Capítulo 2

IPSec

Una de las principales preocupaciones en el IPv6 es la seguridad. Durante la existencia del IPv4 se manifestaron sus debilidades y flaquezas en su diseño puesto que nunca se contempló la seguridad como aspecto fundamental. Esto ha cambiado y para esta versión se hace imperativa la implementación de un conjunto de protocolo destinados a ofrecer seguridad desde el inicio de la conexión hasta el punto final de la misma, y a esto se le ha llamado IPSec. Por lo cual en este capítulo haremos una breve exposición de dicho conjunto de protocolos y sus características.

Capítulo 2 IPSec

El conjunto de protocolos en el IPSec (***Internet Protocol Security***) tienen como finalidad hacer más seguras las comunicaciones dentro del IP, autenticando y cifrando cada paquete del flujo de datos. Es un protocolo diseñado por la IETF, que se definió en el *RFC4301*. También incluye protocolos para establecer la autenticación mutua entre agentes al inicio de la sesión y la negociación de llaves criptográficas durante la sesión. IPSec puede ser usado para proteger flujos de datos entre un par de hosts, ya sean servidores o clientes, entre un par de puertas de enlace (*gateway*) de seguridad, ya sean firewalls o ruteadores, o entre una puerta de enlace un hosts. IPSec es un esquema de seguridad en modo dual, de punto a punto, operante en la capa 3 del modelo *OSI*.

2.1 Componentes

Los protocolos que usa IPSec son:

IKE (***Internet Key Exchange***) para llevar a cabo una asociación de seguridad (***SA***, *security asociation*) al llevar las negociaciones de los protocolos y algoritmos, además de generar las llaves de cifrado y autenticación que serán usadas por IPSec.

Encabezado de Autenticación (***AH*** *authentication header*) para proveer integridad y autenticación de origen de datos para los datagramas IP y para proveer protección contra los ataques de respuesta (*reply attacks*).

El encabezado de carga de seguridad de encapsulamiento (***ESP*** *encapsulating security payload*) para proveer confidencialidad, autenticación de origen de datos, integridad sin conexión (*conectionless*), un servicio anti-respuesta, un tipo de secuencia parcial de integridad y una limitada confidencialidad de flujo de tráfico. **ESP** también soporta configuraciones de sólo cifrado y sólo autenticación, aunque esto se desaconseja. A diferencia del encabezado de autenticación ***ESP*** no protege el encabezado de paquete IP. En el modo de túnel, donde el paquete completo original es encapsulado con un nuevo encabezado de paquete, la protección que ofrece ***ESP*** abarca a todo el paquete, incluyendo el encapsulado, mientras que el encabezado exterior continua sin protección. Este encabezado opera directamente al principio del IP, usando el número 50 del IP. Observamos la forma del encabezado de carga seguridad en el cuadro 4 de la siguiente página.

0-7 bits	8-15 bits	16-23 bits	24-31 bits
Índice de parámetros de seguridad (*SPI*)			
Números de Secuencia.			
Carga útil de datos (variable)			
	Relleno (0-255 bytes)		
		Long. de relleno	Prox. encabezado
Autenticación de datos (variable)			

Cuadro 5 "Encabezado de Carga de Seguridad"

2.2 Trama IPSec

La trama del conjunto de protocolos IPSec se compone de los encabezados de autenticación y el encabezado de próximo encabezado.

Encabezado de Autenticación (***AH***)

El encabezado de autenticación es parte del conjunto de protocolos Elipse. Este garantiza la integridad sin conexión (*conectionless*) y autenticación del origen de los paquetes IP. Además puede, opcionalmente, proteger contra los ataques de respuesta (*reply attacks*) usando la técnica de deslizamiento de ventanas (*sliding windows*) y descartando paquetes viejos. El encabezado de autenticación protege la carga IP y todos los campos de encabezados de un datagrama IP con excepción de los campos que vayan a modificarse durante su trayectoria.

En IPv4, los campos de encabezados variables y por lo tanto inautenticados, incluyen al campo (***DSCP*** *differentiated services code point) de apuntador de código de servicios diferenciados, tipo de servicios (TOS type of servicie*), banderas, fragment *offset, t*iempo de vida (***TTL*** *time to live*) y el encabezado de suma de verificación *(Checksum).*

El encabezado de autenticación trabaja directamente al principio del *IP*, usando el número de protocolo *IP* 51.

0-7 bits	**8-15 bits**	**16-23 bits**	**24-31 bits**
Prox. Encabezado	Long. carga útil	Reservado	
Índice de parámetros de seguridad (*SPI*)			
Número de secuencia.			
Autenticación de datos (variable)			

Cuadro 6 " Encabezado de Autenticación "

El encabezado de Próximo encabezado, que se muestra en el cuadro 5, es un campo de ocho bits que identifica el tipo de la próxima carga útil después del encabezado de autenticación (*AH*). El valor de este campo se escoge del conjunto de números de protocolo IP que se definió en el más reciente *RFC* de asignación de números del *IANA* (*Internet Assigned Number Authority*).

- La longitud de carga útil es el tamaño de del paquete del encabezado de autenticación.

- La parte de reserva se utilizará en el futuro, se llenará de ceros hasta entonces

- El índice de parámetros de seguridad (*SPI*) identifica a los parámetros de seguridad, los cuales en combinación con la dirección ip identifica la asociación de seguridad implementada en este paquete.

- El número de secuencia es un número monotónico incremental, usado para prevenir ataques de respuesta.

- La autenticación de datos contiene el valor de chequeo de integridad (*ICV integrity check value*) necesario para autenticar el paquete.

2.3 Arquitectura IPSec

La arquitectura de IPSec especifica la base en la cual todas las implementaciones serán construidas y define los servicios de seguridad proveídos por IPSec, cómo y dónde pueden ser usados, cómo serán los paquetes construidos y procesados, y la interacción de procesamiento de IPSec con las políticas de seguridad.

Esta arquitectura define hasta que nivel podrá ser definido y usado por el usuario de acuerdo a las políticas de seguridad, permitiendo que cierto tráfico sea identificado para recibir el nivel de protección deseable.

IPSec fue definido para proveer un alto nivel de seguridad criptográfica, para ambas versiones del IP. Componiéndose de los siguientes encabezados que proveen seguridad en el tráfico: el encabezado de autenticación **AH** (***Autentication Header***) y el encabezado de encapsulamiento de carga útil de seguridad **ESP** (**Encapsulating Security Payload**), incluyendo los protocolos que generan y administran las llaves de cifrado, IKE (**Internet Key Exchange**) e ISAKMP (**Internet Security Key Association and Key Management Protocol**).

IPSec maneja a través de las asociaciones de seguridad SA (**Security Association**) su esquema de interoperabilidad, controladas por el índice de parámetros de seguridad SPI (**Security Parameter Index**), que se norman por las políticas de seguridad SP (**Security Policy**); las cuales se almacenan en bases de datos. También se define como dichas bases de datos se relacionarán con las distintas funciones de procesamiento de IPSec, y como distintas implementaciones del IPSec pueden coexistir.

Las políticas establecidas pueden tener dos vertientes, las estáticas y las dinámicas. Las políticas estáticas serán previamente establecidas y contendrán valores fijos, los cuales establecerán los parámetros que se negociarán; estableciendo canales seguros. O pueden ser dinámicas, en cuyo caso se podrán usar protocolos de administración de llaves como ISAKMP.

2.4 Protocolo del encabezado de autenticación

El encabezado de encapsulamiento de carga de seguridad, se define en el *RFC 4303*, tiene como objetivo principal proporcionar confidencialidad, especificando el modo de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en un datagrama IP. Puede ofrecer servicios de antiréplica, integridad y autenticación del origen de los datos incorporando un mecanismo similar al a AH. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel).

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de llave simétrica. Típicamente se usan algoritmos de cifrado por bloques (DES), de modo que la longitud de datos a cifrar tenga que ser un múltiplo de tamaño de bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno cuya finalidad es añadir caracteres de relleno al campo de datos para ocultar así su longitud real, y por lo tanto las características del tráfico.

El encabezado de autenticación de definió en el RFC 4302, es un encabezado de IPSec usado para proporcionar integridad en los datos, autenticación en el origen de los datos y opcionalmente servicios de anti-réplica en los datagramas IP. No proporciona ninguna garantía de confidencialidad.

Se suele situar justo antes de los datos, de forma que los proteja de posibles atacantes. Ha sido diseñado de forma muy versátil, de manera que puede incluirse antes que otros encabezados para asegurar que las opciones que acompañan al datagrama sean las correctas.

2.5 Métodos de autenticación

La autenticación en IPSec se logra a tráves de algoritmos de autenticación, tales como MD5, SHA-1, HMAC, RIPEMD-160.

2.6 Asociaciones de seguridad y políticas

Una SA es la forma básica de comunicación en IPSec refiriéndose a un contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los encabezados de IPSec a utilizar, las transformaciones, las llaves y la duración de validez de dichas llaves. Las SA son de un solo sentido, cada entidad con IPSec tendrá una SA para el tráfico entrante y otra para el trafico saliente; además de que son específicas para cada encabezado. Cuando se implementa IPSec, se crea una base de datos de las SA denominada SAD donde se almacenan todas las SA de dicha implementación.

La manera que tiene las SA de identificarse de manera única, es a través de los SPI. Estos son entidades de 32 bits, por los cuales se comunican dos entidades de manera segura e indicarán los parámetros usados, tales como llaves y algoritmos.

Para el manejo de las SA's se establecen dos tareas principalmente: creación y eliminación; que a su vez se pueden ejecutar de manera manual o dinámica a través de un protocolo de intercambio de llaves como IKE. La creación de llaves se lleva a través de la negociación de los parámetros de las SA y la correspondiente actualización de la SAD. El manejo manual de llaves es obligatorio en toda implementación, el proceso de asignación del SPI y la negociación de parámetros es totalmente manual y permanecerán hasta que sean manualmente borrados. Para el manejo dinámico de las llaves se utiliza IKE.

2.7 Protocolo de intercambio

El conjunto de protocolos que forman IPSec están diseñados con capacidad de expansión que dan servicios de seguridad como el control de acceso, integridad, confidencialidad y autenticación. El mismo es capaz de proteger paquetes IP entre hosts y gateways, gaterías, hosts, etc. Este conjunto de protocolos puede ser implementado en IPv4 de manera opcional, y aunque en IPv6 se debería implementar de manera obligada, esto también puede no serlo.

Una de las características de IPSec es su posibilidad de acoplamiento a otras tecnologías, aunado al hecho de que es posible cambiar los algoritmos criptográficos estándar por otros más robustos.

IPSec maneja una especificación de arquitectura que deberá ser la base de todas las implementaciones, definiendo los servicios que esta proveerá, como se procesara la información y dónde, además de como se deben de definir las políticas de seguridad a usar en la misma. Ha sido diseñado para proveer seguridad criptográfica para ambas versiones del IP. Tiene dos encabezados que proveen la seguridad del tráfico de información (*AH* [authenticaction header] y *ESP [encapsulating security payload]*), protocolos que generan y administran las llaves (ISAKMP [internet security association and key managment protocol] e IKE [intenet key exchange].

El esquema de interoperabilidad de IPSec se maneja a través de SAs (Security Associations) las cuales son controladas por un SPI (Security Parameter Index), y regidas por un SPs (Security Policy) que se configuran previamente; tanto las SAs como las SPs se almacenan son almacenadas en sus respectivas bases de datos: SAD para las asociaciones de seguridad y SPD para las políticas. La arquitectura de IPSec también define la interacción que hay entre estas bases de datos con las diferentes funciones de procesamiento de IPSec (cifrado y descifrado) y define cómo varias implementaciones de IPSec pueden existir.

Los parámetros que se negocian para establecer los canales seguros se indican bajo las políticas preestablecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de administración de llaves como ISAKMP (Internet Security Association and Key Managment Protocol). Estas políticas determinan si dos entidades son capaces de comunicarse entre sí y cuál sería la transformación a usar en un caso dado.

IPSec proporciona los siguientes servicios de seguridad:

Control de acceso

Previene el uso no autorizado de recursos, garantizando que sólo acceden a la información y a los recursos los usuarios que tiene permiso para ellos.

Integridad

Implica que los datos no puedan ser modificados o corrompidos de manera alguna desde su transmisión hasta su recepción en una comunicación.

Autenticación

Definen mecanismos para garantizar la procedencia de la información, de modo que se puede verificar que realmente es el remitente autorizado quien lo envió.

Protección a la réplica

Asegura que una transacción sólo se pueda llevar a cabo una vez, a menos que se autorice una repetición de la misma. Nadie debería poder grabar una transacción para luego replicarla para aparentar múltiples transacciones del remitente original, por ejemplo.

Confidencialidad

Implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas, asegurando la privacidad de la información al no ser consultada por terceras personas.

Confidencialidad limitada en el flujo de tráfico

Este servicio se refiere a ocultar las direcciones fuente y destino, la longitud del mensaje, o la frecuencia de la comunicación. En el contexto de IPSec, usando ESP en modo túnel, especialmente en un gateway de seguridad, puede proporcionar un cierto nivel de confidencialidad en el flujo de tráfico.

IPSec proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. Cuando se implementa IPSec en un firewall o enrutador, éstos proporcionan una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza el perímetro.

Por otro lado, al estar implementado en la capa de red, debajo de los protocolos TCP/UDP resulta “transparente” para las aplicaciones, es decir, no hay necesidad de realizar alguna configuración desde el punto de vista de usuario final ni del servidor. También IPSec tiene la capacidad de ofrecer seguridad individual si ésta fuese indispensable, resultando útil para los empleados que accedan a la red desde el exterior vía telefónica. Además, es posible asegurar una subred virtual dentro de una organización para las aplicaciones más sensibles.

Facilita el comercio electrónico de negocio a negocio al proporcionar una infraestructura segura sobre la cual realizar transacciones usando cualquier aplicación, por ejemplo las extranets.

Los algoritmos permitidos para la protección con IPSec, tanto los usados para autenticación como los usados para cifrado, idealmente desempeñan dos metas incompatibles: proveer máxima protección contra una gran variedad de ataques matemáticos, de análisis criptológico y de fuerza bruta; y por otro lado, requerir un procesamiento mínimo en el lado de cada participante dentro de la comunicación. Aunque los documentos de IPSec decretan algoritmos específicos para proveer un grado estándar, con seguridad interoperable, se pueden implementar algoritmos adicionales ya sea para dominio público o privado.

Todos los algoritmos son algoritmos de bloque, empiezan en el inicio del mensaje y cada bloque es procesado uno a la vez. El tamaño del bloque es parte de la definición de cada algoritmo, donde el más común es de 8 bytes (64 bits). Cada bloque pasa de cierto modo por algún procesamiento repetitivo donde cada iteración de ese procesamiento es conocido como ciclo. El número de ciclos es algunas veces considerado como una característica importante en la criptografía de un algoritmo. Cada ciclo, en turno, consiste de una función de ciclo, la cual es un procesamiento que constituye cada ciclo del cifrado. La función de ciclo puede ser simple y sencilla, o extremadamente compleja. Algunos algoritmos tienen múltiples funciones de ciclo que se pueden aplicar a uno o más ciclos.

En muchos algoritmos, la llave secreta más completa no es usada como función hash o para cifrar cada bloque, sino para generar múltiples sub-llaves, o ciclos de llave donde a su vez cada ciclo puede incorporar una o más sub-llaves. Si cada bloque fuera cifrado o manejado por una función hash separadamente, se presentarían ataques más fáciles, ya que el contenido de algunas partes del paquete de Internet serían conocidas. En el caso de una función hash, el hash final se debe reflejar en todos los bits de todo el bloque de entrada, no solo en el último bloque. En el caso de un algoritmo de cifrado, si cada bloque es descifrado separadamente, sin hacer referencia a ningún otro bloque, los bloques previsibles pueden ser atacados más fácilmente una vez que la llave fue conocida y todo el bloque puede ser descifrado. Por esta razón, todo algoritmo de manera obligatoria en IPSec incorpora dentro de su definición un mecanismo de retroalimentación, es decir, el cifrado o autenticación de cada bloque tiene como una de sus entradas la salida calculada criptográficamente del bloque previo.

La seguridad de los algoritmos criptográficos dependerá de la complejidad de su criptografía y de su robustez. Sin embargo, un algoritmo criptográfico no es suficiente para garantizar la seguridad de las comunicaciones debido a que varios factores juegan un papel muy importante, como por ejemplo, la implementación en hardware o software, o bien, la generación de llaves secretas que deberán tener una apropiada longitud, complejidad y ser generadas, intercambiadas, administradas y almacenadas de una manera segura.

El protocolo IPSec ha sido diseñado en forma modular de modo que se puedan seleccionar determinados algoritmos para cifrado y autenticación sin afectar a otras partes de la implementación.

Sin embargo, han sido definidos algunos algoritmos de manera estándar para soportar todas las implementaciones y asegurar la interoperabilidad en el mundo global de Internet, como son AES (en etapa de evaluación) para sustituir a DES y 3DES, considerados actualmente para cifrado, así como MD5 y SHA-1 como funciones hash para autenticación. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico, como por ejemplo IDEA o Blowfish.

Para los algoritmos de autenticación se utilizan las funciones hash (o primitivas hash), cuya funcionalidad es usada principalmente para resolver el problema de integridad y autenticidad del origen de los mensajes.

Una función hash o "función resumen" es un algoritmo que, aplicado a un mensaje determinado, crea una representación digital o hash de una longitud fija mucho menor que el mensaje original, pero substancialmente único a él, de tal manera, que no sea factible, dado solamente el hash, reconstruir el mensaje original, es decir, las funciones hash son de una sola dirección. Un simple ejemplo de una función hash sería contar el número de letras del mensaje, si es par asociamos un 0 y si es impar un 1. El principal inconveniente de este sistema es que pueden existir colisiones (dos mensajes diferentes producen la misma salida) por lo que conviene que las funciones tengan un rango de salida lo suficientemente grande (128 bits o más) para poder considerarlas libres de colisión.

2.8 Implementaciones

IPSec puede ser implementado en hosts, en conjunto con un enrutador, o con un firewall (para crear gateways de seguridad). La implementación es configurada dependiendo de los requerimientos de seguridad de los usuarios. A continuación se menciona la implementación de IPSec en varios dispositivos de red (hosts y enrutadores). La implementación en hosts es más útil cuando se desea una seguridad punto a punto; sin embargo, en casos cuando la seguridad se desea sobre una parte de la red, es mejor la implementación en enrutadores que incluyen VPNs e intranets.

Implementación en hosts:

La implementación en hosts tiene las siguientes ventajas:
- Provee una seguridad punto a punto.
- Capacidad de implementarse en todos los modos de IPSec.
- Proporciona seguridad en el flujo de datos.
- Capacidad para conservar la autenticación de los usuarios en las conexiones establecidas por IPSec.

Esta implementación puede ser clasificada en dos distintas subimplementaciones:

Implementación integrada con el Sistema Operativo (OS):

Como IPSec es un protocolo de nivel de red, puede ser implementado como parte del mismo, donde IPSec necesita los servicios del nivel IP para construir el encabezado IP. Este modelo es idéntico a la implementación de otros protocolos del nivel de red como ICMP.

Implementación que se coloca entre los niveles de red y de enlace de la pila del protocolo .

Se denomina implementación BITS (Bump in the Stack), y es utilizado para que las compañías encargadas de dar soluciones en VPN e intranets puedan proporcionan una solución completa, dado que la solución que se integra con el OS limita las capacidades para proporcionar soluciones avanzadas.

Implementación en enrutadores

La implementación en enrutadores tiene la capacidad de proporcionar seguridad al flujo de paquetes entre dos redes sobre una red pública, como lo es Internet, por medio de un túnel; además de autenticar y autorizar a los usuarios que entran a la red privada para comunicarse sobre Internet construyendo sus VPN o intranets.

Existen dos tipos de implementación en enrutadores:

1. Implementación nativa: Esta implementación es análoga a la implementación en hosts integrada con el OS. En este caso, IPSec es integrado con el software del enrutador

2.“Bump in the Wire” (BITW): Es similar a la implementación BITS, pero en este caso IPSec es implementado en un dispositivo de cifrado externo dedicado conectado a la interfaz física del enrutador. Este dispositivo normalmente no ejecuta ningún algoritmo de ruteo, sino solamente es usado para asegurar los paquetes.

A la fecha existen diversas implementaciones; sin embargo, la mayoría limitadas a la aplicación de VPNs únicamente de forma nativa, por lo que IPSec es denominado por algunos como el "protocolo VPN". En los últimos años han emergido proyectos para implementar seguridad en sistemas operativos, usando esquemas BITS, en busca de brindar una plataforma base de seguridad que sea independiente de las aplicaciones utilizadas por el usuario.