SIGLAS Y ACRONIMOS

AH	Encabezamiento de Autenticación
AP	Punto de Acceso
ATM	Modo de Transferencia Asincrónica
CA	Autoridad Certificante
CHAP	Protocolo de Autenticación por Desafío
ESP	Encapsulado de Seguridad de Datos
FH	Salto de Frecuencias
ID	Identificación
IDS	Sistema de Detección de Intrusiones
IEEE	Instituto de Ingenieros Electricistas y Electrónicos
IETF	Fuerza de Tareas de Ingeniería Internet
IKE	Intercambio de Claves Internet
IP	Protocolo Internet
IPSec	Seguridad IP
IPX	Intercambio de Paquetes Internet (Novell)
ISDN	Red Digital de Sistemas Integrados
ISP	Proveedor de Servicio Internet
LAN	Red de Area Local
L2F	Despacho de Capa 2
L2TP	Protocolo de Tunelización de Capa 2
MPPC	Compresión Punto a Punto de Microsoft
MPPE	Encripción Punto a Punto de Microsoft
MS-CHAP	CHAP de Microsoft
NAT	Traductor de Direcciones de Red
NetBEUI	Interfaz de Usuario NetBIOS Extendido
NetBIOS	Sistema Básico de Entradas y Salidas de Red
OTP	Contraseña de Unica Vez
PAP	Protocolo de Autenticación de Contraseña
PDA	Asistente Digital Personal
PIN	Número de Identificación Personal
PKI	Infraestructura de Claves Públicas
PPP	Protocolo Punto a Punto
PPTP	Protocolo de Tunelización Punto a Punto
RADIUS	Servicio de Autenticación de Usuarios Remotos por Discado Entrante
RC4	Encriptador de Rivest, versión 4
SMS	Servidor de Administración de Sistemas (Microsoft)
SNMP	Protocolo Simple para Administración de Red
SSL	Capa de Sockets Seguros
TACACS+	Sistema Plus de Control de Acceso a Controlador de Acceso a Terminales
TCP	Protocolo de Control de Transmisión
UDP	Protocolo de Datagramas del Usuario
VPN	Red Privada Virtual
WAN	Red de Amplio Alcance
WEP	Protocolo Equivalente de Cableado
Wi-Fi	Fidelidad Inalámbrica
XAUTH	Autenticación Extendida

IPSec - Seguridad IP (*)

Ing. Carlos Ormella Meyer

IPSec es un conjunto de protocolos de seguridad que permite agregar encriptado y autenticación a las comunicaciones IP. Mientras el encriptado puede evitar que un usuario no autorizado como típicamente un hacker pueda leer un mensaje, el autenticado puede evitar los ataques a un sitio originados de sitios externos no deseados o hasta de dentro de la propia red del sitio.

RESUMEN EJECUTIVO

IPSec (IP Seguro) es un conjunto de protocolos de seguridad que permite agregar encriptado y autenticación a las comunicaciones IP.

Las necesidades de *privacidad*, *autenticación* e *integridad* de un mensaje se cubren con dos de los protocolos incluidos en IPSec: *AH* y *ESP*. El primero provee autenticado y por extensión también integridad, y el segundo básicamente encriptado para asegurar la privacidad.

Si bien ESP también opcionalmente puede proveer autenticación, no encapsula todo el datagrama dejando abierto el primer encabezamiento, algo que puede ser una necesidad sin exponer mayormente la seguridad.

Pero más recomendable resulta usar ambos protocolos juntos cada uno con sus funciones específicas.

IPSec es un protocolo de Capa 3 resultando totalmente transparente a las aplicaciones. Se viene usando cada vez más en las *VPNs* (Redes Privadas Virtuales) tanto para acceso remoto como intranets extendidas y especialmente en extranets.

IPsec se puede usar directamente entre las máquinas que se comunican, o bien a través de un túnel entre los dispositivos periféricos, llamados *gateways de seguridad*, que las conectan a través de Internet. Las formas de conectividad resultantes se llaman así *modo transporte* y *modo túnel* respectivamente.

Un tercer protocolo integrante de IPSec llamado *IKE* -también mencionado por su nombre anterior, ISAKMP/Oakley- se usa para un intercambio segurod de las claves con que se manejan los otros componentes de IPSec.

IKE puede operar con claves precompartidas, firmas digitales o con claves públicas basadas en certificados digitales.

El especial nivel de procesamiento que exige especialmente el encriptado a todo lo largo de los paquetes, puede señalar en algunos casos a soluciones por hardware en sitios que necesiten establecer gran cantidad de túneles y con fuerte tráfico en ellos.

S eguramente en cualquier red hay cierto tráfico que contiene información *confidencial*; pueden ser datos de compras y/o ventas, o planes de marketing que se espera no conozca la competencia, o bien datos de personas como sueldos, antecedentes, información médica, etc.

La solución típica para un problema como el planteado pasa por el encriptado de los mensajes.

Pero también la información referida al principio sólo debiera ser leída por ciertas personas, es decir por parte de usuarios autorizados para cada caso, incluso hasta probablemente no desde cualquier sitio sino desde ciertas máquinas o sistemas específicos. Este punto se vuelve más crítico a medida que se difunden las **extranets** (ver **LAN & WAN**®, abril 1999, pag. 6).

En realidad en el segundo planteo podríamos separar dos partes, especialmente cuando las comunicaciones se hacen a través de una WAN como Internet: una cosa es autenticar un sitio, una máquina, y otra autenticar o mejor dicho identificar a un usuario.

Ocurre que precisamente al intervenir una red pública y, de nuevo, muy especialmente con Internet y con mayor razón aún con una extranet, lo primero que debiera lograrse es una autenticación plena de los puntos o máquinas que se conectan, y en un segundo nivel, prever la identificación de los usuarios.

Limitándonos entonces a individualizar los sitios y máquinas que se comunican, tenemos un proceso de autenticación.

Podríamos decir entonces que nos estamos planteando una cuestión básicamente de transporte que al menos incluye la red pública de comunicaciones de datos como Internet. Al menos la conexión entre los puntos fronteras de los sitios en que se encuentran los usuarios que se quieren comunicar. Y que posiblemente sea sólo opcional la comunicación dentro ya de cada uno de los sitios en cuestión.

IPSec o Seguridad IP es una solución conjunta a la problemática planteada. IPSec es un conjunto de protocolos de seguridad de la que permite precisamente agregar encriptado y autenticación a las comunicaciones IP.

Mientras el encriptado puede evitar que un usuario no autorizado como típicamente un hacker pueda leer un mensaje, el autenticado puede evitar los ataques a un sitio originados de sitios externos no deseados o hasta de dentro de la propia red del sitio.

IPSec opera introduciendo seguridad en la capa 3 de Red. En consecuencia no hace falta introducir ningún cambio en las aplicaciones sino simplemente que el tráfico se haga bajo IP.

En este punto es conveniente hacer notar que otras soluciones de seguridad son específicas para ciertas aplicaciones. Por ejemplo **SSL** (ver **LAN & WAN**®, junio 1998, pag. 14) trabaja solamente con **HTTP**, **SSH** con sesiones Telnet, **PGP** (ver **LAN & WAN**®, junio 1999, pag. 20) u otros protocolos similares con e-mail, etc.

Como IPSec en cambio es totalmente transparente para las aplicaciones, se puede trabajar con todo lo que se cargue sobre TCP/IP como HTTP, FTP, Telnet, SMTP, etc. Incluso, si es necesario, IPSec puede trabajar con otros protocolos de seguridad de capas superiores como el ya mencionado SSL, **S/MIME** (ver **LAN & WAN**®, enero 1999, pag. 26) u **OpenPGP** (ver **LAN & WAN**®, junio 1999, pag. 22).

IPSec se ha hecho conocer especialmente por su uso preferencial en la implementación de **VPNs** (ver **LAN & WAN**®, mayo 1998, pag. 8) y en general para proveer acceso remoto a través de conexiones discadas, así como por el soporte específico por parte de proveedores como por ejemplo Cisco que lo incluye en sus enrutadores.

También es fuerte la influencia del proyecto **ANX** (*Intercambio de Red Automotor*) del Grupo de Acción de la Industria Automotor, para el cual IPSec es el principal protocolo de interoperabilidad en VPNs.

IPSec cumple requisitos más amplios de los considerados al principio. Recordemos por cierto las tres principales condiciones de una mensajería segura:

• **Privacidad o Confidencialidad**: Que el mensaje sea leído sólo por el destinatario previsto.
• **Autenticación**: Que el mensaje venga de quién dice que viene.
• **Integridad**: Que el mensaje no se haya modificado en su camino entre los extremos que se comunican.

Tal como decíamos, admeás de las tres condiciones comentadas, IPSec cubre adicionalmente otras cuestiones que pueden verse como complementarias de las anteriores. Ellas son:

• Administración automatizada de claves.
• Protección contra *replay* (repetición).

El primer punto se refiere obviamente a todo lo referente al manejo de claves y firmas digitales.

La función **antireplay** (antirepetición), por su parte, constituye una característica que refuerza la **integridad** del mensaje ya mencionada. Se trata de detectar la posible inserción de paquetes falsos en medio de una corriente de paquetes que viajan a través de Internet. Para ello se recurre a un etiquetado con números secuenciales, de modo tal que si llega un paquete con un número fuera de cierto rango establecido, el paquete se desecha de inmediato.

Adicionalmente, IPSec soporta el uso de Certificados Digitales bajo el formato estandarizado X.509 v.3. De esta manera, IPSec puede integrarse en programas **PKI** (ver **LAN & WAN**®, marzo y abril 1999, pag. 37 y 24 respectivamente) lográndose autenticación a nivel de usuarios así como superior y global seguridad de red.

La popularización de IPSec pasa por un adecuado soporte a nivel de browsers y sistemas operativos.

Mientras que hacia arriba en la pila de protocolos, IPSec se muestra como transparente, hacia abajo de la misma puede complementar otros servicios. Por ejemplo podría trabajar con L2TP el nuevo protocolo de tunelización de Capa 2. Si bien, como veremos IPSec puede perfectamente establecer túneles, un enlace remoto podría establecerse con un túnel basado en **L2TP** con autenticación propia pero con encriptado más exigente bajo IPSec.

Los protocolos que componen IPSec son ESP, AH e IKE. Los dos primeros componen los servicios de seguridad del IPSec, mientras que IKE básicamente administra las claves.

ESP (*Encapsulado de Seguridad de Datos*) y **AH** (*Encabezamiento de Autenticación*) definen básicamente los métodos de encriptado y autenticación respectivamente. De cualquier manera, ESP también puede adicionalmente ofrecer autenticación. Más adelante se revisará más la aparente superposición así como la decisión de optar por el uso de ambos protocolos o uno de ellos solamente.

IKE (*Intercambio de Claves Internet*), por su parte, es el protocolo de maneja las claves entre dos dispositivos que se comunican estableciendo sendas conexiones cada una de ella conocida como **SA** (*Asociación de Seguridad*). IKE es el nuevo nombre usado en lugar de ISAKMP/Oakley con la versión 8 de **ISAKMP** (*Protocolo de Administración de Claves y Asociación de Seguridad Internet*) y Oakley, un protocolo de distribución de claves. IKE en realidad es un híbrido de ISAKMP, Oakley y **SKEME**, donde este último presenta una técnica versátil para el intercambio de claves.

La operación con IPSec se facilita gracias al propio IP de Capa 3. Efectivamente, este protocolo tiene en su encabezamiento un campo denominado **Protocolo** de 8 bits.

Dicho campo permite individualizar el protocolo que sigue al IP y que si bien en principio podría ser lógicamente de Capa 4 de Transporte (TCP o UDP para el caso), también podría ser otro protocolo de Capa 3 que aunque sea parte del IP trabaje como complemento del mismo requiriendo su identificación específica. Aquí es donde justamente aparece un protocolo como **ICMP**, de "reconocido" uso por parte de muchos hackers (ver **LAN & WAN**®, mayo 1999, pag. 16/17).

Los protocolos en cuestión se identifican por un número asignado por **IANA** (*Autoridad Internet de Números Asignados*). Así tenemos los más conocidos 1 para ICMP, 6 para TCP, 17 para UDP, etc. Y, precisamente, para los protocolos de seguridad ya mencionados del IPSec se asignaron los números 50 para el ESP y 51 para el AH.

De esta manera entonces se puede insertar el encabezamiento IPSec adecuado entre el encabezamiento IP y el de Capa 4, por ejemplo TCP. El nuevo encabezamiento (ESP o AH) se insertará *después* del encabezamiento IP y *antes* del encabezamiento TCP o UDP de Capa 4.

De la manera indicada incluso el sistema es compatible también como la nueva versión del IP, **IPv6** (ver **LAN & WAN**®, junio 1997, pag. 30). Mientras que con esta última versión todos los dispositivos de red tendrán que manejar IPSec, con la versión actual se está incorporando a enrutadores, firewalls, conmutadores y servidores de acceso remoto, entre otros.

Adicionalmente a los servicios de seguridad, IPSec se puede trabajar con compresión. Para el caso se usa **LZW** (Lempel-Ziv-Welch) presente por cierto en muchos enrutadores. Sin embargo la compresión debe hacerse antes del encriptado porque de lo contrario generalmente en reducir la extensión tiende a aumentarla en alrededor de un 10 %. Hay que tener presente que el proceso de compresión permite un mejor rendimiento en cuanto a tiempo de respuesta al usar mejor el ancho de banda correspondiente. Adicionalmente puede mejorar el aspecto de seguridad al reducir la necesidad de fragmentar paquetes (proceso en que se pueden producir intrusiones indebidas).

MODOS DE OPERACION

Una **SA** o *Asociación de Seguridad* detalla los servicios de seguridad que se aplicarán al tráfico correspondiente entre dos dispositivos que se conectan. Cada extremo que se comunica establece una SA intercambiando las claves de seguridad correspondiente. Más adelante se ve más en detalle el concepto SA.

Aquí se presentan dos alternativas para extender las características de seguridad del IPSec. Puede serlo sólo al medio de transporte a través de una WAN pública como Internet, para lo cual se lo instala en los dispositivos de borde o frontera de cada extremo de la WAN (enrutadores o firewalls) que para el caso operan como **gateways**. Pero también se puede extender de extremo a extremo entre las propias máquinas o hosts que se comunican.

La protección del IPSec en cada caso es muy diferente.

Cuando la conexión se realiza entre los hosts extremos que se comunican, el datagrama queda con el encabezamiento IP original (y único en este caso) al frente del mismo, con la inserción interna del encabezamiento IPSec y encriptado correspondiente que entonces actuará sólo sobre las capas superiores (TCP o UDP). Este modo de operación se llama **Transporte** (parte superior de la Figura 1).

Para operar en este modo es necesario que las máquinas que se comunican soporten IPSec. En este modo de operación si bien los datos van encriptados, el encabezamiento IP queda sin encriptar, es decir con las direcciones de origen y destino a la vista y, por lo tanto, expuestas a un escaneado y posible uso indebidos.

La otra alternativa es más usual. Ahora los hosts que se comunican lo hacen por medio de los gateways que se conectan a la WAN. Figurativamente puede decirse que los gateways establecen un túnel a través del cual pasan los paquetes de los hosts en cuestión. Por esto precisamente este modo de operación se llama **Túnel** (parte inferior de la Figura 1).

Un túnel se establece anteponiendo al datagrama de capa 3 un *nuevo* encabezamiento IP con las direcciones IP de los gateways de origen y destino, encabezamiento que entonces encapsula al paquete original. De esta manera el encabezamiento IP original, con las direcciones IP de los "verdaderos" origen y destino (es decir los hosts) puede protegerse por medio del encriptado. Con este modo de operación no hace falta hacer ningún cambio en los hosts que se están comunicando a través de los gateways, puesto que simplemente los paquetes correspondientes se tunelizan y destunelizan en cada gateway que para el caso soportan IPSec.

Precisamente por todo lo comentado en este punto, para las comunicaciones bajo IPSec directamente entre extremos el modo de transporte es una opción. Para un mayor grado de seguridad también se puede establecer un túnel al estilo de los gateways comentados antes. Esta situación es aplicable por ejemplo con usuarios remotos o móviles que no están en red y generalmente entran a Internet vía líneas telefónicas discadas. Claro que estas máquinas aisladas deben soportar IPSec en la pila de protocolos.

Muchos enrutadores, firewalls y servidores de acceso remoto soportan IPSec en el modo túnel, mientras que hay software de base y aplicación en los que se implementa el modo transporte.

Veamos un poco el detalle de ambos modos de comunicación.

Modo Transporte

El modo de transporte responde a la forma nativa de comunicación bajo IPSec, puesto que puede cumplir sus funciones básicas de encriptado y autenticado a todo lo largo de una comunicación.

Ya dijimos que en este modo el encabezamiento IPSec se inserta entre el encabezamiento IP (el único en este modo) y el encabezamiento siguiente, generalmente de Capa 4, TCP o UDP.

El modo de transporte puede ser útil especialmente para evitar accesos indebidos dentro de las propias redes donde se encuentra cada una de las máquinas que se comunican. Tengamos presente que en este caso los datos de los paquetes bajo IPSec viajan encriptados no sólo a través de Internet sino dentro de las propias LANs o intranets de los extremos.

Modo Túnel

Ya dijimos que en el modo túnel se usan sendos gateways entre las redes que se comunican. Se podría pensar que puede bastar instalar un único túnel entre dos redes específicas para las comunicaciones de los hosts pertenecientes a las mismas. Pero esto no es así. En realidad hace falta *un túnel por cada máquina que se conecta*; por lo tanto entre dos redes podría haber varios túneles en "paralelo".

Como hemos comentado antes, el encriptado y la propia autenticación se realizan entre los gateways de las redes que se comunican. Los paquetes que van tanto desde un host al gateway de su red como los que hacen el recorido inverso de gateway a host viajan en texto plano sin encriptar. En todo caso se supone que cada una de las redes es segura en sí misma.

La mayor seguridad que ofrece el modo túnel en el recorrido entre gateways es que tanto los datos como el encabezamiento IP original y el TCP viajan encriptados, y lo único en texto abierto es el nuevo encabezamiento IP que simplemente comunica los gateways así como el encabezamiento ESP (que por otra parte se autentica), tal como se ve más adelante. Esto nos dice entonces que visto desde dentro del propio Internet no sólo no se pueden leer los datos propiamente dichos sino que tampoco se puede saber ni de qué máquina viene ni a qué máquina va el paquete en cuestión.

Para instalar un túnel IPSec cada gateway se configura definiendo los puntos extremos o subredes que se comunican, los algoritmos de encriptado y autenticado (es decir de hecho si trabajarán bajo AH o ESP) e incluso, si se usa, el secreto precompartido que permite identificar a los extremos que se comunican, tema que también se revisa más adelante.

La configuración de una máquina es un proceso directo y sin complicaciones. Cuando hay subredes el proceso es más complejo debido a la forma en que IKE realiza la negociación de una SA y las fases con las que trabaja surge de lo que se expone en el punto correspondiente.

El modo túnel es usual entre firewalls que operen también como gateways de seguridad entre redes que se conectan a través de Internet. Incluso se puede aprovechar el encapsulado y seguir usando direcciones IP internas no registradas.

AUTENTICACION E INTEGRIDAD

La palabra autenticación puede ser algo confusa especialmente por el múltiple uso que se le da. No precisamente por el sentido original del vocablo mismo sino por el dativo respecto a qué se aplica.

Efectivamente, en nuestro caso se puede autenticar el autor de un mensaje, o el origen de una dirección IP, o el contenido de un mensaje. Sin embargo la "autenticación" de un mensaje se asocia en términos de seguridad informática a la **integridad** del mismo, algo que puede realizarse a nivel de aplicación, es decir con el mensaje completo.

Necesitamos una solución similar para autenticar usuarios, algo que sabemos no pueden manejar las capas inferiores del modelo OSI. Concretamente para autenticar el autor de un mensaje se necesitará un mecanismo como los **certificados digitales** (ver **LAN & WAN**®, junio 1998, pag. 16) basados en X.509, tal que con el sistema de doble clave permita que el mensaje sea encriptado con la clave privada del autor del mensaje de modo tal que al desencriptarla con su clave pública identifique completamente al autor del mensaje. Sin embargo los certificados digitales requieren la intervención de una **CA** es decir una *Autoridad de Certificación*. Los certificados digitales no forman parte de IPSec aunque lógicamente se pueden usar.

También se puede trabajar con una contraseña que asume la forma de secreto precompartido entre las partes.

Por otra parte se dispone de un proceso de autenticación que incluya todo un datagrama, es decir básicamente el encabezamiento IP y el campo de datos correspondiente, el mecanismo de autenticación no sólo puede servir para acreditar la dirección IP de origen (es decir que el paquete viene de la máquina que dice venir) sino también los propios datos del datagrama.

Para autenticar usuarios también se podría recurrir a mecanismos como tarjetas token o RADIUS (ver **LAN & WAN**®, octubre 1998, pag. 22).

También se necesita autenticar los intercambios de claves (que maneja IKE según se ve más adelante) entre dos hosts, para lo cual hay varios procedimientos según veremos.

La autenticación se puede realizar de varias maneras. La forma original de hacerlo es mediante un mecanismo de clave compartida entre las partes (y que maneja el protocolo IKE según se ve más adelante). Para el caso el host que envía un datagrama calcula un valor de chequeo resultante de los datos del datagrama y de dicha clave, valor que agrega a la cola del datagrama en un campo denominado **Datos de Autenticación** para su posterior envío. El host que recibe el datagrama separa el valor de chequeo recibido por un lado y vuelve a tratar el datagrama con la clave compartida. Si el resultado obtenido coincide con el valor de chequeo recibida, considera válido el datagrama en cuestión.

El resultado agregado al datagrama original recibe el nombre de **MAC** o *Código de Autenticación del Mensaje* aunque también se lo conoce como **ICV** o *Valor de Chequeo de Integridad* y como *Suma de Chequeo Criptográfico*. Por supuesto que este MAC nada tiene que ver con otro MAC más conocido de capa 2 es decir el *Control de Acceso al Medio* que incluso aparece como el primer encabezamiento de un paquete (Figura 2).

Si bien originalmente para las claves se usaron cifradores en bloques (como DES), últimamente se han desarrollado versiones MAC en que se usan funciones **hash** como **MD5** (*Compendio de Mensajes # 5*), desarrollado por RSA Data Security, o **SHA-1** (*Algoritmo Hash Seguro # 1)*, desarrollado por el gobierno americano y que suele referirse simplemente como SHA. Las ventajas de estas versiones radica en que las funciones *hash* son más rápidas cuando se las implementa por software, no hay restricciones de exportación y hay muchas bibliotecas gratuitas disponibles.

En forma similar a lo comentado antes, en el mecanismo de autenticación de un datagrama con una función *hash* se toma una clave como segundo parámetro de entrada y por lo tanto la salida del depende tanto del datagrama como de la clave. De manera similar al tratamiento de mensajes con funciones *hash*, la salida es un **compendio** (*digest*) del datagrama original. Como ya sabemos, el compendio de un mensaje sirve para comprobar la integridad de un mensaje, es decir que no haya sido modificado en su tránsito.

Las versiones de mecanismos de autenticación que trabajan con funciones *hash* son una forma de *funciones seudoaleatorias* (*prf*) y se conocen como **HMAC**, es decir *MAC con hash*. HMAC está definido en la RFC 2104 (ver recuadro **El Proceso HMAC**) y las claves están generadas por medio de mecanismo IKE.

Específicamente, para los sistemas ya mencionados se habla de **HMAC-MD5** y **HMAC-SHA** que, por otra parte, también suelen mencionarse como **MD5 con clave** y **SHA con clave**, respectivamente.

EL PROCESO HMAC

Si bien simplificadamente se puede decir que una clave compartida se agrega al datagrama tras lo cual se aplica al conjunto la función *hash*, el proceso es más elaborado. Efectivamente, con HMAC la operación de compendio se realiza dos veces.

En una primera etapa, se aplica a la clave la operación OR exclusive con una cadena fija de entrada de 64 bytes anexando el resultado al mensaje, tras lo cual se aplica al conjunto la función *hash*. La segunda etapa consiste en anexar lo obtenido en la etapa anterior al resultado de una nueva operación OR Exclusive con una cadena fija de salida de 64 bytes, para finalmente aplicar al conjunto nuevamente la función *hash*.

Cuando se trabaja con MD5 el compendio producido tendrá 16 bytes (128 bits) mientras que con SHA-1 será de 20 bytes (180 bits). Sin embargo la misma norma acepta el uso del resultado en forma *truncada*, de modo que en la cola del datagrama el campo Datos de Autenticación puede tener una extensión menor que las referidas. En este caso se refiere, por ejemplo, como HMAC-MD5-80 para indicar que sólo se transmiten los primeros 80 bits (10 bytes) del compendio.

PRIVACIDAD

De cualquier manera, la autenticación es sólo eso: Un paquete IP puede autenticarse pero aún así su contenido está en texto plano es decir directamente leíble.

Para *Acuerdo (compliance) con IPSec*, la norma RFC 2406 ha establecido un único algoritmo de encriptado, el **DES** (*Norma de Encriptado de Datos*) en el modo **CBC** (*Encadenamiento de Bloques de Cifrado*) generalmente reconocido como DES-CBC. La operación con CBC (ver **LAN & WAN**®, junio 1999, pag. 24) necesita trabajar con un **IV** (*Vector de Inicialización*) explícito para establecer el estado inicial del algoritmo. Puede operar con claves de 40 o 56 bits, siendo la primera extensión la permitida para exportar de USA.

Se encuentran otros algoritmos simétricos (ver **LAN & WAN**®, enero 1999, pag. 27), tales como:

• **Triple DES** o simplemente **3DES**; es el DES de 56 bits corrido tres veces consecutivas. También se lo usa en el modo CBC, es decir 3DES-CBC. Hay dos versiones: 3DES de 112 y 168 bits donde estos números se refieren a que usan dos o tres claves respectivamente.
• **RC5** (*Encriptador de Rivest, versión 5*) trabaja con claves de longitud variable de hasta 256 bits.
• **IDEA** (*Algoritmo Internacional para Encriptado de Datos*) encripta en bloques de 64 bits con claves de 128 bits.
• **Blowfish** trabaja en bloques aceptando claves de longitud variable de 32 a 448 bits.
• **CAST** acepta claves de longitud variable de 40 a 128 bits y trabaja en bloques de 64 bits.

ENCABEZAMIENTO DE AUTENTICACION, AH

Este encabezamiento permite realizar la autenticación de los datagramas asegurando la integridad de los datos incluyendo la dirección IP de origen, así como también proporcionar protección contra las repeticiones (replay) de datagramas.

Los datos de autenticación surgen como ya se vió de combinar una función *hash* con una clave. El valor correspondiente se coloca en el campo Datos de Autenticación.

Por su parte, la protección de replay se provee por medio del campo Número de Secuencia.

En cuanto a los modos de operación (parte izquierda de la Figura 3) tenemos que en el modo transporte AH se inserta a *continuación* del encabezamiento IP y antes del ESP (si se trabaja también con este protocolo) u otro encabezamiento de protocolo de mayor nivel como TCP o UDP.

A su vez, en el modo túnel AH se inserta por *delante* del encabezamiento IP. Un nuevo encabezamiento IP se agrega por delante del conjunto. Si bien la autenticación cubre también este último campo, la norma especifica que no lo hará sobre los campos que puedan cambiar de valor en la trayectoria. Esto puede ocurrir, por ejemplo, con el campo **Tiempo de Vida** cuyo valor va decreciendo de a uno cada vez que el datagrama pasa por un enrutador.

El **encabezamiento AH** (Figura 4) está definido en la RFC 2406 y tiene los siguientes campos:

• **Próximo Encabezamiento**: 1 byte.
• **Longitud del Encabezamiento**: 1 byte (expresado en palabras de 32 bits, menos 2).
• **Reservado**: 2 bytes.
• **SPI**: 4 bytes.
• **Número de Secuencia**: 4 bytes.
• **Datos de Autenticación**, más conocido como **MAC** o **ICV**: máximos de 16 (MD5) o 20 (SHA-1) bytes, o menos todavía -aunque con un mínimo de la mitad en cada caso- si se trabaja en la forma *truncada*.

Detalles de algunos de los principales componentes son los que siguen:

• **Próximo Encabezamiento**. Identifica el tipo de datos de la carga útil, es decir el campo que sigue al AH. Para identificar al protocolo de la capa superior usa la misma numeración del campo Protocolo del IP original (es decir: 1 para ICMP, 6 para TCP, 17 para UDP, etc.).
• **SPI** o *Indice del Parámetro de Seguridad*: número arbitrario de 32 bits que define para el receptor el grupo de protocolos de seguridad que se está usando: algoritmos y claves así como la duración de estas últimas y su correspondiente refresco periódico para prevenir ataques.
• **Número de Secuencia**. Conocido anteriormente como *Prevención de Repetición* (*Replay Prevention*), es un número que por medio de unn contador va aumentando de a 1 cada vez que se aplica a un paquete consecutivo enviado a una misma dirección y usando el mismo SPI. No sólo mantiene el orden sino que protege contra ataques replay o sea cuando un atacante copia un paquete y lo envía fuera de secuencia para confundir a los extremos. La función antirepetición es opcional pero este campo siempre aparece en cada datagrama pese a que la máquina que lo reciba pueda no usarlo. Aunque por su longitud de 32 bits puede llegar a casi 4.300 millones antes de volver a comenzar, los contadores tanto del transmisor como receptor deben resetearse antes de alcanzar el máximo. El reseteo implica establecer una nueva SA y por lo tanto una nueva clave.
• **Datos de Autenticación**. Es el compendio calculado que servirá al receptor para compararlo con el que obtenga luego de aplicar la misma función *hash* al datagrama.

AH puede usarse solo, con ESP (como se ve más adelante) o bien anidado cuando se usa en el modo túnel.

ENCAPSULADO DE SEGURIDAD DE DATOS, ESP

Es el mecanismo para proveer privacidad o confidencialidad a datagramas IP por medio del encriptado de los datos correspondientes. Adicionalmente puede proveer autenticación.

A diferencia del AH, el ESP afecta a un datagrama en más de un sitio: agrega un encabezamiento propio así como una cola y a veces también información en el campo de datos. La cola por cierto también varía según si se trabaja no sólo con encriptado sino también con autenticado.

De la misma manera que el AH, en el modo transporte el encabezamiento ESP (parte derecha de la Figura 3) se inserta a *continuación* del encabezamiento IP y antes de otro encabezamiento de protocolo de mayor nivel como TCP o UDP.

A su vez, también en forma similar al AH, en el modo túnel el encabezamiento ESP se inserta por *delante* del encabezamiento IP, y se agrega un nuevo encabezamiento IP por delante del conjunto. Si bien la autenticación cubre también este último campo, la norma especifica que no lo hará sobre los campos que puedan cambiar de valor en la trayectoria. Esto puede ocurrir, por ejemplo, con el campo **Tiempo de Vida** cuyo valor va decreciendo de a uno cada vez que el datagrama pasa por un enrutador.

En ambos modos el **encriptado** incluye todos los campos *posteriores* al encabezamiento ESP (pero no éste mismo), mientras que el **autenticado** incluye todo lo encriptado *más* el propio campo ESP.

Con respecto al autenticado debe notarse que *con ESP no se autentica el encabezamiento IP externo*, es decir el encabezamiento IP original en el caso del modo transporte, o el encabezamiento IP agregado en el modo túnel.

Veamos cada una de las partes de un datagrama bajo ESP tal como está definido en la RFC 2406 (Figura 5).

El **encabezamiento ESP** tiene los siguientes campos:

• SPI: 4 bytes.
• Número de Secuencia: 4 bytes.

El **campo de datos IP** comienza como es usual con el encabezamiento TCP, seguido por los datos propiamente dichos de las capas superiores. Pero si se requiere el Vector de Inicialización, IV, este encabezamiento inicia el campo de datos seguido por el TCP.

La **Cola del ESP** tiene los siguientes campos:

• **Relleno**: para completar con el campo de datos un múltiplo de 32 bits.
• **Longitud de Relleno**: identifica el anterior.
• **Próximo encabezamiento**: 1 byte.
• **Datos de Autenticación**, también referido como **MAC** o **ICV**. Es opcional y sólo aparece si se usa ESP con autenticación. Tiene 16 (MD5) o 20 (SHA-1) bytes, o menos todavía -aunque con un mínimo de la mitad en cada caso- si se trabaja en la forma *truncada*.

Veamos algunos detalles de los principales componentes.

• **SPI** o *Indice del Parámetro de Seguridad*. El mismo del AH.
• **Número de Secuencia**. Igual que en el caso del AH.
• **Datos de la Carga Util**. Longitud variable. Si el algoritmo con que se lo encripta requiere datos de sincronización, es decir lo que se llama **IV** o *Vector de Inicialización* (ya mencionado antes) los datos correspondientes pueden ir en este mismo campo.
• **Relleno**. Básicamente se usa por dos motivos. Por un lado si el algoritmo de encriptado requiere que el texto a encriptar sea un múltiplo de cierta cantidad de bytes (dado por ejemplo por el tamaño de los bloques con que trabaja). También es necesario para hacer que el encabezamiento hasta este punto tenga una longitud que sea un múltiplo impar de 16 bits. De esta manera los dos próximo campos que siguen, de 8 bits cada uno, harán que el encabezamiento incluyéndolos sea un múltiplo par de 16 bits.
• **Longitud del relleno**. Indica la longitud del campo anterior.
• **Próximo Encabezamiento**. Identifica el tipo de datos de la carga útil del propio ESP. Bajo IPv4 identifica al protocolo de la capa superior usando la misma numeración del campo Protocolo del IP original (es decir: 1 para ICMP, 6 para TCP, 17 para UDP, etc.).
• **Datos de Autenticación**. El mismo del AH.

ESP puede usarse solo con encriptado así como con encriptado y autenticado. También puede usarse con encriptado *Nulo*, es decir sin encriptado pero con autenticado, forma que se comenta en el punto siguiente. Finalmente, ESP también puede usarse en combinación con AH según se ve enseguida.

¿AH o/y ESP?

Si lo único que se busca es *integridad* del contenido de un datagrama incluyendo la dirección IP de origen, el AH puede proveer perfectamente la autenticación necesaria.

Si sólo se busca *confidencialidad o privacidad* en cuanto a la recepción por parte del host debido, hay que encriptar usando ESP.

Como vemos, en principio ninguno de los dos mecanismos de seguridad ofrece una solución completa. Y, por otra parte, no es muy conveniente usar encriptado sin autenticación.

Si se necesitan ambas cosas, se presentan dos opciones. O se usa ESP con autenticación, o bien se trabaja con ESP y AH combinados. Veamos cada caso.

ESP con autenticación propia ofrece mejor rendimiento que usando ESP y AH combinados. Esto se debe principalmente a que se trabaja con una única operación HMAC.

Sin embargo, la autenticación ESP no es la misma que con AH. Efectivamente, a diferencia de AH, ESP no protege -es decir no autentica- el primer encabezamiento IP -sea el original en el caso del modo transporte, sea el agregado en el modo túnel. Cualquier alteración en dicho primer encabezamiento permitiría por ejemplo aprovechar la fragmentación de datagramas IP cambiando valores en el campo correspondiente y de esta manera insertar datagramas de ataque; otra posibilidad es que ante la ausencia de información de la longitud del resto del datagrama (el encabezamiento TCP no la proporciona) se facilitan posibles agregados ilegítimos y el correspondiente asalto a una sesión por parte de un hacker.

Por otra parte hay implementaciones que pueden conducir al uso combinado de ESP y AH. Un ejemplo puede ser cuando los hosts que se comunican están en sendas subredes por detrás de los correspondientes gateways de seguridad. En este caso los hosts podrían implementar correr IPSec bajo AH mientras que los gateways tunelizarían bajo ESP con sólo encriptado. De esta manera en el túnel a través de Internet se daría la combinación ESP y AH.

Comentamos antes el caso del ESP con encriptado *Nulo*, es decir sin encriptado pero con autenticado, De esta manera se logra una especie de AH pero manteniendo sin autenticar el encabezado IP, lo que permite trabajar con **NAT** (*Traductor de Direcciones*).

ASOCIACION DE SEGURIDAD, SA

Ya dijimos que los dispositivos que quieren comunicarse bajo IPSec establecen una conexión denominada **SA** o *Asociación de Seguridad* que especifica los servicios de seguridad que se aplicarán al tráfico correspondiente.

Una SA es una conexión IPSec entre dos hosts, o entre dos gateways VPN, o incluso entre un host y un gateway extremo de un túnel IPSec. Como en realidad una SA es unidireccional, habrá dos SAs por cada conexión. Además, dos mismos extremos pueden establecer múltiples pares de SAs, uno para cada sesión de comunicaciones. Además, es función de IKE establecer la negociación automática de SAs.

Básicamente se identifica una SA por medio de un número de 32 bits elegido aleatoriamente, llamado SPI, y por la dirección de destino correspondiente. El número en cuestión se inserta en el encabezamiento IPSec. En el otro extremo dicho número permite identificar la SA correspondiente y, por lo tanto, el procesamiento en cuestión.

Una base de datos relaciona SPI con los parámetros que se quiere caractericen la conexión. Los principales datos de dicha base de datos son el algoritmo identificador (clave) de autenticación AH; algoritmo identificador (clave) de encriptado ESP; tiempos de vida de las claves, y el IV o Vector de Inicialización para establecer el estado inicial de los algoritmos.

La SA define los parámetros de una conexión IPSec en una base de datos adecuada. Entre estos podemos mencionar el el servicio de seguridad es decir protocolo IPSec usado (AH o ESP), los algoritmos de encriptado y autenticación a usar en las comunicaciones, así como las propias claves incluyendo las de cada sesión de encriptado, existencia y tamaño de algún elemento de sincronización de encriptado (IV), el tiempo de vida de las claves y de la propia SA, y otros parámetros adicionales de control.

Si bien no es parte de la especificación IPSec algunos productos permiten estipular la vida de una clave no sólo en segundos sino también en bytes. Esta última variante viene bien para grandes transferencias como backups.

Respecto a los servicios de seguridad propiamente dichos, las SAs pueden estar orientadas a host o al propio usuario.

Una SA **orientada al host** trabaja con la misma clave de sesión para todos los usuarios de dicho host. Esta forma es la más común.

Con una SA **orientada al usuario**, en cambio, cada usuario tendrá una clave de sesión diferente.

IKE

El intercambio de claves puede realizarse de tres maneras: **Manual**, **SKIP** e **ISAKMP/Oakley**.

En ambientes pequeños se puede usar el método manual especificado en la RFC 1825, donde el usuario configura manualmente cada sistema con su propia clave así como con las claves de otros sistemas. Se pueden

usar claves para cada enrutador, o para el firewall que conecta un sistema a Internet en cuyo caso se puede seleccionar qué tráfico encriptar y cuál no. Los proveedores permiten establecer un archivo plano que relaciona los identificadores de una SA con los parámetros correspondientes.

Las otras dos formas de intercambio de claves ya responden a sistemas de administración automática de claves.

En primer lugar tenemos **SKIP** o *Administración Simple de Claves para Protocolos Internet* fue propuesto por Sun e implementado originalmente por algunos fabricantes. Realiza la distribución de claves a nivel de paquetes soportando una transferencia segura en base al sistema de dos claves de Diffie-Hellman. Sin embargo la IETF no la adoptó finalmente como norma.

La norma elegida, **ISAKMP** o *Asociación de Seguridad Internet y Protocolo de Administración de Claves* combinada con Oakley fue elegida como norma para IPv6 y opcional para IPv4.

ISAKMP no establece las claves de una sesión, tarea que en este caso asume Oakley al permitir diferentes métodos de autenticación incluyendo variantes con **desconocimiento** (*repudio*) o **no desconocimiento** (*no repudio*) de la recepción de un mensaje, así como la negociación de los atributos de la SA. La flexibilidad en los métodos de autenticación facilita no sólo el establecimiento de VPNs (ver **LAN & WAN**®, mayo 1998, pag. 8) sino incluso el acceso a la red de una empresa por parte de trabajadores a domicilio o *telecommuters* (ver **LAN & WAN**®, noviembre 1998, pag. 6).

Opcionalmente también se puede lograr **Secreto Perfecto de Entrega**. Este concepto se refiere a un método para generar una nueva clave que no dependa de la que esté en uso.

Hoy en día la norma ha sido renombrada como IKE o Intercambio de Claves Internet. En IKE, en realidad, al par ISAKMP/Oakley se incorpora un técnica conocida como SKEME para un intercambio más versátil de las claves.

Una vez que un host reconoce la identidad del otro y viceversa, los intercambios de información bajo IKE se realizan por medio de mensajes en el puerto 500 del UDP.

En las operaciones con IKE los host generan un valor que los identifica: un **cookie**. Los *cookies* tienen una extensión de 8 bytes y una de las formas recomendadas de generarlos es aplicando una función *hash* rápida como MD5 a un conjunto formado por las direcciones IP de origen y destino, los puertos UDP de origen y destino, y un secreto local de caracter aleatorio. Un *cookie* así formado no sólo identifica un host sino que permite identificar y rechazar mensajes inválidos sin necesidad de recurrir al encriptado con la consiguiente carga de ciclos de máquina. De esta manera incluso se logra una herramienta eficiente contra ataques del tipo Negación de Servicio (ver **LAN & WAN**®, mayo 1999, pag. 16).

El intercambio de claves provisto por IKE se realiza en *dos fases* o pasos referidas al establecimiento de sendos pares de SAs, la primera relacionada específicamente con IKE en cuanto a la transferencia de parámetros de seguridad y la segunda con el IPSec propiamente dicho, es decir, las claves de autenticado y encriptado para la transferencia de los datos.

Operativamente la fase 1 puede verse como la generación de una clave maestra y subsidiarias, mientras que en la fase 2 se derivan de las anteriores las claves que se usarán para la transferencia de datos.

Fase 1

Esta fase puede verse como el establecimiento de la política básica de seguridad. Para ello el host que inicia la negociación de una SA envía una o varias propuestas al otro host. Estas propuestas definen los protocolos de autenticación y encriptado posibles, la vida de las claves y si se usará Secreto Perfecto de Entrega. La respuesta del segundo host incluirá la elección apropiada correspondiente. Todo este proceso implica un uso intensivo de recursos como se comenta luego.

En esta fase se establece el intercambio de claves autenticadas. Hay cuatro métodos diferentes de autenticación: firma digital, dos variantes con encriptado de clave pública y clave precompartida.

Las diferencias aparecen en la determinación de la denominada **clave maestra**.

• **Firma Digital**. Esta solución trabaja bajo el algoritmo de combinación Diffie-Hellman en forma similar al sistema de claves públicas, aunque son los propios hosts los que generan sus propias claves (pública y privada). Para distinguir este método del tradicional es costumbre usar la palabra **valor** en lugar de *clave*; cada host genera entonces su propio par **valor público** y **valor privado**, similares conceptualmente a la *clave pública* y *clave privada*. Se basa en el **valor secreto compartido** de Diffie-Hellman aplicado a la concatenación de números aleatorios generados por ambas partes que se usan *una única vez* y se conocen como **nonces** o **ad-hoc**.

• **Encriptado de Clave Pública**. Se basa en la aplicación de una función *hash* a la concatenación de ambos *nonces* con la concatenación de ambos *cookies*.

• **Claves Precompartidas**. Aplica la clave precompartida a la concatenación de los *nonces*.

La autenticación con *firma digital* se basa en que el intercambio se autentica firmando un *hash* que ambos hosts pueden obtener.

Gracias al encriptado la autenticación con *encriptado de claves públicas* ofrece una notable ventaja respecto de la autenticación con firma digital. Esto no es sólo por la doble barrera interpuesta a un hacker (intercambio Diffie-Hellman y encriptado) sino también porque cada host puede reconstruir en forma independiente cada lado del intercambio.

Sin embargo, el encriptado tradicional con claves públicas agrega un considerable overhead ya que hay que realizar dos operaciones de encriptado con una clave pública y otras dos de desencriptado de una clave privada.

Aquí precisamente aparece el *modo revisado de encriptado con clave pública* que reduce a la mitad las operaciones comentadas gracias a trabajar con una clave derivada del *nonce*.

Finalmente, el sistema de *clave precompartida* implica un procedimiento previo ajeno a IKE para establecer dicha clave. IKE simplemente la usará para autenticar el intercambio. Por cierto hay que tener presente que la clave sólo puede identificarse por medio de la direcciones IP de los hosts.

En lo que sigue nos referiremos específicamente al sistema de firma digital. También nos permitimos usar directamente la palabra **clave** en lugar de *valor* por ser la forma habitual de referirse a los elementos correspondientes aunque no provengan de un sistema de claves públicas con la correspondiente **CA** (*Autoridad de Certificación*).

La fase 1 se puede realizar de dos modos diferentes: **Modo Principal** y **Modo Agresivo**. Mientras el Modo Principal opera en *seis mensajes*, el Modo Agresivo realiza las mismas operaciones en sólo *tres mensajes* combinando los parámetros correspondientes. Si bien el Modo Agresivo es más rápido que el primero no provee protección de la identidad de los hosts intervinientes. Además, el soporte de este modo es opcional. Revisamos a continuación el Modo Principal.

Los seis mensajes de este modo pueden tomarse de a dos, uno del host iniciador al host que responde, y otro en sentido inverso. En todos los casos el primer mensaje de cada par lo realiza el host iniciador, tras lo cual el otro host valida el mensaje recibido y, si la validación es positiva, genera un mensaje de confirmación similar al recibido.

En una primera parte (mensajes 1 y 2) se negocian las características de las SAs IKE por medio de los correspondientes atributos, además de generar cada uno de los hosts un **cookie** con el que se identifica la SA correspondiente.

La segunda parte del Modo Principal se refiere especialmente al intercambio de las claves públicas Diffie-Hellman. Este protocolo trabaja con el mecanismo conocido como aritmética del módulo, es decir con el resto de divisiones de ciertos números por otro número llamado precisamente módulo (ver recuadro **Operación con Módulos**). Para el caso, Diffie-Hellman genera claves públicas a partir de funciones exponenciales de las claves privadas correspondientes, determinándose en la inicialización de los sistemas la base de exponenciación y el propio módulo.

En la segunda parte (mensajes 3 y 4) se realiza el intercambio de claves públicas bajo Diffie-Hellman así como datos auxiliares necesarios para el intercambio. Bajo este esquema asimétrico de dos claves, cada host primero establece por su cuenta una clave privada y a continuación la clave pública correspondiente.

Luego del intercambio de las claves públicas, cada host genera una clave que es el módulo de la clave pública del otro host elevada a una potencia igual a la clave privada propia. Se puede demostrar matemáticamente que los resultados de ambos hosts son iguales (ver recuadro **Generación de Claves Públicas Bajo Diffie-Hellman**). Además, nadie más podría generar este número sin conocer una cualquiera de las claves privadas. Por eso se lo llama **valor secreto compartido** o simplemente **clave secreta compartida** ya mencionada.

El intercambio ya mencionado, además de las claves públicas incluye también sendos números generados aleatoriamente en cada host denominados **nonces** o valores *ad hoc*.
Aplicando HMAC-MD5 a la clave secreta compartida y los *nonces* de los dos hosts, las máquinas establecen una misma **clave maestra**.

A partir de esta clave maestra se determinan *tres claves* en forma concatenada, lo que implica que la primera se usa también como parámetro adicional para determinar la segunda, y en forma similar la segunda se usa para la tercera. Las tres claves se determinan en el orden que sigue: material para claves IPSec, autenticación ISAKMP y encriptado ISAKMP.

Finalmente (mensajes 5 y 6) los hosts proveen una autenticación mutua del intercambio Diffie-Hellman. Primero el host iniciador se identifica por medio de su dirección IP y Firma Digital. Para esta última genera primero una función *hash* generada a partir de la clave maestra, ambas claves públicas y *cookies*, y la propia dirección IP. La función *hash* se firma con la clave privada del host correspondiente.

Como es usual, para validación se usa la firma digital. La identificación de un host es la propia dirección IP. Por lo tanto el host iniciador envía al otro host por un lado su dirección IP y por el otro su firma digital respecto de dicha dirección. Ambos elementos se envían encriptados con la clave correspondiente es decir la tercera clave derivada de la clave maestra según se vió antes.

OPERACION CON MODULOS

La aritmética del módulo consiste en tomar el resto de la división entre dos números dados donde uno de ellos llamado **módulo** divide al otro número.

La forma usual de representación es:

y = x mod p

o bien:

y = x % p

En ambos casos *y* es el resto de la división entre *x* y *p* debiéndose cumplir que:

x - y = a * p

con *a* un número entero, lo que significa que el primer miembro de la ecuación es un múltiplo del módulo *p*. Por ejemplo:

4 = 49 mod 5

o bien:

4 = 49 % 5

puesto que 49 - 4 = 9 * 5

La operación conocida como **XOR** es decir **O Exclusivo** (*Exclusive OR*) es un caso particular de este tema, ya que se trata de una *suma binaria*, es decir que trabaja con **módulo 2**. La operación XOR se caracteriza por entregar un bit igual a 1 cuando las dos entradas son diferentes, y un bit igual a 0 cuando son iguales. Realizando las operaciones bajo el módulo 2, tendremos:

$0 \oplus 0 = 0/2 = 0$ con resto 0

$0 \oplus 1 = 1/2 = 0$ con resto 1

$1 \oplus 0 = 1/2 = 0$ con resto 1

$1 \oplus 1 = 2/2 = 1$ con resto 0

Para obtener la firma digital previamente establece el compendio *hash* de su dirección IP. La función *hash* se genera a partir de la clave maestra, ambas claves públicas y *cookies*. Sobre este compendio se aplica la clave privada del host para establecer la firma digital correspondiente.

Como es habitual, el otro host obtendrá de vuelta un compendio al desencriptar con la clave pública del primer host. A su vez aplicará la misma función sobre la dirección IP recibida para obtener su propio compendio. La dirección IP será auténtica si ambos compendios coinciden.

GENERACION DE CLAVES PUBLICAS BAJO DIFFIE-HELLMAN

Se trabaja con un número primo de elevado valor como *módulo* ***p*** y otro número entero menor que ***p*** llamado *base* ***g***.

Cada host genera un número secreto como *clave privada* ***x*** menor que ***p-1***.

Cada *clave pública* ***y*** resulta de tomar el módulo de la base elevada a la clave privada:

$y = g^x \pmod p$

y análogamente para el otro host:

$y' = g^{x'} \pmod p$

Luego del intercambio mutuo de las claves públicas, cada host aplica el módulo al resultado de tomar como base la clave pública del otro host con un exponente igual a la clave privada propia. Se puede demostrar que ambos resultados serán iguales, es decir:

$z = y'^x \pmod p = y^{x'} \pmod p$

ya que estas operaciones por cierto son respectivamente iguales a:

$z = (g^{x'})^x \pmod p = (g^x)^{x'} \pmod p$

Fase 2

Una vez establecido un canal seguro en el paso anterior viene la Fase 2 que se realiza en el **Modo Rápido** por medio de *tres mensajes*. Esta fase define, como dijimos, las SAs y las claves del IPSec. Este modo es mucho más simple que los otros dos de la fase 1 y su carga computacional es menor puesto que trabaja con operaciones matemáticas mucho más simples.

El primer mensaje del host iniciador indica al otro host el tipo de protocolo (ESP, AH o ESP+AH) a usar incluyendo el SPI, así como los algoritmos correspondientes.

Con el segundo mensaje, y previa autenticación, el segundo host reconoce y acepta el uso de lo establecido en el primero.

Finalmente, el tercer mensaje simplemente indica que el primer host está en funcionamiento, tras lo cual ambos hosts pueden comenzar a usar los protocolos en cuestión.

La fase 2 se realiza con la frecuencia establecida en el proceso de inicialización.

RENDIMIENTO

Los diferentes procesos que implica la implementación del IPSec requieren un mayor o menor nivel de procesamiento. Esto se nota más con ESP. Efectivamente, en este caso no es solamente el agregado de un encabezamiento extra y una cola, así como en todo caso la autenticación del encabezamiento completo sino el proceso completo de encriptado y desencriptado de todos los paquetes que se movilizan, especialmente con la complejidad de los algoritmos correspondientes. Y aún con AH simplemente, el proceso de establecer compendios y firmas digitales en un extremo y los chequeos en el otro son funciones mucho más complejas que enrutar o traducir direcciones IP.

Todo esto indudablemente afecta de alguna manera el rendimiento de una red y hasta el del mismo gateway si realiza otras funciones.

De cualquier manera, las principales limitaciones no vienen del lado de Internet mismo dada la baja velocidad con que se trabaja generalmente.

En este punto, la compresión de datos realizada antes del encriptado puede mejorar considerablemente el rendimiento.

El rendimiento de un dispositivo puede medirse por dos parámetros: **retardo** y **respuesta**.

El *retardo* es el tiempo que tardan los datos desde que salen del origen hasta que llegan al destino. En la práctica se toma como el tiempo adicional de procesamiento en el gateway.

La *respuesta*, por su parte, que suele considerarse también como ancho de banda se mide en paquetes manejados por unidad de tiempo. Puede ser importante que un gateway maneje un ancho de banda mayor al de la red a la que está conectado. Sino se corre el riesgo que deseche paquetes provocando interrupciones en el tráfico, con efectos directos en tráficos bajo UDP y a veces aún los que trabajan con TCP.

Los mayores retardos aparecen cuando en la misma máquina se están realizando operaciones de otro tipo. Un firewall, por ejemplo, puede verse notablemente recargado por las mayores exigencias de cómputo al hacerlo funcionar también como gateway de seguridad con todo lo que implica el procesamiento IPSec. Es muy diferente actuar sobre encabezamientos que sobre un datagrama completo con mecanismos de encriptado, a los que se agrega el overhead del tratamiento de intercambio de claves con algoritmos del tipo de exponenciación modular que requieren un fuerte uso de la CPU.

Lo anterior parece señalar a los sistemas de hardware como más adecuados, especialmente algunos que ofrecen incluso procesamiento paralelo. Sin embargo estos refinamientos pueden ser muy útiles con una gran cantidad de conexiones bajo IPSec y con fuerte actividad en las mismas, algo no muy común en la mayoría de los casos en nuestros países latinos.

LIMITACIONES Y NUEVOS DESARROLLOS

Es conveniente tener presente que con IPSec la administración del acceso debe realizarse por separado; tampoco realiza funciones NAT algo necesario cuando las redes internas no usan numeración IP registrada.

Hay datos como los números de puertos TCP o UDP que algunos enrutadores suelen usar para la asignación de ancho de banda o distribución del tráfico entre servidores (algo que suelen hacer los ISPs) así como para establecer la secuencia de paquetes con fines de monitoreo. Con el IPSec dichos datos viajan encriptados por lo que no es posible su uso.

Otra de las cuestiones que suelen poner de manifiesto las implementaciones IPSec es cierto desfasaje o falta de sincronismo en los timeouts de dos hosts relacionado con el tiempo de vida de las claves, mecanismo por otra parte particularmente aconsejable con claves limitadas a 40 bits como las que usamos en nuestros países. Este problema puede provocar caídas de sesión cuando un extremo sigue enviando datos mientras el otro la ha dado por terminada.

Si bien está normalizado IPSec también sigue evolucionando. De hecho hay un nuevo comité llamado IPSecond con una variedad de objetivos, incluyendo salvar las limitaciones comentadas, tales como:

• Seteado en encabezamiento IP de datos internos.
• Cliente IPSec remoto para soportar cambios automáticos de direcciones IP como el IP Móvil (ver **LAN & WAN**®, julio, agosto y setiembre 1999, pag. 31, 24 y 22 respectivamente).
• QoS.
• Definición de políticas de seguridad.
• Descubrimiento de puntos extremos de un túnel.

• IPSec sobre protocolos no IP.

Por otro lado también se está buscando desarrollar un juego de APIs que enlace IPSec con la próxima versión 6.0 de la norma SOCKS, con la que se puede adicionar control de acceso y traducción automática de direcciones.

PRODUCTOS

Algunos productos son de solo software, otros vienen combinados con hardware. Pueden venir combinados en servidores VPN o bien en firewall, mientras otros son cajas que incluyen exclusivamente el gateway de seguridad. Un listado adecuado puede ser el que sigue:

• Gateways de seguridad/VPN: IntraPort Server de Compatible Systems, F-Secure VPN+ 4.0 de Data Fellows, VPN IPsec de E-Lock, LANRover VPN Gateway de Intel Network Systems, SafeNet VPN de IRE, Gauntley VPN Server de Network Associates, Contivity Extranet Switch de Nortel, cIPro-VPN de Radguard, Ravlin de Redcreed, Pathbuilder de 3Com, PERMIT Gate de Timestep/Newbridge Networks, AdmiteOne de Trilogy, VPNware VSU de VPNnet,

• Firewalls: Raptor de Axent, Firewall-1 de CheckPoint Software Technologies, PIX con tarjeta Ravlin IPSec de Cisco.

• Sistema Operativo de Enrutador: IOS de Cisco.

Algunos productos agregan soporte de tarjetas token de autenticación o servidores RADIUS.

Todavía hay productos que trabajan con SKIP, pero no hay que olvidar que la norma IPSec no lo soporta, por lo que es necesario el soporte IKE o ISAKMP.

Las implementaciones pueden llegar a realizarse bajo esquemas como cliente-servidor pero también servidor-servidor. Algunos productos sólo soportan uno de estos esquemas.

Hay variaciones con respecto a la detección de claves canceladas. Hay quienes responden en forma inmediata, pero hay otros productos que reaccionan recién al refrescar las claves o aún recién al término de la sesión existente.

Interoperabilidad

La comunicación adecuada especialmente entre gateways IPSec de diferente marca, o un gateway con un firewall es fundamental para la difusión del IPSec.

La cuestión es más amplia aún. Productos de diferente origen deben poder intercambiar claves y mensajes encriptados con cualquier otro producto conforme IPSec.

En este punto **ICSA** (*Asociación Internacional de Seguridad de Computadores*) ha establecido la certificación de interoperabilidad de productos. ICSA por cierto es quien realiza las pruebas en el proyecto ANX mencionado al principio.**&**

(*) Publicado en el número 80 de la revista LAN & WAN®, octubre 1999. ***E-mail: lanywan@ciudad.com.ar***

« « « « « » » » » »