ANEXO B

"IPSEC"

B.1 Introducción

En cualquier red hay cierto tráfico que contiene información confidencial (por ejemplo 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).

Si lo que se busca es proteger los datos de usuarios no autorizados, una solución típica incluirá el encriptado de la información. Un aspecto a tener en cuenta es que la información sólo debe ser accedida por los usuarios autorizados, y probablemente no desde cualquier sitio sino desde ciertas máquinas o sistemas específicos. Ello implica dos tipos de autenticaciones, relativas al sitio y al usuario.

IPSec es una solución conjunta a la problemática planteada. IPSec es un conjunto de protocolos de seguridad que permite encriptar y autenticar a las comunicaciones IP. Mientras que el encriptado puede evitar que un usuario no autorizado pueda acceder a la información, 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 trabaja solamente con HTTP, SSH con sesiones Telnet, PGP u otros protocolos similares con e-mail, etc. IPSec en cambio es totalmente transparente para las aplicaciones, se puede trabajar con todo lo que se transporte sobre TCP/IP como HTTP, FTP, Telnet, SMTP, etc. Incluso, soporta protocolos de seguridad de capas superiores tales como SSL, S/MIME u OpenPGP.

La popularidad de IPSec esta relacionada con su capacidad para implementar VPNs *(Virtual Private Network´s*) y en general para proveer acceso remoto a través de conexiones discadas. IPSec cumple requisitos más amplios de los considerados al inicio de esta sección. Las tres principales condiciones de una mensajería segura son:

- 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.

Además de las tres condiciones previas, IPSec cubre adicionalmente otras cuestiones complementarias. Ellas son:

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

El primer punto se refiere al manejo de claves y firmas digitales. La función *antireplay* (antirepetición), por su parte, constituye una característica que refuerza la integridad del mensaje. Se trata de detectar la posible inserción de paquetes falsos en medio de un flujo 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. La popularización de IPSec pasa por un adecuado soporte a nivel de *browsers* y sistemas operativos.

Desde el punto de vista de los protocolos de las capas superiores a la capa 3 del modelo de referencia OSI, IPSec es transparente y respecto de protocolos de la capa de enlace, IPSec podría trabajar con L2TP el nuevo protocolo de tunelización en Capa 2. Si bien, como se estudiara más adelante, 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 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 que maneja las claves entre dos dispositivos que se comunican estableciendo sendas conexiones cada una de ella conocida como SA (Asociación de Seguridad).

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

B. 2 Conceptos Generales y Modos de IPSec

Para comprender el funcionamiento de IPSec, es necesario entender el concepto de Asociación de Seguridad o SA. Una SA 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 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 *firewall*s) que para el caso operan como *gateway*s. Pero también se puede extender de extremo a extremo entre *host*s que se comunican.

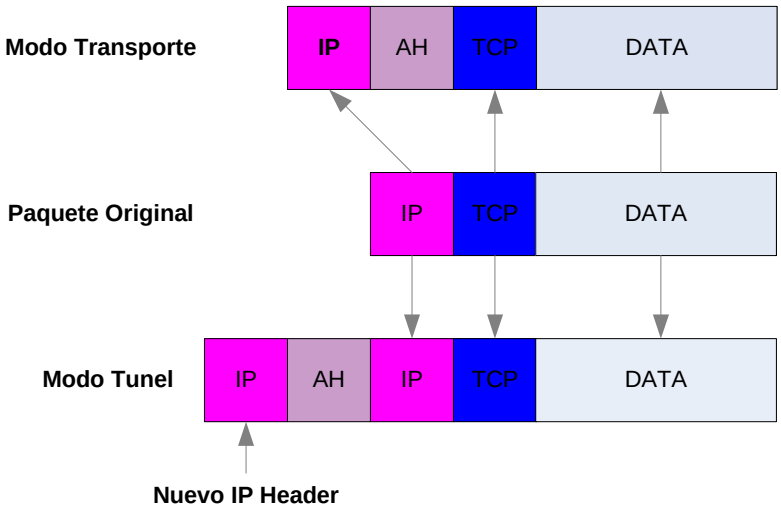

Figura B.1: Modos de Operación de IPSec

La protección del IPSec en cada caso es muy diferente. Cuando la conexión se realiza entre los *host*s 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 (Figura B.2). 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 *snnifers* y a posibles usos indebidos. La otra alternativa es más usual y los *host*s que se comunican lo hacen por medio de los *gateway*s que se conectan a la WAN (Figura B.3). Figurativamente puede decirse que los *gateway*s establecen un túnel a través del cual pasan los paquetes de los *host*s en cuestión. Por esto precisamente este modo de operación se llama Túnel.

Un túnel se establece anteponiendo al datagrama (capa de red) un nuevo encabezamiento IP con las direcciones IP de los *gateway*s 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 *host*s) puede protegerse por medio del encriptado. Con este modo de operación no hace falta hacer ningún cambio en los *host*s que se están comunicando a través de los *gateway*s, 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 *gateway*s 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, *firewall*s 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.

En resumen, IPSec soporta dos modos de operación conocidos como Modo Transporte y Modo Túnel. 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. Hay que tener 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.

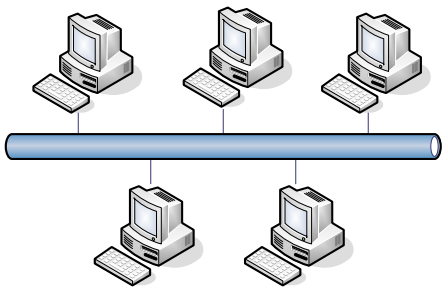

Figura B.2: Aplicación de IPSec en modo transporte (LAN)

En el Modo Túnel se usan sendos *gateway*s 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 *host*s 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".

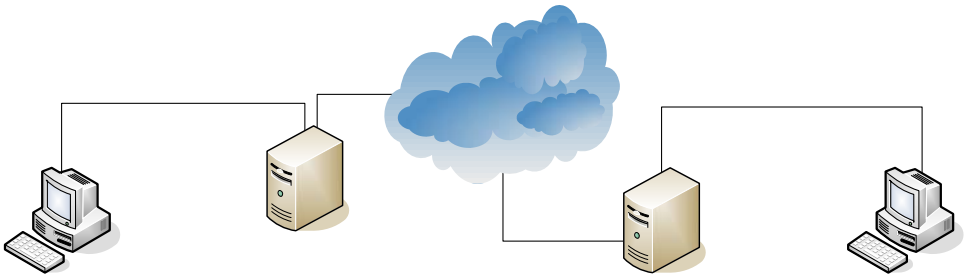

Figura B.3: Aplicación de IPSec en modo Túnel (WAN)

Tal como ya ha sido explicado, el encriptado y la propia autenticación se realizan entre los *gateway*s 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 *gateway*s 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 *gateway*s 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 surgen de lo que se expone en el punto correspondiente. El modo túnel es usual entre *firewall*s 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.

B. 2.1 Autenticación e Integridad

La palabra autenticación puede resultar algo confusa, especialmente por la diversidad de significados que se le otorga. 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. Se necesita solución similar para autenticar usuarios, algo que 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 basados en el sistema de doble clave tal que el mensaje sea encriptado con la clave privada del autor del mensaje y desencriptado con su clave pública. Sin embargo los certificados digitales requieren la intervención de una Autoridad de Certificación (AC). 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 (el paquete proviene de la máquina que dice venir) sino también los propios datos del datagrama. También se necesita autenticar los intercambios de claves (protocolo IKE) entre dos *host*s, 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 (protocolo IKE) en donde, 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 recibido, considera válido el datagrama en cuestión. El resultado agregado al datagrama original recibe el nombre de MAC o Código de Autenticación del Mensaje. 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, 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

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 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.

B. 2.2 Privacidad

Un paquete IP puede autenticarse pero aún así su contenido está en texto plano y puede ser leido por entidades no autorizadas. La norma RFC 2406 (IP Encapsulating Security Payload) ha establecido un único algoritmo de encriptado, el DES (Norma de Encriptado de Datos).

B. 2.3 Encabezamiento de Autenticación (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.

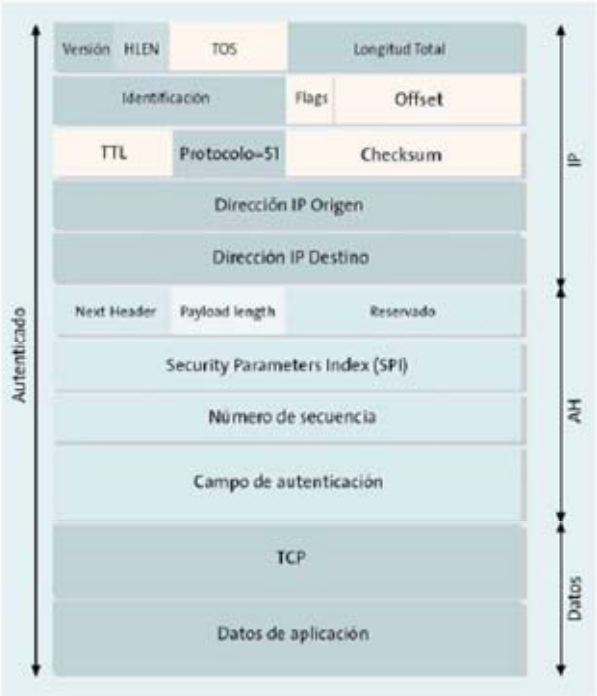

Figura B.4: Formato de paquete bajo el protocolo AH

En cuanto a los modos de operación 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 TTL (tiempo de vida) cuyo valor va decreciendo de a uno cada vez que el datagrama pasa por un enrutador. El encabezamiento AH (Figura B.4) está definido en la RFC 2406. 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 ampo Protocolo del IP original (es decir: 1 para ICMP, 6 para TCP, 17 para UDP, etc.).
- *SPI* o *Índice 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 un 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.

B. 2.4 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 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.

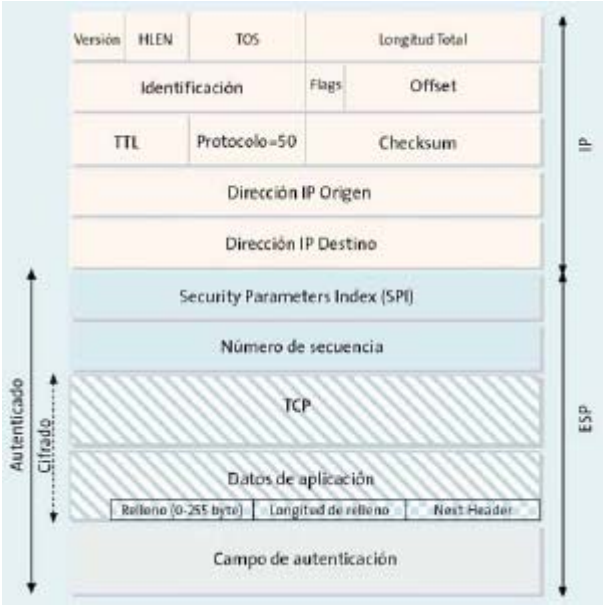

Figura B.5: Formato de paquete utilizando el protocolo ESP

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 B.5). El campo de datos IP comienza como es usual con el encabezamiento TCP, seguido por los datos propiamente dichos de las capas superiores. Veamos algunos detalles de los principales componentes.

- SPI o Índice del Parámetro de Seguridad. El mismo del AH.
- Número de Secuencia. Igual que en el caso del AH.
- Datos de la Carga Útil. 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.

B. 2.5 Elección del Modo de Operación (AH/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. 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. A continuación se analizara 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 el encabezamiento IP en cualquiera de los modos (original en el modo transporte, adicionado en el modo túnel). Cualquier alteración en el 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 *host*s que se comunican están en sendas subredes por detrás de los correspondientes *gateway*s de seguridad. En este caso los *host*s podrían implementar IPSec bajo AH mientras que los *gateway*s 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 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).

B. 2.6 Asociación 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 *host*s, o entre dos *gateway*s 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.

El intercambio de claves utilizando IKE puede realizarse de tres maneras. 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 que no serán abordados en este trabajo pero pueden ser estudiados, pues hay abundante literatura en Internet sobre ello.