Introducción a la Seguridad con IP Seguro en Internet (IPSec)

M. en C. Mauricio Olguín Carbajal
M. en C. Israel Rivera Zárate
Profesores del CIDETEC-IPN
Adrián Martínez Ramírez
Erika Rocío Barrón
Luis Arturo Rivera Quimby
Fausto Israel Padilla Godínez.
Alumnos de Especialidad de Redes de Computadoras
UNITEC Campus Marina Nacional

Antes de que surgiera IPSec, las soluciones existentes en el mercado para conseguir la transmisión segura de datos en Internet por medio del protocolo IP eran implementaciones dependientes del fabricante que las promulgaba; dicho de otra manera, eran soluciones aisladas. Aunque suelen funcionar bien, tienen el inconveniente de que los protocolos de seguridad de distintos fabricantes son incompatibles entre sí o difíciles de conciliar; si una empresa y todos los agentes con los que se relaciona utilizan la misma solución tecnológica no habrá problema. Sin embargo, lo habitual es que exista cierta heterogeneidad en cuanto a los equipos de comunicaciones, sistemas operativos, medios de transporte de datos, etc…, lo que hace que el uso de una única solución de seguridad propietaria sea poco práctico.

IPSec fue publicado en el año de 1994 en el documento RFC 1636, logrando con su creación anular esa incompatibilidad, puesto que está basado en estándares siendo esto una ventaja a su favor. Su diseño es totalmente independiente del sistema operativo, de la plataforma computacional y de las tecnologías subyacentes empleadas, por lo que su interoperabilidad está asegurada (**Figura 1**). Además, es lo suficientemente abierto como para incorporar en el futuro los avances tecnológicos y criptográficos que sean necesarios. Tan es así que se incluye como parte integral en IPv6.

Introducción

Si bien es cierto en la actualidad se vive en un mundo en el que impera la necesidad de un constante intercambio de información vía Internet e Intranet, muchas veces dicha información debe ser confidencial, por lo que se debe proveer un medio que ofrezca seguridad para su transporte. Es importante señalar que cuando se menciona la palabra "seguro" no se habla únicamente a la confidencialidad de la comunicación, sino también se hace referencia a la integridad de los datos que para muchas compañías y entornos de negocios puede ser un requisito mucho más crítico que la confidencialidad.

Es por eso que surge IPSec el cuál cuenta con innumerables características así como cualidades que satisfacen las necesidades de seguridad, confidencialidad y autenticidad de la información.

IPSec proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP entre otros) y aborda

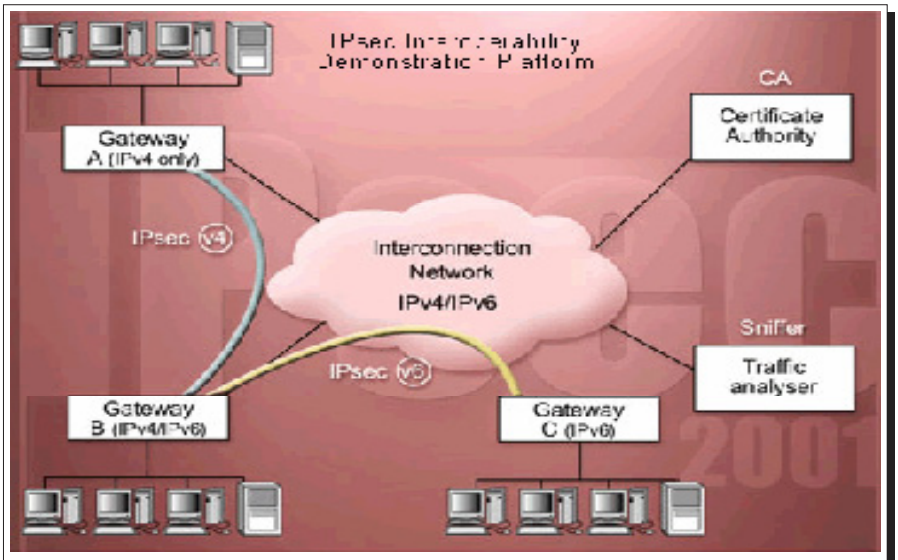

Figura 1. Plataforma IPsec.

las carencias en cuanto a seguridad del Protocolo IP. Dichas carencias son muy graves, tal como se ha constatado en los últimos años, y afectan a la infraestructura misma de las redes IP.

El Protocolo IPSec

IPSec es un estándar de gran utilidad que ofrece servicios de seguridad en redes IP de cualquier índole, el cuál está formado por un conjunto de estándares del IETF (Internet Engineering Task Force) que conjuntamente proporcionan servicios de seguridad en la capa IP de las comunicaciones entre sistemas electrónicos, y por añadidura a todos los protocolos de niveles superiores que están basados en IP (TCP, UDP, ICMP, y otros).

Hoy en día los protocolos basados en IP tienen una presencia universal en las redes telemáticas. Desde cualquier red local común hasta la propia Internet están basados en este protocolo para su funcionamiento. Uno de los problemas que enfrenta IP es la dificultad para asegurar las comunicaciones. Con "asegurar" no sólo se refiere a seguridad de acceso a sistemas (que es lo primero en que se suele pensar), sino también a establecer medios de comunicación que puedan evitar la intercepción de la información y su manipulación, así como asegurar la confidencialidad de los datos intercambiados.

Otra cuestión importante es que es capaz de proteger aplicaciones y dispositivos que, en realidad, ni siquiera conozcan la existencia de IPSec, ya que la protección se genera en las capas OSI inferiores.

Aunque muchos administradores de sistemas todavía no lo utilizan, en la actualidad IPSec está presente en la práctica en la totalidad de los equipos de comunicaciones y sistemas operativos modernos como Windows 2000/XP/2003, y otros como Solaris 10, Linux o MacOS (**Figura 2**).

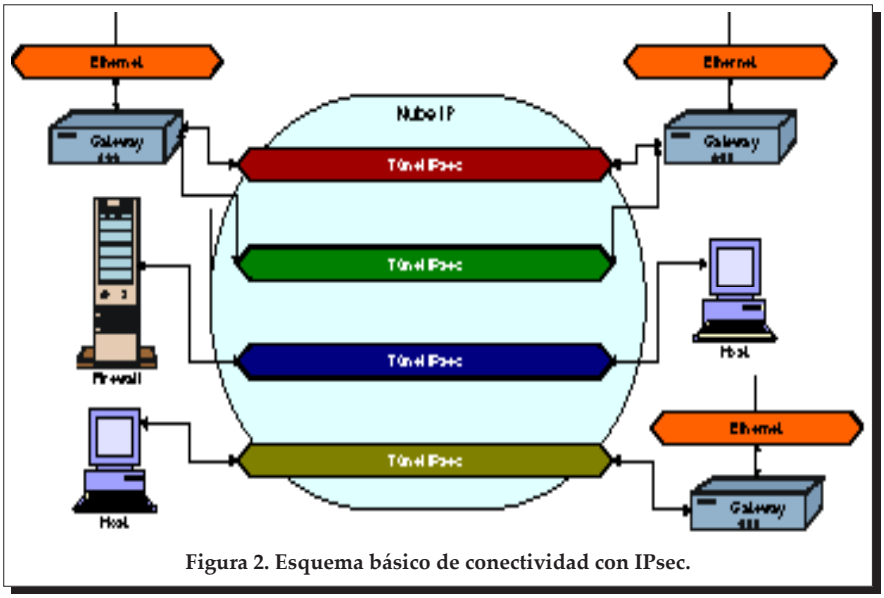

Figura 2. Esquema básico de conectividad con IPsec.

Servicios de Seguridad Ofrecidos por IPSec

IPsec tiene la capacidad de encargarse de tareas que tienen que ver con la seguridad, asumiendo la administración de todas ellas o sólo algunas en función de las necesidades que existen en cada nodo; por ejemplo:

• **Control de acceso:** Aquí se hace referencia a dos puntos importantes; autenticación y autorización. La autenticación sirve para asegurar de que los interlocutores son en verdad quienes dicen ser y que están ubicados en donde deben estar.

Por otra parte, la autorización implica que, aún cuando un interlocutor se haya autenticado éste pueda tener acceso a los recursos de red IP que solicita. Ejemplificando lo anterior, pudiera ser que un empleado cuenta con una credencial de acceso a la empresa donde labora, pero está credencial no es valida para ciertas zonas que se encuentran restringidas para dicho empleado. Lo que ofrece es algo similar a un cortafuegos con filtro de paquetes pudiéndose considerar para crearlo cuestiones como el protocolo, los puertos, las direcciones IP de origen y destino y otros parámetros técnicos de los paquetes.

• **Confidencialidad:** ofrece cifrado del tráfico de datos y ocultación del tipo de comunicación. Dicho en otras palabras, los datos son transformados carácter por carácter con la finalidad de que no puedan ser interpretados por algún intruso. Esto asegura que, aunque alguien intercepte las comunicaciones entre dos nodos, no va a ser capaz de descifrar su contenido, entendiéndose por cifrado a la transformación carácter por carácter o bit por bit.

• **Autenticación e integridad:** si bien ocultar la información es importante, la comunicación no será muy efectiva si se permite que cualquiera pueda interceptar los paquetes y modificarlos, o bien hacerlos llegar haciéndose pasar por quien no es. IPSec proporciona la capacidad de certificar que los que intervienen en la comunicación son quiénes dicen ser. También es responsable de asegurar la integridad de los datos, es decir,

que si alguien los altera durante el tránsito entre dos nodos los cambios serán detectados y no se admitirá el engaño.

• **Detección de repeticiones:** existe un tipo de ataque que permite a un usuario malintencionado capturar paquetes (aunque estén correctamente autenticados) y reenviarlos al destinatario varias veces con el objeto de que los acepte y por lo tanto el mensaje transmitido se ofusque. Para evitar este tipo de intentos, IPSec incluye un sistema de detección de paquetes repetidos. Para conseguirlo hace uso de un número de secuencia que se agrega en el encabezado de los paquetes y que va protegido por el sistema de integridad de modo que los intrusos no tienen forma de poderlo modificar.

Protocolos Básicos de IPSec

IPSec está constituido por un conjunto de estándares de criptografía que lo dotan de sus especiales características. Utiliza algoritmos de clave pública como RSA, algoritmos de resumen digital (SHA1, MD5), certificados digitales X509 y algoritmos de cifrado de clave simétrica como DES, IDEA, Blowfish o AES. Todos estos elementos forman parte de IPSec como pequeñas piezas que se pueden conectar sin interferir unas en otras. Esto hace que sea posible utilizar todo tipo de algoritmos existentes en la actualidad o en el futuro. Sin embargo, y en aras de conseguir la mayor interoperabilidad posible, la implementación mínima de IPSec debe ofrecer ciertos elementos estándar que siempre se deben soportar. En concreto, siempre estarán disponibles los algoritmos MD5 y SHA-1 para cálculo de huellas digitales (Hashes) y los algoritmos DES y triple DES para cifrado simétrico con clave privada.

El funcionamiento de IPSec está basado en la existencia de dos componentes de suma importancia:

• **El protocolo de gestión de claves llamado IKE (*Internet Key Exchange*),** que es el encargado de hacer las negociaciones de todos los parámetros necesarios de conexión y seguridad, incluyendo como su propio nombre indica, las claves utilizadas para el cifrado de datos.

• **El protocolo de seguridad**. Éste protocolo tiene como función principal proteger el tráfico de datos en IP. El estándar define dos protocolos de seguridad que pueden ser utilizados con IPSec: ***Authentication Header* (AH)** y ***Encapsulating Security Payload* (ESP)**.

A continuación se da una breve explicación de ambos. Es bueno señalar que el segundo de ellos es más completo y ofrece más funcionalidad que el primero, pero AH es una buena elección en ocasiones si no se necesita confidencialidad.

El Protocolo de Gestión de Claves

La distribución de claves de un modo seguro es fundamental para que IPSec funcione, puesto que si las claves se ven comprometidas toda la seguridad de las comunicaciones se vendría abajo y estaría en manos de cualquier intruso. Es por eso que la robustez del mecanismo de intercambio de claves es la pieza clave del sistema.

Antes de estudiar el protocolo IKE es necesario aclarar un concepto importante en IPSec: la asociación de seguridad **(SA, *Security Association*)**. Una SA es un canal de comunicación que conecta dos nodos y a través del cual se mueven en un único sentido los datos protegidos criptográficamente. Es importante resaltar el hecho de que una SA sólo gestiona datos en una dirección, es decir, de un nodo al otro con el que se comunica pero no a la inversa. Esto implica que cuando se crea una conexión IPSec protegida entre dos nodos en realidad lo que se obtienen son dos SA, una en cada sentido.

El protocolo de control IKE se encarga de intercambiar claves entre los nodos, acordar entre éstos qué algoritmos de cifrado y parámetros de control se utilizarán, y de establecer las asociaciones de seguridad (una en cada sentido). IKE no está pensado de manera específica para IPSec, sino que es un protocolo estándar de gestión de claves que se utiliza en otros ámbitos.

El proceso de negociación de la comunicación entre los dos nodos mediante IKE se lleva a cabo en dos fases. En la primera de ellas se establece un canal seguro y se autentican entre sí ambos nodos. Este canal consigue mediante un algoritmo de cifrado simétrico y un algoritmo de autenticación de mensajes. La autenticación mutua se consigue de dos formas posibles:

1. Utilización de secreto compartido. En este caso ambos nodos que se intentan comunicar deben conocer una determinada cadena de caracteres que constituye el secreto común. Mediante el uso de funciones de resumen digital (*hash*) cada nodo demuestra al otro que conoce el secreto sin tener que transmitir éste por la red. Para reforzar este mecanismo de autenticación tan débil cada par de nodos IPSec debe compartir un secreto diferente. Debido a ello, en configuraciones grandes que impliquen un número elevado de nodos, la gestión de claves con este sistema es inviable y hay que usar métodos de autenticación más robustos.

2. Utilización de certificados digitales. El uso de certificados X509v3 permite distribuir de forma segura la clave pública de cualquier nodo y solventa el problema del método anterior cuando entran en juego muchos nodos que se comunican de forma segura. Utilizando criptografía de clave pública y disponiendo de un certificado digital en cada nodo es posible comprobar la identidad de cualquiera de ellos gracias al par de claves pública / privada. La desventaja de este método es que se necesita disponer de una infraestructura de clave pública (PKI) que lo soporte, aunque no es un problema excesivamente complicado de solventar.

La segunda fase de la negociación en la comunicación es la que se encarga, tras obtener la autenticación y el canal seguro IKE, de los parámetros de seguridad específicos que se van a utilizar durante el resto de la comunicación (recuerde que IKE es un protocolo de inicio de sesión genérico que protege el establecimiento de la comunicación con el protocolo subyacente que protege, en este caso IPSec). El nodo que ha iniciado la comunicación informa al otro de todas las opciones de comunicación que tenga disponibles (algoritmos de cifrado, parámetros de éstos, etc…), con la prioridad que se haya establecido. Este último, el receptor, aceptará automáticamente la primera de las opciones ofrecidas por el emisor que coincida con las que tiene disponibles. Con esto queda establecida la sesión IPSec.

Protocolo de Seguridad AH

El protocolo de encabezado de autenticación (AH), es utilizado cuando lo único que se necesita es garantizar la autenticidad y la integridad de los paquetes IP que se intercambian en la comunicación. Es decir, asegura al nodo receptor que la información que está recibiendo procede del origen esperado y que además ésta no ha sido alterada en modo alguno durante el tránsito. Sin embargo, este protocolo no establece mecanismos para asegurar la confidencialidad de los datos, que pueden ser leídos en claro por cualquiera que los intercepte. En determinados casos puede ser una situación tolerable siendo suficiente la integridad y autenticación del origen. De este modo no se carga innecesariamente a los equipos que utilizan IPSec añadiendo un cifrado de datos si no se necesita.

Como su propio nombre deja entrever, AH basa su funcionamiento en la existencia de una cabecera de autenticación que se inserta entre la cabecera IP estándar y los datos transportados, que pueden ser TCP, UDP, etc... Su funcionamiento es, en realidad, bastante sencillo, utilizando un algoritmo de autenticación de mensajes. Lo que se hace es calcular la huella digital o hash a una combinación de una clave más el mensaje que se transmite. Esta huella digital identifica de manera única y simultánea tanto al mensaje como al emisor, ya que éste es el único, aparte del receptor, que conoce la clave utilizada. Esta clave se acuerda durante el protocolo de control IKE.

El resumen digital o extracto obtenido se incluye en la cabecera de autenticación que se transmite junto a la información. El receptor repite el cálculo en el otro extremo de la comunicación ya que tiene los elementos suficientes para hacerlo (la clave acordada durante IKE y el mensaje que se transmite en claro). Si el extracto (o huella digital) obtenido coincide con el de la cabecera de autenticación significa que ni el paquete ni el contenido han sido modificados durante el tránsito, ya que la única forma de obtener ese resultado es usando ambos elementos, y la clave sólo la conocen los dos nodos que intervienen en la comunicación.

Protocolo de Seguridad ESP

El protocolo ESP (*Encapsulating Security Payload*) ofrece la parte de la seguridad que le falta al protocolo AH: la confidencialidad. Para ello durante IKE se acuerda el modo en que se van a cifrar los datos que se transmitirán y de qué manera se incluye esta información dentro de los paquetes que se comunican. Como característica adicional ESP puede incorporar servicios de integridad y autenticación de origen, usando una técnica muy similar a la del protocolo AH.

Como es obvio, se trata de un protocolo mucho más complejo que el anterior. Encapsula los paquetes IP a transmitir utilizando una cabecera IP propia bastante compleja y una cola. Estos elementos encierran a los datos transmitidos, que se encuentran cifrados en su interior.

La confidencialidad de la información en ESP se obtiene usando un algoritmo de cifrado simétrico (que son menos costosos que los de clave pública). Lo más habitual es que se utilice un algoritmo de cifrado en bloque como DES o triple-DES, por lo que el mensaje a cifrar tiene que ser múltiplo del tamaño de dicho bloque. Este hecho obliga a veces a rellenar el mensaje para que se ajuste a esta condición, lo cual se aprovecha además para ocultar su longitud real antes del cifrado, haciendo más difícil todavía el análisis del tráfico. El proceso es similar al anterior, ambos nodos que se comunican conocen una clave que han acordado previamente. Ésta se utiliza como la clave para el algoritmo de cifrado de los datos antes de enviarlos, y también se usa para crear la cabecera de autentica-

ción. En el extremo del receptor la misma clave acordada se usa para descifrar el paquete encriptado y para comprobar la cabecera.

Es bueno recalcar que todo el sistema se vendría abajo si no existiera forma de intercambiar las claves de modo seguro. Todos los componentes de IPSec trabajan en conjunto para obtener el resultado final de alta seguridad, aunque cada uno de ellos tiene una función independiente que incluso puede ser reutilizada en otros contextos.

Modos de Funcionamiento de IPSec

Los protocolos de seguridad analizados proporcionan dos modos de funcionamiento que se pueden escoger tanto para AH como en ESP.

1. Modo transporte. Este modo de funcionamiento permite la comunicación punto a punto entre los nodos que se quieren relacionar con IPSec. Se utiliza cuando ambos extremos son capaces de utilizar directamente el protocolo IPSec.

2. Modo túnel. Este modo se utiliza cuando alguno de los dispositivos que se comunican (uno de ellos o ambos) no es el encargado de realizar las funciones de IPSec. Este es el modo de funcionamiento más habitual cuando se usan dispositivos de encaminamiento que aíslan una red privada de una pública, centralizando todo el proceso de tráfico IPSec en un único punto. De este modo, por ejemplo, los equipos internos de una red local y sus aplicaciones no tienen porqué implementar ni entender IPSec. Se comunican normalmente (sin protección alguna) con el nodo que procesa IPSec y es éste el que se encarga de realizar las funciones por todos ellos comunicándose con otro dispositivo IPSec en el otro extremo. De este modo se protegen las direcciones privadas, se centraliza la administración del protocolo de seguridad en un único punto, y se puede utilizar IPSec en sistemas que, en un principio, no estaban preparados para utilizarlo. Una de las principales aplicaciones del modo túnel es establecer de manera sencilla y barata Redes Privadas Virtuales (o VPN) a través de redes públicas. Ello permite intercomunicar entre sí, a través de Internet, redes locales o equipos aislados con las mismas garantías de seguridad que si estuviesen en una red privada, aunque usen internamente direcciones IP no válidas en la Red.

Aplicaciones de IPSec en el Día a Día

Una vez que se ha leído este documento se pudiera pensar en una multitud de aplicaciones prácticas para IPSec. Entre ellas se encuentran:

• **Control de acceso y autorización de comunicaciones.** Gracias a las capacidades de filtrado de IPSec se puede decidir exactamente cómo se realizan las comunicaciones a través de IP con cualquiera de los protocolos de alto nivel. Si además los protocolos son TCP o UDP es posible controlar qué se hace con el tráfico en función de las direcciones IP y los puertos de origen y destino. Se obtiene casi las mismas capacidades que las que ofrece básicamente un cortafuegos (salvando las distancias).

• **Conexión segura de oficinas y creación de intranets distribuidas.** Con IPSec se puede hacer que las distintas sucursales y oficinas de una empresa trabajen a través de líneas ADSL o RDSI como si estuviesen en realidad en una misma red local física y sin necesidad de líneas dedicadas punto a punto: directamente sobre Internet y con total garantía. Esto significa un elevado ahorro de costes unido a una gran comodidad.

• **Relación segura con proveedores, distribuidores, socios, y otros agentes del entorno.** Para intercambio de información comercial y técnica, emisión de datos electrónicos (EDI) y comercio electrónico entre empresas.

• **Tele trabajo y acceso de viajantes y personal desplazado.** Los trabajadores que se encuentran de viaje o trabajan desde sus casas podrán acceder a la red de la empresa con total seguridad para buscar información en ciertas bases de datos, remitir pedidos e informes, consultar su correo interno o su agenda o acceder a la Web interna departamental.

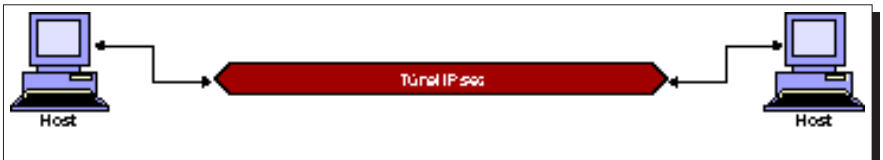

Figura 4. IPsec en modo túnel.

Conclusiones

En este artículo se ha presentado el protocolo IPSec desde el punto de vista técnico y funcional, así como algunos ejemplos de sus aplicaciones en el mundo real.

Se pudo constatar la gran importancia con la que cuenta IPSec, así como la manera en que logra conjuntar características muy importantes para poder ofrecer confidencialidad, autenticidad e integridad en una red. De igual manera se ha logrado recapitular el antes y después de la existencia de IPSEC, pudiendo dar cuenta de que dicha tecnología vino a dar una mejoría en la seguridad puesto que está basada en estándares, es decir, su diseño es independiente del sistema operativo, de la plataforma computacional y de las tecnologías subyacentes empleadas, por lo que su interoperabilidad está asegurada.

Referencias

[1] www.webopedia.com/TERM/I/IPsec.html

[2] www.netbsd.org/Documentation/network/ipsec/