Análisis del protocolo IPSec: el estándar de seguridad en IP

Santiago Pérez Iglesias
Telefónica Investigación y Desarrollo

IPSec es un conjunto de estándares del IETF para incorporar servicios de seguridad en IP y que responde a la necesidad creciente de garantizar un nivel de seguridad imprescindible para las comunicaciones entre empresas y comercio electrónico.

En este trabajo se ofrece una breve introducción a los detalles técnicos del estándar IPSec y se discuten los servicios de seguridad que proporciona. Finalmente se presentan varios escenarios prácticos, donde se detallan las ventajas que ofrece utilizar un protocolo de seguridad estándar como IPSec.

INTRODUCCIÓN

IPSec [1] es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros). Por fin existe un estándar que aborda las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y, tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP.

Todas las soluciones anteriores se basaban en soluciones propietarias que dificultaban la comunicación entre los distintos entornos empresariales, al ser necesario que éstos dispusiesen de una misma plataforma. La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF [2] y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6.

Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable: todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes [3], lo cual constituye una garantía para los usuarios.

Otra característica destacable de IPSec es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI y, aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Entre los beneficios que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación. Las *extranets* son un ejemplo.
- Permite construir una red corporativa segura sobre

redes públicas, eliminando la gestión y el coste de líneas dedicadas.

- Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

Es importante señalar que cuando citamos la palabra "seguro" no nos referimos únicamente a la confidencialidad de la comunicación, también nos estamos refiriendo a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad. Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente.

DESCRIPCIÓN DEL PROTOCOLO IPSEC

IPSec es, en realidad, un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de *hash* (MD5, SHA-1) y certificados digitales X509v3.

En la Figura 1 se observa como IPSec es el resultado de la complementariedad de varias de estas técnicas.

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de *hash*. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES [4] que se espera sea el más utilizado en un futuro próximo.

Figura 1. Tecnologías utilizadas en IPSec

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: *IP Authentication Header* (AH) e *IP Encapsulating Security Payload* (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.

- Un protocolo de gestión de claves *Internet Key Exchange* (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El protocolo AH

El protocolo AH [5] es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (ver la Figura 2). AH es realmente un protocolo IP nuevo, y como tal el IANA le ha asignado el número decimal 51. Esto significa que el campo *Protocolo* de la cabecera IP contiene el valor 51, en lugar de los valores 6 ó 17 que se asocian a TCP y UDP respectivamente. Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, *flags*, *offset* y *checksum* (ver la Figura 2).

El funcionamiento de AH se basa en un algoritmo HMAC [6], esto es, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función *hash* a la combinación de unos datos de entrada

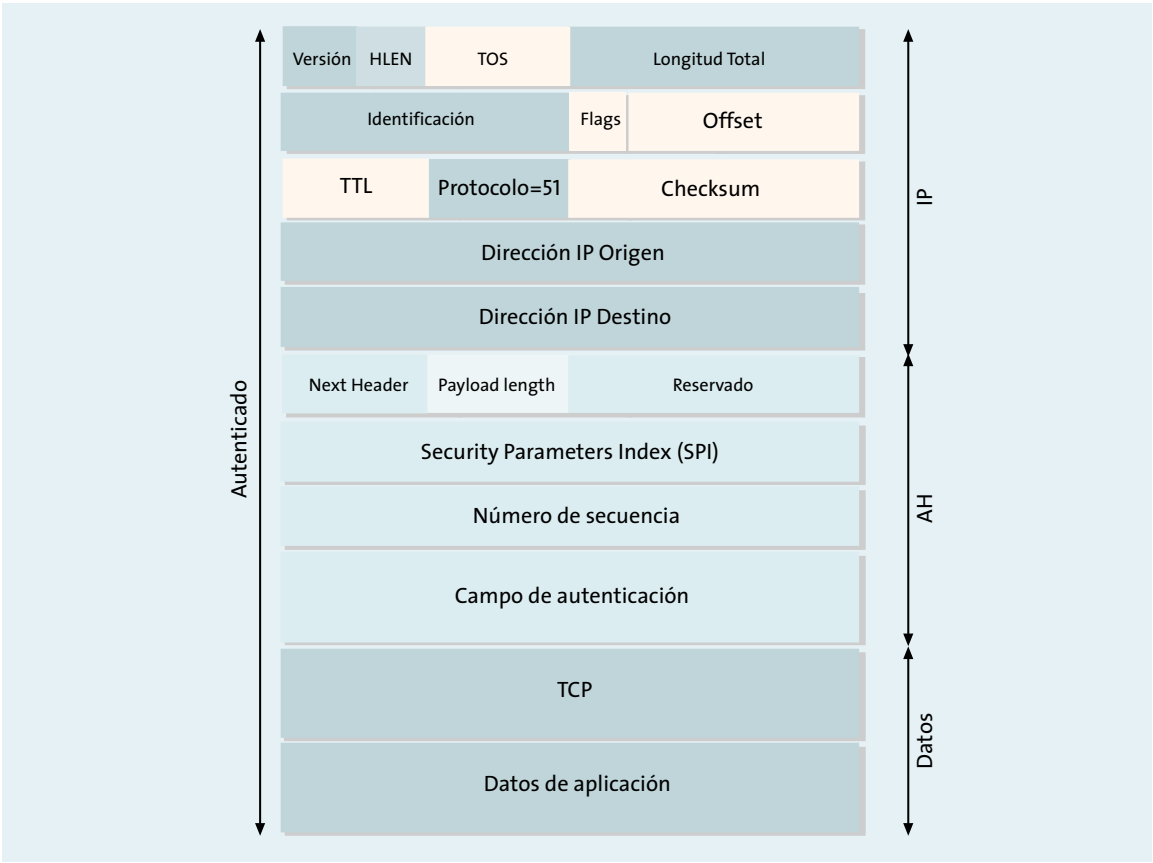

Figura 2. Estructura de un datagrama AH

y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

En la Figura 3 se muestra el modo en que funciona el protocolo AH. El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el

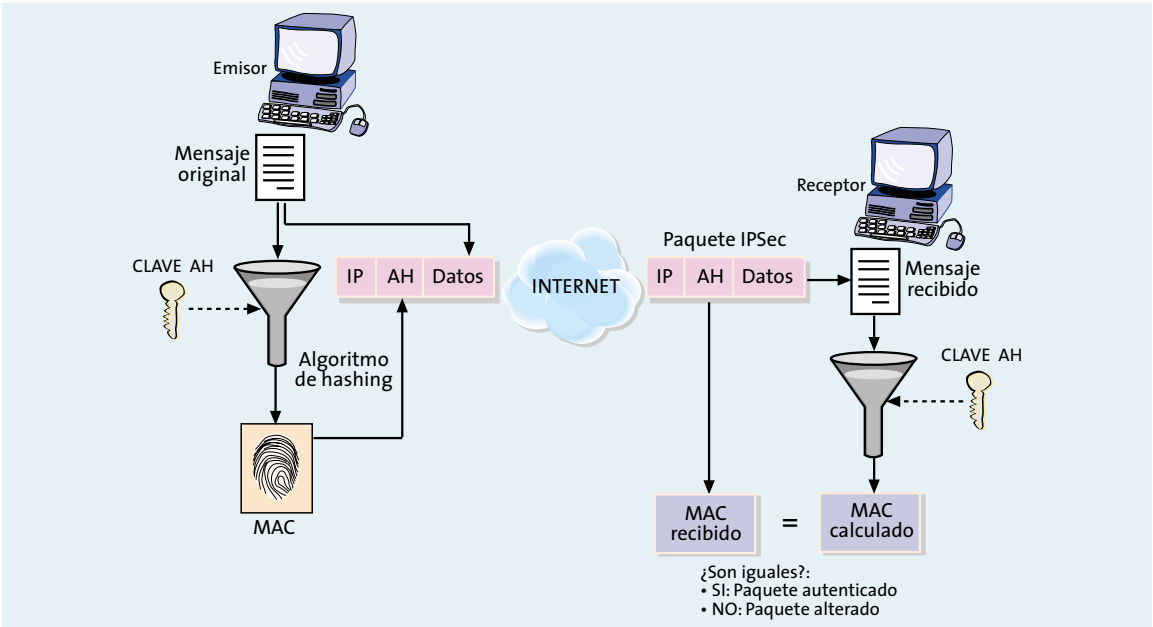

Figura 3. Funcionamiento del protocolo AH

cálculo del extracto y comparándolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave, y que dicha clave (en la Figura 3, clave AH) sólo la conocen el emisor y el receptor.

El protocolo ESP

El objetivo principal del protocolo ESP (*Encapsulating Security Payload*) [7] es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo). En la Figura 4 se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

El IANA ha asignado al protocolo ESP el número decimal 50 [8]. Esto implica que el campo *Protocolo* de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, está cifrado, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 byte, en la mayoría de los casos). Por esta razón existe un campo de relleno, tal como se observa en la Figura 4, el cual tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y, por tanto, las características del tráfico. Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque

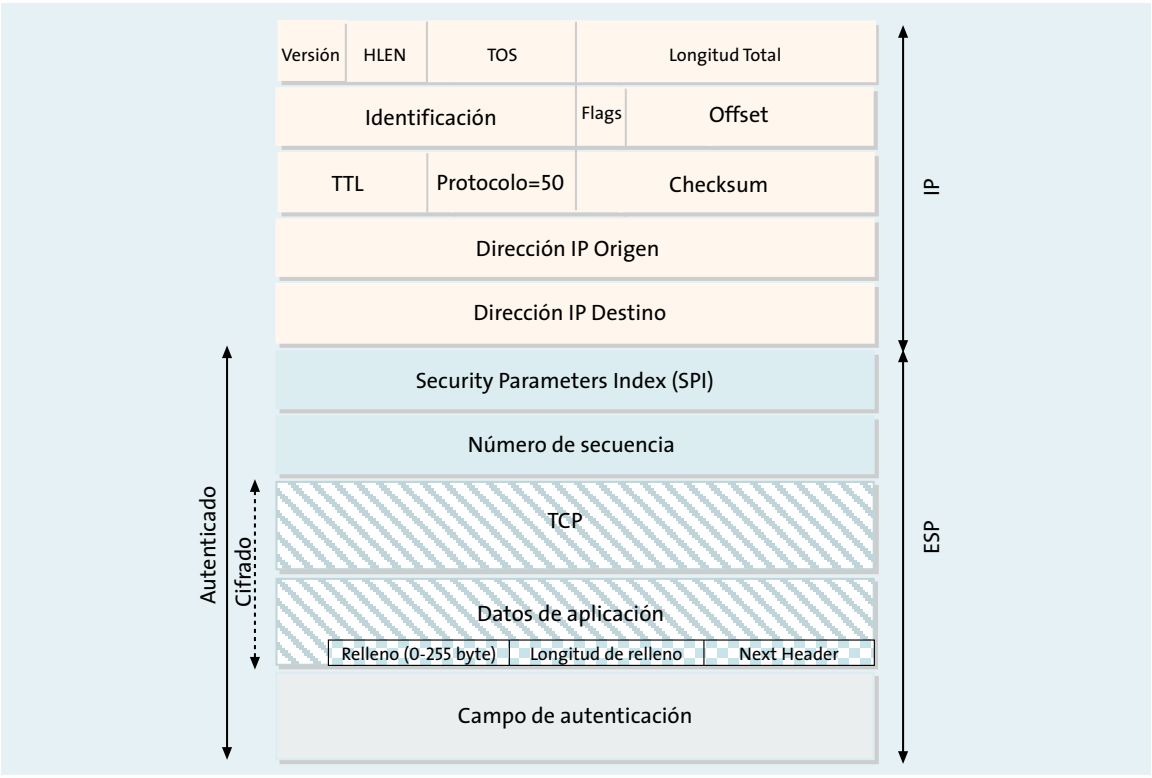

Figura 4. Estructura de un datagrama ESP

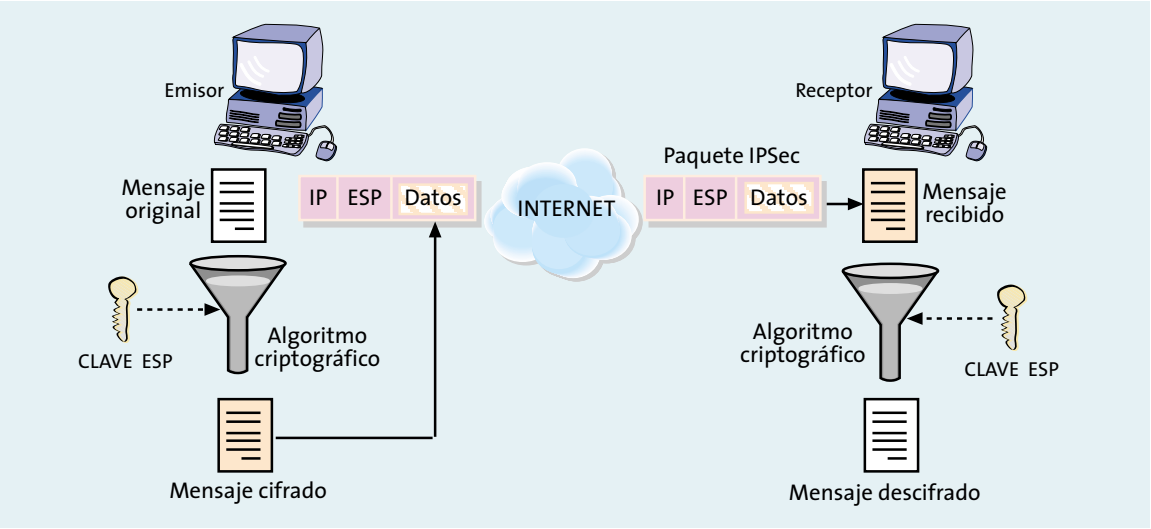

Figura 5. Funcionamiento del protocolo ESP

estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

En la Figura 5 se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bit ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de *hash* y como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE, que veremos más adelante.

Los modos transporte y túnel

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSec. Tanto ESP como AH proporcionan dos modos de uso:

1. El *modo transporte*. En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

2. El *modo túnel*. En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

   El modo túnel es empleado principalmente por los *gateways* IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo. El modo túnel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (RPV) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet.

IPSec puede ser implementado bien en un *host* o bien en un equipo dedicado, tal como un *router* o un *firewall*, que cuando realiza estas funciones se denomina *gateway* IPSec. La Figura 6 muestra los dos modos de funcionamiento del protocolo IPSec, donde:

1. En la Figura 6a se representan dos *hosts* que entienden IPSec y que se comunican de forma segura. Esta comunicación se realiza en modo transporte, por tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.

2. En la Figura 6b se muestran dos redes que utilizan para conectarse dos *gateways* IPSec y, por tanto, emplean una implementación en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los *gateways* IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales. Sin embargo ambos PCs envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración.

IKE: el protocolo de control

Un concepto esencial en IPSec es el de asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs.

El IETF ha definido el protocolo IKE [9] para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2.

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley. ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

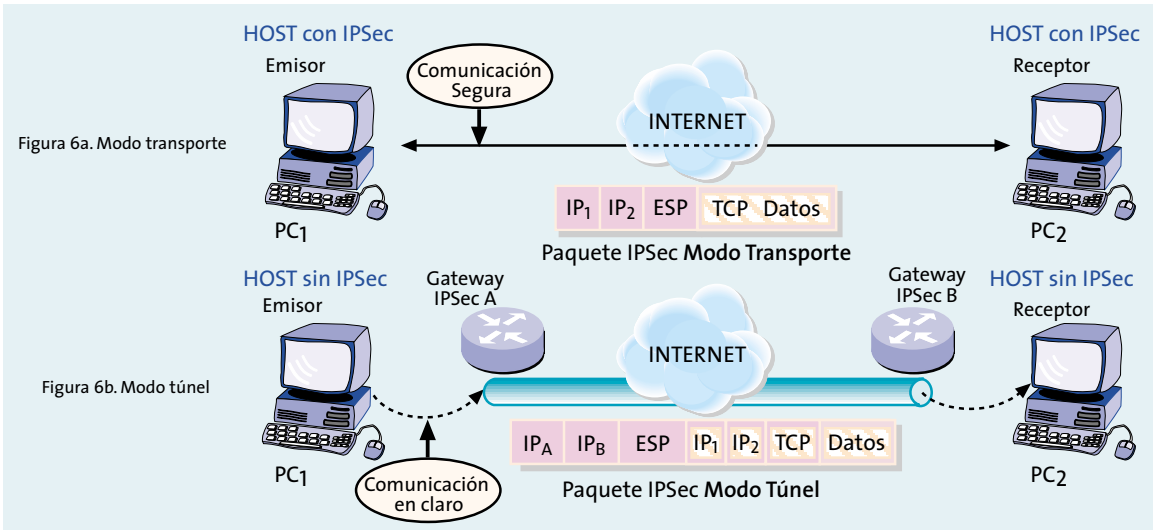

Figura 6. Los modos de funcionamiento transporte y túnel de IPSec

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

1. La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado.

   Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.

   Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

   - El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones *hash* cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.

   - En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública), cuya integración se tratará con detalle más adelante.

2. En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec.

   Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

En la Figura 7 se representa de forma esquemática

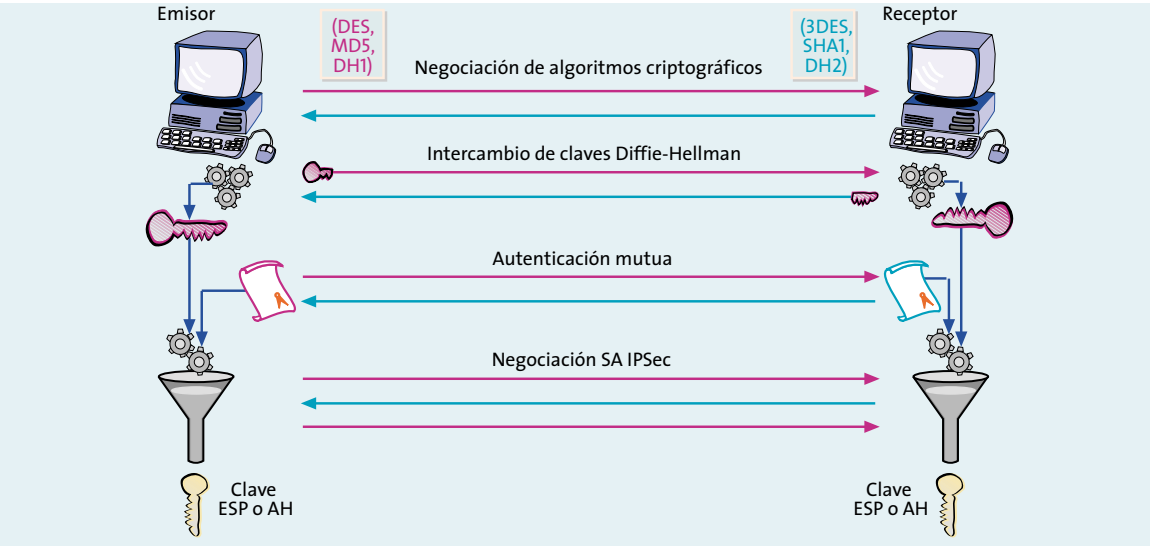

Figura 7. Funcionamiento del protocolo IKE

el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH.

Integración de IPSec con una PKI

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. La existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación de IPSec en un entorno de teletrabajadores o usuarios móviles.

Bajo el nombre de PKI (Infraestructura de Clave Pública) se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (en adelante CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3 [10] como formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado. Esto hace que existan varias alternativas según el fabricante de que se trate.

En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta LDAP al directorio de la PKI. Típicamente, los periodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación.

Para la solicitud y descarga de certificados existe un protocolo denominado SCEP [11], que se ha convertido en un estándar de facto en las operaciones de registro y descarga de certificados para aplicaciones IPSec. SCEP es un protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados.

En la Figura 8 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL.

SERVICIOS DE SEGURIDAD OFRECIDOS POR IPSEC

En este apartado se analizan las características de los servicios de seguridad que ofrece IPSec. Dichos servicios son:

- *Integridad y autenticación del origen de los datos*

  El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se comentó anteriormente, esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

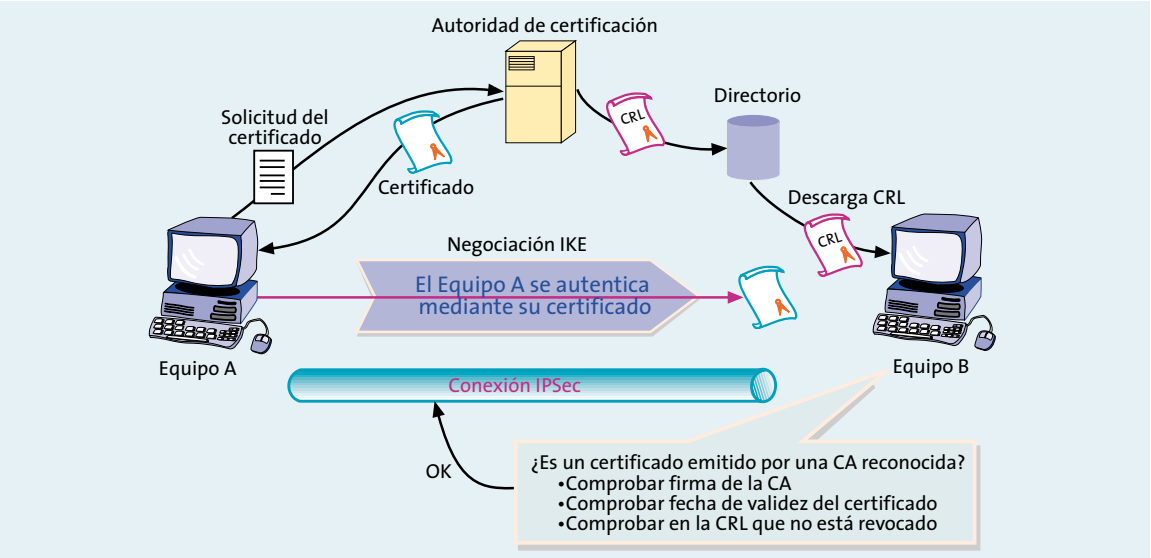

Figura 8. Integración de una PKI en IPSec

■ *Confidencialidad*

El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Ésta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado. El análisis de tráfico es un riesgo que debe considerarse seriamente, recientemente se ha documentado [12] la viabilidad para deducir información a partir del tráfico cifrado de una conexión SSH. Es previsible que este tipo de ataques se harán más habituales y sofisticados en el futuro, conforme se generalice el cifrado de las comunicaciones.

■ *Detección de repeticiones*

La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un número de secuencia incluido en la cabecera ESP o AH, el emisor incrementa dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados.

Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

■ *Control de acceso: autenticación y autorización*

Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec. Esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen y destino, el byte "TOS" y otros campos. Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro

corporativo, pero impidiendo el paso de tráfico hacia máquinas especialmente protegidas.

- *No repudio*

  El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

APLICACIONES PRÁCTICAS DE IPSEC

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cual sea el medio de transporte (FR, PPP, xDSL o ATM). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP.

En este apartado veremos como el protocolo IPSec proporciona una solución viable para tres escenarios:

1. Interconexión segura de redes locales.

2. Acceso seguro de usuarios remotos.

3. Extranet o conexión de una corporación con sus *partners* y proveedores.

Para cada uno de los escenarios mencionados se desarrolla una aplicación práctica concreta y se presentan las ventajas de utilizar IPSec

La interconexión segura de redes locales (intranet)

La mayoría de las corporaciones utiliza IP como medio de transporte universal, y las que todavía no usan IP tienen planes de migrar completamente a esta tecnología en un futuro próximo. Asimismo, la naturaleza distribuida de las empresas hace necesaria una infraestructura de comunicaciones que interconecte todas sus oficinas o puntos de venta. Por *intranet* se entiende una red de comunicaciones basada en una infraestructura de comunicaciones pública o privada que conecta todos los puntos de trabajo de una empresa y que tiene como medio común IP.

En la Figura 9 se muestra un ejemplo de *intranet* en entorno financiero. Dicha *intranet* conecta todas las oficinas bancarias con el centro de proceso de datos (CPD) de un gran banco. La seguridad es vital en este entorno, y los requisitos de confidencialidad e integridad de las comunicaciones se cubren perfectamente mediante el uso de la tecnología IPSec.

En la actualidad, incluso las oficinas bancarias más pequeñas disponen de una infraestructura informáti-

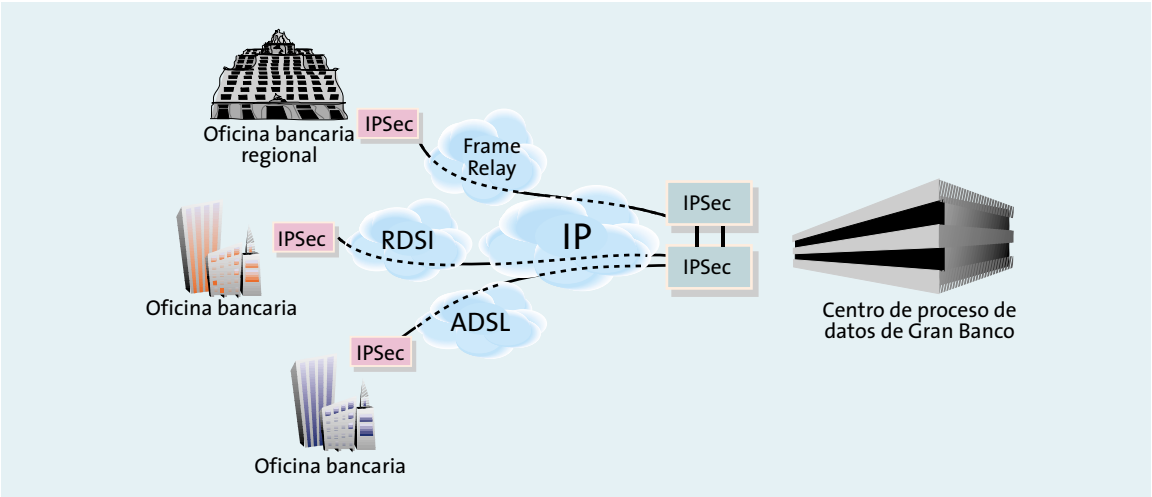

Figura 9. Interconexión de redes locales en entorno financiero

ca que consta de una red local con varios PCs que usan una variedad de aplicaciones y protocolos para los que es imposible o muy costoso añadir mecanismos de seguridad. Sin embargo, todo el tráfico de esta red local está basado en IP o puede ser encapsulado en IP, de modo que la instalación de un *gateway* IPSec es la mejor solución para garantizar la seguridad de las comunicaciones de la oficina con el exterior.

Como puede observarse en la Figura 9, es habitual que las oficinas bancarias, debido a su elevado número, presenten una gran diversidad de tecnologías de acceso. Para grandes bancos con presencia multinacional y oficinas dispersas en muchos países esta diversidad será mayor, de forma que incluso podría plantearse la conexión de algunas oficinas directamente a través de Internet. En cualquier caso, IPSec garantiza la protección de las comunicaciones con independencia de la tecnología de acceso empleada.

En cuanto al centro de proceso de datos, los requisitos críticos son la fiabilidad y la capacidad para mantener un elevado número de sesiones simultáneas. En el mercado están disponibles *gateways* IPSec comerciales que incorporan la posibilidad de configuración redundante y el establecimiento de 25.000 túneles simultáneos o más. Estas prestaciones son suficientes incluso para las redes bancarias más grandes.

El acceso seguro de usuarios remotos

La gran mayoría de las empresas necesitan proporcionar a sus usuarios algún procedimiento para el acceso remoto a los recursos corporativos. Estos usuarios con necesidades de acceso remoto pueden ser agentes de ventas, teletrabajadores o directivos en viaje de negocios; en todos los casos se requiere la necesidad de poder acceder de forma segura a los sistemas informáticos de la empresa a cualquier hora y en cualquier lugar, incluso en el extranjero. Además, las previsiones de futuro apuntan a que estas necesidades de acceso remoto van a crecer espectacularmente.

La tecnología IPSec permite comunicar el PC del usuario remoto a las máquinas del centro corporativo, de modo que se soporten todas las aplicaciones IP de forma transparente. Mediante la instalación de un software en el PC, denominado "cliente IPSec", es posible conectar remotamente dicho equipo móvil a la red local de la corporación de forma totalmente segura, con la ventaja de que el usuario remoto, desde cualquier lugar del mundo, del mismo modo que si estuviese físicamente en su oficina, podrá:

- Leer y enviar correo.
- Acceder a discos compartidos en red.
- Acceder al servidor web corporativo.
- Consultar la agenda.

El uso del estándar IPSec permite garantizar la confidencialidad y la autenticación de las comunicaciones extremo a extremo, de modo que esta solución de acceso remoto se integra perfectamente con los sistemas de seguridad de la red corporativa.

En la Figura 10 se presenta un escenario típico de

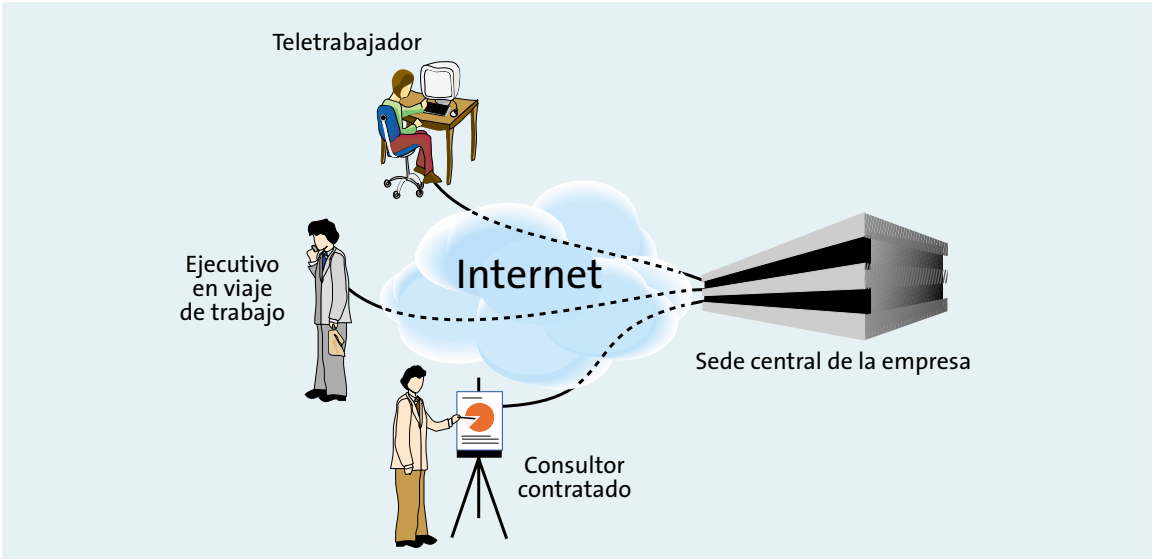

Figura 10. Acceso seguro de usuarios remotos a una corporación

acceso remoto seguro a una corporación. En nuestro ejemplo esta corporación, o empresa, se dedica a la producción de software informático. Esta empresa, al igual que cualquier compañía del sector de las tecnologías de la información, comparte una serie de características únicas. Podemos destacar la deslocalización de los recursos humanos, ya que cada vez es más habitual que los empleados trabajen fuera de su oficina, bien por estar en viaje de trabajo o bien por estar en su casa como teletrabajadores. También será muy frecuente la colaboración en proyectos de consultores externos contratados, para los cuales es necesario habilitar acceso a los recursos de la empresa.

Dada la creciente competitividad en el sector informático, la protección de la propiedad intelectual, de la información estratégica y de nuevos productos, e incluso de la propia imagen de la empresa, imponen requisitos de control de acceso y de confidencialidad que hacen imprescindible la implantación de un sistema de acceso remoto que sea suficientemente seguro.

El protocolo IPSec permite construir una solución que cumple estos requisitos de seguridad. En este entorno, los usuarios remotos dispondrán de un software instalado en su PC de trabajo que les permitirá establecer una conexión segura con la red local de la compañía. La variedad de sistemas operativos no supone dificultad alguna, ya que todos los sistemas operativos recientes como Windows 2000 o Solaris 8 incluyen un cliente IPSec. Asimismo, para los sistemas operativos más difundidos, y que no integran IPSec, existen aplicaciones de cliente IPSec, tanto comerciales como de libre distribución. Incluso existe un cliente IPSec para Palm Pilot.

Para garantizar la seguridad de esta solución y evitar intrusiones, como las que han afectado a Microsoft y otras corporaciones en el pasado [13], es necesario complementar la tecnología IPSec con el uso, en los equipos remotos, de cortafuegos personales y autenticación fuerte mediante certificados digitales X.509 residentes en tarjeta inteligente.

Desde el punto de vista del administrador de la red informática de la corporación, los requisitos prioritarios serán la facilidad de gestión y la necesidad de autenticar de forma fiable a cada usuario. La integración de IPSec con una infraestructura de clave pública (PKI) proporciona una respuesta adecuada a estos requisitos.

La extranet

Por *extranet* se entiende una red de comunicaciones que interconecta a una empresa con todos los agentes con los cuales mantiene relaciones comerciales: consumidores, proveedores y *partners*. En este escenario la interoperabilidad que ofrece el estándar IPSec es una ventaja clave frente a otras soluciones; cada empresa comprará equipos de fabricantes distintos, pero todos ellos podrán conectarse de forma segura utilizando IPSec como lenguaje común.

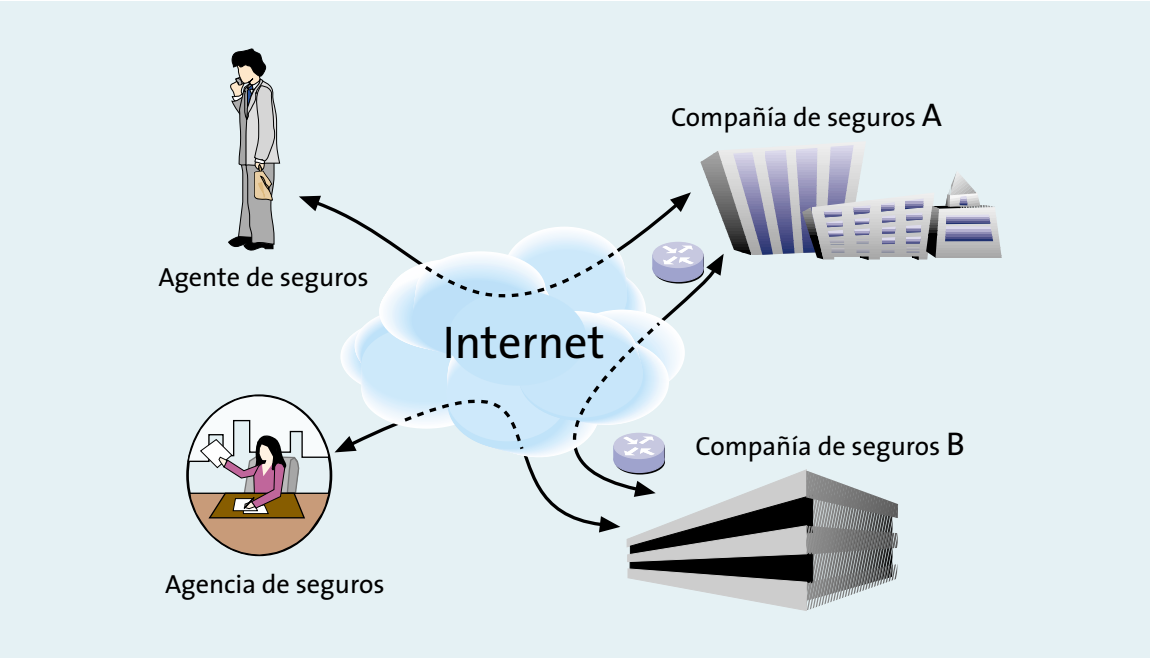

Figura 11. Extranet aplicada en el sector de seguros

La tendencia actual es la aparición de *extranets* en las que convergen todas las empresas que participan en un mismo sector productivo. Previsiblemente, el comercio electrónico negocio a negocio (B2B) evolucionará en este sentido, para proporcionar puntos de encuentro virtuales en los que se establezcan relaciones comerciales de empresa a empresa de forma segura. Estos mercados virtuales especializados se articularán de forma natural en torno a la elaboración de un producto o la provisión de un servicio concreto: fabricación del automóvil y el tipo de industria que lleva asociada, distribución y comercialización de alimentos, sector asegurador, etc.

En nuestro caso tomaremos como ejemplo el sector asegurador: una *extranet* que conecte las compañías aseguradoras y los agentes de ventas debe cumplir unos estrictos requisitos de seguridad, que incluso están regulados por normativas legales. Este es un ejemplo claro en el que IPSec aparece como la solución más apropiada, dado que es una tecnología avalada por estándares internacionales, garantiza la interoperabilidad entre los equipos de distintos fabricantes y proporciona el más alto nivel de seguridad gracias a las técnicas criptográficas más modernas.

En la Figura 11 se muestra un esquema de una *extranet* para el sector de seguros. En dicha figura se puede observar como dos compañías se comunican de forma segura para intercambiar información sobre las pólizas de seguros. Al mismo tiempo los agentes de ventas y las oficinas de seguros pueden acceder a la información comercial necesaria para su negocio. Una *extranet* como esta puede llevarse a cabo perfectamente usando IPSec; para ello se requiere la instalación de un *gateway* IPSec en cada uno de los puntos de presencia de la *extranet*, mientras que el equipamiento de los agentes de ventas se reduce a un PC portátil con un cliente IPSec.

CONCLUSIONES

IPSec es un estándar de seguridad extraordinariamente potente y flexible. Su importancia reside en que aborda una carencia tradicional en el protocolo IP: la seguridad. Gracias a IPSec ya es posible el uso de redes IP para aplicaciones críticas, como las transacciones comerciales entre empresas. Al mismo tiempo, es la solución ideal para aquellos escenarios en que se requiera seguridad, independientemente de la aplicación, de modo que es una pieza esencial en la seguridad de las redes IP.

El protocolo IPSec es ya uno de los componentes básicos de la seguridad en las redes IP. En este momento se puede considerar que es una tecnología suficientemente madura para ser implantada en todos aquellos escenarios en los que la seguridad es un requisito prioritario. Dentro de este artículo se han descrito, desde un punto de vista técnico, las características del protocolo IPSec, así como los servicios de seguridad que proporciona. Finalmente, se han presentado varios ejemplos de aplicaciones prácticas en las que IPSec se constituye como la solución más apropiada para garantizar la seguridad de las comunicaciones.

Glosario de Acrónimos

AES *Advanced Encryption Standard*
AH *Authentication Header*
CA *Certificate Authority* (Autoridad de Certificación)
CRL Lista de Certificados Revocados
ESP *Encapsulating Security Payload*
IANA *Internet Assigned Number Authority.* En 1999 sustituida por ICANN.
IETF *Internet Engineering Task Force*
IKE *Internet Key Exchange*
IP *Internet Protocol*
LDAP *Lightweight Directory Access Protocol*
MAC *Message Authentication Code*
PKCS *Public Key Common Standards*
PKI Infraestructura de Clave Pública
RPV Red Privada Virtual
SA *Security Association* (Asociación de Seguridad)
SCEP *Simple Certificate Enrollment Protocol*

Referencias

1. S. KENT and R. ATKINSON: *Security Architecture for the Internet Protocol.* RFC 2401, noviembre de 1998.
2. IP Security Protocol (IPsec), IETF page: **http://www.ietf.org/html.charters/ipsec-charter.html**
3. ICSA Certified IPsec Products: **http://www.icsa.net/html/communities/ipsec/certification/certified_products/index.shtml**
4. AES Home page: **http://www.nist.gov/aes/**
5. S. KENT and R. ATKINSON: *IP Authentication Header*. RFC 2402, noviembre de 1998.
6. H. KRAWCZYK, M. BELLARE and R. CANETTI: HMAC: *Keyed-Hashing for Message Authentication.* RFC 2104, febrero de 1997.
7. S. KENT and R. ATKINSON: *IP Encapsulating Security Payload (ESP)*. RFC 2406, noviembre de 1998.
8. Protocol Numbers: **http://www.iana.org/assignments/protocol-numbers**
9. D. HARKINS and D. CARREL: *The Internet Key Exchange.* RFC 2409, noviembre de 1998.
10. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile.* RFC 2459, enero de 1999.
11. ANDREW NOURSE: *Internet Draft.* Febrero de 2001 (Draft-nourse-scep-04.txt).
12. Análisis de tráfico del protocolo SSH, versión 1: **http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt**
13. **http://news.zdnet.co.uk/story/0,,s2082326,00.html**