(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 993**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00936931 .5**
(96) Fecha de presentación : **15.06.2000**
(97) Número de publicación de la solicitud: **1186146**
(97) Fecha de publicación de la solicitud: **13.03.2002**

(54) Título: **Un método y disposición para proporcionar seguridad a través de conversión de direcciones de red utilizando tunelado y compensaciones.**

(30) Prioridad: **15.06.1999 US 333829**

(45) Fecha de publicación de la mención BOPI:
18.07.2011

(45) Fecha de la publicación del folleto de la patente:
18.07.2011

(73) Titular/es: **TECTIA Oyj**
Kumpulantie 3
00520 Helsinki, FI

(72) Inventor/es: **Kivinen, Tero y**
Ylönen, Tatu

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Un método y disposición para proporcionar seguridad a través de conversión de direcciones de red utilizando tunelado y compensaciones.

La invención se refiere en general al campo de las comunicaciones seguras entre ordenadores en redes de transmisión de datos basadas en conmutación de paquetes. Más concretamente, el invento se refiere al campo de la implementación y mantenimiento de conexiones de comunicaciones seguras a través de una Conversión o Transformación de direcciones de red (NAT: Network Adress Translation) o conversión de protocolo.

El Grupo de Trabajo de Ingeniería de Internet (IETF) ha normalizado el conjunto de programas (suite) de protocolo IPSEC (Internet Protocol Security); las normas se conocen bien a través de los Request For Comments o documentos RFC números RFC2401, RFC2402, RFC2406, RFC2407, RFC2408 y RFC2409 que se mencionan en la lista de referencias anexa. Los protocolos IPSEC proporcionan seguridad al Protocolo de Internet o IP especificado en sí mismo en el documento RFC791. IPSEC realiza la autenticación y encriptación a nivel de paquete generando una nueva cabecera IP que añade delante del paquete una Cabecera de Autenticación (AH) o una cabecera de Carga (Payload) de Seguridad de Encapsulación (ESP). El paquete original se autentica criptográficamente y puede ser encriptado opcionalmente. El método usado para autenticar y encriptar opcionalmente un paquete se identifica mediante un valor de índice de parámetros de seguridad (SPI) almacenado en las cabeceras AH y ESP. El documento RFC número RFC2401 especifica un modo de transporte y un modo de entunelación (tunnelling) para paquetes; el presente invento puede aplicarse con independencia de cuál de estos métodos sea el utilizado.

En los últimos años, cada vez más fabricantes y proveedores de servicios de Internet han empezado a desarrollar la conversión de direcciones de red (NAT). Se encuentran referencias a NAT al menos en el documento RFC número RFC1631, así como en los documentos que están identificados en la lista de referencias anexa como Srisuresh98Terminology, SrisureshEgevang98, Srisuresh98Scurity, HoldregeSrisuresh99, TYS99, Rekhter99, LoBorella99 y BorellaLo99. Hay dos formas fundamentales de conversión de direcciones, ilustradas de forma esquemática en Figs. 1a y 1b: el equipo NAT 101 y el puerto NAT 151. El equipo NAT sólo convierte las direcciones IP en un paquete entrante 102 de modo que un paquete saliente 103 tiene una dirección IP distinta. El puerto NAT 151 también toca los números puerto TCP y UDP (Protocolo de Control de Tráfico; Protocolo de Datagrama de Usuario) en un paquete entrante 152, multiplexando varias direcciones IP a una sola dirección IP en un paquete saliente 153 y desmultiplexando correspondientemente una dirección IP simple en diversas direcciones IP para paquetes que viajan en el sentido contrario (no mostrado). Los puertos NAT son especialmente habituales en los entornos domésticos y de pequeñas oficinas. En las Figs. 1a y 1b se muestra, solamente con fines de claridad gráfica, la separación física de las conexiones de entrada y salida para dispositivos NAT; en la práctica hay muchas formas posibles de conectar físicamente una NAT.

La conversión de direcciones de red tiene lugar más frecuentemente en el extremo o borde de las redes locales (es decir, conversión entre múltiples direcciones locales privadas por un lado y unas pocas direcciones públicas encaminables globalmente en el otro). La mayoría de las veces se utiliza un puerto NAT y hay una sola dirección encaminable globalmente. En la Fig. 1b se ilustra de forma esquemática un red local 154. Este tipo de disposiciones se están haciendo extremadamente comunes en los mercados domésticos y pequeñas oficinas. Algunos proveedores de servicios de Internet han empezado también a dar a sus clientes direcciones privadas y a realizar la conversión de direcciones de red de dichas direcciones en sus redes básicas. En general, la conversión de direcciones de red se ha analizado ampliamente y en profundidad, por ejemplo en el grupo de trabajo NAT dentro de Internet Engineering Task Force. Los principios operativos de un dispositivo NAT son ampliamente conocidos, y existen muchas implementaciones de múltiples proveedores disponibles en el mercado, incluidas varias implementaciones con códigos fuentes de acceso gratis. La operación típica de un NAT se puede describir de modo que mapea direcciones IP y combinaciones de puertos para diferentes direcciones IP y combinaciones de puertos. El mapeo se mantendrá constante durante la duración de una conexión de red, pero puede cambiar (despacio) con el tiempo. En la práctica, la funcionalidad de NAT se integra con frecuencia en un cortafuego o un encaminador.

La Fig. 1c ilustra un ejemplo práctico del caso de una comunicación de red en la que un nodo de transmisión 181 está ubicado en una primera red de área local (también conocida como la primera red privada) 182, que tiene un puerto NAT 183 para conectarse a una red general 184 de transmisión de datos basada en conmutación de paquetes de amplia área, como la Internet. Esta última consta de un gran número de nodos interconectados de forma arbitraria. Un nodo receptor 185 se sitúa en una segunda red de área local 186 que está a su vez acoplada a una red de área-ancha a través de un NAT 187. Las denominaciones “nodo transmisor” y “nodo receptor” son algo engañosas, dado que se necesita una comunicación bidireccional para establecer una red de servicios segura. El nodo de transmisión es el que inicia la comunicación. También se utilizan los términos “Iniciador” y “Respondedor” para el nodo transmisor y el nodo receptor, respectivamente.

El propósito de la Fig. 1c es enfatizar el hecho de que los nodos de comunicación no se percatan ni del número o la naturaleza de los dispositivos intermedios a través de los cuales se comunican ni de la naturaleza de las transformaciones que tienen lugar. Además de las NATs, hay otro tipo de dispositivos en la red de Internet que pueden modificar legalmente paquetes durante su transmisión. Un ejemplo típico es el convertidor de protocolo,

cuya principal función es convertir el paquete en un protocolo diferente sin perturbar la operación normal. Su uso conlleva problemas muy similares al caso de la NAT. Un ejemplo bastante sencillo pero importante es la conversión entre IPv4 e IPv6, que son diferentes versiones del Protocolo de Internet. Los mencionados convertidores serán extremadamente importantes y comunes en un futuro próximo. Un paquete puede sufrir numerosas conversiones de este tipo a lo largo de su recorrido, y es posible que los puntos finales de las comunicaciones utilicen de hecho un protocolo diferente. Lo mismo que NAT, la conversión de protocolo tiene lugar habitualmente en encaminadores y cortafuegos.

En la comunidad IPSEC se sabe bien que el protocolo IPSEC no funciona adecuadamente en las conversiones de direcciones de red. Este problema se ha analizado en al menos los documentos referidos como HoldregeSrisuresh99 y Rekhter99.

En la solicitud de patente finlandesa número 974665 y la correspondiente solicitud PCT número FI98/701032 (publicada en 15 de Julio de 1999 como WO-A-99/35799) se ha presentado un determinado método para realizar conversión de direcciones IPSEC y un método de autenticación de paquetes que es sensible a las conversiones de direcciones y conversiones de protocolo en ruta del paquete. En dichas solicitudes se ha presentado adicionalmente un dispositivo de red transmisora y un dispositivo de red receptora que son capaces de utilizar las ventajas del método mencionado anteriormente. Sin embargo, en dichas solicitudes de patentes previas permanecen sin resolverse algunos de los problemas relativos al suministro de servicios de seguridad en red sobre conversión de direcciones de red.

La patenten US-A-5 793 763 proporciona un sistema y un método para convertir direcciones locales IP a una única dirección IP global de acuerdo con el bien conocido principio de las redes NAT. Los paquetes que llegan de la red Internet se apantallan mediante un algoritmo de seguridad adaptable.

La publicación WO-A-98/32065 muestra cómo se conecta un dispositivo de seguridad en red entre un cliente protegido y una red. El dispositivo de seguridad en red negocia una clave de sesión con cualquier otro cliente protegido. De este modo, quedan encriptadas todas las comunicaciones entre los dos clientes. El dispositivo de seguridad realiza la conversión de direcciones entre la dirección del cliente y su propia dirección antes de transmitir los paquetes a la red y después de haber recibido los paquetes de la red.

Otras publicaciones del estado de la técnica anterior son: DATA COMMUNICATIONS, MCGRAW HILL, NEW YORK, US, Journal Article, Vol.26, Nr. 16, Noviembre de 97, páginas 55-59, Rodney Thayer: Bulletproof IP with authentication and encryption, IPSec adds a layer of armor to IP"; IEEE, COMPUTER, Vol. 31, Issue 9, Septiembre de 1998, páginas 43-47, Rolph Oppliger: "Security at the Internet Layer", ISSN: 0018-9162; IETF, Internet Draft, 06.02.98, RG. Moskowitz: "Network Address Translation issues with IPsec", <URL:http:/www.alternic.org/drafts/drafts-m-n/draft-moskowitz-net66-vpn-00.txt>; IETF, Internet Draft, 22.08.97, RG. Moskowitz: "Network Address Translation issues with IPsec", <URL:http:/www.alternic.org/drafts-m-n/draft-moskowitz-net66-vpn-nat-00.txt>; e IETF, Internet Draft, 04.98, G. Tsirtis: "AATN Components & Mechanism", <URL:http:/www.alternic.org/drafts/drafts-t-u/draft-tsirtis-aatn-mech-00.txt>. Estas publicaciones describen diversos aspectos ya conocidos de las NATs y aseguran la transmisión en redes de paquetes de datos.

Es un objetivo de la presente invención presentar un método y los correspondientes dispositivos para proporcionar servicios de seguridad en red sobre conversión de direcciones de red de forma fiable y ventajosa.

Esto se consigue con los métodos definidos por las reivindicaciones independientes 1, 21 y 22 y los aparatos descritos en las reivindicaciones independientes 24 y 25.

La Fig. 1a ilustra el uso conocido de un equipo NAT,

La Fig. 2b ilustra el uso conocido de un puerto NAT,

La Fig. 1c ilustra una conexión de comunicación conocida entre nodos a través de una red de transmisión de datos basada en conmutación de paquetes,

La Fig. 2a ilustra una cierta carga de proveedor ID aplicable dentro del contexto de la invención,

La Fig. 2b. ilustra una cierta carga neta (payload) privada aplicable dentro del contexto de la invención,

La Fig. 2c ilustra una cierta estructura de cabecera combinada aplicable dentro del contexto de la invención,

La Fig. 3 ilustra ciertos pasos del método relativos a la aplicación de la invención,

La Fig. 4 ilustra una transformación de estructuras de cabecera acordes con un aspecto de la invención, y

La Fig. 5 ilustra un diagrama de bloques simplificado de un dispositivo de red utilizado para implementar el método de acuerdo con la invención.

La presente invención combina y amplía algunos de los métodos de conversión de direcciones de red, entunelación sobre UDP, IKE y los mecanismos de extensión IKE, de una forma nueva y con actividad inventiva para producir un método para comunicaciones seguras a través de conversiones de direcciones de red y conversiones de protocolo. El método puede hacerse de forma totalmente automática y transparente para el usuario.

Un punto clave relacionado con la aplicabilidad del invento es que – en la fecha de prioridad de la presente solicitud de patente – en general, sólo TCP (descrito en RFC793) y UDP (descrito en RFC768) funcionan sobre NAT. Esto es debido a que la mayoría de las NATs usadas en la práctica son puertos NATs, y ésta es la forma en que NAT proporciona el máximo de beneficios con respecto a la escasez de direcciones IP encaminables globalmente. La invención no está, sin embargo, limitada al uso de UDP y TCP tal y como se conocen en la fecha de prioridad de esta solicitud de patente: en general puede decirse que la UDP y TCP son ejemplos de protocolos que determinan la información de identificación de conexión (es decir, direccionamiento y numeración de puertos) que es mapeada a otra forma en el proceso de conversión de dirección. Cabe esperar que en el futuro surjan otros tipos de protocolos de comunicación y de transformaciones de dirección.

Los diversos aspectos de la invención se refieren a:

- determinar si un equipo distante soporta un cierto método que es típicamente un método de comunicación segura acorde con la invención (el aspecto “métodos soportados”),

- determinar qué conversiones de direcciones de red y/o conversiones de protocolo tienen lugar en los paquetes, en caso de haber alguno (el aspecto “conversiones en curso”),

- entunelar paquetes dentro de un protocolo cuidadosamente seleccionado, típicamente UDP, para hacerlos recorrer NATs (el aspecto “entunelación seleccionada”),

- usar un método de mantenimiento en activación para asegurar que los dispositivos NAT involucrados y otros dispositivos que usan tiempos límite para mapeos, no pierdan el mapeo para los equipos de comunicación (el aspecto “mantenimiento en activación”),

- compensar las conversiones que tienen lugar antes verificando el código de autenticación de mensaje para paquetes AH (el aspecto “compensación/autenticación”) y

- realizar conversiones de direcciones ya sea en el nodo emisor o en el receptor para compensar los diversos equipos que han sido mapeados a una dirección pública simple (el aspecto “compensación/mapeo”).

Se llama entunelación al proceso de encapsulación de paquetes de datos para transmisión sobre una red lógica distinta. Típicamente, en el caso de protocolo IP, la entunelación implica añadir una nueva cabecera IP delante del paquete inicial, estableciendo apropiadamente el campo de protocolo en la nueva cabecera, y enviando el paquete al destino deseado (extremo del túnel). También se puede realizar la entunelación modificando los campos de la cabecera del paquete inicial o remplazándolo por otra cabecera, siempre que en el proceso se conserve la cantidad de información sobre el paquete inicial suficiente para que al final de túnel se pueda reconstruir dicho paquete de forma suficientemente parecida al paquete inicial que entró en el túnel. La cantidad exacta de información que debe pasar con el paquete depende de los protocolos de red, y la información puede pasar ya sea de modo explícito (como parte del paquete entunelación) o implícito (por el contexto, como por ejemplo determinado por paquetes transmitidos previamente o por un identificador de contexto en el paquete entunelado).

En el estado de la técnica se conoce bien cómo entunelar paquetes sobre una red. Al menos los documentos que se han referenciado como RFC1226, RFC1234, RFC1241, RFC1326, RFC1701, RFC1853, RFC2003, RFC2004, RFC2107, RFC2344, RFC2401, RFC2406, RFC2473 y RFC2529 están relacionados con el tema de la entunelación. Por ejemplo, RFC1234 presenta un método para entunelar marcos IPX sobre UDP. En ese método, los paquetes se entunelan a un puerto fijo UDP y a la dirección IP del desencapsulador.

El protocolo IPSEC mencionado en la descripción de los antecedentes utiliza casi siempre el protocolo IKE o Intercambio de Clave Internet (conocido por los documentos RFC2409, RFC2408 y RFC2407) para autenticar las partes que se comunican entre ellas, derivando un secreto compartido conocido solamente por las partes que se comunican, negociando los métodos de autenticación y encriptación que deben usarse en la comunicación, y acordando un valor del índice de parámetro de seguridad (SPI) así como un conjunto de selectores que serán los usados en la comunicación. El protocolo IKE se conocía previamente como el ISAKMP/Oakley, donde el acrónimo ISAKMP responde a Internet Security Association Key Management Protocol. Además de la ya mencionada negociación normal especificada en la norma IKE, IKE también incluye ciertos mecanismos de extensión. La carga pago de ID del Vendedor, divulgada en el documento de referencia RFC2408, permite a las partes en comunicación determinar si la otra parte soporta un particular mecanismo de extensión privada. El IPSEC DOI (Domain of Interpretation), conocido como RFC2407, reserva ciertos valores numéricos para dichas extensiones privadas.

En la actualidad, la ya conocida carga neta (payload) de datos de identificación de Fabricante o Vendedor se define para que tenga el formato ilustrado en la Fig. 2a, donde la columna de números se corresponde con las posiciones de los bits. El campo de ID 201 del Fabricante es, para los fines de esta invención, la parte más importante de la

carga de datos de identificación de Vendedor. A continuación se explica cómo se puede realizar, en el contexto del protocolo IKE, la negociación sobre si un equipo distante soporta un determinado método para proporcionar comunicaciones sobre una red segura. La terminología utilizada aquí está tomada de los documentos IKE.

El protocolo IKE determina la llamada Fase 1 del intercambio mutuo de mensajes entre el Iniciador (es decir, el nodo que primero envía un paquete al otro) y el Respondedor (es decir, el nodo que primero recibe un paquete). La Fig. 3 ilustra un intercambio de los primeros mensajes Fase 1 entre el Iniciador y el Respondedor. De acuerdo con el aspecto de la invención "métodos soportados", ambos dispositivos incluyen una cierta Carga de identificación (ID) del Fabricante en un determinado mensaje Fase 1 que es preferiblemente su primer mensaje Fase 1. Esta carga indica que soportan el método en cuestión.

En la Fig. 3, 201´ muestra esquemáticamente los campos de ID del Fabricante contenidos en el primer (u otro) mensaje Fase 1 del Iniciador y 201´´ muestra esquemáticamente los campos ID del Fabricante contenidos en el primer (u otro) mensaje Fase 1 del Respondedor. La presencia de un determinado método se indica mediante un campo ID del Fabricante en la carga de ID del Fabricante que consiste básicamente en una identificación de dicho método: preferiblemente será el hash MD5 de una cadena de identificación previamente conocida, por ejemplo "SSH IPSEC NAT Traversal Version 1", sin ningún cero a la derecha ni nuevas líneas. La generación de hashes MD5 de secuencias arbitrarias de caracteres es una técnica ampliamente conocida en el estado de la técnica, por ejemplo de la publicación RFC1321 mencionado en la lista de referencias.

A continuación se abordará el aspecto de la invención "conversiones en curso". Además de la Fase 1 mencionada anteriormente, el protocolo IKE determina la llamada Fase 2 del intercambio mutuo de mensajes entre el Iniciador y el Respondedor. De acuerdo con el aspecto de la invención "conversiones en curso" las partes pueden determinar qué conversiones tendrán lugar incluyendo la dirección IP que ven en las cargas privadas de ciertos mensajes de Modo Rápido Fase 2, que son preferiblemente sus primeros mensajes de Modo Rápido Fase 2. Cualquier número no utilizado en el intervalo de números de la carga neta privada puede usarse para designar dicho uso de la carga neta privada (por ejemplo 157, que es un número no utilizado hasta la fecha de prioridad de la presente solicitud de patente).

La carga neta privada usada para desvelar la conversión en curso puede tener por ejemplo el formato ilustrado en la Fig. 2b. El campo 211 contiene un código de tipo que identifica los tipos de direcciones que aparecen en los campos 212 y 213. El campo 212 contiene la dirección del Iniciador tal y como lo ve el nodo que envía el mensaje, y el campo 213 contiene la dirección del Respondedor tal y como la ve el nodo que envía el mensaje. La Fig. 3 muestra el intercambio de los (primeros) mensajes Modo Rápido Fase 2 entre el Iniciador y el Respondedor de modo tal que el mensaje enviado por el primero incluye los campos correspondientes 211´, 212´ y 213´ y el mensaje enviado por el último incluye los campos 211´´, 212´´ y 213´´.

De acuerdo con la práctica habitual, las direcciones del Iniciador y del Respondedor se incluyen en la cabecera del paquete que contiene la carga neta de la Fig. 2b. Las direcciones en las cabeceras son sensibles a las conversiones de direcciones y otros procesos mientras que las direcciones en la carga neta privada no lo son. Cuando se recibe el paquete con la carga neta de la Fig. 2b, las direcciones contenidas en él se comparan con las que se ven en la cabecera. Si son distintas, se produce entonces una conversión de direcciones de red en el paquete. Posteriormente se hará referencia al uso del número de puerto estándar IKE 500 junto con la aplicación de la invención; como un modo adicional de detectar conversiones ocurridas, los números de puerto del paquete recibido pueden ser también comparados con el número de puerto estándar IKE 500 para determinar si se han producido conversiones de puertos.

Un aspecto de cierta importancia a la hora de gestionar las direcciones es que el puerto fuente UDP del paquete puede guardarse para un posterior uso. Generalmente se guardarán con las estructuras de datos para las asociaciones de seguridad Fase 1 ISAKMP, y se utilizarán para establecer el proceso de compensación para las asociaciones de seguridad Fase 2 IPSEC.

Para implementar el aspecto de la invención "conversiones ocurridas" aplicando el método descrito arriba, los equipos deben modificar sus cargas netas de identificación Fase 2: la carga neta ilustrada en la Fig. 2b no es conocida en las normas existentes. Una posibilidad consiste restringir las cargas netas a los tipos ID_IPV4_ADDR e ID_IPV6_ADDR que serían apropiadas para una operación huésped-a-huésped.

A continuación se hará referencia a los aspectos de la invención "entunelación seleccionada", "compensación/autenticación" y "compensación/mapeo". De acuerdo con este aspecto de la invención, los paquetes de datos reales pueden entunelarse sobre la misma conexión que se use para establecer las características de seguridad de la conexión de comunicación, por ejemplo la conexión UDP usada para IKE. Esto asegura que los paquetes de datos reales experimenten las mismas conversiones que sufrieron los paquetes IKE cuando se determinó la conversión. Partiendo de que se ha determinado el número de puerto estándar 500 para IKE, esto significaría que todos los paquetes se envían con origen puerto 500 y destino puerto 500, de modo que se necesita un procedimiento para distinguir los paquetes IKE auténticos de los que contienen datos encapsulados. Una posible forma de hacerlo consiste en valerse del hecho de que la cabecera de IK usada por los paquetes IKE auténticos contiene un campo de Cookie del Iniciador: se puede especificar que los Iniciadores que soportan este aspecto de la

invención no generan nunca galletas (cookies) con todo ceros en los cuatro primeros bytes. Por tanto se usa el valor cero en esos 4 bytes para reconocer el paquete como un paquete de datos entunelados. De este modo, los paquetes de datos entunelados tendrían cuatro bytes de ceros al principio de la carga neta UDP, mientras que los paquetes IKE auténticos nunca los tendrían.

La Fig. 4 ilustra la encapsulación de paquetes reales IPSEC en UDP para su transmisión. Básicamente, se insertan en el propio paquete una cabecera UDP 403 y una pequeña cabecera intermedia 404 después de la cabecera IP 401 ya en el paquete (con el campo de protocolo copiado en la cabecera intermedia). La cabecera IP 401 se modifica ligeramente dando lugar a una cabecera IP modificada 401´. La carga neta IP 402 permanece inalterada. No se debe malinterpretar la sencilla ilustración del paquete IPSEC sin encapsular a la izquierda: este paquete no es de texto común sino que ha sido procesado según AH o ESP u otro correspondiente protocolo de conversión antes de su encapsulación en UDP.

E en el presente documento y sin carácter limitativo de la generalidad, se supone que la encapsulación de acuerdo con la Fig. 4 la realizan siempre los mismos nodos que realizan el procesamiento IPSEC (ya sea un nodo final o un dispositivo VPN). Debe observarse también que en vez de encapsular los paquetes IPSE en UDP, podrían encapsularse en TCP. Esta opción requeriría probablemente el uso de falsos inicios y terminaciones de sesión de tal modo que el primer paquete tenga el bit SYN y el último paquete tenga bit FIN, tal y como se especifica en el protocolo TCP.

Al encapsular un paquete real de datos o un “datagrama” según la Fig. 4, se altera la cabecera IP original 401 – definida en RFC791 – dando lugar a una cabecera IP modificada 401´ de la siguiente manera:

- El campo de Protocolo en la cabecera IP (no mostrado separadamente) se remplaza por el protocolo 17 para UDP de acuerdo con RFC768,

- El campo de Longitud Total en la cabecera IP (no mostrado separadamente) se aumenta en el tamaño combinado de las cabeceras UDP e intermedia (16 bytes en total) y

- Se vuelve a calcular el campo de Cabecera Verificar-suma en la cabecera IP (no mostrado separadamente) siguiendo las normas dadas en RFC791.

Tal y como se ve en la Fig.4, se insertan una cabecera UDP 403 – según se define en RFC768 – y una cabecera intermedia 404 después de la cabecera IP. La cabecera UDP tiene 8 octetos y la cabecera intermedia también tiene 8 octetos, dando un total de 16 octetos. En la explicación que sigue, se tratan ambas cabeceras como si fueran una sola. El formato más conveniente para la cabecera combinada es el mostrado en la Fig. 2c. Los campos en esta cabecera se fijan de la siguiente manera:

- El campo Puerto de Origen 221 se asigna al 500 (el mismo que IKE). Si el paquete va a través de una red NAT, esta puede ser diferente cuando se recibe el paquete.

- El campo Puerto de Destino 222 se asigna al número de puerto desde el que el otro extremo parece estar enviando los paquetes. Si el paquete va a través de una red NAT, el receptor puede ver aquí un número de puerto distinto.

- El campo Longitud UDP 223 es la longitud de la cabecera UDP más la longitud del campo de datos UDP. En este caso, también se incluye la cabecera intermedia. El valor se calcula en bytes como 16 más la longitud de la carga neta del paquete IP original (sin incluir la cabecera IP original, que se incluye en el campo Longitud de la cabecera IP).

- El campo Verificar-suma UDP 224 se fija preferiblemente en 0. El verificar-suma UDP es opcional, y no interesa comprobarlo o calcularlo con este mecanismo de entunelación. Se supone que la integridad de los datos está protegida por una cabecera AH o ESP dentro del paquete entunelado.

- El campo Cero obligatorio 255: Este campo debe contener un valor fijo acordado previamente, que es preferiblemente todo ceros. El campo se solapa con los cuatro primeros bytes del campo Cookie del Iniciador en una cabecera IKE auténtica. Un Iniciador que soporte este aspecto de la invención no debe usar una cookie en la que los primeros cuatro bytes sean cero. Estos bytes cero se usan para separar los paquetes entunelados de los paquetes ISAKMP reales. Naturalmente se pueden elegir algún otro valor fijado distinto de “todo ceros”, pero el valor debe fijarse unos valores para este uso particular.

- El campo Protocolo 226: El valor de este campo se copia del campo Protocolo ya conocido en la cabecera IP original (no mostrado separadamente en la Fig. 4)

- El campo Reservado 227: preferiblemente enviado como todo ceros; ignorado en la recepción.

El emisor inserta esta cabecera en cualquier paquete entunelado a un destino detrás de una NAT. La información sobre si se está usando una NAT se puede almacenar en el gestor de políticas según el criterio de SA (Asociación

de la Seguridad). El encapsulado al que se refiere la Fig. 4 se puede ejecutar ya sea como una transformación nueva o como parte de las ya conocidas transformaciones AH y ESP.

La operación de encapsulado utiliza el número de puerto UDP y la dirección IP del equipo distante que se determinaron durante la negociación IKE.

El receptor desencapsula los paquetes de esta encapsulación antes de realizar el procesamiento AH o ESP. La desencapsulación elimina esta cabecera y actualiza los campos de Protocolo, Longitud y Verificar-suma de la cabecera IP. Para esta operación no se necesita ningún dato de configuración (número de puerto, etc.)

La desencapsulación sólo ha de ejecutarse si coinciden todos los siguientes selectores:

- La dirección de destino es la dirección de destino de este equipo,
- la dirección de origen es la dirección de origen de un equipo con el que este equipo ha acordado usar este túnel,
- el campo de Protocolo indica UDP,
- el valor del campo de puerto de Destino es 500 y
- el valor del campo de puerto de Origen indica el puerto con el que este equipo ha acordado usar esta entunelación. (obsérvese que puede haber muchas direcciones de origen y puertos a los que se aplique esta entunelación; cada uno de ellos se trata con un juego distinto de selectores).

Durante la desencapsulación se puede substituir la dirección de origen del paquete recibido por la dirección de origen real recibida durante la negociación IKE. Esto aplica la compensación para la verificación de AH MAC. En la fase post-tratamiento que sigue se vuelve a cambiar la dirección. Gracias a esta compensación se pueden usar las conversiones estándar AH y ESP sin modificación alguna.

En la Fig. 3 se muestra esquemáticamente como bloque 301 el proceso AH/ESP en el nodo emisor, el bloque 302 muestra esquemáticamente la encapsulación de datagramas a UDP, el bloque 303 muestra esquemáticamente la desencapsulación de datagramas desde UDP y el bloque 304 muestra esquemáticamente el proceso AH/ESP en el nodo receptor.

Después de que el paquete se ha desencapsulado desde AH o EPS se debe aplicar una compensación adicional. Esta desencapsulación adicional debe tratar el hecho de que el paquete saliente atravesó realmente una NAT (ilustrado esquemáticamente en bloque 305 de la Fig. 3) y en consecuencia el paquete de texto común también debe sufrir una transformación similar. El receptor debe ver la dirección del dispositivo NAT como la dirección del equipo en vez de como la dirección interna original. Alternativamente, el emisor del paquete podría haber realizado esta compensación antes de encapsularlo en AH o ESP.

Existen varias alternativas para esta compensación adicional según los diversos casos especiales (la mejor compensación depende de cada aplicación particular):

- Asignar un intervalo de direcciones de red para este proceso (es decir, usar el intervalo 169.254.x.x. para el enlace local. – no importan los valores reales, lo que se desea es fundamentalmente una red arbitraria que no esté usando nadie más). Se asigna una dirección de este intervalo para cada combinación <natip, ownip, natport, ownport>, donde natip significa dirección IP de la NAT, ownip la dirección IP propia del dispositivo de tratamiento, natport significa el número de puerto en la NAT y ownport quiere decir el número del puerto del propio equipo del proceso. La dirección distante del paquete se substituye por esta dirección antes de que el paquete sea enviado a las colas de protocolo.
- El verificar-suma TCP para equipos internos se debe recalcular, como parte de la compensación, en caso de que hayan cambiado las direcciones del equipo o los números de puerto. Los cálculos de verificar-suma TCP pueden ser incrementales tal y como se conoce de RFC1071. Puede ser necesario aplicar el puerto NAT para el puerto de origen.
- Cuando se utilice como VPN entre dos sitios que usen espacios de direcciones privadas incompatibles (posible solapamiento), se debe aplicar la conversión de direcciones para compatibilizar dichas direcciones con las direcciones locales.
- Cuando se utilice como VPN entre dos sitios que usen espacios de direcciones privada compatibles (no solapamiento), y se aplica un modo de túnel, puede no ser necesario una compensación adicional.
- Puede resultar necesario realizar conversión de direcciones para los contenidos de paquetes de ciertos protocolos, tales como FTP (divulgado por RFC959) o H.323. También se analizan otros temas parecidos en la referencia dada como HoldregeSrisuresh99.

- También es posible usar en el servidor direcciones aleatorias para el cliente, y aplicar conversión de direcciones a esta dirección. Esto podría permitir al servidor distinguir entre múltiples clientes situados tras la misma red NAT, y podría evitar la configuración manual del espacio de dirección local.

- La operación de compensación puede interactuar o no con la cola TCP/IP en la máquina local para reservar números de puerto UDP.

En general, esta invención no limita el procedimiento usado para compensar en los paquetes internos la NAT que tenga lugar en las cabeceras externas. El procedimiento óptimo para realizar dicha compensación puede encontrase por experimentación entre las alternativas presentadas anteriormente, o podría presentarse otro procedimiento óptimo.

A continuación se hará referencia al aspecto “mantener-activo” del invento, es decir asegurar que las conversiones de direcciones de red realizadas en la red no se modifican después de que se hayan determinado las conversiones que tienen lugar. Los conversores de direcciones de red guardan en memoria caché la información de mapeo de las direcciones, de modo que pueden invertir el mapeo para los paquetes de respuesta. Si se usa TCP, el conversor de direcciones puede mirar en el bit FIN de la cabecera TCP para determinar cuándo puede desaparecer un determinado mapeo. Sin embargo, para UDP no hay indicación explicita de finalización de flujos. Por esta razón, muchas NATs limitan bastante el tiempo de espera de mapeos para UDP (incluso tanto como 30 segundos). Por tanto, se hace necesario forzar el mantenimiento del mapeo.

Una forma posible de asegurar el mantenimiento de los mapeos consiste en enviar paquetes de activación con frecuencia suficiente para que la conversión de direcciones permanezca en la memoria caché. Al calcular la frecuencia necesaria debe tenerse en cuenta que los paquetes pueden perderse en la red, y en consecuencia deberán enviarse muchos paquetes de activación dentro del intervalo más corto en que se haya estimado que la red NAT puede olvidar el mapeo. La frecuencia apropiada depende tanto del período de tiempo en el que el mapeo permanece memorizado en caché como de la probabilidad de pérdida de paquetes en la red; se puede llegar a los valores óptimos de frecuencia para cada situación mediante ensayos en cada una de ellas.

Los paquetes de activación no necesitan contener más información significativa que las cabeceras necesarias que son iguales a las cabeceras de paquetes de datos para asegurar que los paquetes de activación sean gestionados exactamente de la misma manera que los paquetes de datos reales. Un paquete de activación puede contener un indicador que lo identifique como paquete de activación y no como paquete de datos; sin embargo también se puede determinar que todos los paquetes que no contengan una información significativa de carga neta se interpreten como paquetes de activación. En la FIG. 3 se ilustra esquemáticamente en el bloque 306 la transmisión de paquetes de activación y en el bloque 307 se ilustra esquemáticamente la recepción y supresión de los mismos. Debe advertirse que el uso de paquetes de activación no es en absoluto necesaria si los paquetes de datos reales se transmiten con la frecuencia necesaria y/o la conexión se mantiene válida sólo durante un espacio de tiempo tan corto (por ejemplo unos pocos segundos) que haga improbable que un equipo intermedio pueda borrar la información de mapeo de su memoria caché. Sólo es necesario transmitir los paquetes de activación en una única dirección, si bien también se pueden transmitir bidireccionalmente; el inconveniente derivado de la transmisión bidireccional es el aumento de tráfico innecesario en la red. La invención no limita la dirección(es) en que los paquetes de activación (si los hay) son transmitidos.

La Fig. 5 es un diagrama de bloque simplificado de un dispositivo de red 500 que puede actuar como Iniciador o Respondedor de acuerdo con el procedimiento de proporcionar comunicaciones seguras sobre conversiones de direcciones de red según la invención. El interfaz de red 501 conecta físicamente el dispositivo de red 500 a la red. El bloque 502 de gestión de direcciones mantiene bajo control las correctas direcciones de red, número de puerto y otra información de identificación pública esencial tanto del dispositivo de red 500 en sí mismo como de su pareja (no mostrado). El bloque IKE 503 es responsable del proceso de gestión de claves y de otras actividades relacionadas con el intercambio de información secreta. El bloque 504 Encriptación/desencriptación ejecuta la encriptación y la desencriptación de datos una vez que el bloque IKE 503 ha obtenido la clave secreta. El bloque 505 de compensación se usa para compensar las conversiones permisibles en los paquetes transmitidos y/o recibidos de acuerdo con la invención. Cualquiera de los bloques 504 y 505 puede usarse para transmitir, recibir y desechar paquetes de activación. El bloque 506 ensamblador/desensamblador es el intermediador entre los bloques 502 a 505 y el interfaz físico 501 de la red. Todos los bloques operan bajo la supervisión de un bloque de control 507 que también se encarga de encaminar la información entre los otros bloques y el resto del dispositivo de la red, por ejemplo para mostrar la información al usuario a través de una unidad de visualización (no mostrada) y para obtener órdenes del usuario a través de un teclado (no mostrado). Los bloques de la Fig. 5 se implementan preferiblemente como procesos operativos previamente programados de un microprocesador, cuya ejecución práctica es conocida como tal por un experto en la materia. También se pueden usar en la práctica de esta invención otras disposiciones distintas a las mostradas en la Fig. 5.

Aunque este invento se ha expuesto en el contexto de IKE, y entunelación usando puerto IKE, debe entenderse que puede aplicarse a otros casos análogos que usen diferentes métodos de formateado de paquetes, diferentes detalles de negociación, diferente protocolo de intercambio de claves, o diferente protocolo de seguridad. El invento

también puede aplicarse a protocolos no IP que tengan las características adecuadas. La invención es igualmente aplicable a ambos protocolos IPv4 e IPv6.

También se pretende que la invención sea aplicable a futuras revisiones de los protocolos IPSEC e IKE.

Del mismo modo se ha de entender que la invención es también aplicable a las conversiones de protocolos, además de a las conversiones de direcciones. Para un experto ha de ser fácil adaptar la presente invención a las conversiones de protocolo a partir de la presente descripción y las explicaciones sobre conversión de protocolo contenidos en solicitudes de patentes presentadas anteriormente por este mismo solicitante.

1. LISTA DE REFERENCIAS

BorellaLo99

M. Borella, J. Lo: Realm Specific IP: Protocol Specification, draft-ietf-nat-rsip-protocol-00.txt, Work in Progress, Internet Engineering Task Force, 1999

HoldregeSrisuresh99

M. Holdrege, P. Srisuresh: Protocol Complications with the IP Network Address Translator (NAT), draft-ietf-nat-protocol-complications-00.txt, Work in Progress, Internet Engineering Task Force, 1999.

LoBorella99

J. Lo, M. Borella: Real Specif IP: A Framework, draft-ietf-nat-rsip-framework-00.txt, Work in Progress, Internet Engineering Task Force, 1999

Rekhter99

Y. Rekhter: Implications of NATs on the TCP/IP architecture, draft-ietf-arch-implications-00.txt, Internet Engineering Task Force, 1999.

RFC768

J. Postel: User Datagram Protocol, RFC 768, Internet Engineering Task Force, 1980.

RFC791

J. Postel: Internet Protocol, RFC 791, Internet Engineering Task Force, 1981

RFC793

J. Postel: Transmission Control Protocol, RFC 793, Internet Engineering Task Force, 1981.

RFC959

J. Postel, J.Reynolds: File Transfer Protocol, RFC 959, Internet Engineering Task, 1985.

RFC1071

R. Braden, D. Borman, C. Partridge: Computing the Internet checksum, RFC 1071, Internet Engineering Task Force, 1988.

RFC1226

B. Kantor: Internet protocol encapsulation of AX.25 frames, RFC 1226, Internet Engineering Task Force, 1991.

RFC1234

D. Provan: Tunneling IPX traffic through IP networks, RFC 1234, Internet Engineering Task Force, 1991.

RFC1241

R. Woodburn, D. Mills: Scheme for an Internet encapsulation protocol: Version 1, RFC 1241 Internet Engineering Task Force, 1991.

RFC1321

R. Rivest: The MD5 message-digest algorithm, RFC 1321, Internet Engineering Task Force, 1992.

RFC1236

P. Tsuchiya: Mutual Encapsulation Considered Dangerous, RFC 1326, Internet Engineering Task Force, 1992.

RFC1631

K. Egevang, P. Francis: The IP Network Address Translator (NAT), RFC 1631, Internet Engineering Task Force, 1994.

RFC1701

S. Hanks, T. Li, D. Farinacci, P. Traina: Generic Routing Encapsulation, RFC 1701, Internet Engineering Task Force, 1994.

RFC1702

S. Hanks, T. Li, D. Farinacci, P. Traina: Generic Routing Encapsulation over IPv4 networks, RFC 1702, Internet Engineering Task Force, 1994.

RFC1853

W. Simpson: IP in IP Tunneling, RFC 1853, Internet Engineering Task Force, 1995.

RFC2003

C. Perkins: IP Encapsulation within IP, RFC 2003, Internet Engineering Task Force, 1996.

RFC2004

C. Perkins: IP Encapsulation within IP, RFC 2004, Internet Engineering Task Force, 1996.

RFC2107

K. Hamzeh: Ascend Tunnel Management Protocol, RFC 2107, Internet Engineering Task Force, 1997.

RFC2344

G. Montenegro: Reverse Tunneling for Mobile IP, RFC 2344, Internet Engineering Task Force, 1998.

RFC2391

P. Srisuresh, D. Gan: Load Sahring using IP Network Address Translation (LSNAT), RFC 2391, Internet Engineering Task Force, 1998.

RFC2401

S. Kent, R. Atkinson: Security Architecture for the Internet Protocol, RFC 2401, Internet Engineering Task Force, 1998.

RFC2402

S. Kent, R. Atkinson: IP Authentication Header, RFC 2401, Internet Engineering Task Force, 1998.

RFC2406

S. Kent, R. Atkinson: IP Encapsulating Security Carga neta, RFC 2406, Internet Engineering Task Force, 1998.

RFC2407

D. Piper: The Internet IP Security Domain of Interpretation for ISAKMP, RFC 2407, Internet Engineering Task Force, 1998.

RFC2408

D. Maughan, M. Schertler, M. Schneider, J. Turner: Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, Internet Engineering Task Force, 1998.

RFC2409

D. Hakins, D. Carrel: The Internet Key Exchange (IKE), RFC 2409, Internet Engineering Task Force, 1998.

RFC2473

A. Conta, S. Deering: Generic Packet Tunneling in IPv6 Specification, RFC 2473, Internet Engineering Task Force, 1998.

RFC2529

B. Carpenter, C. Jung: Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, RFC 2529, Internet Engineering Task Force, 1999.

Srisuresh98Terminology

P. Srisuresh: IP Network Address Translator (NAT) Terminology and Considerations, draft-ietf-nat-terminology-01.txt, Work in Progress, Internet Engineering Task Force, 1998.

Srisuresh98Security

P. Srisuresh: Security Model for Network Address Translator (NAT) Domains, draft-ietf-nat-security-01.txt, Work in Progress, Internet Engineering Task Force, 1998.

SrisureshEgevang98

P. Srisuresh, K. Egevang: Traditional IP Network Address Translator (Traditional NAT), draft-ietf-nat-traditional-01.txt, Work in Progress, Internet Engineering Task Force, 1998.

TYS99

W. Teo, S. Yeow, R. Singh: IP Relocation through twice Network Address Translators (RAT), draft-ietf-nat-rnat-00.txt, Work in Progress, Internet Engineering Task Force, 1999.

REIVINDICACIONES

1. Procedimiento para la comunicación segura de paquetes entre un primer dispositivo de ordenador (181, INICIADOR) y un segundo dispositivo de ordenador (185, RESPONDEDOR) a través de una red (184) de transmisión de datos basada en conmutación de paquetes que incluye dispositivos de ordenador intermedios (183, 187, 305), donde al menos uno de los citados dispositivos de ordenador mencionados realiza una conversión de direcciones de red y/o una conversión de protocolo, **caracterizado** porque dicho procedimiento comprende los pasos consistentes en:

- determinar qué conversiones de direcciones de red deben tener lugar, caso de haberla, en los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador,

- con el fin de habilitar el traslado de las conversiones de direcciones de red que se hayan determinado, tomar paquetes (301) acordes con un primer protocolo y encapsularlos (302) en paquetes acordes con un segundo protocolo, cuyo segundo protocolo sea capaz de trasladar conversiones de direcciones de red,

- transmitir desde un primer dispositivo de ordenador al segundo dispositivo de ordenador los citados paquetes acordes con el segundo protocolo mencionado y

- con el fin de invertir la encapsulación (302) que se realizó para posibilitar el traslado de las conversiones de direcciones de red, desencapsular (303) dichos paquetes transmitidos según el citado segundo protocolo para transformarlos en paquetes (304) acordes con el citado primer protocolo.

2. Procedimiento según reivindicación 1, **caracterizado** porque el paso consistente en tomar paquetes (301) acordes con un primer protocolo y encapsularlos (302) en paquetes acordes con un segundo protocolo, comprende los subpasos consistentes en

- tomar paquetes acordes con el Protocolo de Internet (401, 402),

- procesar dichos paquetes de acuerdo con el conjunto de programas (suite) de protocolo IPSEC y

- encapsular los paquetes procesados en paquetes acordes con el Protocolo de Datagramas de Usuario (401´, 403, 404).

3. Procedimiento según reivindicación 1, **caracterizado** porque el paso consistente en tomar paquetes (301) acordes con un primer protocolo y encapsularlos (302) en paquetes acordes con el segundo protocolo, comprende los subpasos consistentes en

- tomar paquetes acordes con el Protocolo de Internet,

- procesar dichos paquetes de acuerdo con el conjunto de programas (suite) de protocolo IPSEC, y

- encapsular los paquetes procesados en paquetes acordes con el Protocolo de Control de Transmisión.

4. Procedimiento según reivindicación 1, **caracterizado** porque además comprende el paso de compensar las conversiones de direcciones de red en el citado segundo protocolo realizadas sobre los paquetes que se han transmitido entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador.

5. Procedimiento según reivindicación 1, **caracterizado** porque adicionalmente comprende el paso de transmitir periódicamente (306, 307) paquetes de activación entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador para asegurar que permanezcan estables las conversiones de direcciones de red que tengan lugar, caso de haberlas, en los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de segundo ordenador.

6. Procedimiento según reivindicación 1, **caracterizado** porque para establecer condicionalmente una conexión de comunicación segura entre un primer dispositivo de ordenador (181, INICIADOR) y un segundo dispositivo de ordenador (185, RESPONDEDOR) a través de una red de transmisión de datos basada en conmutación de paquetes (184) que incluye dispositivos de ordenador intermedios (183, 187, 305), donde al menos uno de dichos dispositivos de ordenador realiza una conversión de direcciones de red y/o una conversión de protocolo, dicho procedimiento consta de los pasos consistentes en

- averiguar (201, 201´) si el segundo dispositivo de ordenador soporta o no un método de comunicación en el que: se determina que ocurran conversiones de direcciones de red, si es que hay alguna, sobre paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador; tomar paquetes conformes con un primer protocolo y encapsularlos de acuerdo con un segundo protocolo, siendo este segundo protocolo capaz de atravesar conversiones de direcciones de red; transmitir los paquetes conformes con dicho segundo protocolo desde el primer dispositivo de ordenador al segundo dispositivo de ordenador; y

desencapsular dichos paquetes, transmitidos de acuerdo con dicho segundo protocolo, a paquetes conformes con el citado primer protocolo,

- como respuesta a un resultado que indique que efectivamente el segundo dispositivo de ordenador soporta dicho método de comunicación, establecer una conexión de comunicación segura entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador en la cual se emplee dicho método de comunicación y

- como respuesta a un resultado que indique que efectivamente el segundo dispositivo de ordenador no soporta dicho método de comunicación, deshabilitar el uso de dicho método de comunicación entre el primer y segundo dispositivos de ordenador.

7. Procedimiento según reivindicación 1, **caracterizado** porque para entunelar paquetes entre un primer dispositivo de ordenador (181, INICIADOR) y un segundo dispositivo de ordenador (185, RESPONDEDOR) a través de una red de transmisión de datos basada en conmutación de paquetes (184) que incluye dispositivos de ordenador intermedios (183, 187, 305), donde al menos uno de los ordenadores mencionados realiza una conversión de direcciones de red y/o una conversión de protocolo, el procedimiento comprende los pasos consistentes en:

- establecer un modo de entunelación bidireccional entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador mediante el intercambio de paquetes conformes con un protocolo de comunicación segura,

- tomar paquetes (301) conformes con un primer protocolo y encapsularlos (302) en el primer dispositivo de ordenador en paquetes conformes con un segundo protocolo, siendo dicho segundo protocolo capaz de atravesar conversiones de direcciones de red,

- transmitir dichos paquetes conformes con dicho segundo protocolo desde el primer dispositivo de ordenador al segundo dispositivo de ordenador,

- en el segundo dispositivo de ordenador, desencapsular (303) los citados paquetes transmitidos conformes con dicho segundo protocolo a paquetes (304) conformes con el mencionado primer protocolo,

- obtener información sobre las conversiones de direcciones de red que se han producido sobre los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador y

- utilizar la información obtenida anteriormente para modificar el modo de entunelación bidireccional establecido entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador.

8. Procedimiento según reivindicación 7, **caracterizado** porque el paso de obtener información sobre las conversiones de direcciones que se han producido sobre los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador, comprende los subpasos consistentes en

- transmitir un paquete entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador, teniendo dicho paquete una parte de cabecera y una parte de carga neta (payload), y

- comparar una dirección de red transmitida en dicha carga neta con una dirección de red transmitida en dicha cabecera para así averiguar qué cambios ha sufrido la dirección de red transmitida en tal cabecera.

9. Procedimiento según reivindicación 7, **caracterizado** porque adicionalmente comprende el paso de transmitir periódicamente paquetes de activación (306, 307) entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador para asegurar que permanezcan estables las conversiones de direcciones de red que tengan lugar, caso de haberlas, en los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador.

10. Procedimiento según reivindicación 7, **caracterizado** porque el paso de utilizar la mencionada información obtenida para modificar la operación de entunelación de paquetes comprende el subpaso de introducir una conversión de direcciones antes de encapsular (302) los paquetes para así compensar las conversiones de direcciones de red realizadas sobres los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador.

11. Procedimiento según reivindicación 7, **caracterizado** porque el paso de utilizar la mencionada información obtenida para modificar la operación de entunelación de paquetes comprende el subpaso de introducir una conversión de direcciones después de desencapsular (303) los paquetes para así compensar las conversiones de direcciones de red realizadas sobres los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador.

12. Procedimiento según reivindicación 1, **caracterizado** porque para entunelar paquetes entre un primer dispositivo de ordenador (181, INICIADOR) y un segundo dispositivo de ordenador (185, RESPONDEDOR) a través

de una red de transmisión de datos (184) basada en conmutación de paquetes que incluye dispositivos de ordenador intermedios (183, 187, 305), existiendo en dicha red de transmisión datos un protocolo de seguridad que comprende una conexión de gestión de claves y emplea un formato de paquetes específico para los paquetes de gestión de claves, el procedimiento comprende los siguientes pasos

- encapsular los paquetes de datos que no son paquetes de gestión de claves en dicho formato de paquetes específico para paquetes de gestión de claves,

- transmitir desde el primer dispositivo de ordenador al segundo dispositivo de ordenador dichos paquetes encapsulados en el formato especifico de paquetes,

- discriminar, en el segundo dispositivo de ordenador, los paquetes de datos encapsulados en el formato específico de los auténticos paquetes de gestión de claves y

- desencapsular los paquetes de datos encapsulados en el formato específico de paquetes.

13. Procedimiento según reivindicación 12, **caracterizado** porque el paso de encapsular los paquetes de datos que no son paquetes de gestión de claves comprende los subpasos de

- encapsular los paquetes de datos que no son paquetes de gestión de claves en un formato de paquete de gestión de claves especificado por el protocolo de Intercambio de Claves en Internet (IKE) que define un determinado campo de Cookie Iniciador e

- insertar dentro del campo Cookie Iniciador de un paquete de datos encapsulado, un valor que indique que el paquete encapsulado es un paquete de datos y no un paquete de gestión de claves.

14. Procedimiento según reivindicación 1, **caracterizado** porque el procedimiento comprende los pasos de

- establecer una conexión de gestión de claves entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador, de acuerdo con un protocolo de seguridad;

- componer un paquete indicador con una parte de cabecera y una parte de carga neta;

- comunicar dicho paquete indicador dentro de la conexión de gestión de claves; y

- comparar la parte de cabecera y la parte de carga neta para determinar qué conversiones de dirección, si las hubiera, han sufrido los paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador.

15. Procedimiento según reivindicación 14, **caracterizado** porque el protocolo de seguridad determina un número de puerto estándar para una conexión de gestión de claves, y además el procedimiento incluye el paso de comparar en el paquete indicador recibido un número de puerto de origen con dicho número de puerto estándar para una conexión de gestión de claves.

16. Procedimiento según reivindicación 1, **caracterizado** porque reconoce un protocolo de seguridad que determina el proceso modo-transporte de paquetes para transmisión y recepción; y donde se ha determinado una verificación-suma de protocolo de alto-nivel para comprobar la integridad de los paquetes recibidos, y comprendiendo este procedimiento los siguientes pasos

- en el primer dispositivo de ordenador, ejecutar el proceso modo-transporte para paquetes que se han de transmitir al segundo dispositivo de ordenador,

- en el segundo dispositivo de ordenador, ejecutar el proceso modo-transporte para paquetes recibidos del primer dispositivo de ordenador, incluyendo dicho proceso modo-transporta la desencapsulación de los paquetes recibidos y

- en el segundo dispositivo de ordenador, actualizar la verificación-suma de del protocolo de alto-nivel para compensar los cambios, si los hubiera, provocados por las conversiones de dirección de red.

17. Procedimiento según reivindicación 16, **caracterizado** porque

- el paso de ejecutar en el primer dispositivo de ordenador el proceso modo-transporte para paquetes transmitidos al segundo dispositivo de ordenador toma la forma de proceso modo-transporte determinado por el conjunto de programas de protocolo IPSEC y

- el paso de ejecutar en el segundo dispositivo de ordenador el proceso modo-transporte para paquetes recibidos desde el primer dispositivo de ordenador toma la forma de proceso modo-transporte determinado por el conjunto de programas de protocolo IPSEC.

18. Procedimiento según reivindicación 16, **caracterizado** además porque comprende los pasos de

- en el primer dispositivo de ordenador, tras ejecutar el proceso modo-transporte para un paquete que va a transmitirse al segundo dispositivo de ordenador, encapsular el paquete procesado en un paquete acorde con un determinado protocolo, siendo dicho segundo protocolo capaz de atravesar conversiones de dirección de red y

- en el segundo dispositivo de ordenador, antes de ejecutar el proceso modo-transporte para un paquete recibido desde el primer dispositivo de ordenador, desencapsular el paquete recibido desde el paquete acorde con dicho segundo protocolo y reemplazar un número de direcciones de red en el paquete des-encapsulado por un número correspondiente de direcciones de red tomados del paquete recibido antes de la desencapsulación.

19. Procedimiento según reivindicación 16, **caracterizado** porque en el paso de actualizar la verificación-suma de protocolo de alto-nivel toma la forma de recalcular la verificación-suma para los paquetes procesados en modo-transporte.

20. Procedimiento según reivindicación 1, **caracterizado** porque para mantener inalterada la forma de las conversiones de direcciones realizadas por los dispositivos de conversión de direcciones de red sobre los paquetes reales de datos encapsulados y transmitidos con cierta información de dirección, entre un primer dispositivo de ordenador (181, INICIADOR) y un segundo dispositivo de ordenador (185, RESPONDEDOR) a través de una red de transmisión de datos basada en conmutación de paquetes (184), dicho procedimiento incluye el paso de

- forzar al menos a uno de los dispositivos de ordenador primero y segundo a transmitir (306) al otro dispositivo de ordenador paquetes de activación con información de dirección idéntica a la de los paquetes de datos reales con una frecuencia lo suficientemente alta como para que los dispositivos de conversión de direcciones de red reutilicen constantemente los mapeos usados por la conversiones de direcciones de red (305) incluso cuando una determinada fracción de los paquetes comunicados entre el primer ordenador y el segundo ordenador se hayan perdido en la red.

21. Procedimiento para trasmitir de forma segura paquetes desde un primer dispositivo de ordenador (181, INICIADOR) a un segundo dispositivo de ordenador (185, RESPONDEDOR) a través de una red de transmisión de datos (184) basada en conmutación de paquetes, que incluye dispositivos de ordenador intermedios (183, 187, 305), donde al menos uno de dichos dispositivos de ordenador ejecuta una conversión de direcciones de red y/o una conversión de protocolo, **caracterizado** por que dicho procedimiento incluye los pasos de:

- determinar qué conversiones de direcciones de red, si las hubiera, tienen lugar sobre paquetes transmitidos desde el primer dispositivo de ordenador al segundo dispositivo de ordenador,

- habilitar las conversiones de direcciones de red, si existen, que se determinó que debían tener lugar, tomando (301) paquetes acordes con un primer protocolo y encapsulándolos (302) en paquetes acordes con un segundo protocolo, siendo dicho segundo protocolo capaz de atravesar conversiones de direcciones de red, y

- transmitir dichos paquetes acordes con dicho segundo protocolo desde el primer dispositivo de ordenador al segundo dispositivo de ordenador.

22. Procedimiento para recibir de forma segura paquetes desde un primer dispositivo de ordenador (181, INICIADOR) a un segundo dispositivo de ordenador (185, RESPONDEDOR) a través de una red de transmisión de datos (184) basada en conmutación de paquetes, que incluye dispositivos de ordenador intermedios (183, 187, 305), donde al menos uno de dichos dispositivos de ordenador ejecuta una conversión de direcciones de red y/o una conversión de protocolo, **caracterizado** por que dicho procedimiento incluye los pasos de:

- determinar qué conversiones de direcciones de red, si las hubiera, tienen lugar sobre paquetes transmitidos entre el primer dispositivo de ordenador y el segundo dispositivo de ordenador,

- recibir paquetes acordes con un segundo protocolo enviados desde el primer dispositivo de ordenador al segundo dispositivo de ordenador, siendo dicho segundo protocolo capaz de atravesar conversiones de direcciones de red, y

- con el fin de invertir una encapsulación (302), que se había realizado para atravesar las conversiones de direcciones de red que se había determinado que tuvieran lugar, desencapsular (303) dichos paquetes transmitidos acordes con el mencionado segundo protocolo en paquetes acordes (304) con un primer protocolo.

23. Procedimiento según cualquiera de las reivindicaciones 1 a 22, que comprende el uso de la carga neta privada de un paquete para revelar las conversiones de direcciones que están teniendo lugar.

24. Aparato para dispositivo de red de transmisión (500) para transmitir paquetes de forma segura a un dispositivo receptor a través de una red de transmisión de datos basada en conmutación de paquetes que incluye

dispositivos intermedios, donde al menos uno de dichos dispositivos realiza una conversión de direcciones de red y/o una conversión de protocolo, **caracterizado** por que el aparato comprende

- medios (502, 503, 504, 506, 507) para determinar qué conversiones de direcciones de red, si las hubiera, tienen lugar sobre los paquetes transmitidos al segundo dispositivo de ordenador, y para posibilitar el transcurso de las conversiones de direcciones de red que se haya determinado que ocurrieron, tomando paquetes acordes con un primer protocolo y encapsulándolos en paquetes acordes con un segundo protocolo, siendo dicho segundo protocolo capaz de atravesar conversiones de direcciones de red, y

- un interfaz (501) para transmitir dichos paquetes acordes con el mencionado segundo protocolo entre el dispositivo emisor y el dispositivo receptor.

25. Aparato para un dispositivo receptor (500) para recibir paquetes de forma segura desde un dispositivo transmisor a través de una red de transmisión de datos basada en conmutación de paquetes que incluye dispositivos intermedios, donde al menos uno de dichos dispositivos realiza una conversión de direcciones de red y/o una conversión de protocolo, **caracterizado** por que el aparato comprende

- un interfaz (501) para recibir dichos paquetes acordes con el mencionado segundo protocolo entre el dispositivo emisor y el dispositivo receptor, siendo dicho segundo protocolo capaz de atravesar conversiones de direcciones de red, y

- medios (502, 503, 504, 506, 507) para determinar qué conversiones de direcciones de red, si las hubiera, tienen lugar sobre los paquetes transmitidos entre el dispositivo transmisor y el dispositivo receptor, y para desencapsular dichos paquetes transmitidos acordes con el mencionado segundo protocolo en paquetes acordes con un primer protocolo con el fin de invertir la encapsulación (302), que se había realizado para atravesar las conversiones de direcciones de red que se había determinado que tuvieran lugar.

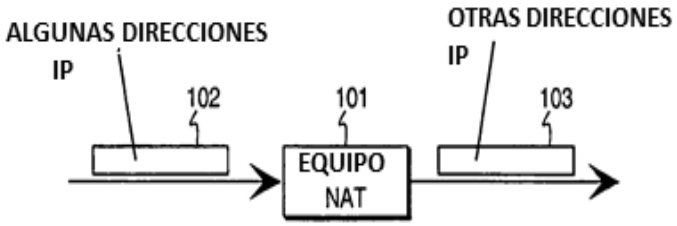

Fig. 1a
ESTADO DE LA TÉCNICA

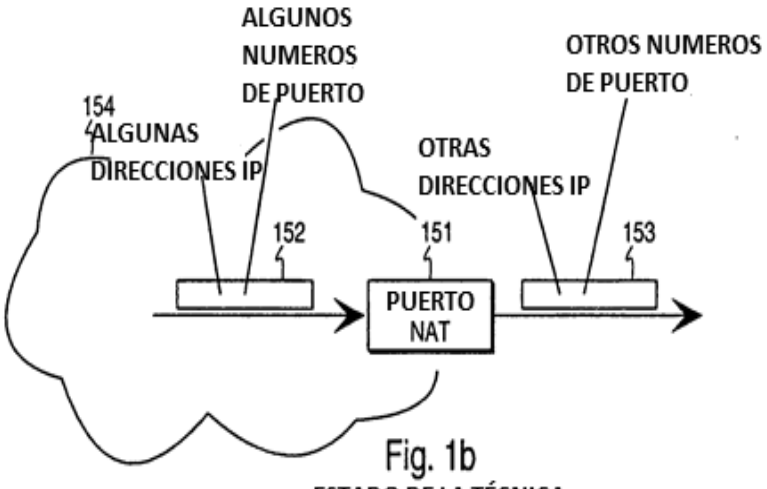

Fig. 1b
ESTADO DE LA TÉCNICA

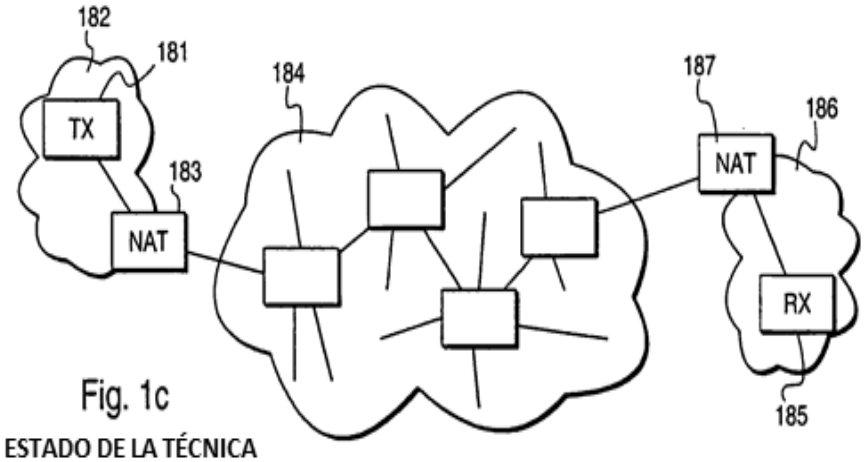

Fig. 1c
ESTADO DE LA TÉCNICA

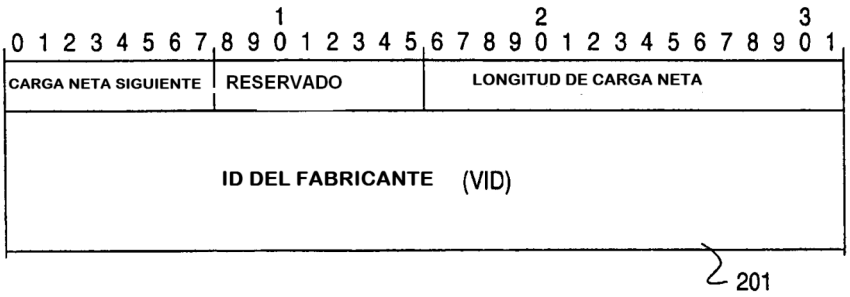

Fig. 2a

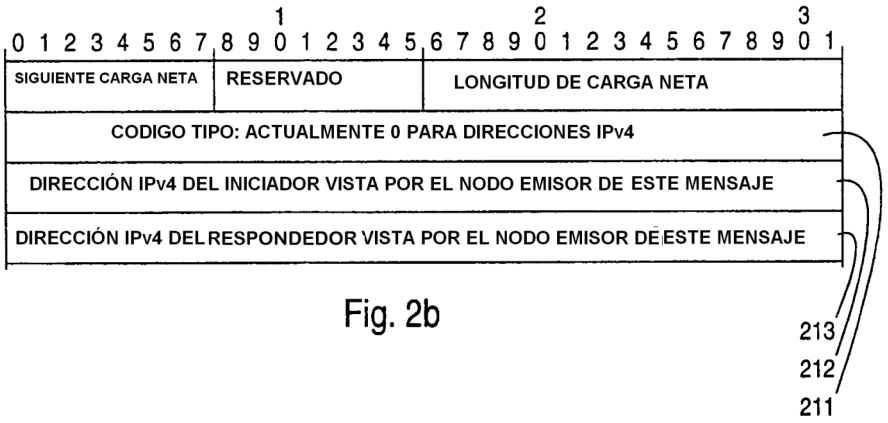

Fig. 2b

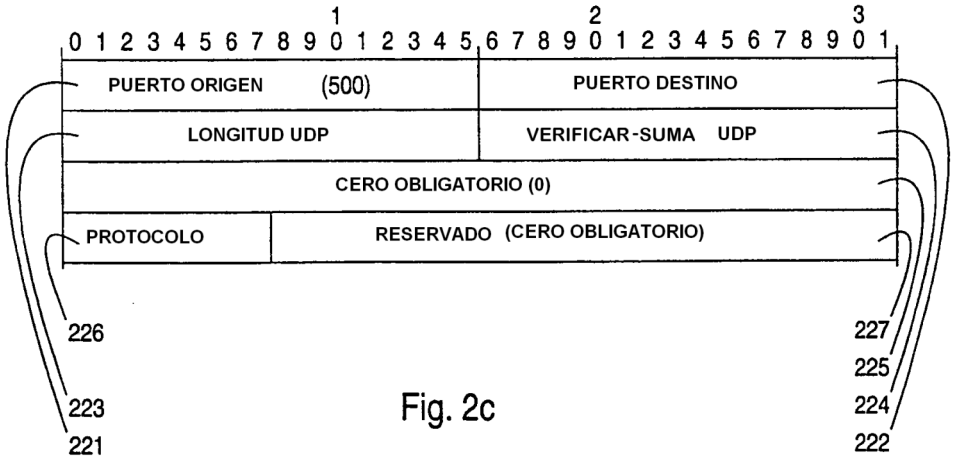

Fig. 2c

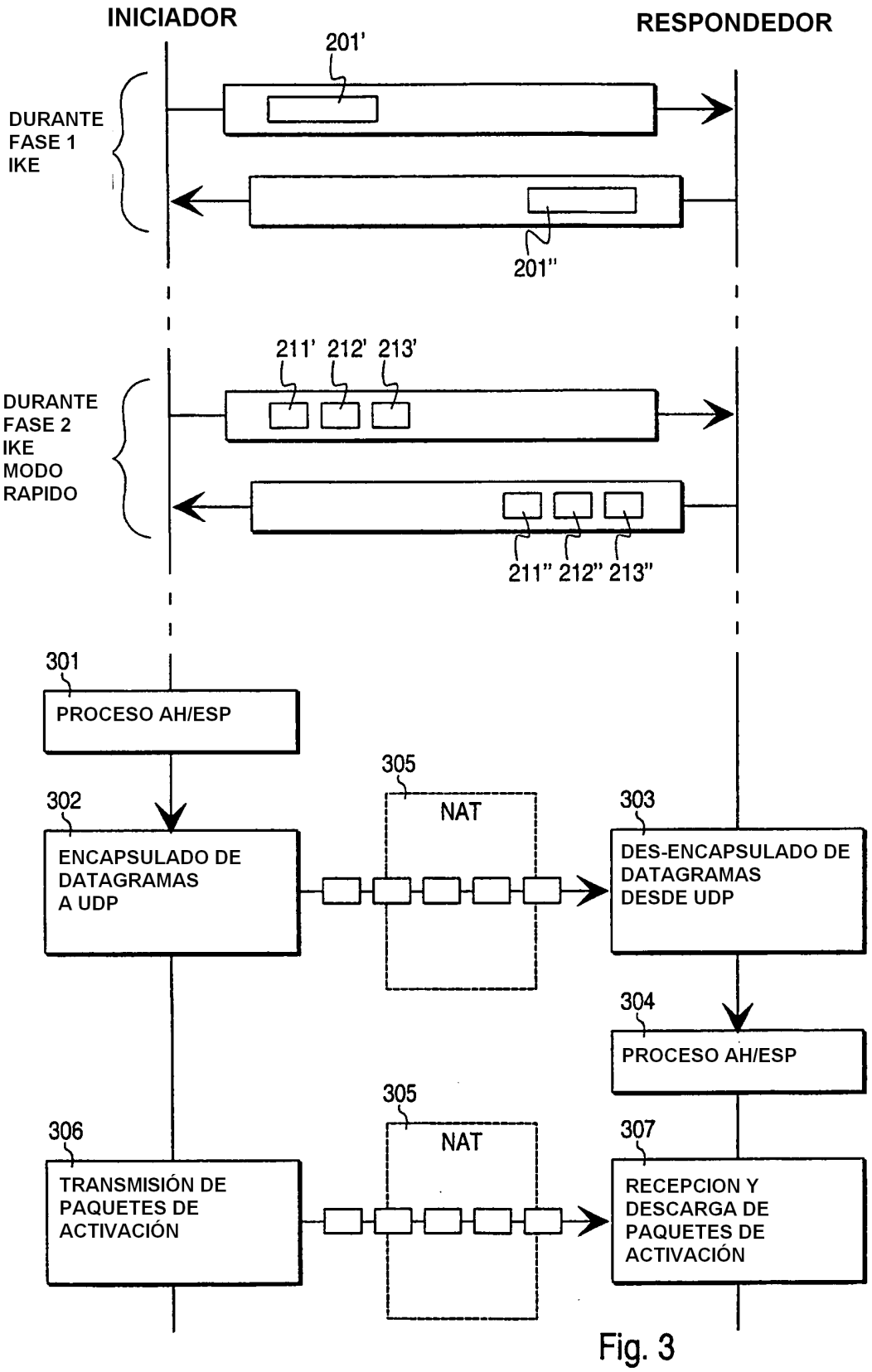
INICIADOR
RESPONDEDOR
201'
DURANTE FASE 1 IKE
201"
211' 212' 213'
DURANTE FASE 2 IKE MODO RAPIDO
211" 212" 213"
301
PROCESO AH/ESP
305
NAT
302
ENCAPSULADO DE DATAGRAMAS A UDP
303
DES-ENCAPSULADO DE DATAGRAMAS DESDE UDP
304
PROCESO AH/ESP
305
NAT
306
TRANSMISIÓN DE PAQUETES DE ACTIVACIÓN
307
RECEPCION Y DESCARGA DE PAQUETES DE ACTIVACIÓN

Fig. 3

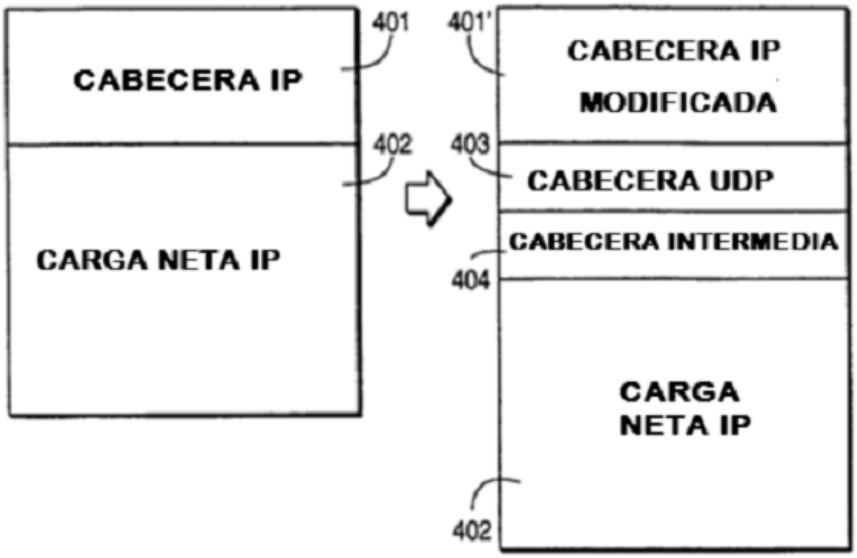
CABECERA IP
CARGA NETA IP
401
402
401'
CABECERA IP
MODIFICADA
403
CABECERA UDP
CABECERA INTERMEDIA
404
CARGA
NETA IP
402

Fig. 4

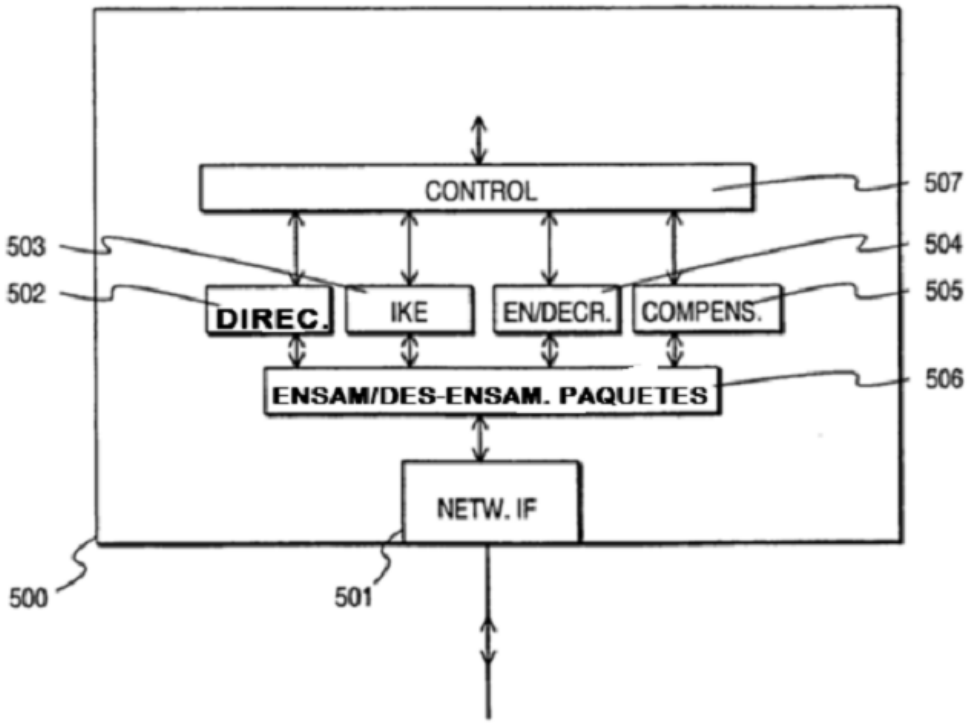
CONTROL
507
503
504
502
DIREC.
IKE
EN/DECR.
COMPENS.
505
ENSAM/DES-ENSAM. PAQUETES
506
NETW. IF
500
501

Fig. 5