, claves, etc. -- Requerido por implementaciones AH --
- o Algoritmos de encriptación ESP, claves, modo IV, IV, etc. -- Requerido por implementación de ESP --
- o Algoritmo de autenticación ESP, Claves, etc. Si el servicio no se selecciona este campo será null -- Requerido por implementaciones ESP --
- o Tiempo de Vida de la SA: un intervalo de tiempo después del cual una SA debe ser reemplazada por una nueva SA (y un nuevo SPI) o debe ser terminada, más un indicador de cuando esta acción debe ocurrir. Esta puede ser expresada como un tiempo o como un contador de byte, o un uso simultáneo de ambos, el primer tiempo de vida que expire tiene prioridad. Una implementación completa DEBE soportar ambos tipos de tiempo de vida. Si se emplea el tiempo de vida y si IKE emplea certificados X.509 para el establecimiento de SA, el tiempo de vida de la SA se debe acotar (restringir) para los intervalos de validez de los certificados y el NextIssueDate [fecha inmediatamente importante] usada en la lista de renovación de certificados (CRLs Certificate Revocation List) del intercambio IKE para las SA. Tanto el que inicia como el que responde son responsables de la restricción del periodo del tiempo de vida de la SA en estos modos. -- Requerido por toda implementación --

  Nota: los detalles de cómo manejar la renovación de las claves cuando expiran las SAs es un tema local. Sin embargo una aproximación razonable es:

  (a) Si se usa el contador de bytes, entonces la implementación DEBERÍA contar el número de bytes a los cuales se le aplica el algoritmo IPsec. Para ESP, este es el algoritmo de encriptación (incluyendo encriptación NULL) y para AH, este es el algoritmo de autentificación. Esto incluye los bytes de relleno,

etc. Note que las implementaciones DEBERÍAN ser capaces de manejar los contadores de los extremos de una SA para tener contadores sincronizados, por ejemplo, por la pérdida de paquetes o porque las implementaciones en los extremos de la SA no hacen las cosas de la misma manera.

(b) DEBERÍAN haber dos clases de tipos de tiempo de vida: un tiempo de vida suave que advierte a la implementación que es necesario iniciar una acción de reemplazo de la SA y un tiempo de vida duro cuando la SA termina.

(c) Si el paquete entero no puede ser entregado durante el tiempo de vida de la SA, el paquete DEBERÍA ser descartado.

o Modo del protocolo IPsec: túnel, trasporte o comodín. Indica el modo de AH o ESP que se aplica al tráfico en esa SA. Note que si este campo es un "comodín", el extremo emisor de la SA, de la aplicación especificará el modo para la implementación IPsec. Este uso del comodín permite que la misma SA sea usada para trasportar el tráfico en modo túnel o en modo trasporte en un paquete, por ejemplo por diferentes sockets. El receptor no necesita conocer el modo para procesar correctamente las cabeceras IPsec del paquete.

--Requerido en (salvo que se defina explícitamente en el contexto):

- Las implementaciones en host debe soportar todos los modos. - Las implementaciones en gateway debe soportar el modo túnel. --

Nota: el uso de comodines para el modo del protocolo de una SA de entrada puede añadir complejidad a la situación en el receptor (solamente a host). Desde tales paquetes una SA puede ser entregada en modo túnel o trasporte, la seguridad de un paquete entrante podría depender en parte del modo que aya sido utilizado para entregarlo. Si por ende una aplicación se ocupa del modo de la SA de un paquete dado, entonces la aplicación necesitará un mecanismo para obtener información del modo aplicado.

o MTU de la Trayectoria: cualquier trayectoria MTU observada y incluyendo el envejecimiento de la variables [and aging variables]. Ver Sección 6.1.2.4 -- Requerido por toda implementación, pero es usado solamente para el tráfico saliente --

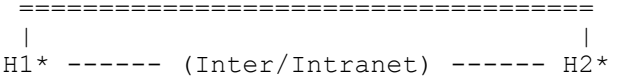
4.5 Combinaciones Básicas de Asociaciones de Seguridad

Esta sección describe cuatro ejemplos de combinaciones de SA que deben ser completamente soportados por hosts IPsec o security gateways. Combinaciones adicionales de HA y/o ESP en modo trasporte y/o túnel pueden ser soportadas a criterio del implementador. Una adecuada implementación debe ser capaz de generar estas cuatro combinaciones y un acuse de recibo de procesamiento, pero DEBERÍA ser posible recibir y procesar cualquier combinación. Los diagramas y textos debajo describen los casos básicos. La leyenda para los diagramas es:

```
==== = una o más SA (AH o ESP, en modo tunes o trasporte)
---- = Conectitividad (o también puede indicar un limite
       administrativo)
Hx   = host x
SGx  = security gateway x
X*   = X soporta IPsec
```

Nota: Las SAs debajo pueden ser AH o ESP. El modo (túnel/trasporte) es determinado por la naturaleza de los extremos. Para SA host-a-host, el modo puede ser trasporte o túnel.

Caso 1. Proporciona seguridad extremo-a-extremo (end-to-end) entre 2 host a través de Internet (o una Intranet).



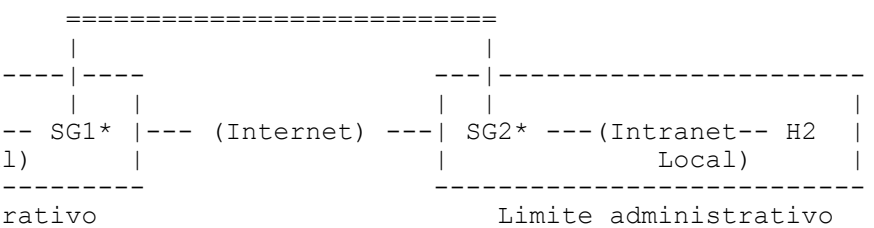
Note que tanto el modo trasporte como el modo túnel pueden ser seleccionados en los host. Las cabeceras de un paquete entre H1 y H2 podrían aparecer en alguna del las siguientes formas:

Modo Trasporte	Modo Túnel
1. [IP1][AH][upper]	4. [IP2][AH][IP1][upper]
2. [IP1][ESP][upper]	5. [IP2][ESP][IP1][upper]
3. [IP1][AH][ESP][upper]	

upper = cabecera de nivel supero/res

Note que tanto el modo trasporte como el modo túnel pueden ser seleccionados en los host. Las cabeceras de un paquete entre H1 y H2 podrían aparecer en alguna del las siguientes formas:

Caso 2. Este caso ilustra el soporte para una Red Privada Virtual simple VPN (Virtual Private Networks).

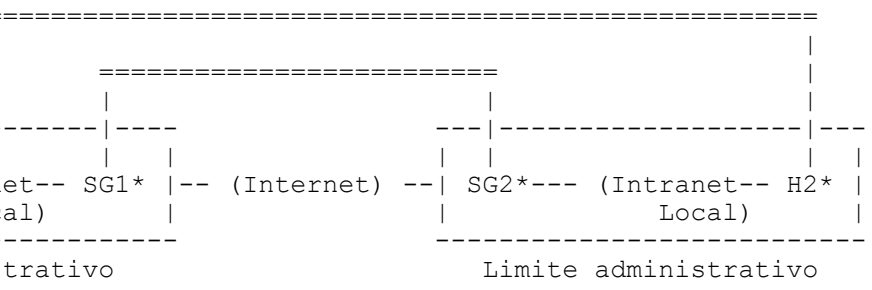


Solo el modo túnel es requerido. Las cabeceras en un paquete entre SG1 y SG2 podrían aparecer en cualquiera de las siguientes formas:

	Modo Túnel
4.	[IP2][AH][IP1][upper]
5.	[IP2][ESP][IP1][upper]

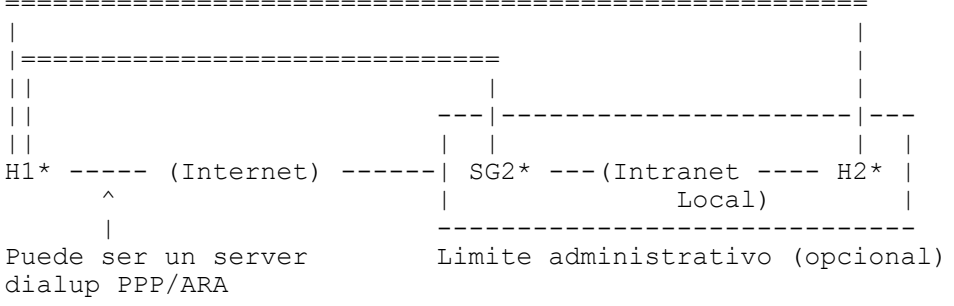
upper = cabecera de nivel supero/res

Caso 3. En este caso se combina el caso 1 y el caso 2, agregando seguridad extremo-a-extremo entre el host emisor y el receptor. No impone ningún nuevo requisito en host o en la security gateway, con excepción de que el security gateway sea configurado para dejar pasar tráfico IPsec (incluyendo tráfico ISAKMP) a los host que están detrás de el.



Caso 4. Este caso cubre la situación en donde un host remoto (H1) utiliza Internet para alcanzar el firewall de una organización (SG2) y después para acceder a algún servidor o a otro host (H2). El host remoto podría ser un host móvil (H1) que marca hasta un servidor local PPP/ARA (no demostrado) en Internet y luego cruza la Internet hacia el firewall de la organización (SG2), etc. Los detalles para el soporte para este caso, (como H1 localiza a SG2, lo autentifica y verifica su autorización

para representar H2) se discuten en la Sección 4.6.3 "Localizando a una Security Gateway"



Solo el modo túnel es requerido entre H1 y H2. Las opciones para la SA entre H1 y SG2 pueden ser una de las opciones del caso 2. Las opciones para la SA entre H1 y H2 pueden ser una de las opciones del caso 1.

Note que en este caso, el emisor debe aplicar la cabecera de trasporte antes que la cabecera del túnel. Por lo tanto la interfase administrativa para la implementación de IPsec debe soportar la configuración de la SPD y la SAD para asegurar este orden de las cabeceras de aplicación en IPsec.

Según la nota de arriba, el soporte para combinaciones adicionales de AH y ESP es opcional. El uso de otras combinaciones de opciones puede afectar negativamente la interoperatibilidad.

4.6 Asociaciones de Seguridad y Gestión de Claves

IPsec exige dar soporte para SA tanto manuales como automatizadas y la gestión criptográfica de claves. El protocolo IPsec, AH y ESP son en gran medida independientes de las técnicas de gestión asociadas a las SA, aunque las técnicas empleadas afectan un poco el servicio de seguridad ofrecido por los protocolos. Por ejemplo los servicios opcionales de anti-replay disponibles para AH y ESP requieren una administración automática de SA. Por otra parte la granularidad empleada para la distribución de claves con IPsec determinará la granularidad de la autentificación proporcionada (véase también una discusión de este tema en la Sección 4.7). En general la autentificación del origen de los datos en AH y ESP esta limitada por el alcance en el uso del secreto del algoritmo de autentificación (o por un protocolo de manejo de claves que cree tales secretos) que se comparten entre las múltiples fuentes posibles.

El siguiente texto describe los requisitos mínimos para ambos tipos de manejo de SA.

4.6.1 Técnicas Manuales

La forma más simple de gestión es administrando en forma manual, en la cual una persona configura manualmente, cada sistema con material clave y administra los datos de las SA relevantes a las comunicaciones seguras con otros sistemas. Las técnicas manuales se usan en ambientes estáticos pequeños, pero la escalabilidad es mala. Por ejemplo una compañía puede crear una VPN usando IPsec en security gateway en varios sitos. Si el número de sitios es pequeño y como todos los sitios están bajo el mismo dominio administrativo, este es un contexto factible para las técnicas administrativas manuales. En este caso el security gateway puede proteger selectivamente el tráfico a y desde otros sitios dentro de la organización usando una configuración manual de claves, mientras que no proteja tráfico para otros destinos. También puede ser apropiado cuando solo se selecciona comunicaciones que necesitan ser seguras. Un argumento similar puede aplicarse al uso de IPsec entrante dentro de una organización para un número pequeño de host y/o gateway. Las técnicas administrativas manuales emplean a menudo configuraciones estáticas y clave simétricas, aunque también existen otras opciones.

4.6.2 Gestión de Claves y Asociaciones de Seguridad Automatizadas

El uso de implementaciones IPsec en general requiere de un estándar para Internet, escalable, automatizado y con protocolos para la administración de SAs. Este soporte es requerido para facilitar el uso de las características anti-replay de AH y ESP y para una adecuada creación de SA bajo demanda, por ejemplo, para el uso de claves orientadas a usuarios o a sesiones. (Un "recambio de claves" en una SA actual implica la creación de una nueva SA con un nuevo SPI, un proceso que generalmente implica el uso automatizado de protocolos de gestión de claves/SA).

El protocolo de gestión de claves automáticas por defecto que usa IPsec es IKE [MSST97, Orm97, HC98] bajo el domino de interpretación de IPsec (a través de ISAKMP) [Pip98]. Se pueden emplear otros protocolos para el manejo automatizado de SA.

Cuando los protocolos de gestión de claves/SA se emplean, la salida de estos protocolos pueden ser empleados para crear múltiples claves, por ejemplo, para una SA ESP simple. Esto puede originarse debido a:

- Los algoritmos de encriptación usan múltiples claves (por ejemplo, Triple DES)

- Los algoritmos de autentificación usan múltiples claves
- Se emplean tanto el algoritmo de encriptación como el algoritmo de autentificación

El Sistema de Gestión de Claves puede proporcionar una cadena separada de bits para cada clave o puede generar una cadena de bits de la cual se extraigan todas las claves. Si una sola cadena de bits es proporcionada, hay que tener en cuenta que las partes del sistema que asignen la cadena de bit a las claves requeridas lo hagan en la misma forma en ambos extremos de la SA. Para garantizar que las implementaciones IPsec en cada extremo de la SA usen los mismos bits para las mismas claves, independientemente de que parte del sistema divide la cadena de bits entre las claves individuales, las claves o clave encriptadas DEBEN ser extraídas de los primeros bits (los de más a la izquierda, de orden superior) y la clave de autentificación debe ser tomada de los bits restantes. El número de bit para cada clave es definido en los RFC pertinentes que especifican los algoritmos. En el caso de claves de encriptación múltiple o claves de autentificación múltiple, la especificación del algoritmo debe especificar el orden en el cual beben ser seleccionados de una cadena simple de bits provisto para el algoritmo.

4.6.3 Localizando un Security Gateway

Esta sección discute asuntos referentes a como un host aprende sobre la existencia de security gateway relevantes y una vez que el host ha contactado a este security gateways, como sabe que este es el security gateway correcto. Los detalles de donde se almacena la información requerida es un tema local.

Considere una situación en la cual un host remoto (H1) es utilizado en Internet para acceder a un servidor o a otro host (H2) y hay un security gateway (SG2), por ejemplo, un firewall, a través del cual el tráfico de H1 se debe pasar. Un ejemplo de esta situación seria un host móvil (usuario itinerante [Road Warrior]) que cruza la Internet al firewall de una organización casera (SG2). (véase el caso 4 de las combinaciones básicas de SA de la Sección 4.5.) Esta situación plantea varios interrogantes:

1. ¿Cómo H1 sabe/aprende sobre la existencia del security gateway SG2?
2. ¿Cómo se autentifica SG2 y una vez que se haya autentificado SG2, como él confirma que SG2 ha sido autorizado para representar H2?
3. ¿cómo SG2 autentifica a H1 y verifica que H1 esté autorizado para entrar en contacto con H2?

4. ¿Cómo H1 sabe/aprende sobre los gateways de respaldo que proporcionan las trayectorias a H2?

Para tratar estos problemas, un host o un security gateway debe tener una interfaz administrativa que permita al usuario o al administrador del sistema configurar la dirección del security gateway para cualquier dirección de destino que se requiera para el uso. Esto incluye la capacidad de configurar:

- La información requerida para localizar y autentificar al security gateway y verificar su autorización de representar al host de destino.
- La información requerida para localizar y autentificar cualquier gateways de respaldo y verificar su autorización de representar al host de destino.

Se asume que la SPD también esta configurada con la información de la política que cubre cualquier otro requisito IPsec para la trayectoria del security gateway y del host de destino.

Este documento no trata el tema como automatizar el descubrimiento/verificación de security gateway.

4.7 Asociaciones de Seguridad y Multicast

La orientación del receptor para la SA implica que, en el caso del tráfico unicast, el sistema de destino seleccionará normalmente el valor del SPI. Teniendo el destino seleccionado en el valor del SPI, no hay ningún problema potencial para que la SA manualmente configurada (por ejemplo, vía un protocolo de gestión de claves) este en conflicto con la SA automáticamente configurada o para que la SA de múltiples fuentes este en conflicto con alguna otra. Para el tráfico multicast, hay sistemas de destino múltiples a través de grupos multicast. Algún sistema o persona se necesitará para coordinar todos los grupos multicast para seleccionar una SPI o SPIs en representación de cada grupo multicast y después comunicar la información IPsec de grupo a todos los miembros legítimos de ese grupo multicast a través de mecanismos no definidos en este RFC.

Múltiples emisores en un grupo multicast DEBERÍAN utilizar una sola SA (y por lo tanto un solo SPI) para todo el tráfico en ese grupo cuando se emplea un algoritmo de encriptación o de autentificación de clave simétrica. En tales circunstancias el receptor, sabe que el mensaje vino de un sistema que poseía la clave para ese grupo multicast pero el receptor generalmente no podrá autentificar que sistema envió el tráfico multicast. Las especificaciones para otros, casos multicast más generales se definen en documentos IPsec posteriores.

Cuando esta especificación fue publicada, los protocolos automatizados para la distribución de claves multicast no eran considerados adecuadamente maduros para la estandardización. Para los grupos multicast que tienen relativamente pocos miembros, la distribución de claves manuales o el uso múltiple de, algoritmos de distribución de claves unicast existentes tales como Diffie-Hellman modificado parecen ser factibles. Un ejemplo del trabajo actual en esta área es el Protocolo de Gestión de Claves para Grupos GKMP (Group Key Management Protocol) [HM97].

5. Procesamiento del Tráfico IP

Según lo mencionado en la sección 4.4.1 La SPD, se debe consultar durante todo el procesamiento del tráfico (de entrada y de salida), incluyendo el tráfico no IPsec. Si no se encuentra ninguna política en el SPD que corresponda con el paquete (para el tráfico de entrada o de salida), el paquete debe ser desechado.

NOTA: Todos los algoritmos criptográficos usados en IPsec guardan su entrada en orden canónico de byte de red (véase el apéndice del RFC 791) y generan su salida en orden canónico de byte de red. Los paquetes IP también se transmiten en orden de byte de red.

5.1 Procesamiento del Trafico IP Saliente

5.1.1 Seleccionando y Usando una SA o grupo de SAs

En un security gateway o una implementación BITW (y en muchas implementación BITS), cada paquete saliente se compara con la SPD para determinar que procesamiento se requiere para el paquete. Si el paquete va a ser descartado, esto es un evento auditadle. Si al tráfico se le esta permitido evitar el procesamiento IPsec, el paquete continúa con el procesamiento "normal" para las condiciones en la cual el procesamiento IPsec está ocurriendo. Si se requiere el procesamiento IPsec, el paquete es asociado con una SA existente (o grupo de SA), o una nueva SA (o grupo de SA) se crea para el paquete. Puesto que un selector de paquetes pueden coincidir con múltiples políticas o con múltiples SAs existentes y puesto que la SPD esta ordenada, pero la SAD no lo esta, IPsec debe:

1. Hacer Corresponder los campos del selector de paquetes con las políticas de salida en el SPD para localizar la primera política apropiada, la cual apuntará a cero o más grupos de SAs en la SAD.

2. Hacer Corresponder los campos del selector de paquetes con ésos grupos de SA encontrados en (1) para localizar el primer grupo de SA que coincida. Si no se encontró ninguna

SAs o ninguna que coincida, se creará un grupo de SA apropiados y vínculos de entrada en la SPD hacia la entrada de la SAD. Si no se encuentra entrada para la gestión de claves, deseche el paquete.

3. Utilizar el grupo de SA encontradas/creadas en (2) para realizar el procesamiento IPsec requerido, por ejemplo, autentificar y encriptar.

En un host basado en sockets que implementación IPsec, la SPD será consultada siempre que se cree un nuevo socket, para determinar, si existe, un procesamiento IPsec que será aplicado al tráfico que fluirá en ese socket.

NOTA: Una adecuada implementación no debe permitir una SA ESP que emplee encriptación NULL y un algoritmo de autentificación NULL. Una tentativa de negociar tal SA es un acontecimiento auditable.

5.1.2 Construcción de Cabeceras para el Modo Túnel

Esta sección describe como manipular las cabeceras internas y externas IP, las cabeceras de extensión, y las opciones para túneles AH y ESP. Esto incluye cómo construir la cabecera (externa) de encapsulado IP, cómo manejar los campos en la cabecera IP interna, y que acciones deben ser tomadas. La idea general esta modelada en el RFC 2003, "IP con Encapsulación IP":

- La Dirección de Origen y la Dirección de Destino en la cabecera IP externa identifican los "extremos" del túnel (al encapsulador y desencapsulador). La Dirección de Origen y la Dirección de Destino en la cabecera IP interna identifican al verdadero emisor y receptor del datagrama, (respectivamente para ese túnel), (véase la nota del punto 3 de la Sección 5.1.2.1 para más detalles de la dirección IP de origen encapsulada.)
- La cabecera IP interior no se puede modificar excepto para decrementar el TTL según se observa debajo, y permanece inmutable durante la entrega hacia el otro extremo del túnel.
- Ningún cambio en las cabeceras opcionales o en las cabeceras de extensión IP internas ocurre durante la entrega del datagrama encapsulado a través del túnel.
- De ser necesario, otras cabeceras de protocolos tales como la cabecera de Autentificación se pueden insertar entre la cabecera IP externa y la cabecera IP interna.

Las tablas de las subsiguientes secciones muestran el manejo para los diferentes campos de la cabecera/opción (la genera = el valor en el

campo exterior se construye independientemente del valor del campo interno).

5.1.2.1 Construcción de Cabeceras en Modo Túnel para IPv4

	<--Como otras Hdr se relacionan en el interior de la Hdr---------->	
IPv4	Hdr externa en el Encapsulador	Hdr interna en el Desencapsulador
Campos de la cabeceras:	----------	----------
Versión	4 (1)	no cambia
Longitud de la Hdr	La genera	no cambia
TOS	Copia de la Hdr interna (5)	no cambia
Longitud total	La genera	no cambia
ID	La genera	no cambia
Banderas (DF,MF)	La genera, DF (4)	no cambia
Offset de fragmento	La genera	no cambia
TTL	La genera (2)	Lo decrementa (2)
Protocolo	AH, ESP, Hdr enrutamiento	no cambia
Checksum	La genera	La genera (2)
Dirección origen	La genera (3)	no cambia
Dirección destino	La genera (3)	no cambia
Opciones	Nuca copiar	no cambia

1. La versión IP en la cabecera encapsulada puede ser diferente que el valor de la cabecera interna.

2. TTL en el interior de la cabecera es decrementado por el encapsulador antes de reenviarlo y por el desencapsulador en caso de reenviar el paquete. (El checksum cambia cuando el TTL cambia.)

   NOTA: El decremento del TTL es una de las acciones usuales que tienen lugar cuando se reenvía un paquete. Los paquetes que se originan en el mismo nodo que los encapsula no tienen su TTL decrementado, pues el nodo que envía está originando el paquete en lugar de reenviarlo.

3. La dirección de origen y destino dependen de la SA, la cual se usa para determinar la dirección de destino, la cual determinará a su vez que dirección de origen (de interfaz de red) se usará para reenviar el paquete.

   NOTA: En principio, la dirección IP de origen encapsulada puede ser alguna de las direcciones de interfase del encapsulador o incluso una dirección diferente de alguna de

las direcciones IP del encapsulador, (por ejemplo, si se actuá como un nodo NAT) siempre que la dirección sea accesible por el encapsulador desde el entorno dentro del cual el paquete es enviado. Esto no causa problema porque actualmente IPsec no tiene ningún requisito de procesamiento de entrada que involucre la Dirección de Origen de la cabecera IP encapsulada. Por lo tanto mientras que los extremos receptores del túnel examinan la Dirección de Destino en la cabecera IP encapsulada, este solo considera la Dirección de Origen en la cabecera IP interna (encapsulada).

4. La configuración determinará si se copia en el encabezado interno (sólo en IPv4), o si coloca un 1 o un cero en el bit DF.

5. Si la cabecera interna es IPv4 (Protocolo = 4), copia el campo TOS. Si la cabecera interna es IPv6 (Protocolo = 41) asigna el campo Class (Clase de Trafico) al campo TOS

5.1.2.2 Construcción de Cabeceras en Modo Túnel para IPv6

IPv6 Campos de la cabeceras:	<--Como otras Hdr se relacionan en el interior de la Hdr----------> Hdr externa en el Encapsulador	Hdr interna en el Desencapsulador
Versión	6 (1)	no cambia
Clase de Trafico	La copia o configura (6)	no cambia
Tipo de Flujo	La copia o configura	no cambia
Longitud de la Carga Útil	La genera	no cambia
Cabecera Siguiente	AH, ESP, Hdr enrutamiento	no cambia
Limite de Saltos	La genera (2)	Lo decrementa (2)
Dirección Origen	La genera (3)	no cambia
Dirección de Destino	La genera (3)	no cambia
Cabeceras de Extensión	Nuca copiar	no cambia

Ver la Sección 5.1.2 para las notas del 1 al 5 que se indican allí

6. Si la cabecera interna es IPv6 (Cabecera Siguiente = 41), se copia el campo Clase de Trafico (Class). Si la cabecera interna es IPv4 (Cabecera Siguiente = 4), asigna el campo TOS (tipo de servicio) al campo Clase de Trafico (Class).

5.2 Procesamiento del Trafico IP Entrante

Antes de ejecutar el procesamiento de AH o ESP, cualquier fragmento IP es reensamblado. Cada datagrama IP de entrada al cual se le aplicó el procesamiento IPsec es identificado por los valores característicos de AH o de ESP en el campo Protocolo Siguiente (o por la cabecera de extensión AH o ESP en el contexto de IPv6).

Nota: El Apéndice C contiene un código simple para chequear la mascara de bits (bismask) para una ventana de 32 paquetes que puede ser usado para implementar el servicio de anti-replay.

5.2.1 Seleccionando y Usando una SA o Grupo de SAs

Asociar el datagrama IP a la SA apropiada es simple debido a la presencia del SPI en la cabecera de AH o de ESP. Observe que las comprobaciones que realiza el selector se hace en las cabeceras internas, no en las cabeceras externas (las del túnel). Los pasos a seguir son:

1. Usar la dirección de destino de los paquetes (cabecera externa IP), protocolo IPsec, y el SPI para buscar la SA en la SAD. Si la búsqueda de la SA falla, se desecha el paquete y se registra e informa el error.

2. Utilice la SA encontrada en (1) para realizar el procesamiento IPsec, por ejemplo, autentifique y desencripte. Este paso incluye hacer corresponder a los selectores del paquete (de estar tuneliado el paquete debe usar la cabecera interna) con los selectores de la SA. La política local determina la especificidad de los selectores de la SA (valor único, lista, rango, comodín). En general, la dirección de destino del paquete debe coincidir con el valor del selector SA. Sin embargo, un paquete ICMP recibido en una SA en modo túnel puede tener una dirección de origen diferente que la que se tiene en la SA y tales paquetes se deben permitir como excepción en esta comprobación. Para un paquete ICMP, los selectores incluyen el paquete problemático (la dirección de origen y destino y puertos; se deberían intercambiar) que debería ser chequeado con el selector de la SA. Note que algunos o todos estos selectores pueden ser inaccesibles debido a limitaciones en alguno de los bits del paquete problemático que el paquete ICMP permite llevar o debido a la encriptación. Ver Sección 6.

   Realice (1) y (2) para cada cabecera IPsec hasta que una Cabecera de Protocolo de Trasporte o una cabecera IP que

no sea parte de este sistema sea encontrada. Mantener un registro de que SAs han sido usadas y el orden en que se usaron.

3. Encuentre una política entrante en la SPD que coincida con el paquete. Esto puede hacerse, por ejemplo, a través de punteros invertidos [backpointers] de las SAs hacia la SPD o haciendo corresponder a los selectores del paquete (cabecera interna si esta tunelizada) con las políticas de entrada en la SPD.

4. Comprobar si el procesamiento IPsec requerido ha sido aplicado, es decir, verificar que las SAs encontradas en (1) y (2) concuerdan con el tipo y orden de SAs requeridas por la política encontrada en (3).

NOTA: La política adecuada que "concuerda" no necesariamente es la primer política de entrada encontrada. Si la comprobación del paso (4) falla, los pasos (3) y (4) se repiten hasta que todas las políticas de entrada hayan sido comprobadas o hasta que la comprobación sea exitosa.

Después de haber realizado esos pasos, pase el paquete resultante a la Capa de Transporte o reenvié el paquete. Observe que cualquier cabecera IPsec procesada en estos pasos puede haber sido retirada, a excepción de esa información, es decir, qué SAs fueron utilizadas y de que forma se usaron, puede ser necesaria para el procesamiento subsiguiente de IPsec o del firewall.

Observe que en el caso de un security gateway, si el reenvío causa un paquete saliente vía una interfaz IPsec habilitada, entonces el proceso adicional de IPsec puede ser aplicado.

5.2.2 Manejo de HA y ESP en Túneles

El manejo de las cabeceras IP internas y externas, de las cabeceras de extensión, y de las opciones para túneles AH y ESP deberían ser realizadas según lo descripto en las tablas de la Sección 5.1.

6. Procesamiento ICMP (Relativo a IPsec)

El enfoque de esta sección es la manipulación de mensajes ICMP de errores. Otro tráfico ICMP, por ejemplo, Echo/Reply deberían ser tratados como otro tráfico y pueden ser protegidos de extremo a extremo usando SAs normalmente.

Un mensaje de error ICMP protegido por ESP o AH y generado por un router DEBERÍA ser procesado y enviado por una SA en modo túnel. La

política local determina si está o no subordinado a la comprobación de la dirección de origen por el router en el extremo destinatario del túnel. Note que si el router en el extremo iniciador del túnel esta reenviando un mensaje de error ICMP para otro router, la comprobación de la dirección de origen podría fallar. Un mensaje ICMP protegido por AH o ESP y generado por un router no debe ser enviado en una SA en modo trasporte (a menos que la SA haya sido establecida para el router actuando como un host, por ejemplo una conexión telnet usada para gestionar un router). Un mensaje ICMP generado por un host DEBERÍA realizar comprobaciones entre los selectores de direcciones IP de origen vinculados a la SA dentro de la cual el mensaje llega. Note que por más que el origen de un mensaje ICMP de error sea autentificado, la cabecera IP reenviada podría no ser válida. Por consiguiente los valores del selector en la cabecera IP DEBERÍAN ser comprobados para asegurar que son consistentes con los selectores de la SA por la cual el mensaje ICMP fue recibido.

La tabla del Apéndice D caracteriza los mensajes ICMP como generados por el host, generados por el router, ambos, desconocidos/no asignados. Los mensajes ICMP que no están dentro de estas dos últimas categorías deberían ser manipulados según lo determine la política del receptor.

Un mensaje ICMP no protegido por AH o ESP sin autentificado, su procesamiento y/o envío puede resultar en denegación de servicio. Esto sugiere que, en general sería aconsejable ignorar tales mensajes. Sin embargo, se espera que muchos router (versus security gateways) no implementarán IPsec para transportar el tráfico y así estricta adhesión a esta regla causaría que muchos mensajes ICMP sean descartados. El resultado es que algunas funciones criticas de IP podrían ser perdidas, por ejemplo, redirección y procesamiento PMTU. De esta manera se DEBE configurar una implementación IPsec para aceptar o rechazar tráfico ICMP (de router) según la política de seguridad local.

Lo que queda de esta sección habla de cómo se DEBE realizar procesamiento PMTU en hosts y en security gateways. Esta sección también trata el procesamiento de mensajes ICMP PMTU autentificados y no autentificados. Sin embargo, como se dijo anteriormente, los mensajes ICMP no autentificados PUEDEN ser descartados según la política local.

6.1 Procesamiento PMTU/DF

6.1.1 Bit DF

Cuando un sistema (host o gateway) agrega una cabecera de encapsulación (túnel ESP o túnel AH), DEBE soportar la opción de

copiar el bit DF del paquete original a la cabecera de encapsulación (y procesar los mensajes ICMP). Esto significa que debe ser posible configurar un tratamiento del sistema del bit DF (fijar, limpiar, copiar la cabecera encapsulada) para cada interfase. (Ver Apéndice B para los fundamentos).

6.1.2 Descubrimiento de la Ruta MTU (PMTU)

Esta sección trata sobre el manejo de IPsec para mensajes de Descubrimiento de la ruta MTU. ICMP PMTU es usado aquí para referirse a un mensaje ICMP para:

IPv4 (RFC 792):
- Tipo = 3 (Destino inalcanzable).
- Código = 4 (Fragmentación necesaria y el DF esta establecido).
- El siguiente salto MTU dentro de 16 bits de menor orden de la segunda palabra de la cabecera ICMP (etiquetado "no usado" en el RFC 792), con los 16 bit de mayor orden puestos en cero.

IPv6 (RFC 1885):
- Tipo = 2 (Paquete demasiado grande).
- Código = 0 (Fragmentación necesaria).
- Siguiente salto MTU en el campo MTU de 32 bit del mensaje ICMP6.

6.1.2.1 Transmisión del PMTU

La cantidad de información retornada con un mensaje ICMP PMTU (IPv4 o IPv6) es limitada y esto afecta a los selectores que están disponibles para usarse en la futura transmisión de información PMTU. (Vea el Apéndice B para una discusión más detallada de este tema.)

o Un mensaje PMTU de 64 bits de la cabecera IPsec: si el mensaje ICMP PMTU contiene solamente 64 bits de la cabecera IPsec (mínimo para IPv4) una security gateway debe soportar las siguientes opciones para las SPI/SA:

   a. Si el host originador puede ser determinado (o los host de origen posibles están limitados a un número manejable), enviar la información PMTU a todos los host originadores posibles.
   b. Si el host originador no puede ser determinado, almacene el PMTU con la SA y espere a que el siguiente paquete llegue del host originador para la SA relevante. Si el paquete o los paquete son más grandes que el PMTU, descarte los paquetes, y cree un mensaje ICMP PMTU con un nuevo paquete y el PMTU

actualizado, y envié el mensaje ICMP sobre el problema al host originador. Guarde la información PMTU para cualquier mensaje que pueda llegar posteriormente. (ver la Sección 6.1.2.4, " Envejecimiento de la PMTU").

- o Mensaje PMTU con más de 64 bits de la cabecera IPsec: Si el mensaje ICMP contiene más información del paquete original, entonces, puede haber suficiente información no oculta para determinar inmediatamente que host trasmitió el mensaje ICMP/PMTU y para proporcionar un sistema con 5 campos (dirección de origen, dirección de destino, puerto de origen, puerto de destino, protocolo de trasporte) necesarios para determinar donde almacenar/actualizar el PMTU. Bajo tales circunstancias, una security gateway debe generar inmediatamente un mensaje ICMP PMTU al recibir un ICMP PMTU de un camino más lejano.

- o La Distribución del PMTU para la Capa de Trasporte: El mecanismo del host para conseguir el PMTU actualizado para la capa de trasporte no tiene cambios, según lo especificado en el RFC 1191 (Descubrimiento de la ruta MTU).

6.1.2.2 Cálculo del PMTU

El cálculo de PMTU para un ICMP PMTU debe tener en cuenta el agregado de cualquier cabecera IPsec: trasporte AH, trasporte ESP, trasporte AH/ESP, túnel ESP, túnel AH. (Vea el Apéndice B para una discusión de las cuestiones de implementación relacionadas).

Nota: el agregado de la cabecera de IPsec podría resultar en un PMTU (visto por el host o aplicación) que es inaceptablemente pequeño. Para evitar este problema la implementación puede establecer un umbral bajo el cual no se reportará un PMTU reducido. En tales casos, la implementación aplicaría IPsec y después fragmentaría el paquete resultante de acuerdo al PMTU. Esto proporcionará un uso más eficiente del ancho de banda disponible.

6.1.2.3 Granularidad del Procesamiento de PMTU

En host, la granularidad con la cual el procesamiento ICMP PMTU puede ser realizado se diferencia dependiendo de la situación de la implementación. Mirando a un host, hay 3 situaciones que son de interés con respecto a cuestiones PMTU (ver Apéndice B para más detalles adicionales de este tema):

a. Integración de IPsec en la implementación nativa IP.
b. Implementación BITS (Bump-in-the-stack), donde IPsec esta implementado por "debajo" de una implementación existente de

una pila de protocolo TCP/IP, entre el IP nativo y los drivers de red.

c. No hay implementación IPsec: Este caso es incluido porque es relevante en el caso donde una security gateway esta enviando información PMTU devuelta a un host.

Solamente en el caso (a) los datos PMTU pueden ser mantenidos en la misma granularidad que las asociaciones de comunicación. En (b) y en (c), la capa IP solo podrá mantener los datos PMTU a la granularidad de la direcciones de origen y destino IP (y opcionalmente TOS), como se describe en el RFC 1191. Esto es una diferencia importante porque más de una asociación de comunicación puede asignarse a las mismas direcciones de origen y destino IP, y cada asociación de comunicación puede tener un diferente costo computacional en la cabecera IPsec (por ejemplo, debido al uso de diferentes trasformaciones o diferentes algoritmos).

La implementación del calculo PMTU y el soporte de PMTUs en la granularidad de asociaciones de comunicaciones es un tema local. Sin embargo, una implementación IPsec basada en socket en un host DEBERÍA mantener la información para cada socket. Los sistemas BITS deben pasar un ICMP PMTU al host de implementación IP, después de adaptarla para cualquier cabecera IPsec con costos computacionales adicionales para esos sistemas. El cálculo de los costos computacionales debería ser determinado por la inspección del SPI y cualquier otro selector de información presente en un mensaje ICMP PMTU devuelto.

6.1.2.4 Envejecimiento de la PMTU

Todos los sistemas (host o gateway) que implementan IPsec y mantienen información de la PMTU, la PMTU asociada a una SA (trasporte o túnel) DEBE "envejecer" y algún mecanismo se debe poner en funcionamiento para actualizar la PMTU dentro de un tiempo razonable, especialmente para descubrir si el PMTU es mas pequeño de lo que necesita ser. Una PMTU tiene que permanecer activa por un lapso de tiempo suficiente para que un paquete llegue de un extremo de origen de la SA de un sistema al otro extremo de la SA y propague un mensaje de error ICMP si la PMTU actual es demasiado grande. Observe que si hay túneles anidados, múltiples paquetes y los tiempos de viaje de ida y vuelta podrían ser requeridos para conseguir que un mensaje ICMP vuelva a un encapsulador o un host de origen.

Los sistemas Deberían usar la metodología descripta en documento "Descubrimiento de la Ruta MTU" (RFC 1191, Sección 6.3), el cual sugiere el receteo periódico del PMTU para el vínculo de datos del primer salto MTU y dejar que los procesos de descubrimientos normales de PMTU actualicen la PMTU cuando sea necesario. Este período debería ser configurable.

7 Auditoría

No todos los sistemas que implementan IPsec implementarán auditoría. Gran parte de la granularidad de la auditoría es de incumbencia local. No obstante varios eventos auditadles están identificados en las especificaciones de AH y ESP y para cada uno de estos eventos un conjunto mínimo de información debería ser incluido en un registro de auditoría, si es definido. Información adicional también puede ser incluida en el registro de auditoría para cada uno de estos eventos, y eventos adicionales, no explícitamente tratados en esta especificación, también pueden registrarse en el registro de auditoría. No existe requisitos para el receptor de trasmitir ningún mensaje al trasmisor pretendido en respuesta a la detección de un evento auditadle, debido al potencial de inducir denegación de servicio a través de tal acción.

8 Uso de la Información de Flujo de Seguridad en Soportes Informáticos

La información de barios niveles de sensibilidad puede ser trasportada en una sola red. Las etiquetas de información (por ejemplo, no clasificada, propiedad de la compañía, secreto) [DoD85, DoD87] son frecuentemente empleadas para distinguir tal información. El uso de etiquetas facilita la clasificación de información, y el soporte a los modelos de seguridad de flujo de información, por ejemplo el modelo Bell-LaPadula [BL73]. Tales modelos, y la tecnología para el soporte correspondiente, están diseñados para prevenir el flujo no autorizado de información sensible, aun frente a ataques de tipo "Caballo de trolla" (Trojan Horse). Convencionalmente los mecanismos de control de acceso (DAC), por ejemplo, mecanismos basados en listas de control de acceso, generalmente no son suficientes para soportar tales políticas y por lo tanto las instalaciones tales como el SPD no son suficientes en tales ambientes.

En el contexto militar la tecnología que soporta tales modelos se denomina "Múltiples Niveles de Seguridad o Seguridad Multinivel (MLS)". Las computadoras y las redes se designan a menudo como "Seguridad de múltiples niveles" si soportan la separación de datos etiquetados junto con políticas de seguridad del flujo de información. Aunque tal tecnología es más ampliamente aplicable que solamente aplicaciones militares, este documento usa el acrónimo "MLS" para señalar la tecnología de acuerdo con bastante de la literatura actual.

Los mecanismos de IPsec pueden fácilmente soportar conexiones de redes MLS. Las conexiones de redes MLS requieren el uso de fuertes Controles de Acceso Obligatorios (MAC), que los usuarios no privilegiados o los procesos no privilegiados son incapaces de

controlar o violar. Esta sección concierne solamente al uso de mecanismos de seguridad IP en habientes MLS (Política de seguridad de flujo de información). Nada en esta sección se aplica a los sistemas que no proporcionan MLS.

Según lo utilizado en esta sección, "la información sensible" puede incluir implementaciones definidas en niveles jerárquicos, categorías, y/o divulgación de información [releasability information].

AH puede ser usado para proporcionar autentificación fuerte como apoyo a las decisiones de control de acceso obligatorios en ambientes MLS. Si la información de sensibilidad IP explícita se utiliza (por ejemplo IPSO [Ken91]) y la confidencialidad no se considera necesaria dentro de un ambiente operacional particular, AH puede ser usado para autentificar el enlace entre las etiquetas de sensibilidad en la cabecera IP y la carga IP (incluyendo datos del usuario). Esto es un avance significativo de las redes etiquetadas de IPv4 donde se confía en la información de la sensibilidad aunque no hay enlaces de autentificación o criptográficos de información en la cabecera IP y los datos del usuario. Las redes IPv4 pueden o no usar etiquetamiento explícito. Envés de usar la información explicita de la sensibilidad, IPv6 normalmente usa la información implícita de la sensibilidad que es parte de la SA IPsec pero no trasmitida con cada paquete. Toda la información explícita de la sensibilidad IP debe ser autentificada usando ESP, AH, o ambos.

La encriptación es útil y puede ser deseable aun cuando todos los host están dentro de un ambiente protegido, por ejemplo, detrás de un firewall o que no tengan conexión externa. ESP puede ser usado, conjuntamente con adecuados algoritmos de gestión de claves y de encriptación, soportando DAC y MAC. (La elección de los algoritmos de encriptación y autentificación y el nivel de aseguramiento de una implementación IPsec determinarán los ambientes en los que una implementación puede ser considerada suficiente para satisfacer los requerimientos MLS.) La administración de claves puede hacer uso de la información de la sensibilidad para proporcionar MAC. Las implementaciones IPsec en los sistemas que demandan proporcionar MLS deberían ser capaces de usar IPsec para proporcionar MAC a comunicaciones basadas en IP.

8.1 Relación Entre SA y la Sensibilidad de los Datos

La Carga de Seguridad Encapsulada y la Cabecera de Autentificación se pueden combinar con apropiadas políticas de Asociaciones de Seguridad para proporcionar una red con múltiples niveles de seguridad. En cada caso cada SA (o grupo de SA) es normalmente usada para una única

instancia de información de sensibilidad. Por ejemplo, "PROPRIETARY - Internet Engineering" debe estar asociaba con una SA diferente (o grupo de SA) que la "PROPRIETARY - Finance".

8.2 Control de la Consistencia de Sensibilidad

Una implementación de Seguridad Multinivel (en host y en router) PUEDE asociar la información de sensibilidad, o un rango de información de sensibilidad con una interfase, o con una dirección IP configurada con su prefijo asociado (este último se refiere algunas veces como una interfase lógica o como un alias de interfases). Si tales propiedades existen la implementación debería comparar la información de sensibilidad asociada con el paquete, con la información de la sensibilidad asociada a la interfase o a la dirección/prefijo desde la cual el paquete llegó, o a través de la cual el paquete saldrá. Esta comprobación verificará que la sensibilidad corresponda, o que la sensibilidad del paquete está dentro del rango de interfases o dirección/prefijo.

Esta comprobación DEBERÍA ser realizada en el procesamiento entrante y saliente.

8.3 Atributos Adicionales de la Seguridad Multinivel (MLS) para las SADs

La Sección 4.4 discute dos bases de datos de Asociaciones de Seguridad (la Base de datos de Políticas de Seguridad (SPD) y la Base de Datos de Asociaciones de Seguridad (SAD)) y los selectores de la política asociada y los atributos de las SAs. La red MLS introduce un selector/atributo adicional:

- Información de sensibilidad

La Información de sensibilidad ayuda a seleccionar los algoritmos apropiados y las fuerzas de claves, de modo que el tráfico obtenga un nivel de protección apropiado a su importancia o sensibilidad como se describe en la sección 8.1. La sintaxis exacta de la información de sensibilidad depende de la implementación.

8.4 Etapas Adicionales del Procesamiento de Entrada para Redes de Seguridad Multinivel

Después que un paquete entrante a pasado por el procesamiento IPsec, una implementación MLS debería primero controlar la sensibilidad del paquete (según lo definido por la SA (o grupo de SA) usada para el paquete) con la interfase o direccionamiento/prefijo según se describe en la Sección 8.2 antes de enviar el datagrama a un protocolo de capa superior o reenviarlo.

El sistema MLS DEBE retener el enlace de los datos recibidos en un paquete protegido por IPsec y la información de la sensibilidad en una SA o en SAs usadas para el procesamiento, por lo tanto las decisiones apropiadas de la política pueden ser realizadas cuando se envía el datagrama a una aplicación o es reenviado. Estas formas de mantener este enlace son específicos de la implementación.

8.5 Etapas Adicionales del Procesamiento de Salida para Redes de Seguridad Multinivel

Una implementación MLS IPsec DEBE realizar dos controles adicionales a parte de los pasos normales detallados en la Sección 5.1.1. Al consultar la SPD o la SAD para encontrar una SA saliente, la implementación MLS DEBE usar la sensibilidad de los datos para seleccionar una apropiada SA (o grupo de SA) saliente. El segundo control se origina antes de enviar el paquete a su destino, y es el control de la consistencia de la sensibilidad descripta en la Sección 8.2.

8.6 Procesamiento Adicional para la Seguridad Multinivel para Security Gateways

Una security gateway con Seguridad multinivel DEBE seguir las reglas de procesamiento entrante y saliente mencionadas anteriormente así como también realizar un procesamiento adicional especifico para la protección intermedia de los paquetes en un ambiente MLS.

Una security gateway PUEDE actuar como proxy saliente, creando SAs para sistemas MLS que originan paquetes reenviados por el gateway. Estos sistemas MLS pueden etiquetar explícitamente los paquetes que se enviarán, o la red entera de origen puede tener características de sensibilidad asociadas con el paquete. La security gateway debe crear y usar apropiadas SAs para AH, ESP o ambas, para proteger el tráfico que envía.

De la misma forma un gateway DEBERÍA aceptar y procesar paquetes salientes AH y/o ESP y reenviarlos apropiadamente, usando etiquetamiento del paquete explicito, o confiando en las características de sensibilidad de la red de destino.

9 Consideraciones de Desempeño

El uso de IPsec impone costos computacionales de desempeño a los host o security gateway que implementan estos protocolos. Estos costos están relacionados con la memoria necesaria para el código IPsec y la estructura de los datos, y el cálculo de los valores de control de integridad, encriptación y desencriptación y la manipulación de cada paquete. Los costos computacionales por cada paquete serán

manifestados por la latencia creciente, y posiblemente reducido a lo largo del proceso. El uso de protocolos de administración de SA/claves, especialmente aquellos que emplean criptografía de clave publica, también agregan costos computacionales de desempeño al uso de IPsec. Estos costos computacionales por asociación estarán manifestados en términos de latencia creciente en el establecimiento de asociaciones. Para muchos host se anticipa que la criptografía basada en software no reducirá el rendimiento, pero la de hardware podrá ser requerido para las security gateways (puesto que representan puntos de agregación), y para ciertos hosts.

El uso de IPsec también impone costos de utilización de ancho de banda en la transmisión, intercambio, y componentes de enrutamiento en la estructura de Internet, componentes no implementados por IPsec. Esto se debe al tamaño creciente del paquete como resultado de agregarle las cabeceras AH y/o ESP, realizando túnel AH y/o ESP (que agrega una segunda cabecera IP) y el tráfico de paquetes incrementado asociado con los protocolos de administración de claves. Se anticipa que, en la mayoría de los casos, esta demanda de incremento de ancho de banda no afectará perceptiblemente la estructura de Internet. Sin embargo, en algunos casos los efectos pueden ser significantes, por ejemplo, transmitir tráfico ESP encriptado sobre un enlace dialup el cual podría ser comprimido.

Nota: La sobrecarga del establecimiento inicial de SA se sentirá en el primer paquete. Este retardo podría impactar en la capa de trasporte y aplicación. Por ejemplo podría causar que TCP trasmitiera el SYN antes de que el intercambio ISAKMP se haga. El efecto del retraso sería diferente en UDP que en TCP porque TCP no debe trasmitir ninguna otra cosa que no sea el SYN hasta que la conexión halla sido establecida, mientras que UDP seguirá adelante y trasmitirá los datos además del primer paquete.

Nota: Como se discute anteriormente, la compresión se puede emplear todavía en capas superiores a la capa IP. Existe un grupo de trabajo

IETF (Protocolo de Compresión de la carga IP (IPPCP)) trabajando en "especificaciones del protocolo que hacen posible realizar compresión sin perdida en cargas individuales antes de que la carga sea procesada por un protocolo que la encripte. Estas especificaciones permitirán que las operaciones de compresión se realicen antes de la encriptación de la carga por protocolos IPsec".

10 Requisitos de Conformidad

Todos los sistemas IPv4 que demandan implementar IPsec DEBEN cumplir con todos los requisitos de este documento. Todos los sistemas IPv6 DEBEN cumplir con todos los requisitos de este documento.

11 Consideraciones de seguridad

El tema de este documento es la seguridad, por lo tanto las consideraciones de seguridad invaden esta especificación.

12 Diferencias con el RFC 1825

Este documento de arquitectura se diferencia sustancialmente del RFC 1825 en detalles y en organización pero las nociones fundamentales son las mismas. Este documento proporciona considerables detalles adicionales en términos de especificaciones obligatorias. Introduce la SPD y la SAD, y la noción de selectores de SA. Se alinea con las nuevas versiones de AH y ESP, que también se diferencian de sus predecesores. Los requisitos específicos para las combinaciones soportadas de AH y ESP son agregadas nuevamente, como los son los detalles de la administración de PMTU.

Agradecimientos

Muchos de los conceptos contenidos en esta especificación fueron derivados de o influenciados por el protocolo de seguridad SP3 del gobierno de USA, ISO/IEC's NLSP, el protocolo de seguridad propuesto swIPe [SDNS, ISO, IB93, IBK93], y el trabajo realizado por la seguridad SNMP y la seguridad SNMPv2.

Por más de tres años (aunque abecés parece mucho más largo), este documento a evolucionado a lo largo de múltiples versiones e interacciones. Durante este tiempo, mucha gente a contribuido con ideas significativa y energía al proceso y al documento mismo. Los autores quisieran agradecer a Karen Seo por proporcionar ayuda extensiva en la revisión, edición, investigación de fondo, coordinación de la versión de esta especificación. Los autores quisierá también agradecer a los miembros del grupo de trabajo de IPsec y IPng con especial mención a los esfuerzos de (en orden alfabético): Steve Bellovin, Steve Deering, James Hughes, Phil Karn, Frank Kastenholz, Perry Metzger, David Mihelcic, Hilarie Orman, Norman Shulman, William Simpson, Harry Varnis, y Nina Yuan.

Apéndice A - Glosario

Esta sección provee definiciones para términos claves que son utilizados en este documento. Otros documentos proporcionan definiciones adicionales y información de trasfondo relacionadas a esta tecnología como por ejemplo [VK83], [HA94]. En este glosario se incluyen términos de servicios de seguridad genéricos y de mecanismos de seguridad, más términos específicos de IPsec.

Control de Acceso
Es un servicio de seguridad que impide el uso no autorizado de un recurso, incluyendo la prevención de el uso de recursos en forma no autorizados. En el contexto IPsec, el recurso cuyo acceso esta siendo controlado es con frecuencia:

- Para un host, ciclos o datos computacionales
- Para un security gateway, una red que esta detrás de un gateway

o

ancho de banda de esa red

Anti-replay
[Ver " integridad" debajo]

Autentificación Este termino se usa informalmente para referirse a la combinación de dos servicios de seguridad distintos, autentificación del origen de los datos y integridad sin conexión. Ver las definiciones debajo para cada uno de estos servicios.

Accesibilidad La accesibilidad, cuando es vista como un servicio de seguridad, trata las preocupaciones de seguridad generadas por ataques contra redes que deniegan o degradan servicios. Por ejemplo en el contexto IPsec, el uso de mecanismo de anty-replay en AH y en ESP soportan accesibilidad.

confidencialidad La confidencialidad es un servicio de seguridad que protege los datos de la exposición (divulgación) no autorizada. El principal interés de la confidencialidad en muchos de los casos es la exposición no autorizada de los datos en el nivel de aplicación, pero la exposición de características externas de comunicación también son de interés en ciertas circunstancias. La confidencialidad del flujo de tráfico es el servicio que trata este último tema encubriendo las direcciones de origen y destino, la longitud del mensaje, frecuencia de comunicación. En el contexto IPsec, usando ESP en modo túnel, especialmente en una security gateway, puede proporcionar algunos niveles de confidencialidad del flujo de tráfico. (ver también análisis de tráfico abajo).

Encriptación La encriptación es un mecanismo de seguridad usado para trasformar datos desde una forma inteligible (texto plano) en una forma ininteligible (texto cifrado), para proporcionar confidencialidad. El proceso de transformación inverso se denomina "desencriptación". Algunas veces el término "encriptación" es usado para referirse genéricamente a ambos procesos.

Autentificación del Origen de los Datos La autentificación del origen de los datos es un servicio de seguridad que verifica la identidad de origen de los datos. Este servicio usualmente trabaja en conjunto con el servicio de integridad sin conexión.

Integridad La integridad es un servicio de seguridad que asegura que la modificación de los datos sea perceptible. La integridad tiene diversas formas para corresponderse con los requerimientos de las aplicaciones. IPsec soporta dos formas de integridad: sin conexión y una forma de integridad de la secuencia parcial. La integridad sin conexión es un servicio que detecta la modificación de un datagrama IP individual, sin considerar el orden de los datagramas cuando estos llegan. La forma de integridad de la secuencia parcial ofrecida en IPsec es referida como integridad anti-replay, y detecta la llagada de datagramas IP duplicados (dentro de una ventana acotada). Esto esta en oposición de la integridad orientada a la conexión, que impone requerimientos más estrictos en el tráfico, por ejemplo, para poder detectar mensajes perdidos o reordenados. Aunque los servicios de autentificación e integridad son frecuentemente citados por separado, en la práctica están relacionados íntimamente y casi siempre ofrecidos en conjunto.

Asociación de Seguridad (SA): Es una conexión lógica unidireccional (en un solo sentido), creada para propósitos de seguridad. Todo el Tráfico que pasa por una SA es provisto por el mismo proceso de seguridad. En IPsec una SA es una abstracción de la capa IP que se implementa a través del uso de AH y ESP.

Security Gateway Un security gateway es un sistema intermedio que actúa como interfase de comunicaciones entre dos redes. El conjunto de host (y redes) en el lado externo de la security gateway es visto como no confiable (o menos confiable), mientras que las redes y host en el lado interno son vistas como confiables (o más confiables). Las subredes internas y host que están proporcionados por una security gateway son presuntos de ser confiables en virtud de que comparten una administración de seguridad común (ver "Subredes Confiables" debajo). En el contexto IPsec una security gateway es un punto en el cual AH y/o ESP es implementado para proporcionar un conjunto de host

internos, proporcionando servicios de seguridad para estos host cuando se comunican con host externos que también implementan IPsec (directamente o a través de otra security gateway).

SPI Acrónimo de "Índice de Parámetros de Seguridad". La combinación de la dirección de destino, protocolo de seguridad y SPI identifican unívocamente a la SA. El SPI es trasportado por los protocolos AH y ESP, para permitir que el nodo receptor seleccione la SA bajo la cual un paquete recibido será procesado. Un SPI solo tiene significado localmente, como lo define el creador de la SA (usualmente el receptor del paquete que lleva el SPI); por lo tanto un SPI es generalmente visto como una secuencia de bits ocultos. Sin embargo el creador de una SA puede elegir interpretar los bits en un SPI para facilitar el procesamiento local.

Análisis del tráfico El análisis del flujo de tráfico de red para propósitos de deducir información que le es útil al adversario. Ejemplo de tal información son: frecuencia de transmisión, identidades de las partes, tamaño de los paquetes, identificadores de flujo, etc. [Sch94]

Subredes confiables Una subred que contiene host y routers que confían mutuamente no se ocupan de ataques pasivos o activos. También hay suposición de que el canal de comunicación subyacente (por ejemplo, una LAN o CAN) no esta siendo atacado por otros métodos.

Apéndice B - Análisis/Discusión de PMTU/DF/Cuestiones de Fragmentación

B.1 Bit DF

¿En el caso donde un sistema (host o gateway) agregue una cabecera de encapsulación (por ejemplo, túnel ESP), el bit DF en el paquete original debería ser copiado en la cabecera de encapsulación?

La fragmentación parece ser adecuada en algunas situaciones, por ejemplo, puede ser apropiado fragmentar paquetes sobre una red con un MTU muy pequeña, por ejemplo, en redes inalámbricas (packet radio network) o en un salto de un teléfono celular a un nodo móvil, en vez de volver a trasmitir PMTU muy pequeñas para usarse sobre el resto de la trayectoria. En otras situaciones, puede ser apropiado fijar el bit DF para conseguir realimentación de routers posteriores sobre las restricciones de PMTU que requieren fragmentación. La existencia de estas situaciones permite a un sistema decidir si fragmenta o no sobre el "enlace" determinado de red, es decir, se necesita que una implementación sea capaz de copiar el bit DF (y procesar los mensajes ICMP PMTU), pero elaborando una opción que será seleccionada sobre la base de la información. En otras palabras, un administrador debería poder configurar el tratamiento del router del bit DF (fijar, limpiar, copiar de la cabecera encapsulada) para cada interfase.

Nota: Si una implementación IPsec bits intenta aplicar diferentes algoritmos IPsec basado en los puertos de origen/destino, será difícil aplicar ajustes en la Trayectoria MTU.

B.2 Fragmentación

Si se requiere, la fragmentación IP ocurre después del procesamiento IPsec dentro de una implementación IPsec. Así como, en modo trasporte AH o ESP se aplica solamente a los datagramas no a los fragmentados. Un paquete IP al cual se le a aplicado AH o ESP pueden ser fragmentados por router en la trayectoria, y tales fragmentos deben ser reensamblados antes que se realice el procesamiento IPsec en el receptor. En modo túnel, AH o ESP se aplica a un paquete IP, la carga del cual puede ser un paquete IP fragmentado. Por ejemplo, un security gateway, implementaciones IPsec "bump-in-the-stack" (BITS), o "bump-in-the-wire" (BITW), pueden aplicar AH en modo túnel a tales fragmentos. Observe que las implementaciones BITW o BITS son ejemplos en donde una implementación IPsec en host puede recibir un fragmento al cual se le aplica modo túnel, sin embargo, si se aplica al modo trasporte, estas implementaciones deben reensamblar los fragmentos antes de aplicar IPsec.

Nota: IPsec siempre tiene que determinar a que campos de la cabecera IP encapsular. Esto es independiente de donde se haya insertado IPsec

y esta intrínsicamente en la definición de IPsec. Por lo tanto cualquier implementación IPsec que no esta integrada dentro de una implementación IP debe incluir un código para construir la cabecera IP necesaria (por ejemplo IP2):

- AH-túnel ---> IP2-AH-IP1-Trasporte-Datos
- ESP-túnel --> IP2-Cabecera_ESP-IP1-Trasporte-Datos-trailer_ESP

****

En resumen, el método de fragmentación/reensamblaje descriptos arriba sobre construcción para todos los casos examinados es:

Método de Implementación	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
Hosts (Integrado en la pilas IP)	Si	Si	Si	Si	Si	Si	Si	Si
Hosts (entre los drivers y la pila IP)	Si	Si	Si	Si	Si	Si	Si	Si
Security Gateway (Integrado en la pilas IP)			Si	Si			Si	Si
Procesador criptográfico externo *								

* Si un sistema de procesamiento criptográfico tiene su propio direccionamiento IP, entonces esta cubierto por el caso del security gateway. Este dispositivo recibe el paquete de un host y realiza el procesamiento IPsec. Tiene que poder manejar el mismo AH, ESP, y el procesamiento relativo a IPv4/IPv6 en modo túnel que una security gateway tendría que manejar. Si no tiene su propio direccionamiento, es similar a la implementación BITS entre los drivers de red y la pila IP.

El siguiente análisis asume que:

1. Hay solamente un modulo IPsec en una pila del sistema. No hay un modulo A de IPsec (añadiendo encriptación/ESP y por lo tanto) ocultando el protocolo de trasporte, puerto de origen, y el puerto de destino del modulo B de IPsec.
2. Hay varios lugares donde IPsec podría ser implementado (como muestra la tabla siguiente).
    a. Hosts con integración de IPsec en la implementación nativa de IPsec. El implementador tiene acceso al código fuente de la pila.
    b. Hosts con implementaciones BITS donde IPsec es implementado entre los drivers de la red local y la pila IP. El acceso al código fuente de la pila no

esta disponible; pero existe interfases bien definidas que permiten al código de IPsec incorporarse en el sistema.

c. Security gateways y procesamiento criptográfico externo con integración de IPsec en la pila.

3. No todos los métodos descriptos arriba son factibles en todos los host. Pero se asume que para cada método, hay ciertos host para los cuales el método es factible.

Para cada una de las 3 categorías descriptas arriba, hay IPv4 y IPv6 en modo trasporte y túnel de AH y modo trasporte y túnel de ESP que dan un total de 24 casos (3x2x4).

Algunos campos de la cabecera y campos de interfase se enumeran aquí para una fácil referencia. No están en el orden en el que van las cabeceras, sino que están listadas para permitir la comparación entre las columnas. (*= no cubierto por la autentificación AH. La autentificación de ESP no cubre ninguna cabecera que la preceda.)

IPv4	IPv6	IP/interfaz de transporte (RFC 1122-Sección 3.4)
Versión = 4	Versión = 6	
Longitud de la Cabecera		
*TOS	Clase, Etiqueta de Fuljo	TOS
Longitud del Paquete	Longitud de la Carga	Longitud
Identificador		ID (Opcional)
*Banderas		DF
*Desplazamiento		
*TTL	*Limite de Saltos	TTL
Protocolo	Cabecera Siguiente	
*Suma de control		
Dirección de Origen	Dirección de Origen	Dirección de Origen
Dirección de Destino	Dirección de Destino	Dirección de Destino
Opciones?	Opciones?	Opciones

? = AH cubre Tipo-Opción y Longitud de la Opción, pero no cubre los Datos de la Opción.

Los resultados de cada uno de los 20 casos se muestran debajo ("se construye" = funcionará si el sistema fragmenta después del procesamiento IPsec saliente y reensambla antes que se realice el procesamiento IPsec entrante). Observe las cuestiones de implementaciones indicadas.

a. Hosts (Integrado dentro de la pilas IP)
   - o AH-trasporte --> (IP1-AH-Transporte-Datos)
     - IPv4 -- se construye
     - IPv6 -- se construye
   - o AH-túnel --> (IP2-AH-IP1-Transporte-Datos)
     - IPv4 -- se construye
     - IPv6 -- se construye
   - o ESP-transporte -->(IP1-Cabecera_ESP-Transporte-Datos-trailer_ESP)
     - IPv4 -- se construye
     - IPv6 -- se construye
   - o ESP-túnel -->(IP2-Cabecera_ESP-IP1-Transporte-Datos-trailer_ESP)
     - IPv4 -- se construye
     - IPv6 -- se construye

b. Host (BITS): coloque IPsec entre la capa IP y los drivers de red. En este caso el módulo IPsec tendría que hacer algo como lo siguiente para la fragmentación y el reensamblaje.
   - Realice el trabajo de fragmentación/reensamblaje y envié/reciba el paquete directamente a/de la capa de red. En modo trasporte AH o ESP esto es correcto. En modo túnel AH o ESP donde el extremo del túnel es el último destino, esto es correcto. Pero en los modos túneles AH o ESP donde el extremo del túnel es diferente del último destino y donde el host de origen es multi-homed, este meto podría resultar en un camino no tan óptimo porque el módulo IPsec no podría obtener la información necesaria (interfase LAN y gateway del siguiente salto) para dirigir el paquete a la apropiada interfase de red. Esto no es un problema si la interfase y la gateway del siguiente salto son las mismas para el último destino y para el extremo del túnel. Pero si son diferentes, IPsec necesitaría saber la interfase LAN y la gateway del siguiente salto para el extremo del túnel. (Nota: El extremo del túnel (security gateway) es altamente probable que este en una trayectoria habitual al último destinó. Pero podría existir más de una trayectoria para el destino, por ejemplo, el host podría estar en una organización con dos firewalls. Y la trayectoria que esta siendo usada podría involucrar al firewall normalmente menos seleccionado) OR
   - Pase el paquete IPsec de nuevo a la capa IP donde se añadirá una cabecera IP extra y el módulo IPsec debería comprobarlo y dejar los fragmentos ahí.

OR
- Pase los contenidos del paquete a la capa IP de tal forma que la capa IP recree una cabecera IP apropiada.

En la capa de red, el modulo IPsec tendrá acceso a los siguientes selectores de el paquete: dirección de origen, dirección de destino, Protocolo Siguiente, y si hay una cabecera de capa de trasporte entonces, el puerto de la dirección de origen y el puerto de la dirección de destino. Uno no puede asumir que IPsec tiene acceso al Nombre. Se asume que la información del selector disponible es suficiente para calcular la entrada a la Política de Seguridad relevante y a la/s Asociación/es de Seguridad.

- o AH-transporte -->(IP1-AH-Transporte-Datos)
  - IPv4 -- se construye
  - IPv6 -- se construye
- o AH-túnel --> (IP2-AH-IP1-Transporte-Datos)
  - IPv4 -- se construye
  - IPv6 -- se construye
- o ESP-transporte -->(IP1-Cabecera_ESP-Transporte-Datos-ESP_trailer)
  - IPv4 -- se construye
  - IPv6 -- se construye
- o ESP-túnel -->(IP2-Cabecera_ESP-IP1-Transporte-Datos-ESP_trailer)
  - IPv4 -- se construye
  - IPv6 -- se construye

c. Security gateways -IPsec incorporado dentro de la pila IP.

Nota: El módulo IPsec tendrá acceso a los siguientes selectores del paquete: dirección de origen, dirección de destino, Protocolo Siguiente, y si hay una cabecera de capa de trasporte entonces, el puerto de la dirección de origen y el puerto de la dirección de destino. No tendrá acceso al Identificador de Usuario (solamente los hosts tienen acceso a la información de Identificador de Usuario.) Algunas implementaciones Bits son diferentes, las security gateways son capaces de buscar la Dirección de Origen en los DNS para proporcionar un Nombre de Sistema, por ejemplo, dentro de una situación que involucre el uso de direcciones IP asignadas dinámicamente en conjunto con entradas DNS dinámicas. Tampoco tendrá acceso a la información de la capa de trasporte si hay una cabecera ESP, o si no es el primer fragmento de un mensaje fragmentado. Se asume que la información del selector disponible es suficiente para calcular la entrada a la Política de Seguridad relevante y a la/s Asociación/es de Seguridad.

```
          o AH-túnel --> (IP2-AH-IP1-Transporte-Datos)
                    - IPv4 -- se construye
                    - IPv6 -- se construye
          o ESP-túnel -->(IP2-Cabacera_ESP-IP1-Transporte-Datos-
                          ESP_trailer)
                    - IPv4 -- se construye
                    - IPv6 -- se construye
```

****

B.3 Descubrimiento de la Trayectoria MTU

Como se mencionó antes, "ICMP PMTU" hace referencia a un mensaje ICMP usado para el descubrimiento de la trayectoria MTU.

La leyenda para los diagramas que están debajo en B.3.1 y B.3.3 (pero no para B.3.2) es:

```
      ==== = SA (AH o ESP, trasporte o túnel)
      ---- = conectitividad (o si esta etiquetado, limite
             administrativo)
      .... = mensaje ICMP (de aquí en adelante designado como ICMP
             PMTU) para :

              IPv4:
              - Tipo = 3 (Destino inalcanzable)
              - Código = 4 (fragmentación necesaria, fijar DF)
              - MTU del Siguiente Salto de los 16 bits de menor orden
                de la segunda palabra de la cabecera ICMP (etiquetado
                como no usado en el RFC 792), con los 16 bits de mayor
                orden puestos a cero.

              IPv6 (RFC 1885):
              - Tipo = 2 (paquete demasiado grande)
              - Código = 0 (Fragmentación necesaria y fijar el DF)
              - MTU del Siguiente Salto del campo MTU de 32 bits del
                ICPM6

      Hx   = host x
      Rx   = router x
      SGx  = security gateway x
      X*   = X soporta IPsec
```

B.3.1 Identificando al Host(s) de Origen

La cantidad de información devuelta por el mensaje ICMP es limitada y esto afecta a los selectores que están disponibles para identificar a

la SA, host de origen, etc. para usarse en transmisiones futuras de la información PMTU.

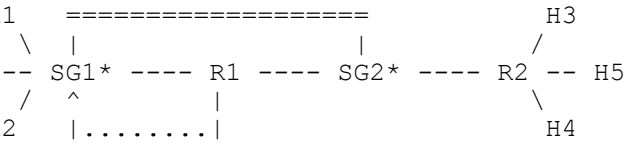
En resumen ... Un mensaje ICMP debe contener la siguiente información del paquete "problemático":

- IPv4 (RFC 792) -- cabecera IP más un mínimo de 64 bits.

Por consiguiente en IPv4, un ICMP PMTU puede identificar solamente a la primera SA (externa). Esto se debe a que ICMP PMTU puede contener solamente 64 bits del paquete "problemático" mas allá de la cabecera IP, que capturará solamente el primer SPI de AH o de ESP. En IPv6, el ICMP PMTU probablemente proporcionará todos los SPIs y los selectores en la cabecera IP, pero quizás no proporcione los puertos de la Dirección de Origen/Destino (en la cabecera de trasporte) o el

protocolo encapsulado (TCP, UDP, etc.). Por otra parte, si se utiliza ESP, los puertos de trasporte y los selectores del protocolo pueden estar encriptados.

Analizando el diagrama de abajo de un túnel entre dos security gateways (según lo mencionado en otra parte, las security gateways no usan modo trasporte)...



Suponiendo que la política de seguridad del SG1 (security gateway 1) es usar una única SA hacia el SG2 para todo el tráfico entre los host H0, H1, H2 y los host H3, H4, H5. Y suponiendo que H0 envía un paquete de datos hacia H5 el cual causa que R1 envié un mensaje ICMP PMTU al SG1. Si el mensaje PMTU tiene solamente el SPI, el SG1 podrá buscar la SA y encontrar la lista de posibles host (H0 , H1, H2, comodín); pero SG1 no tendrá forma de saber que H0 envió el tráfico que activó el mensaje ICMP PMTU.

Paquete Original	Procesamiento IPsec posterior	Paquete ICMP
		Cab. IP-3 (Origen = R1, Destino = SG1)
		Cab. ICMP (contiene el PMTU)
		Cab. IP-2 (Origen = SG1, Destino = SG2)
	Cabecera IP-2	Un mínimo de 64 bits de la cab. ESP (*)
	Cabecera ESP	
Cabecera IP-1	Cabecera IP-1	
Cabecera TCP	Cabecera TCP	
Datos TCP	Datos TCP	
	Trailer ESP	

(*) Los 64 bits incluirán bastante de la cabecera ESP (o AH) para incluir el SPI.
- ESP: SPI (32 bits), Número de Secuencia (32 bits) - AH : Cabecera Siguiente (8 bits), Longitud de la Carga (8 bits), Reservado (16 bits), SPI (32 bits)

Esta limitación en la cantidad de información que vuelve con un mensaje ICMP crea un problema en la identificación de los host de origen para el paquete (para saber a quien trasmitir la futura información ICMP PMTU). Si el mensaje ICMP contiene solamente 64 bits de la cabecera IPsec (mínimo para IPv4), los selectores de IPsec (por ejemplo, direcciones de origen y destino, Protocolo Siguiente, puertos de Origen y de Destino, etc.) se perderían. Pero el mensaje de error ICMP aun proporcionará al SG1 el SPI, la información PMTU y las gateways de origen y destino para la SA relevante.

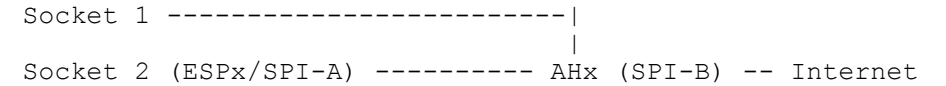
La security gateway de destino y el SPI definen únicamente una SA que a su vez define un conjunto de posibles host de origen. En este punto, la SG1 podría:

a. Enviar la información PMTU a todo los posibles host de origen. Esto no funcionaría bien si la lista de host es un comodín o si muchos o la mayoría de los host no estuvieran enviando hacia el SG1; pero esto funcionaría si el SPI/destino/etc. estuvieran asociados a un número pequeño de host.
b. Almacenar el PMTU con el SPI/etc. y esperar hasta que el próximo o los próximos paquetes lleguen del host(s) de origen para la SA relevante. Si el paquete o los paquetes son más grandes que el PMTU descarte los paquetes, y compare el o los mensajes ICMP PMTU con el o los nuevos paquetes y el PMTU actualizado y envíe el o los mensaje ICMP sobre el problema a el o los host de origen. Esto implica un retraso en la notificación al host(s) de origen, pero evita los problemas de (a).

Puesto que solamente el último método es factible en todos los casos, una security gateway DEBE proporcionar tal método como una opción. Sin embargo, si el mensaje ICMP contiene más información del paquete original, habrá suficiente información para determinar inmediatamente a que host trasmitir el mensaje ICM/PMTU y proporcionar a este sistema con los 5 campos (dirección de origen, dirección de destino, puerto de destino, puerto de origen, y protocolo de trasporte) necesarios para determinar donde almacenar/actualizar el PMTU. Bajo tales circunstancias, una security gateway debe generar un mensaje ICMP PMTU inmediatamente al recibir un ICMP PMTU de una trayectoria futura. Nota: El campo Protocolo Siguiente no estará contenido en el mensaje ICMP y el uso de encriptación ESP puede ocultar los campos de los selectores que han sido encriptados.

B.3.2 Cálculo de PMTU

El cálculo del PMTU de un ICMP PMTU tiene que considerar la adición de cualquier cabecera IPsec por H1 - trasporte AH y/o ESP, o túnel ESP o AH. Dentro de un único host, múltiples aplicaciones pueden compartir un SPI y la concatenación de SA puede ocurrir. (Ver la Sección 4.5 Combinaciones Básicas de SA, para la descripción de las combinaciones que DEBEn ser soportadas.) El diagrama que sigue ilustra un ejemplo de SA entre un par de host (visto desde la perspectiva de uno de los host.) (ESPx o AHx = modo trasporte)



Para averiguar el PMTU para cada socket que se asocia a SPI-B, será necesario tener punteros invertidos [backpointers] de SPI-B para cada una de las dos trayectorias que conducen al socket 1 y al Socket 2/SPI-A.

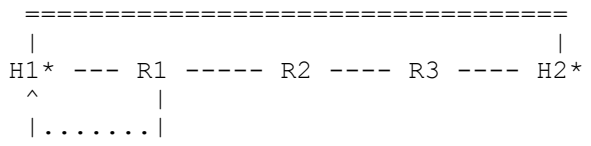
B.3.3 Granularidad para Mantener Datos PMTU

En host, la granularidad con la cual el procesamiento ICMP PMTU puede ser realizada difiere dependiendo de la situación de implementación. Mirando a un host, hay tres situaciones que son de interés para cuestiones PMTU:

a. Integración de IPsec dentro de la implementación IP nativa
b. Implementaciones BITS, donde IPsec es implementado "por debajo" de una implementación existente de una pila de protocolo TCP/IP, entre el IP nativo y los drivers de red locales.
c. Ninguna implementación IPsec: este caso esta incluido por que es relevante en los casos donde una security gateway esta enviando de vuelta la información PMTU a un host.

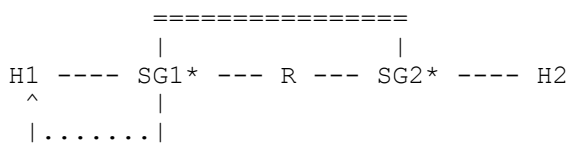
Solamente en el caso (a) se puede mantener los datos PMTU al mismo nivel de granularidad que las asociaciones de comunicación. En los otros casos, la capa IP mantendrá los datos PMTU en la granularidad de las direcciones de Origen y de Destino IP (y opcionalmente TOS/Clase), según lo descripto en el RFC 1191. Esto es una diferencia importante, por que más de una asociación de comunicación puede estar asociada a las mismas direcciones de origen y destino IP, y cada asociación de comunicación puede tener cantidades diferentes de sobrecarga informática en la cabecera IPsec (por ejemplo debido al uso de trasformaciones diferentes o algoritmos diferentes.) Esto esta ilustrado en los siguientes ejemplos.

En los casos (a) y (b)... Suponga que usted tiene la siguiente situación. H1 esta enviando hacia H2 y el paquete que sé envía de R1 hacia R2 excede el PMTU del salto de red entre ellos.



Si R1 es configurado para no fragmentar el tráfico del suscriptor, R1 envía un mensaje ICMP PMTU con el adecuado PMTU hacia H1. El procesamiento de H1 variaría con la naturaleza de la implementación. En el caso (a) (IP nativo), los servicios de seguridad están ligados a los sockets o al equivalente. Aquí la implementación IP/IPsec en H1 puede almacenar/actualizar el PMTU para el socket asociado. En el caso (b), la capa IP en H1 puede almacenar/actualizar el PMTU solo para la granularidad de las direcciones de Origen y Destino y posiblemente TOS/Clase, según lo observado arriba. Por lo tanto puede que el resultado no sea tan óptimo, puesto que la PMTU para una SRC/DST/TOS/Clase dada será la sustracción de mayor cantidad de cabecera IPsec usada por cualquier asociación de comunicación entre un origen y un destino.

En el caso (c), bebe haber una security gateway para hacer cualquier procesamiento IPsec. Entonces suponiendo que usted tenga la siguiente situación. H1 esta enviando hacia H2 y el paquete para ser enviado de SG1 hacia R excede el salto de red PMTU entre ellos.



Como se describe arriba para el caso (b), la capa IP en H1 puede almacenar/actualizar el PMTU para solamente la granularidad de las direcciones de Origen y Destino, y posiblemente TOS/Clase. Por lo tanto puede que el resultado no sea tan óptimo, puesto que la PMTU para una SRC/DST/TOS/Clase dada será la sustracción de mayor cantidad de cabecera IPsec usada para cualquier asociación de comunicación entre un origen y un destino.

B.3.4 Mantenimiento de Socket a Través de Datos PMTU

La implementación del cálculo de PMTU (Sección B.3.2) y el soporte para PMTUs en la granularidad de "asociaciones de comunicación" individuales (Sección B.3.3) es un tema local. No obstante una implementación IPsec en un host basada en socket DEBERÍA mantener la información a través de la base de socket. Sistemas BITS deben comunicar un ICMP PMTU a la implementación IP del host, después de adaptarla a alguna cabecera IPsec supletoria que se agregue a estos sistemas. La determinación de la cabecera supletoria debería estar determinada por el análisis del SPI y cualquier otra información del selector presente en un mensaje ICMP PMTU reenviado.

B.3.5 Entrega de Datos PMTU a la Capa de Trasporte

Los mecanismos del host para trasmitir el PMTU actualizado a la capa de trasporte son invariables, según lo especificado en el RFC 1191 (Descubrimiento de la Trayectoria MTU)

B.3.6 Envejecimiento de los Datos PMTU

Este tema fue visto en la Sección 6.1.2.4

Apéndice C - Ejemplo de Código de Secuencia de Espacio de Ventana

Este apéndice contiene una rutina que implementa un control de máscara de bit (bitmask) para una ventana de 32 paquetes. Esta rutina fue proporcionada por James Hughes (jim_hughes@stortek.com) y Harry Varnis (hgv@anubis.network.com) y es un ejemplo de implementación. Observe que este código controla si hay reenvíos y actualiza la ventana. Así el algoritmo, como se muestra, debería ser solamente convocado después de que el paquete haya sido autentificado. Los implementadores pueden desear considerar dividir el código para realizar el control de reenvíos antes de calcular el ICV. Si el paquete no es un reenvío, el código calcularía el ICV, (descarte cualquier paquete defectuoso) y si el paquete es correcto, actualice la ventana.

```
#include <stdio.h>
#include <stdlib.h>
typedef unsigned long u_long;

enum {
    ReplayWindowSize = 32
};

u_long bitmap = 0;                  /* session state - must be 32 bits */
u_long lastSeq = 0;                      /* session state */

/* Returns 0 if packet disallowed, 1 if packet permitted */
int ChkReplayWindow(u_long seq);

int ChkReplayWindow(u_long seq) {
    u_long diff;

    if (seq == 0) return 0;             /* first == 0 or wrapped */
    if (seq > lastSeq) {                /* new larger sequence number */
        diff = seq - lastSeq;
        if (diff < ReplayWindowSize) {  /* In window */
            bitmap <<= diff;
            bitmap |= 1;                /* set bit for this packet */
        } else bitmap = 1;          /* This packet has a "way larger" */
        lastSeq = seq;
        return 1;                       /* larger is good */
    }
    diff = lastSeq - seq;
    if (diff >= ReplayWindowSize) return 0; /* too old or wrapped */
    if (bitmap & ((u_long)1 << diff)) return 0; /* already seen */
    bitmap |= ((u_long)1 << diff);              /* mark as seen */
    return 1;                           /* out of order but good */
}
```

```
char string_buffer[512];

#define STRING_BUFFER_SIZE sizeof(string_buffer)

int main() {
    int result;
    u_long last, current, bits;

    printf("Input initial state (bits in hex, last msgnum):\n");
    if (!fgets(string_buffer, STRING_BUFFER_SIZE, stdin)) exit(0);
    sscanf(string_buffer, "%lx %lu", &bits, &last);
    if (last != 0)
    bits |= 1;
    bitmap = bits;
    lastSeq = last;
    printf("bits:%08lx last:%lu\n", bitmap, lastSeq);
    printf("Input value to test (current):\n");

    while (1) {
        if (!fgets(string_buffer, STRING_BUFFER_SIZE, stdin)) break;
        sscanf(string_buffer, "%lu", &current);
        result = ChkReplayWindow(current);
        printf("%-3s", result ? "OK" : "BAD");
        printf(" bits:%08lx last:%lu\n", bitmap, lastSeq);
    }
    return 0;
}
```

Apéndice D - Categorización de Mensajes ICMP

La tabla siguiente caracteriza los mensajes ICMP como generado por el host, generado por el router, por ambos, en disponibilidad/desconocido. El primer conjunto es de IPv4 y el segundo es de IPv6.

IPv4

Tipo	Nombre/código	Referencia
GENERADO POR EL HOST:		
3	Destino Inaccesible	
	2 Protocolo Inaccesible	[RFC792]
	3 Puerto Inaccesible	[RFC792]
	8 Origen del Host Incomunicado	[RFC792]
	14 Violación de la Precedencia del Host	[RFC1812]
10	Selección del Router	[RFC1256]

Tipo	Nombre/código	Referencia
GENERADO POR EL ROUTER:		
3	Destino Inaccesible	
	0 Red Inaccesible	[RFC792]
	4 Fragmentación Necesaria, no fue Fijada la Fragmentación	[RFC792]
	5 Error en la Ruta de Origen	[RFC792]
	6 Red de Destino Desconocida	[RFC792]
	7 Destino del host Desconocido	[RFC792]
	9 Comm. W/Red esta Administrativamente Prohibido	[RFC792]
	11 Destino de Red Inaccesible para el Tipo de Servicio	[RFC792]
5	Redireccionamiento	
	0 Datagrama de Redireccionamiento de Red (o Sub Red)	[RFC792]
	2 Datagrama de Redireccionamiento para el Tipo de Servicio & Red	[RFC792]
9	Anuncio de Router	[RFC1256]
18	Respuesta a la Mascara de Dirección	[RFC950]

IPv4

Tipo	Nombre/código	Referencia
GENERADOS POR EL ROUTER Y EL HOST:		
0	Echo Reply	[RFC792]
3	Destino Inaccesible	
	1 Host Inaccessible	[RFC792]
	10 Comm. W/Host de Destino Administrativamente Prohibido	[RFC792]
	12 Host de Destino Inaccesible por el Tipo de Servicio	[RFC792]
	13 Comunicación Administrativamente Prohibida	[RFC1812]
	15 Precedencia de Limite en Efecto	[RFC1812]
4	Apaciguando al Origen (Source Quench)	[RFC792]
5	Redireccionamiento	
	1 Datagrama de Redireccionamiento para el Host	[RFC792]
	3 Datagrama de Redireccionamiento para el Tipo de Servicio y Host	[RFC792]
6	Dirección de Host Alternativa	[JBP]
8	Echo	[RFC792]
11	Tiempo Excedido	[RFC792]
12	Problema de Parámetros	[RFC792,RFC1108]
13	Marca de Tiempo	[RFC792]
14	Respuesta de Marca de Tiempo	[RFC792]
15	Solicitud de Información	[RFC792]
16	Respuesta de Información	[RFC792]
17	Solicitud de Dirección de Mascara	[RFC950]
30	Traceroute	[RFC1393]
31	Error de Conversión de Datagrama	[RFC1475]
32	Redireccionamiento del Host Móvil	[Johnson]
39	SKIP	[Markson]
40	Photuris	[Simpson]

Tipo	Nombre/código	Referencia
Tipo Disponible o Generador por Desconocido:		
1	Disponible	[JBP]
2	Disponible	[JBP]
7	Disponible	[JBP]
19	Reservado (para Seguridad)	[Solo]
20-29	Reservado (Para Experimento de Fuerza)	[ZSu]
33	IPv6 Donde Estas	[Simpson]
34	IPv6 Acá Estoy	[Simpson]
35	Solicitud De Registración Móvil	[Simpson]
36	Repuesta De Registración Móvil	[Simpson]
37	Solicitud de Nombre de Dominio	[Simpson]
38	Respuesta de Nombre De Dominio	[Simpson]
41-255	Reservado	[JBP]

IPv6

Tipo	Nombre/código	Referencia
Generado por el Host:		
1	Destino Inaccesible	[RFC 1885]
4	Puerto Inaccesible	

Tipo	Nombre/código	Referencia
Generado por el router:		
1	Destino Inaccesible	[RFC1885]
0	Sin Ruta para el Destino	
1	Comm. w/esta Administrativamente Prohibido	
2	Sin un Vecino	
3	Dirección Inaccesible	
2	Paquete Demasiado Grande	[RFC1885]
0		
3	Tiempo Excedido	[RFC1885]
0	Limite de Salto Excedido en Transito	
1	Limite de Reensamblaje de Fragmento Excedido	

Tipo	Nombre/código	Referencia
Generados por el router y el host:		
4	Parámetro Problema	[RFC1885]
0	Encuentro de Campo de Cabecera Errónea	
1	Encuentro de Tipo de cabecera siguiente no Reconocido	
2	Encuentro de Opción IPv6 no Reconocida	

Referencias

[BL73] Bell, D.E. & LaPadula, L.J., "Secure Computer Systems: Mathematical Foundations and Model", Technical Report M74-244, The MITRE Corporation, Bedford, MA, May 1973.

[Bra97] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

[DoD85] US National Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, US Department of Defense, Ft. Meade, MD., December 1985.

[DoD87] US National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, Version 1, US Department of Defense, Ft. Meade, MD., 31 July 1987.

[HA94] Haller, N., and R. Atkinson, "On Internet Authentication", RFC 1704, October 1994.

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

[HM97] Harney, H., and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094, July 1997.

[ISO] ISO/IEC JTC1/SC6, Network Layer Security Protocol, ISO-IEC DIS 11577, International Standards Organisation, Geneva, Switzerland, 29 November 1992.

[IB93] John Ioannidis and Matt Blaze, "Architecture and Implementation of Network-layer Security Under Unix", Proceedings of USENIX Security Symposium, Santa Clara, CA, October 1993.

[IBK93] John Ioannidis, Matt Blaze, & Phil Karn, "swIPe: Network-Layer Security for IP", presentation at the Spring 1993 IETF Meeting, Columbus, Ohio

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

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

[Ken91] Kent, S., "US DoD Security Options for the Internet Protocol", RFC 1108, November 1991.

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

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

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

[Sch94] Bruce Schneier, Applied Cryptography, Section 8.6, John Wiley & Sons, New York, NY, 1994.

[SDNS] SDNS Secure Data Network System, Security Protocol 3, SP3, Document SDN.301, Revision 1.5, 15 May 1989, published in NIST Publication NIST-IR-90-4250, February 1990.

[SMPT98] Shacham, A., Monsour, R., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, August 1998.

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

[VK83] V.L. Voydock & S.T. Kent, "Security Mechanisms in High-level Networks", ACM Computing Surveys, Vol. 15, No. 2, June 1983.

Renuncia de Responsabilidades

Las opiniones y la especificación expresadas en este documento son la de los autores y no son necesariamente las de sus empleadores. Los autores y sus empleadores niegan específicamente la responsabilidad de cualquier problema que se presenta de la puesta en práctica o implementación correcta o incorrecta de uso de este diseño.

Información de los Autores

Stephen Kent
BBN Corporation
70 Fawcett Street
Cambridge, MA 02140
USA

Phone: +1 (617) 873-3988
EMail: kent@bbn.com

Randall Atkinson
@Home Network
425 Broadway
Redwood City, CA 94063
USA

Phone: +1 (415) 569-5000
EMail: rja@corp.home.net

Declaración de Copyright Completa

IMPLICITAS DE COMERCIALIZACION O IDONEIDAD PARA UN PROPOSITO ESPECIFICO.

Notas del Traductor

Los Términos que aparecen entre "[]" que no sean referencias reflejan la palabra/s en inglés de las palabra/s que se encuentran (en español) a la izquierda, debido a que NO ESTOY SEGURO de que sea la correcta traducción del término o simplemente para que no se pierda el VERDADERO sentido del texto.

Esta presente traducción fue realizada por Hugo Adrian Francisconi para mi tarjado de tesis de "Ingeniero en Electrónico" en la Facultad U.T.N. (Universidad Nacional Tecnología) Regional Mendoza - Argentina. Si le interesa IPsec y quieres saber más podes bajarte mi trabajo de tesis, "IPsec en Ambientes IPv4 e IPv6" de http://codarec6.frm.utn.edu.ar, para el cual traduje varios RFCs al español relacionados con IPsec. Cualquier sugerencia debate o comentario sobre este presente tema o traducción será bien recibida en adrianfrancisconi@yahoo.com.ar

Se a realizado el máximo esfuerzo para hacer de esta traducción sea tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". El traductor no será responsable ante cualquier persona o entidad con respecto a cualquier pérdida o daño que pudiera resultar emergente de la información contenida en está traducción.

Derechos de Copyright Sobre Esta Traducción

Datos del Traductor

Nombre y Apellido del Traductor: Hugo Adrian Francisconi
Domicilio: Carril Godoy Cruz 2801, Villa Nueva-Guay Mallen-Mendoza-Argentina
Código Postal: 5500
Tel: 054-0261-4455427
E-mail: adrianfrancisconi@yahoo.com.ar