(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 287 697**

(51) Int. Cl.:
H04L 12/56 (2006.01)
H04L 29/08 (2006.01)
H04L 29/12 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04710878 .2**
(86) Fecha de presentación : **13.02.2004**
(87) Número de publicación de la solicitud: **1714434**
(87) Fecha de publicación de la solicitud: **25.10.2006**

(54) Título: **Método de direccionamiento y aparato para establecer conexiones de protocolo de identidad de anfitrión (HIP) entre nodos legados y nodos HIP.**

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (publ)
164 83 Stockholm, SE

(72) Inventor/es: **Salmela, Patrik;**
Wall, Jorma y
Jokela, Petri

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

(45) Fecha de publicación de la mención BOPI:
16.12.2007

(45) Fecha de la publicación del folleto de la patente:
16.12.2007

DESCRIPCIÓN

Método de direccionamiento y aparato para establecer conexiones de protocolo de identidad de anfitrión (HIP) entre nodos legados y nodos HIP.

Antecedentes del invento

1. **Campo del invento**

El presente invento se refiere a un método de garantizar, al menos parcialmente, la seguridad de las comunicaciones entre un equipo anfitrión no habilitado para HIP (protocolo de identidad de anfitrión) y otro equipo anfitrión que si esté habilitado para HIP. El presente invento se refiere, también, a un sistema de comunicaciones y a un equipo representante para HIP que utiliza dicho método.

2. **Descripción de la técnica relacionada**

Cuando se concibió originalmente Internet, los equipos anfitriones tenían posiciones fijas y existía una confianza implícita entre usuarios a pesar de la falta de seguridad real o de protocolos de identificación de los equipos anfitriones, y esta situación se prolongó incluso al crecer su aceptación y el uso de la tecnología. Había poca necesidad de considerar técnicas para enfrentarse a la movilidad de los equipos anfitriones ya que los ordenadores eran relativamente voluminosos e inmóviles.

Al producirse la revolución de la industria de los ordenadores y de las telecomunicaciones, al principio de los años 90, podía disponerse más fácilmente de ordenadores y equipos de comunicaciones más pequeños y el invento de la World Wide Web (red de ámbito mundial) y todos los servicios que nacieron con ella, Internet llegó a ser, finalmente, atractiva para los usuarios medios. La combinación de un creciente uso de la red y de las telecomunicaciones entre móviles creó la necesidad de una gestión segura de la movilidad en Internet.

El creciente número de participantes involucrados y las transacciones monetarias que exigían determinados servicios, generó también la necesidad de un nivel de seguridad incrementado para las aplicaciones. En la actualidad, los protocolos de cifrado más ampliamente utilizados, por ejemplo SSL/TLS, se ejecutan en las capas de nivel superior de la red, por ejemplo TCP.

Teniendo en cuenta las cuestiones de seguridad y de gestión de la movilidad anteriormente mencionadas, se han introducido la norma Mobile IP (IP para móviles) (C. Perkins, "Soporte IP de movilidad para IPv4", RFC 3220, IETF, 2002) y la norma Mobile IPv6 (IP versión 6 para móviles) (D. Johnson, C. Perkins, J. Arkko, "Soporte de movilidad en IPv6", Internet Draft, en elaboración, draft-ietf-mobileip-ipv6.24.txt, IETF, 2003). Estas especificaciones se planificaron, conjuntamente, para proporcionar soporte de movilidad para la Internet de siguiente generación. El trabajo relacionado con la seguridad se lleva a cabo en la forma de IPsec (seguridad de protocolo de Internet), y actividades relacionadas, tales como diversos protocolos de intercambio de claves, siendo el objetivo proporcionar seguridad en la capa IP. Sin embargo, la experiencia ha mostrado que resulta francamente difícil conseguir movilidad y seguridad combinadas observando las normas en vigor.

Una dirección de IP describe una situación topológica de un nodo en la red. La dirección de IP se utiliza para encaminar el paquete del nodo fuente al destino. Al mismo tiempo, la dirección de IP se utiliza, también, para identificar el nodo, ofreciendo dos funciones diferentes en una sola entidad. Es como una persona que responda con la dirección de su propia casa cuando se le pregunta quién es. Cuando se considera, también, la movilidad, la situación se complica todavía más: como en este esquema, las direcciones de IP actúan como identificadores del equipo anfitrión, no deben cambiarse; sin embargo, como las direcciones de IP también describen situaciones topológicas, han de cambiar necesariamente cuando un equipo anfitrión cambia de situación en la red. Evidentemente, es imposible conseguir, al mismo tiempo cambios dinámicos y estabilidad.

En el caso del IP para móviles, la solución es utilizar una posición origen fija que proporcione una "dirección origen" para el nodo. La dirección origen identifica el nodo y, a la vez, proporciona una posición estable cuando se encuentra en origen. La información sobre la posición corriente está disponible en forma de dirección de invitado, que se utiliza con fines de encaminamiento, cuando el nodo está fuera de origen.

Otra solución al problema consiste en separar las funciones de identificación y de localización, y este es el enfoque adoptado en la propuesta de HIP (R. Moskowitz, P. Nikander, P. Jokela, "Protocolo de identidad de anfitrión", Internet Draft, en elaboración, draft-moskowitz-hip-07.txt, IETF, 2003). El HIP separa los papeles de localización e identidad de las direcciones IP introduciendo un nuevo nombre-espacio, la identidad del anfitrión (HI). En el HIP, la identidad del anfitrión es, básicamente, una clave pública de cifrado de un par de claves pública-privada. La clave pública identifica a la parte que mantiene la única copia de la clave privada. Un anfitrión que posea la clave privada del par de claves puede probar directamente que "es propietario" de la clave pública que se utiliza para identificarle en la red. La separación también proporciona medios para gestionar, de manera segura, la movilidad y el multi-origen.

El HIP se describe con mayor detalle en lo que sigue, pero no se trata de la única propuesta basada en la idea de separación de posición e identidad. FARA (D. Clark, R. Braden, A. Falk, V.Pingali, "FARA: Reorganizando la

arquitectura de direcciones", ACM SIGCOMM, 2003 Workshops, 25 y 27 de Agosto de 2003) es un modelo generalizado de ideas que proporciona una armazón a partir de la cual puede derivarse la arquitectura real. FARA podría hacer uso del HIP cuando se verifican las identificaciones de nodo y, en consecuencia, HIP podría ser parte de un caso particular de FARA. La propuesta PeerNet (J. Eriksson, M.Faloutsos, S. Krishmamurthy, "Red de iguales: Empujando la relación entre iguales hacia abajo de la pila", IPTPS '03, 20-21 de Febrero de 2003) también describe la separación de posición e identidad. La I^3 (Internet Indirection Infrastructure", ACM SIGCOMM '02, 19-23 de Agosto de 2002), también define una separación entre información de identidad y de encaminamiento.

Además, el direccionamiento en conexiones parcialmente basadas en el HIP entre nodos habilitados para HIP y legado se describe en el trabajo de L. Eggert, "Mecanismos de encuentro del protocolo de identidad de anfitrión (HIP)", Internet Draft, draft-eggert-hip-rendezvous.txt, IETF, 2004.

El protocolo de identidad de anfitrión introduce una separación entre la información de posición y la de identidad en la capa IP. Además de la separación, se define un protocolo para negociar asociaciones de seguridad (SA) entre nodos habilitados para HIP.

Con el HIP, cada anfitrión tiene una o más identidades, que pueden adoptarse a largo o a corto plazo, que pueden emplearse para identificarle en la red. Con el HIP, un identificador es la clave pública de par de claves pública-privada. Cuando el anfitrión posee la clave privada, puede probar que realmente es el "propietario" de esta identidad que representa la clave pública; es parecido a enseñar una tarjeta de identidad.

Cada anfitrión puede generar claves a corto plazo para uso durante cortos períodos de tiempo. Son útiles cuando no es necesario que el nodo se identifique ulteriormente con la misma identidad. Por ejemplo, la compra de libros en una librería puede ser una relación a largo plazo, mientras que el ponerse en contacto con un servidor una sola vez para recoger perfiles de usuario, puede considerarse como una acción a corto plazo. En este último caso, puede crearse una identidad a corto plazo para evitar una diseminación más amplia de la identidad a largo plazo.

La identidad de anfitrión (HI) del HIP, al ser una clave pública, puede ser muy larga y, por tanto, no resultar práctica en todas las situaciones. En el HIP, la HI se representa mediante una etiqueta de identidad del anfitrión (HIT) con una longitud de 128 bits, que es generada a partir de la HI, troceándola. Así, la HIT identifica una HI. Como la HIT tiene 128 bits de largo, puede utilizarse para aplicaciones IPv6 directamente, ya que tiene exactamente la misma longitud que las direcciones IPv6.

Cuando se utiliza el HIP, las capas superiores, incluyendo las aplicaciones, ya no ven la dirección de IP. En su lugar, ven la HIT como la "dirección" del anfitrión destino. La información de localización se oculta en una nueva capa, como se describirá más adelante. Las direcciones de IP ya no identifican los nodos; únicamente se las utiliza para encaminar los paquetes en la red.

Las aplicaciones no tienen un interés especial en la información sobre localización, pero necesitan conocer la identidad de sus iguales. La identidad está representada por la HIT. Esto quiere decir que la dirección de IP solamente tiene importancia en las capas inferiores, en lo que respecta al encaminamiento. Las HIT que utilizan las aplicaciones deben hacerse corresponder con las direcciones de IP correspondientes antes de que ningún paquete abandone el anfitrión. Esto se consigue en una nueva capa de identidad de anfitrión, como se describe en lo que sigue.

La figura 1 de los dibujos adjuntos ilustra las diversas capas en HIP, que comprenden la capa estándar 4 de transporte, la capa 8 de red y la capa 10 de enlace, con un proceso 2 que se comunica con la capa 4 de transporte situada debajo de ella. Con el HIP, una nueva capa 6 de identidad de anfitrión está dispuesta entre la capa 4 de transporte y la capa 8 de red.

Localmente, cada HI y su HIT asociada se hacen corresponder con las direcciones de IP del nodo. Cuando los paquetes abandonan el anfitrión, se elige el camino correcto (por cualquier medio que sea) y en el paquete se incorporan las direcciones de IP correspondientes como direcciones de fuente y de destino. Cada paquete que llega de la capa superior contiene la HIT del par como dirección de destino. La correspondencia entre la HIT y la información de posición puede encontrarse en la capa 6 de HI. De ahí, la dirección de destino se convierte en la dirección de IP asignada, y la HIT de la fuente se convierte en la dirección de IP de la fuente.

La asignación de correspondencia entre una HIT de un par y una dirección de IP puede recuperarse de diversas formas, una de las cuales es a partir de un servidor DNS. La información de posición puede ser actualizada por el nodo igual en cualquier momento. El procedimiento de actualización se describirá con más detalle en la subsección de gestión de movilidad.

El HIP define un intercambio de mensajes de base que contiene cuatro mensajes, una iniciación de diálogo de cuatro vías, y éste es utilizado para crear una asociación de seguridad (SA) entre anfitriones habilitados para HIP. Durante el intercambio de mensajes, se utiliza el procedimiento Diffie-Hellman para crear una clave de sesión y para establecer un par de asociaciones de seguridad (AS) para encapsular carga útil de seguridad (ESP) IPsec entre los nodos.

La Figura 2 de los dibujos adjuntos ilustra el funcionamiento de la iniciación de diálogo de cuatro vías. Las partes en negociación son el iniciador, que comienza la conexión, y el respondedor. El iniciador comienza la negociación enviando un paquete I1 que contiene las HIT de los nodos que participan en la negociación. La HIT de destino puede, también, ser puesta a cero si la HIT del respondedor no es conocida por el iniciador.

Cuando el respondedor acepta el paquete I1, envía de vuelta un paquete R1 que contiene un rompecabezas que ha de ser resuelto por el iniciador. El protocolo está diseñado de modo que el iniciador debe realizar la mayor parte de los cálculos durante la resolución del rompecabezas. Esto proporciona cierta protección frente a los ataques de DoS El R1 inicia, también, el procedimiento Diffie-Hellman, que contiene la clave pública del respondedor junto con los parámetros Diffie-Hellman.

Una vez recibido el paquete R1, el iniciador resuelve el rompecabezas y envía un fragmento de información en un paquete I2 junto con un valor SPI de IPsec y su clave pública de cifrado al respondedor. El respondedor verifica que se ha resuelto el rompecabezas, autentifica al iniciador y crea las SA de ESP para IPsec. El mensaje R2 final contiene el valor SPI del respondedor.

Las SA entre los anfitriones se limitan a las identidades de anfitrión, representadas por las HIT. Sin embargo, los paquetes que viajan por la red no contienen la información real de HI, sino que el paquete que llega es identificado y se le asigna la correspondencia con la SA correcta utilizando el valor del índice de parámetro de seguridad (SPI) en la cabecera de IPsec. La Figura 3 de los dibujos adjuntos ilustra las estructuras de paquete, lógica y real, cuando viaja por la red.

A partir de lo que antecede, es evidente que cambiando la información de posición del paquete no se origina problema alguno para el tratamiento en IPsec. El paquete sigue estando correctamente identificado mediante el uso del SPI. Si, por alguna razón, el paquete es encaminado a un destino equivocado, el receptor no es capaz de abrirlo al no poseer la clave correcta.

Cuando un paquete saliente llega a la capa de HI desde la capa superior, se verifica la HIT de destino a partir de la SADB (base de datos de asociaciones de seguridad) de IPsec. Si se encuentra una SA que case con la HIT de destino, el paquete es cifrado utilizando la clave de sesión asociada con la SA.

La HIT no puede ser utilizada para encaminar el paquete. Así, las direcciones de destino (y de fuente) deben cambiarse para casar con las direcciones de IP de los nodos. Estas asignaciones de correspondencia se almacenan, como se ha mencionado antes, en la capa de HI. Una vez que se han cambiado las direcciones, el paquete puede ser enviado al red, donde es encaminado al destino utilizando la información sobre la dirección de IP.

En el anfitrión receptor, se utiliza el valor SPI para encontrar la SA correcta a partir de la SADB de Ipsec. Si se encuentra una entrada, las direcciones de IP pueden cambiarse a las HIT correspondientes y puede descifrarse el paquete utilizando la clave de la sesión.

La movilidad se define como la situación en que un anfitrión se mueve mientras mantiene activo su contexto de comunicaciones o, dicho de otro modo, mientras el anfitrión cambia su posición topológica, descrita por la dirección de IP, mientras conserva activas todas las conexiones existentes. Los procesos que se ejecutan en el anfitrión no aprecian la movilidad excepto, posiblemente, si cambia la calidad del servicio que se tiene.

El anfitrión móvil puede cambiar de posición dentro de una red de acceso, entre diferentes tecnologías de acceso o, incluso, entre diferentes regiones de direcciones de IP, por ejemplo entre las redes IPv4 e IPv6. En el HIP, la aplicación no aprecia el cambio de versión de la dirección de IP. La capa de HI oculta completamente el cambio a las capas superiores. Naturalmente, el nodo igual debe ser capaz de tratar la actualización de posición que cambia la versión de IP y los paquetes deben poder ser encaminados utilizando alguna dirección compatible. Si un nodo carece de conectividad IPv4 e IPV6, puede utilizar un equipo representante que realice la conversión de versión de la dirección y proporcione conectividad en nombre del nodo.

Con multi-origen se hace referencia a una situación en la que un punto final tiene varios trayectos de comunicaciones paralelas que puede utilizar. Usualmente, el multi-origen es el resultado de que el anfitrión tenga varias interconexiones de red (multi-origen en anfitrión final) o se debe a que una red entre el anfitrión y el resto de la red tenga trayectos redundantes(multi-origen en un sitio).

Con el HIP, la separación entre la información sobre identidad y sobre posición deja claro que la identificación del paquete y el encaminamiento, pueden separarse una de otro en forma definida. El anfitrión que recibe un paquete identifica al remitente obteniendo, primero, la clave correcta y descifrando luego el paquete. Así, las direcciones de IP que se encuentran en el paquete carecen de importancia.

Un nodo móvil en HIP (HMN) que se desplace en la red puede cambiar su punto de unión a Internet constantemente. Cuando se cambia el punto de conexión, también lo hace la dirección de IP. Esta información sobre la posición cambiada debe ser enviada a los nodos iguales, es decir, los nodos interlocutores en HIP (HCN), y esto se ilustra en la Figura 4 de los dibujos adjuntos. La misma dirección puede ser enviada, también, a un agente transitario (FA) del HMN, de forma que el HMN pueda ser alcanzado, también, a través de un punto más estable. El sistema DNS es dema-

siado lento para ser utilizado con información que cambie de situación constantemente. Por tanto, debe contarse con una dirección más estable que pueda ser utilizada para conectar el HMN. Esta dirección es la dirección proporcionada por el FA.

El protocolo de multi-origen y de movilidad HIP (P. Nikander, J. Arkko, P. Jokela, "Movilidad de anfitrión final y multi-origen con protocolo de identidad de anfitrión", Internet Draft, en elaboración, draft-nikander-hip-mm-00.txt, IETF. 2003) define un paquete de redirección (REA) que contiene la dirección de IP corriente del HMN. Cuando el HMN cambia de situación y de dirección de IP, genera un paquete de REA, firma el paquete con la clave privada que casa con la HI utilizada y envía el paquete al nodo igual y al FA.

Cuando el nodo igual recibe el paquete de REA, tiene que iniciar un proceso de verificación de dirección para la dirección de IP incluida en el paquete de REA. La verificación de dirección es necesaria para evitar la aceptación de actualizaciones falsas a partir del HMN. Envía un paquete de comprobación de dirección (AC) a la dirección que se encontró en el paquete de REA. Cuando el HMN recibe una AC que casa con la REA enviada anteriormente, responde con un paquete de contestación a la comprobación de dirección (ACR). Después de que el nodo igual ha recibido el paquete de ACR, se completa la verificación de dirección y se puede sumar la dirección de IP como información de situación del HMN.

Como el HMN puede moverse entre redes que utilizan diferentes versiones de dirección de IP, la dirección recibida por el HCN puede ser, también, de una familia de direcciones diferente que la de la dirección previa.

El HCN puede soportar solamente una versión de dirección de IP. En este caso, el HCN debe utilizar algún otro nodo representante que pueda emplearse para encaminar paquetes a la red con otra versión diferente de direcciones de IP.

Un anfitrión HIP multi-origen, con múltiples direcciones de IP configuradas en diferentes interconexiones, conectadas a diferentes redes de acceso, tiene muchas más posibilidades de tratar el tráfico hacia un nodo igual. Como tiene múltiples direcciones de IP que presentan su situación corriente en la red, puede querer hacer llegar todas estas direcciones a sus nodos iguales. Para ello, el nodo HIP multi-origen crea un paquete de REA que contiene todas las direcciones que sea capaz de utilizar hacia ese nodo particular. Este conjunto de direcciones puede contener todas las direcciones que tenga, o un subconjunto de estas direcciones. Cuando el nodo igual recibe el paquete de REA con las direcciones múltiples, debe realizar una verificación de dirección para cada una de estas direcciones con el fin de evitar posibles falsas actualizaciones.

El HCN envía un conjunto de paquetes de AC destinado a las direcciones de IP incluidas en el paquete de REA. Cuando el HMN recibe estas AC, responde a cada una de ellas con ACR. El HCN puede determinar, a partir de los paquetes de ACR recibidos, cuales de las direcciones eran válidas.

Las direcciones falsas, o a las que no se puede realizar un encaminamiento, del paquete de REA, pueden deberse a que el HMN es un nodo malintencionado, a que tiene un error en la ejecución de la pila, o a que el HMN puede encontrarse en una red que utilice direcciones privadas no encaminables en Internet.

Un nodo HIP multi-origen es capaz de utilizar todas las conexiones disponibles, pero el uso eficiente de las conexiones requiere un sistema de política que tenga conocimiento de las redes de acceso subyacentes y pueda controlar el uso de las mismas. Tal sistema de política puede utilizar diferentes clases de información, preferencias de usuario, preferencias de operador, entrada de las conexiones de red, tales como QoS, etc.

Con el fin de iniciar el intercambio de HIP con un nodo móvil, el nodo iniciador ha de conocer cómo alcanzar el nodo móvil. Aunque para esta función podría utilizarse un DNS dinámico para nodos con movimiento infrecuente, una alternativa al uso del DNS en esta forma es la utilización de la pieza de infraestructura estática antes introducida, el agente transitario, denominado también servidor de encuentro HIP). En lugar de registrar su dirección dinámica corriente con el servidor de DNS, el nodo móvil registra la o las direcciones de su o de sus agentes transitarios. El nodo móvil mantiene al o a los agentes transitarios continuamente actualizados con su o sus direcciones de IP corrientes. Un agente transitario simplemente envía el paquete de HIP inicial desde un iniciador al nodo móvil en su posición corriente. Todos los otros paquetes circulan entre el iniciador y el nodo móvil. Típicamente, hay muy poca actividad en un agente transitario, fundamentalmente actualizaciones de direcciones y envío de paquetes HIP. Así, un agente transitario puede soportar gran número de potenciales nodos móviles. Los nodos móviles deben confiar en el agente transitario para mantener apropiadamente sus correspondencias entre direcciones de IP y HIT. Un agente transitario puede ser utilizado, incluso, para nodos que tienen una posición fija ya que, con frecuencia, se da el caso de que nodos fijos puedan cambiar su dirección de IP frecuentemente, por ejemplo, cuando se asigna cada vez que un proveedor de servicios para ese nodo establece una conexión de Internet.

EL agente transitario también es necesario si ambos nodos son móviles y se mueven, ambos, al mismo tiempo. En ese caso, los paquetes de redirección de HIP se cruzarán en la red y nunca alcanzarán el nodo igual. Para resolver esta situación, los nodos deben recordar la dirección del agente transitario y reenviar el paquete de redirección de HIP al agente transitario si no se recibe contestación.

El nodo móvil mantiene su dirección corriente en el agente transitario estableciendo una asociación de HIP con el agente transitario y enviándole paquetes de redirección de HIP. Un agente transitario permitirá que dos sistemas móviles utilicen el HIP sin ningún sistema extraño (además del propio agente transitario), incluyendo el DNS si tienen un método que no es una petición al DNS, para conseguir la HI y la HIT del otro.

En el caso de equipo legado, un anfitrión puede no estar habilitado para HIP y la única opción es identificar las conexiones entre los anfitriones que utilizan direcciones de IP. Esto no es seguro. La situación puede mejorarse situando un equipo representante para HIP entre el anfitrión habilitado para HIP y el anfitrión que no puede utilizar el HIP. Un escenario típico sería una pequeña LAN corporativa en la que los terminales cliente no estuviesen habilitados para HIP. El tráfico es encaminado a anfitriones interlocutores (que están habilitados para HIP) a través del equipo representante para HIP.

Esta disposición se ilustra en la Figura 5 de los dibujos adjuntos. En la Figura 5 se muestra un anfitrión legado 12 en comunicación con un nodo 14 habilitado para HIP (que tiene el nombre de dominio "hip.foo.com") a través de un equipo representante 16 para HIP. El anfitrión legado 12 accede al equipo representante 16 para HIP mediante una red de acceso 18 mientras que el equipo representante 16 para HIP accede al nodo 14 habilitado para HIP por la Internet 20. Para asegurar parcialmente la conexión entre el anfitrión legado 12 y el nodo 14 habilitado para HIP, todas las comunicaciones entre el equipo representante 16 para HIP y el nodo 14 habilitado para HIP se realizan a través de una asociación de seguridad establecida entre el equipo representante 16 para HIP y el nodo 14 habilitado para HIP, en forma similar a la descrita en lo que antecede con referencia a la Figura 3.

Sin embargo, incluso antes que pueda establecerse la asociación de seguridad 22, representada en la Figura 5, para permitir la comunicación entre el anfitrión legado 12 y el nodo 14 para HIP, surge un problema cuando el primero intenta resolver la dirección de IP del nodo 14 para HIP enviando una petición a un servidor de DNS 24-1 (y en su momento al servidor DNS 24-2) cuando el nodo 14 para HIP está situado detrás de un agente transitario 26, como se ha descrito anteriormente. El servidor DNS 24-1 devolverá una HIT del nodo 14 para HIP junto con la dirección de IP del agente transitario 26. Como el nodo legado 12 no está habilitado para HIP, despreciará la HIT y comenzará a enviar mensajes al agente transitario 26. Sin la HIT, el agente transitario 26 no podrá resolver la dirección de destino de estos mensajes, ya que los más probable es que varios nodos habilitados para HIP empleen el mismo agente transitario 26. Igualmente. como el nodo legado 12 desecha la HIT y solamente utiliza la dirección de IP del nodo 14 para HIP cuando se inicia una conexión, el equipo representante 16 habilitado para HIP no puede iniciar la negociación en HIP entre él mismo y el nodo 14 para HIP, ya que no conoce la HIT del nodo 14 para HIP.

Es deseable proporcionar un método para asegurar, al menos parcialmente, las comunicaciones entre un primer anfitrión que no está habilitado para HIP y un segundo anfitrión que está habilitado para HIP a través de un equipo representante habilitado para HIP, que evite los problemas antes mencionados.

Sumario del invento

De acuerdo con un primer aspecto del presente invento, se proporciona un método para asegurar, al menos parcialmente, las comunicaciones, a través de un equipo representante habilitado para HIP, entre un primer anfitrión que no está habilitado para HIP y un segundo anfitrión que sí lo está, cuyo método comprende: enviar una petición desde el primer anfitrión para resolver la dirección de IP del segundo anfitrión; recuperar, en respuesta a dicha petición, una dirección de IP y la HIT asociada con el segundo anfitrión; devolver, en respuesta a dicha recuperación, desde el equipo representante, una dirección de IP sustituta asociada con el segundo anfitrión; mantener en el equipo representante una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada; y, al recibirse un mensaje de iniciación de sesión en el equipo representante, procedente del primer anfitrión, que incluya como dirección de destino la dirección de IP sustituta, hacer valer la correspondencia para negociar una conexión en HIP entre el equipo representante y el segundo anfitrión.

El método puede comprender buscar la dirección de IP recuperada y la HIT recuperada a partir de la correspondencia basándose en la dirección de IP sustituta del mensaje de iniciación de sesión, y llevar a cabo la negociación en el HIP utilizando la dirección de IP y la HIT recuperadas para localizar e identificar al respondedor en la negociación en el HIP junto con una dirección de IP y una HIT del equipo representante para localizar e identificar al iniciador de la negociación en el HIP.

La dirección de IP recuperada puede ser la dirección de IP de un agente transitario utilizado por el segundo anfitrión y, además, el método comprende iniciar la negociación en el HIP entre el equipo representante y el segundo anfitrión enviando el paquete inicial de negociación en el HIP al agente transitario.

El método puede comprender, además, a continuación de la recepción de la dirección de IP real del segundo anfitrión en el equipo representante durante la negociación en el HIP, incluir la dirección de IP real en la correspondencia mantenida en el equipo representante. La dirección de IP recuperada puede ser reemplazada en la correspondencia por la dirección de IP real tras su recepción en el equipo representante.

La dirección de IP recuperada puede ser la dirección de IP real del segundo anfitrión.

El método puede comprender la generación de la dirección de IP sustituta en el equipo representante.

El método puede comprender, además, para un mensaje saliente recibido en el equipo representante una vez establecida la conexión del HIP incluyendo como su dirección de destino la dirección de IP sustituta, utilizar la correspondencia para encaminar el mensaje por la conexión de HIP al segundo anfitrión. Esto puede suponer la búsqueda de la dirección IP real y la HIT recuperadas a partir de la correspondencia basándose en la dirección de IP sustituta del mensaje saliente, y encaminar el mensaje saliente al segundo anfitrión utilizando la dirección de IP real y la HIT recuperadas para localizar e identificar el destino del mensaje, y utilizar una dirección de IP y la HIT del equipo representante para localizar e identificar la fuente del mensaje.

El método puede comprender, además, completar el establecimiento de comunicaciones entre el primero y el segundo anfitriones enviando un mensaje de iniciación de sesión desde el equipo representante al segundo anfitrión por la conexión de HIP, contestar con un mensaje de acuse de recibo de sesión a partir del segundo anfitrión hacia el equipo representante por la conexión de HIP y encaminar el mensaje de acuse de recibo de sesión al primer anfitrión. El mensaje de acuse de recibo de sesión puede ser un mensaje TCP ACK.

El mensaje de iniciación de sesión puede ser un mensaje TCP SYN.

El método puede comprender, además, para un mensaje entrante recibido en el equipo representante desde el segundo anfitrión por la conexión de HIP establecida, utilizar una función NAT del equipo representante para encaminar el mensaje al anfitrión de destino apropiado.

La petición antes mencionada puede ser una petición de DNS. El equipo representante puede interceptar la petición de DNS procedente del primer anfitrión. El equipo representante puede realizar la operación de recuperación de la dirección de IP y de la HIT asociadas con el segundo anfitrión.

El equipo representante puede recuperar la dirección de IP y la HIT asociadas con el segundo anfitrión a partir de un servidor DNS externo. O bien, el equipo representante puede recuperar la dirección de IP y la HIT asociadas con el segundo anfitrión a partir de un servidor de DNS externo.

De acuerdo con un segundo aspecto del presente invento, se proporciona un sistema de comunicaciones que comprende un primer anfitrión que no está habilitado para HIP, un segundo anfitrión que sí lo está y un equipo representante para HIP, en el que: el primer anfitrión comprende medios para enviar una petición para resolver la dirección de IP del segundo anfitrión; el equipo representante comprende medios para recuperar, en respuesta a dicha petición, una dirección de IP y una HIT asociada con el segundo anfitrión, para devolver, en respuesta a dicha recuperación, una dirección de IP sustituta asociada con el segundo anfitrión, para mantener una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada, y para utilizar la correspondencia, al recibirse un mensaje de iniciación de sesión procedente del primer anfitrión, que incluya como su dirección de destino la dirección de IP sustituta, para negociar una conexión de HIP entre el equipo representante y el segundo anfitrión.

De acuerdo con un tercer aspecto del presente invento, se proporciona un método para uso por un equipo representante habilitado para HIP, para establecer la seguridad de las comunicaciones, al menos parcialmente, a través del equipo representante, entre un primer anfitrión que no está habilitado para HIP y un segundo anfitrión que sí lo está, cuyo método comprende: recibir una petición del primer anfitrión para resolver la dirección de IP del segundo anfitrión; en respuesta a dicha petición, recuperar una dirección de IP y una HIT asociadas con el segundo anfitrión; en respuesta a dicha recuperación, devolver una dirección de IP sustituta asociada con el segundo anfitrión, y mantener una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada; y, al recibirse un mensaje de iniciación de sesión procedente del primer anfitrión, que incluye como su dirección de destino la dirección de IP sustituta, utilizar la correspondencia para negociar una conexión de HIP entre el equipo representante y el segundo anfitrión.

De acuerdo con un cuarto aspecto del presente invento, se proporciona un equipo representante habilitado para HIP, para uso con el fin de establecer, al menos parcialmente, la seguridad de las comunicaciones a través del equipo representante entre un primer anfitrión que no está habilitado para HIP y un segundo anfitrión que sí lo está, que comprende: medios para recibir una petición procedente del primer anfitrión para resolver la dirección de IP del segundo anfitrión; medios para recuperar, en respuesta a dicha petición, una dirección de IP y una HIT asociadas con el segundo anfitrión para devolver, en respuesta a dicha recuperación, una dirección de IP sustituta asociada con el segundo anfitrión, y mantener una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada; y medios para utilizar la correspondencia, al recibirse un mensaje de iniciación de sesión procedente del primer anfitrión que incluya como su dirección de destino la dirección de IP sustituta, para negociar una conexión de HIP entre el equipo representante y el segundo anfitrión.

De acuerdo con un quinto aspecto del presente invento, se proporciona un programa de ordenador que, cuando se ejecuta en un equipo representante habilitado para HIP, hace que el equipo representante lleve a la práctica un método de acuerdo con un tercer aspecto del presente invento.

De acuerdo con un sexto aspecto del presente invento, se proporciona un programa de ordenador que, cuando se carga en un equipo representante habilitado para HIP, hace que el equipo representante incluya todas las características de acuerdo con el cuarto aspecto del presente invento.

El programa de ordenador puede ejecutarse en un medio portador, que puede ser un medio de transmisión o un medio de almacenamiento.

Breve descripción de los dibujos

La Figura 1, descrita en lo que antecede, ilustra las diversas capas del protocolo de identidad de anfitrión;

la Figura 2, descrita también en lo que antecede, ilustra el funcionamiento de la iniciación de diálogo de cuatro vías en el protocolo HIP;

la Figura 3, descrita también en lo que antecede, ilustra las estructuras de paquete lógica y real en el HIP;

la Figura 4, descrita también en lo que antecede, ilustra el cambio entre IPv6 e IPv4;

la Figura 5, descrita también en lo que antecede, es un diagrama esquemático que ilustra la red general establecida para comunicaciones entre un anfitrión legado y un nodo habilitado para HIP, a través de un equipo representante habilitado para HIP;

la Figura 6 es un diagrama de intercambio de mensajes que ilustra, esquemáticamente, un método para establecer, al menos parcialmente la seguridad de las comunicaciones entre un anfitrión legado y un anfitrión habilitado para HIP, de acuerdo con una realización del presente invento;

la Figura 7 ofrece una ilustración esquemática, más detallada, de las estructuras de paquete utilizadas en TCP, UDP, ESP y HIP; y

las Figuras 8 a 12 son diagramas de intercambio de mensajes que muestran los pasos del método de la Figura 6 con mayor detalle.

Descripción detallada de las realizaciones preferidas

Se describirá ahora una realización del presente invento en el marco general del sistema antes descrito con referencia a la Figura 5. Una realización del presente invento proporciona un método de garantizar, al menos parcialmente, la seguridad en las comunicaciones entre el anfitrión legado 12, que no está habilitado para HIP, y el anfitrión 14 para HIP, que está habilitado para HIP, a través de equipo representante 16 habilitado para HIP. Se describirá ahora el funcionamiento de una realización del presente invento con referencia al diagrama de intercambio de mensajes de la Figura 6. Los pasos representados en la Figura 6 se ilustran también, con mayor detalle, en las Figuras 8 a 12, mientras que la Figura 7 ofrece una visión general más detallada de las estructuras de paquete utilizadas en TCP, UDP (protocolo de datagrama de usuario), ESP y HIP.

Consideremos situación en que el anfitrión legado 12 desea iniciar una comunicación entre él mismo y el anfitrión 14 para HIP. El anfitrión legado 12 conoce el nombre de dominio del anfitrión 14 para HIP, que es "hip.foo.com" y, como primer paso (marcado como "A" en las Figuras 6 y 8), el anfitrión legado 12 envía una petición de sistema de nombre de dominio (DNS) a su servidor de DNS usual, con el fin de resolver la dirección de IP del anfitrión 14 para HIP. Sin embargo, en lugar de ser recibida directamente en un servidor de DNS, en una realización del presente invento la petición de DNS es interceptada por el equipo representante 16 para HIP, que a su vez envía una petición de DNS al servidor de DNS 24-1 (esto está marcado como "B" en las Figuras 6 y 8).

En respuesta a esta petición de DNS, el servidor de DNS 24-1 comunica con el servidor de DNS 24-2 "foo.com" para recuperar una dirección de IP y una HIT asociadas con el anfitrión 14 para HIP (marcado como "C" en las Figuras 6 y 9). Dado que, en este ejemplo, el anfitrión 14 para HIP está utilizando en agente transitario (FA) 26 como "dirección de origen", como antes se ha descrito, la dirección de IP y la HIT recuperadas por la petición de DNS son la dirección de IP 3ffe:200::1 (IP_{fn}) del agente transitario 26 y la HIT del anfitrión 14 para HIP, denominada en este caso HIT_{hip}: Obsérvese que este no siempre ocurre que se requieran varios servidores de DNS para resolver una dirección de IP; si la información se encuentra a partir del primer servidor, no habría necesidad de utilizar servidores de DNS adicionales.

Como el equipo representante para HIP sabe que el anfitrión iniciador que envió la petición de DNS no está habilitado para HIP, el equipo representante 16 para HIP no devuelve la información de DNS (HIT_{hip}; IP_{fa}). En cambio, el equipo representante 16 para HIP genera una dirección de IP sustituta IP_{res} que, en este ejemplo, es 3ffe:401::5. El equipo representante 16 para HIP mantiene una correspondencia {HIT_{hip};IP_{fa};IP_{res}} entre la HIT recibida del servidor de DNS 24, la dirección de IP recuperada del servidor de DNS 24 y la dirección de IP sustituta generada por el equipo representante 16 para HIP. Esta correspondencia es necesaria para tratar el encaminamiento de comunicaciones subsiguientes, como se describirá en lo que sigue. La generación de la dirección de IP sustituta, IP_{res}, y el mantenimiento de la correspondencia está marcado como "D" en las Figuras 6 y 9.

Entretanto, el equipo representante 16 para HIP envía una respuesta de DNS de vuelta al anfitrión legado 12 con la dirección de IP sustituta, IP_{res}, y esto está marcado con "E" en las Figuras 6 y 9. La dirección de IP sustituta, IP_{res} será utilizada por el anfitrión legado 12 como dirección de destino para todas las comunicaciones subsiguientes que envíe hacia el anfitrión 14 para HIP.

Cuando el anfitrión legado 12 está preparado para iniciar una conexión con el anfitrión 14 para HIP, envía un mensaje de iniciación de sesión, TCP SYN, que tiene como dirección de destino la dirección de IP sustituta, IP_{res}; esto está marcado con "F" en las Figuras 6 y 10. Como la dirección de IP sustituta, IP_{res} fue generada por el equipo representante 16 para HIP y mantenida en la correspondencia M, el equipo representante 16 para HIP reconoce la dirección de destino del mensaje de iniciación procedente del anfitrión legado 12 (marcado como "F.1" en la Figura 10) y asume la subsiguiente responsabilidad para el establecimiento y el tratamiento de las comunicaciones entre el anfitrión legado 12 y el anfitrión 14 para HIP.

El equipo representante 16 para HIP utiliza entonces la correspondencia M para negociar una conexión segura para HIP (asociación de seguridad) entre el equipo representante 16 para HIP y el anfitrión 14 para HIP. La negociación llevada a cabo entre el equipo representante 16 para HIP y el anfitrión 14 para HIP, es muy similar a la iniciación de diálogo de cuatro vías anteriormente descrita con referencia a la Figura 2, siendo el iniciador, en este ejemplo, el equipo representante 16 para HIP y siendo el respondedor el anfitrión 14 para HIP. El comienzo de la negociación en el HIP está marcado con "G" en las Figuras 6 y 10. Debe observarse que, cuando se utiliza en este documento la expresión "asociación de seguridad", ha de tenerse en cuenta que incluye el caso en que se cree un par de asociaciones de seguridad entre ambos anfitriones, una asociación de seguridad que gestiona el tráfico en una dirección y otra que lo gestiona en la otra dirección; lógicamente existiría un conducto para SA entre los dos anfitriones pero, físicamente, habría dos SA.

Haciendo uso de la correspondencia M, el equipo representante 16 para HIP determina que el paquete I1 debe ser enviado a la dirección de IP IP_{fa}, que es la dirección de IP del agente transitario 26 utilizado por el anfitrión 14 para HIP. El paquete I1 contiene las HIT de los nodos que participan en la negociación, es decir, HIT_{hip} y $HIT_{representante}$. Esta correspondencia está marcada como "H" en las Figuras 6 y 10. Cuando el paquete I1 es recibido por el agente transitario 26, éste prepara una correspondencia de HIT_{hip} para la dirección de IP real, IP_{hip} y lleva a cabo su función usual de envío del paquete 12 recibido al anfitrión 14 de HIP localizado mediante IP_{hip}.

A continuación de la recepción del paquete I1 en el anfitrión 14 para HIP, se forma el resto de la negociación para la iniciación de diálogo de cuatro vías, como se ha descrito en lo que antecede, con referencia a la Figura 2, mediante el envío de los paquetes R1, I2 y R2. Una vez completada esta negociación, se ha establecido la asociación de seguridad 22 entre el equipo representante 16 para HIP y el anfitrión 14 para HIP, y esto está marcado por "I" en las Figuras 6 y 10.

Ahora que se ha establecido la asociación de seguridad 22, el equipo representante 16 para HIP continúa enviando el mensaje de iniciación TCP SYN al anfitrión 14 para HIP. La función de traducción de la dirección de red (NAT) y de correspondencia ejecutada, se muestra con mayor detalle en la parte inferior de la Figura 11 y está marcada como "L1" en esa figura. El anfitrión 14 para HIP responde con un mensaje PCP ACK dirigido a la dirección de IP del equipo representante 16 para HIP que, en este ejemplo, es 3ffe:300::1; estos dos pasos están marcados como "J" en las Figuras 6 y 11. Finalmente, el equipo representante 16 para HIP devuelve un mensaje PCP ACK al anfitrión legado 12 en su dirección de IP 3ff3:400::50 para completar el procedimiento de iniciación de TCP; esto está marcado con "K" en las Figuras 6 y 12. Se observará que el mensaje TCP ACK, marcado como "J" en las Figuras 6 y 11, procedente del anfitrión 14 para HIP y dirigido al equipo representante 16 para HIP contenía, como su dirección de IP de destino la dirección de IP del equipo representante 16 para HIP y no la dirección de IP del anfitrión legado 12. Se describirá ahora el método por el que el equipo representante 16 para HIP conoce, subsiguientemente, cómo enviar el mensaje TCP ACK al anfitrión legado 12 correcto.

Solamente se establece una asociación de seguridad 12 entre el equipo representante 16 para HIP y el nodo 14 para HIP, y esta asociación de seguridad 22 es utilizada por múltiples anfitriones legados que comunican con el anfitrión 14 para HIP. La correspondencia M antes descrita está asociada con una asociación de seguridad y no con un anfitrión legado particular, tal como el anfitrión legado 12. Como la asociación de seguridad 22 y su correspondencia M asociada, deben ser utilizadas por una pluralidad de anfitriones legados, la correspondencia M no puede incluir información relacionada con un anfitrión legado particular tal como, por ejemplo, la dirección de IP del anfitrión legado que fue inicialmente responsable del establecimiento de la asociación de seguridad 22. En cambio, la función de traducción de dirección de red (NAT) en el equipo representante para HIP trata la correspondencia de paquetes para la dirección de IP correcta del anfitrión legado.

Para este fin, se utilizan los números de puerta de la capa superior, como para la función NAT usual. Para el tráfico entre el anfitrión 14 para HIP y el anfitrión legado 12 a través del equipo representante 16 para HIP, la dirección de la fuente cuando el paquete de IP llega al equipo representante 16 para HIP procedente del anfitrión 14 para HIP es, originalmente, la dirección de IP del anfitrión 14 para HIP. La dirección de IP sustituta IP_{hip} es recuperada a partir de la correspondencia M asociada con la asociación de seguridad 22 y reemplazada como dirección de fuente del paquete de IP. El paquete de IP es cambiado a la función NAT del equipo representante 16 para HIP y, empleando la información sobre la dirección de IP de la fuente y los números de puerta con fines de asignación de correspondencia a las direcciones. El número de puerta no puede utilizarse por sí solo, ya que dos anfitriones legado podrían estar utilizando el mismo número de puerta. La función NAT normalizada lleva a cabo, también, una correspondencia de puertas ya que, de otro modo, la traducción de la dirección no funcionará si dos anfitriones utilizan el mismo número de puerta fuente para comunicación hacia el mismo nodo externo. Cuando se ejecuta una correspondencia de NAT, también se consulta el protocolo, ya que UDP y TCP pueden utilizar los mismos números de puerta.

Por ejemplo, para dos anfitriones legado LH1 y LH2 que se comunican con el anfitrión 14 para HIP externo que escucha en la puerta 10000:

LH1:puerta fuente 5000, puerta dst 10000, srcIP IP_{lh1}, dstIP IP_{res}

LH2:puerta fuente 5000, puerta dst 10000, srcIP IP_{lh2}, dstIP IP_{res}

El equipo representante 16 para HIP prepara la correspondencia para la conexión saliente (vinculada al anfitrión para HIP), como sigue:

LH1:puerta fuente 5001, puerta dst 10000, srcIP $IP_{representante}$, dstIP IP_{hip}

LH2:puerta fuente 5002, puerta dst 10000, srcIP $IP_{representante}$, dstIP IP_{hip}

Lo que antecede es, por tanto, justamente la función NAT estándar, excepto porque la dirección de destino también es cambiada por el equipo representante 16 para HIP de IP_{res} a IP_{hip}.

El anfitrión 14 para HIP ve dos conexiones separadas desde el equipo representante 16 para HIP con la misma dirección de IP. Para el tráfico entrante (vinculado a LH) desde el anfitrión 14 para HIP, el equipo representante 16 para HIP puede preparar ahora la correspondencia:

dst $IP_{representante}$,src IP_{hip},dst puerta 5001, src puerta 10000 => dst IP_{lh1}; src IP_{res};dst puerta 5000; src puerta 10000

dst $IP_{representante}$,src IP_{hip},dst puerta 5002, src puerta 10000 => dst IP_{lh2}; src IP_{res};dst puerta 5000; src puerta 10000

La función de NAT para paquetes entrantes se ilustra también, con mayor detalle, en la parte inferior de la Figura 12 y está marcada con "K".

Una vez establecida la asociación de seguridad 22 entre el equipo representante 16 para HIP y el anfitrión 14 para HIP, las subsiguientes comunicaciones entre el anfitrión legado 12 y el anfitrión 14 para HIP no pasan por el agente transitario 26, que solamente es utilizado para enviar el paquete I1 inicial, como antes se ha descrito. Por tanto, para una asociación de seguridad 22 establecida, ya no se necesita la dirección de IP del agente transitario (IP_{fa}) en la correspondencia M asociada con la asociación de seguridad 22. En cambio, se necesita la información sobre posición corriente (dirección de IP IP_{hip}) del anfitrión 14 para HIP.

Por tanto, la dirección de IP del agente transitario 26 (IP_{fa}) puede ser reemplazada en la correspondencia M por la dirección de IP del anfitrión 14 para HIP (IP_{hip}). Dicho de otro modo, la correspondencia M se cambia de {HIT_{hip}; IP_{fa}; IP_{res}} a {HIThip; IPhip; IP_{res}). Esto se ilustra en la Figura 10 mediante "H.1). De esta forma, a cualesquiera paquetes subsiguientes enviados desde el anfitrión legado 12 que tengan como dirección de destino la dirección IP sustituta, IP_{res}, les puede ser asignada una correspondencia mediante el equipo representante 16 para HIP sobre la asociación de seguridad 22 utilizando la correspondencia M modificada y les puede enviar directamente al anfitrión 14 para HIP en el lugar IP_{hip}. A las direcciones de IP de fuente y de destino se les asigna una correspondencia en el equipo representante 16 para HIP de {dst=IP_{res};src=IP_{lh}} a {dst=IP_{hip};src=$IP_{representante}$}, tomándose la correspondencia a partir de la correspondencia M modificada. El equipo representante 16 para HIP recibe la dirección de IP real, IP_{hip} del anfitrión 14 para HIP a partir del paquete R1 durante la negociación de HIP.

Aunque se ha descrito en lo que antecede una realización del presente invento, en la cual el anfitrión 14 para HIP está situado detrás de un agente transitario 26, el presente invento tendrá aplicación, también, cuando el anfitrión 14 para HIP no utilice agente transitario. Por ejemplo, si el anfitrión 14 para HIP (con nombre de dominio "hip.foo.com") tiene una dirección de IP fija, IP_{fija},, sin agente transitario, una petición de DNS devolverá la dirección de IP fija, IP_{fija} y la HIT_{hip} del anfitrión 14 para HIP. Cuando un anfitrión legado 12 intente resolver la dirección de IP para "hip.foo.com", el equipo representante 16 para HIP interceptará esta petición de DNS y recuperará, por sí mismo, IP_{fija} y HIT_{hip} a partir de la DNS. El equipo representante 16 para HIP no puede saber, generalmente, que la dirección de IP devuelta desde el servidor de DNS 24 es la dirección de IP real del anfitrión 14 para HIP y no la dirección de IP de un agente transitario utilizado por el anfitrión 14 para HIP y, por tanto, genera una dirección de IP sustituta, IP_{res}, como se ha descrito en lo que antecede y devuelve esta dirección de IP sustituta al anfitrión legado 12, como anteriormente. El equipo representante 16 para HIP mantiene la correspondencia {HIT_{hip}; IP_{fija}; IP_{res}} quedando a la escucha de un paquete TCP SYN para IP_{res}, al recibir el cual negocia con el anfitrión 14 para HIP basándose en {HIT_{hip};IP_{fija}} a partir de la correspondencia. Una vez establecida la asociación de seguridad, los paquetes destinados a IP_{res} son recogidos por el equipo representante 16 para HIP y enviados a {HIT_{hip};IP_{fija}} utilizando la correspondencia. Esto se parece mucho al procedimiento anteriormente descrito, excepto en que IP_{fa} nunca se guarda en la correspondencia y, por tanto, nunca es reemplazada. En cambio, la correspondencia comprende, desde el principio, la dirección de IP del anfitrión 14 para HIP.

Si fuese posible que el equipo representante 16 para HIP determinase que la dirección de IP recuperada del servidor de DNS 24 era la dirección de IP real del anfitrión 14 para HIP, entonces una alternativa a la generación de una dirección de IP sustituta consistiría, simplemente, en devolver la dirección de IP real del anfitrión 14 para HIP al anfitrión legado 12. Esto abriría la posibilidad de que las comunicaciones entre el anfitrión legado 12 y el anfitrión 14 para HIP pudieran "saltarse" el equipo representante 16 para HIP completamente, ya que el anfitrión legado 12 tiene la dirección de IP real del anfitrión 14 para HIP. Si fuese este el caso, entonces las comunicaciones no quedarían aseguradas por medio del protocolo HIP pero, no obstante, las comunicaciones serían posibles basándose en la norma TCP/IP. Sin embargo, en redes pequeñas, con un trayecto saliente del anfitrión legado 12 hacia el equipo representante 16 para HIP, seguiría siendo posible que el equipo representante 16 para HIP actuase como pasarela de seguridad entre el anfitrión legado 12 y el anfitrión 14 para HIP, con una asociación de seguridad establecida en forma muy parecida a lo que antecede, pero sin que se requiriese correspondencia entre una dirección de IP sustituta y la dirección de IP real del anfitrión 14 para HIP. Por tanto, en este último caso, la correspondencia M comprendería solamente la dirección de IP IP_{hip} del anfitrión 14 para HIP y la HIT del anfitrión 14 para HIP, HIT_{hip}.

Aunque en lo que antecede se ha descrito que el equipo representante 16 para HIP envía una petición de DNS a un servidor de DNS 24 externo, es posible que el equipo representante 16 para HIP también pudiera prestar la función de servidor de DNS, sin que fuese necesaria una petición de DNS externa.

Se apreciará que el funcionamiento de uno o más de entre el anfitrión legado 12, el equipo representante 16 para HIP y el anfitrión 14 para HIP puede ser controlado mediante un programa que se ejecute en el dispositivo. Dicho programa operativo puede almacenarse en un medio legible por ordenador o podría, por ejemplo, estar incorporado en una señal tal como una señal de datos descargable proporcionada a partir de un sitio de red de Internet. Ha de interpretarse que las reivindicaciones adjuntas cubren un programa operativo en sí mismo, o grabado en un portador, o en forma de señal o en cualquier otra forma.

Un experto en la técnica apreciará que las realizaciones del presente invento no están limitadas a ningún protocolo particular para cada una de las capas, por ejemplo, en las capas de transporte o de red, y que funcionarán dentro del marco del HIP, cualquiera que sea el protocolo de direccionamiento o de transporte que se utilice en ese marco.

REIVINDICACIONES

1. Un método de garantizar, al menos parcialmente, la seguridad de comunicaciones, a través de un equipo representante (16) para protocolo de identidad de anfitrión, HIP, entre un primer anfitrión (12) que no está habilitado para HIP y un segundo anfitrión (14) que está habilitado para HIP, cuyo método comprende:

enviar una petición desde el primer anfitrión para resolver la dirección de protocolo de Internet, IP, del segundo anfitrión;

en respuesta a dicha petición, recuperar una dirección de IP y una etiqueta de identidad de anfitrión, HIT, asociadas con el segundo anfitrión;

en respuesta a dicha recuperación, devolver desde el equipo representante para HIP una dirección de IP sustituta, asociada con el segundo anfitrión;

mantener en el equipo representante para HIP una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada; y

al recibirse un mensaje de iniciación de sesión en el equipo representante para HIP procedente del primer anfitrión, que incluya como su dirección de destino la dirección de IP sustituta, utilizar la correspondencia para negociar una conexión a través de HIP entre el equipo representante para HIP y el segundo anfitrión.

2. Un método como se reivindica en la reivindicación 1, que comprende buscar la dirección de IP recuperada y la HIT recuperada a partir de la correspondencia basándose en la dirección de IP sustituta en el mensaje de iniciación de sesión, y llevar a cabo la negociación a través del HIP utilizando la dirección de IP y la HIT recuperadas para localizar e identificar el respondedor en la negociación a través de HIP, junto con la dirección IP y la HIT del equipo representante para localizar e identificar al iniciador en la negociación a través de HIP.

3. Un método como se reivindica en la reivindicación 1 o en la reivindicación 2, en el que la dirección de IP recuperada es la dirección de IP de un agente transitario utilizado por el segundo anfitrión, y que comprende además iniciar la negociación a través de HIP entre el equipo representante y el segundo anfitrión enviando el paquete de negociación a través de HIP al agente transitario.

4. Un método como se reivindica en la reivindicación 3, que comprende además, a continuación de la recepción de la dirección IP real del segundo anfitrión en el equipo representante durante la negociación a través de HIP, incluir la dirección de IP real en la correspondencia mantenida en el equipo representante.

5. Un método como se reivindica en la reivindicación 4, en el que la dirección de IP recuperada es sustituida en la correspondencia por la dirección de IP real a continuación de su recepción en el equipo representante.

6. Un método como se reivindica en la reivindicación 1 o la reivindicación 2, en el que la dirección de IP recuperada es la dirección de IP real del segundo anfitrión.

7. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, que comprende generar la dirección de IP sustituta en el equipo representante.

8. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, que comprende además, para un mensaje saliente recibido en el equipo representante después de haberse establecido la conexión a través de HIP que incluye como su dirección de destino la dirección de IP sustituta, utilizar la correspondencia para encaminar el mensaje por la conexión HIP hacia el segundo anfitrión.

9. Un método como se reivindica en la reivindicación 8 cuando depende de la reivindicación 4, que comprende buscar la dirección de IP real y la HIT recuperadas a partir de la correspondencia basándose en la dirección de IP sustituta del mensaje saliente, y encamina el mensaje saliente hacia el segundo anfitrión utilizando la dirección de IP real y la HIT recuperadas para localizar e identificar el destino del mensaje, y utilizar una dirección de IP y la HIT del equipo representante para localizar e identificar la fuente del mensaje.

10. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, que comprende además, completar el establecimiento de las comunicaciones entre el primero y el segundo anfitriones enviando el mensaje de iniciación de expedición desde el equipo representante al segundo anfitrión por la conexión de HIP, contestar con un acuse de recibo de sesión procedente del segundo anfitrión hacia el equipo representante por la conexión de HIP, y encaminar el mensaje de acuse de recibo de sesión hacia el primer anfitrión.

11. Un método como se reivindica en la reivindicación 10, en el que el mensaje de acuse de recibo de sesión es un mensaje TCP ACK.

12. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, en el que el mensaje de iniciación de sesión es un mensaje TCP SYN.

13. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, que comprende además, para un mensaje entrante recibido en el equipo representante procedente del segundo anfitrión por la conexión de HIP establecida, utilizar una función de NAT del equipo representante para encaminar el mensaje hacia el anfitrión de destino apropiado.

14. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, en el que la petición es una petición de DNS.

15. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, en el que el equipo representante ejecuta el paso de recuperar la dirección de IP y de la HIT asociadas con el segundo anfitrión.

16. Un método como se reivindica en la reivindicación 15, en el que el equipo representante recupera la dirección de IP y la HIT asociadas con el segundo anfitrión a partir de un servidor de DNS externo.

17. Un método como se reivindica en la reivindicación 15, en el que el equipo representante recupera la dirección de IP y la HIT asociadas con el segundo anfitrión a partir de un servidor de DNS interno.

18. Un método como se reivindica en cualquiera de las reivindicaciones precedentes, en el que el equipo representante intercepta la petición procedente del primer anfitrión.

19. Un sistema de comunicaciones, que comprende un primer anfitrión (12) que no está habilitado para protocolo de identidad de anfitrión, HIP, un segundo anfitrión (14) que está habilitado para HIP, y un equipo representante (16), en el que:

el primer anfitrión comprende medios para enviar una petición a fin de resolver la dirección de protocolo de Internet, IP, del segundo anfitrión;

el equipo representante comprende medios para recuperar, en respuesta a dicha petición, una dirección de IP y una etiqueta de identidad de anfitrión, HIT, asociada con el segundo anfitrión, para devolver, en respuesta a dicha recuperación, una dirección de IP sustituta asociada con el segundo anfitrión, para mantener una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada, y para utilizar la correspondencia, al recibirse un mensaje de iniciación de sesión procedente del primer anfitrión que incluye, como su dirección de destino, la dirección de IP sustituta, para negociar una conexión a través de HIP entre el equipo representante para HIP y el segundo anfitrión.

20. Un método para uso por un equipo representante (16) a través de un protocolo de identidad de anfitrión, HIP, de comunicaciones, al menos, parcialmente seguras, a través del equipo representante para HIP, entre un primer anfitrión (12) que no está habilitado para HIP y un segundo anfitrión (14) que está habilitado para HIP, cuyo método comprende:

recibir una petición procedente del primer anfitrión para resolver la dirección de protocolo de Internet, IP, del segundo anfitrión;

en respuesta a dicha petición, recuperar una dirección de IP y una etiqueta de identidad de anfitrión, HIT, asociadas con el segundo anfitrión;

en respuesta a dicha recuperación, devolver una dirección de IP sustituta asociada con el segundo anfitrión, y mantener una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada; y

al recibirse un mensaje de iniciación de sesión procedente del primer anfitrión que incluye como su dirección de destino la dirección de IP sustituta, utilizar la correspondencia para negociar una conexión de HIP entre el equipo representante para HIP y el segundo anfitrión.

21. Un equipo representante (16) para protocolo de identidad de anfitrión, HIP, para uso con el fin de garantizar una seguridad, al menos parcial, de las comunicaciones, a través del equipo representante para HIP, entre un primer anfitrión (12) que no está habilitado para HIP y un segundo anfitrión (14) que está habilitado para HIP, que comprende:

medios para recibir una petición procedente del primer anfitrión para resolver la dirección de protocolo de Internet, IP, del segundo anfitrión;

medios para recuperar, en respuesta a dicha petición, una dirección de IP y una etiqueta de identidad de anfitrión, HIT, asociadas con el segundo anfitrión, para devolver, en respuesta a dicha recuperación, una dirección de IP sustituta asociada con el segundo anfitrión, y mantener una correspondencia entre la dirección de IP sustituta, la dirección de IP recuperada y la HIT recuperada; y

medios para utilizar la correspondencia al recibirse un mensaje de iniciación de sesión procedente del primer anfitrión que incluye, como su dirección de destino, la dirección de IP sustituta, para negociar una conexión de HIP entre el equipo representante para HIP y el segundo anfitrión.

22. Un programa de ordenador que, cuando se ejecuta en un equipo representante para HIP, hace que el equipo representante lleve a la práctica un método como el reivindicado en la reivindicación 20.

23. Un programa de ordenador que, cuando se carga en un equipo representante para HIP, hace que éste incorpore todas las características de un equipo representante para HIP como se reivindica en la reivindicación 21.

24. Un programa de ordenador como se reivindica en la reivindicación 22 o la reivindicación 23, llevado en un medio portador.

25. Un programa de ordenador como se reivindica en la reivindicación 24, en el que el medio portador es un medio de transmisión.

26. Un programa de ordenador como se reivindica en la reivindicación 24, en el que el medio portador es un medio de almacenamiento.

FIG. 1

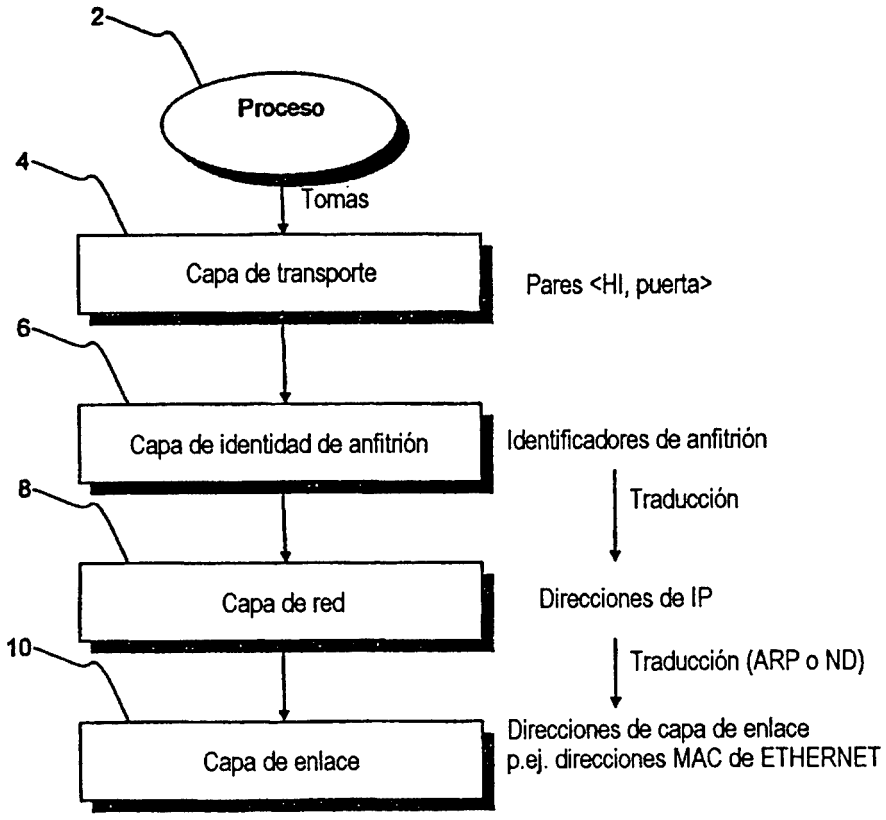

2
Proceso
4
Tomas
Capa de transporte
Pares <HI, puerta>
6
Capa de identidad de anfitrión
Identificadores de anfitrión
Traducción
8
Capa de red
Direcciones de IP
Traducción (ARP o ND)
10
Capa de enlace
Direcciones de capa de enlace
p.ej. direcciones MAC de ETHERNET

FIG. 2

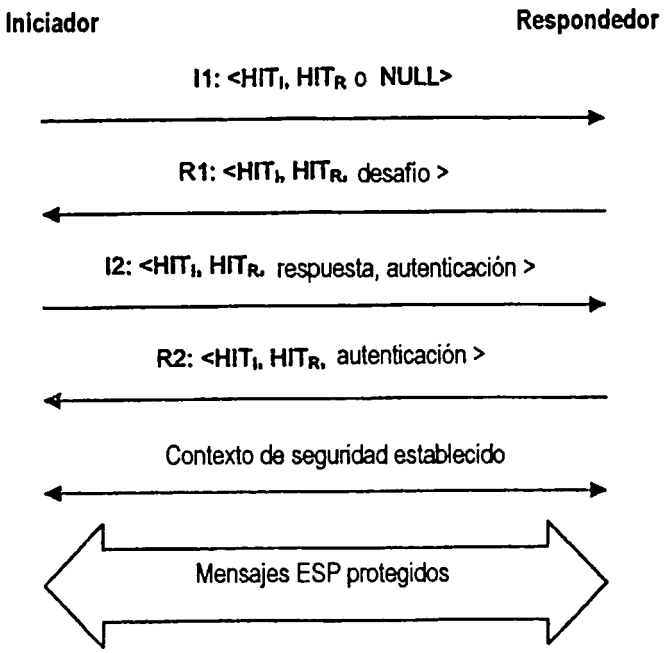

Iniciador
Respondedor
I1: <HIT$_I$, HIT$_R$ o NULL>
R1: <HIT$_I$, HIT$_R$, desafío >
I2: <HIT$_I$, HIT$_R$, respuesta, autenticación >
R2: <HIT$_I$, HIT$_R$, autenticación >
Contexto de seguridad establecido
Mensajes ESP protegidos

FIG. 3

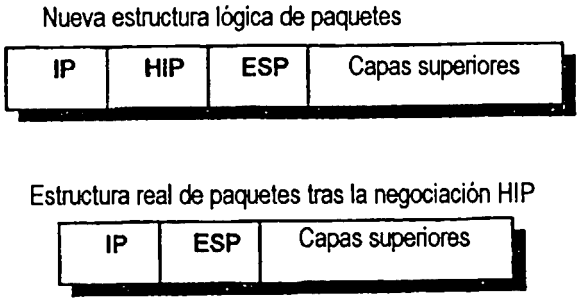

Nueva estructura lógica de paquetes
IP
HIP
ESP
Capas superiores
Estructura real de paquetes tras la negociación HIP
IP
ESP
Capas superiores

FIG. 4

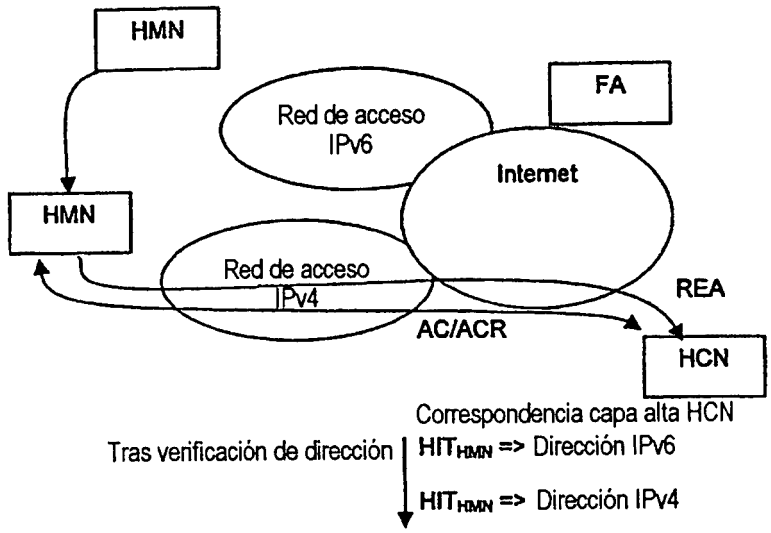

HMN
FA
Red de acceso
IPv6
Internet
HMN
Red de acceso
IPv4
REA
AC/ACR
HCN
Correspondencia capa alta HCN
Tras verificación de dirección
HIT HMN => Dirección IPv6
HIT HMN => Dirección IPv4

FIG. 5

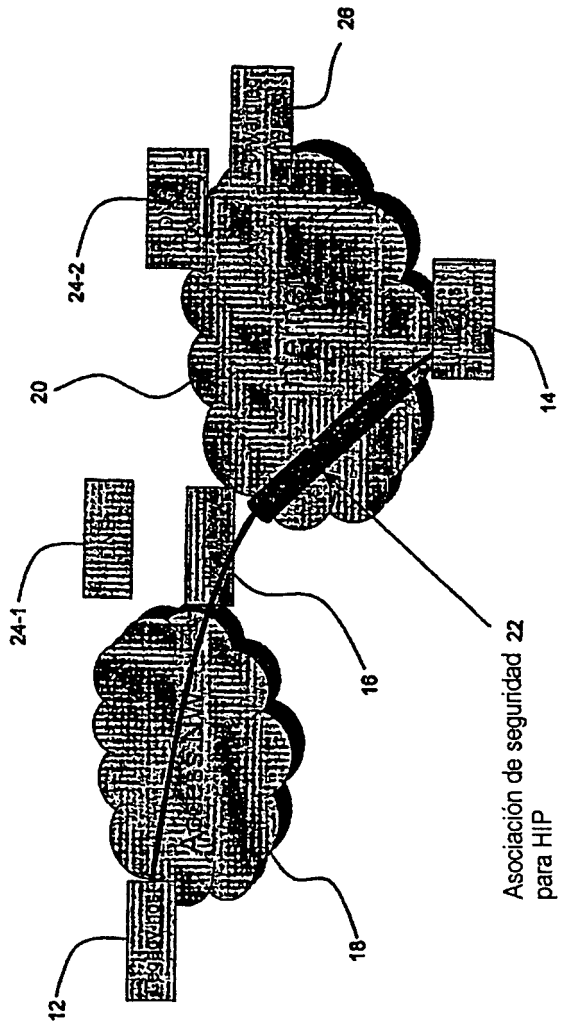


FIG. 6

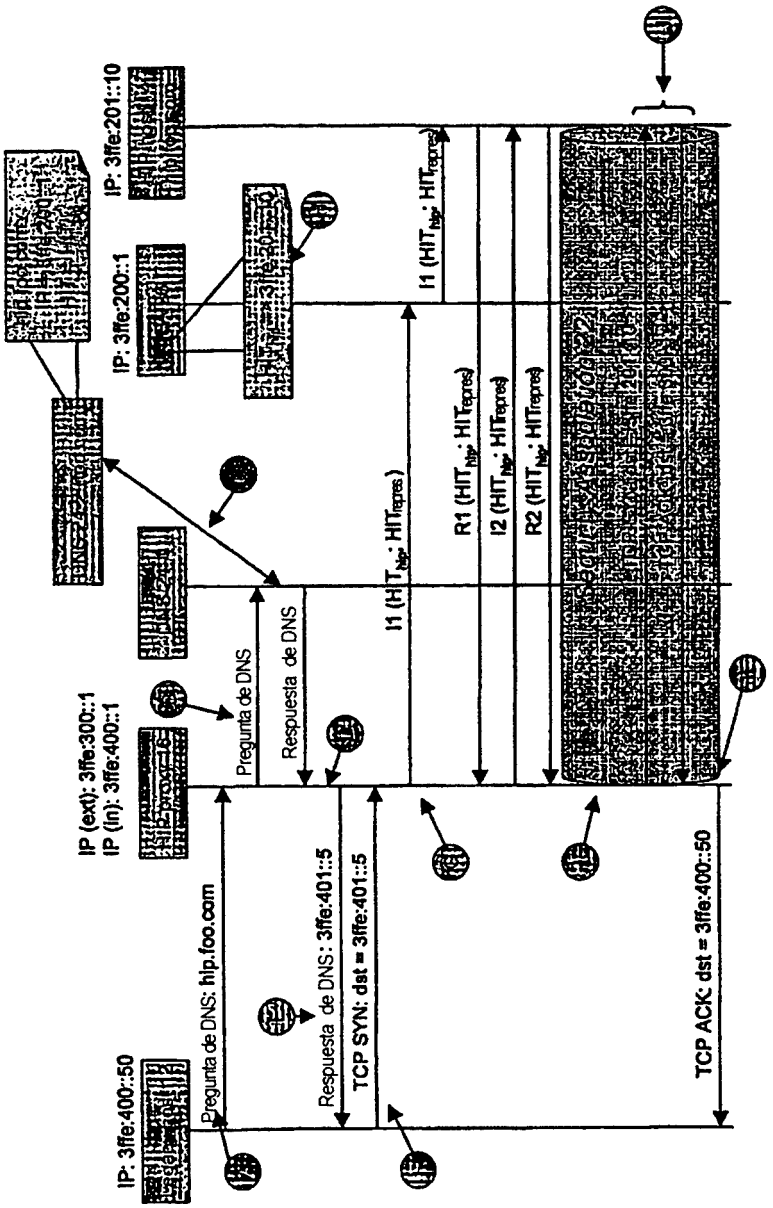
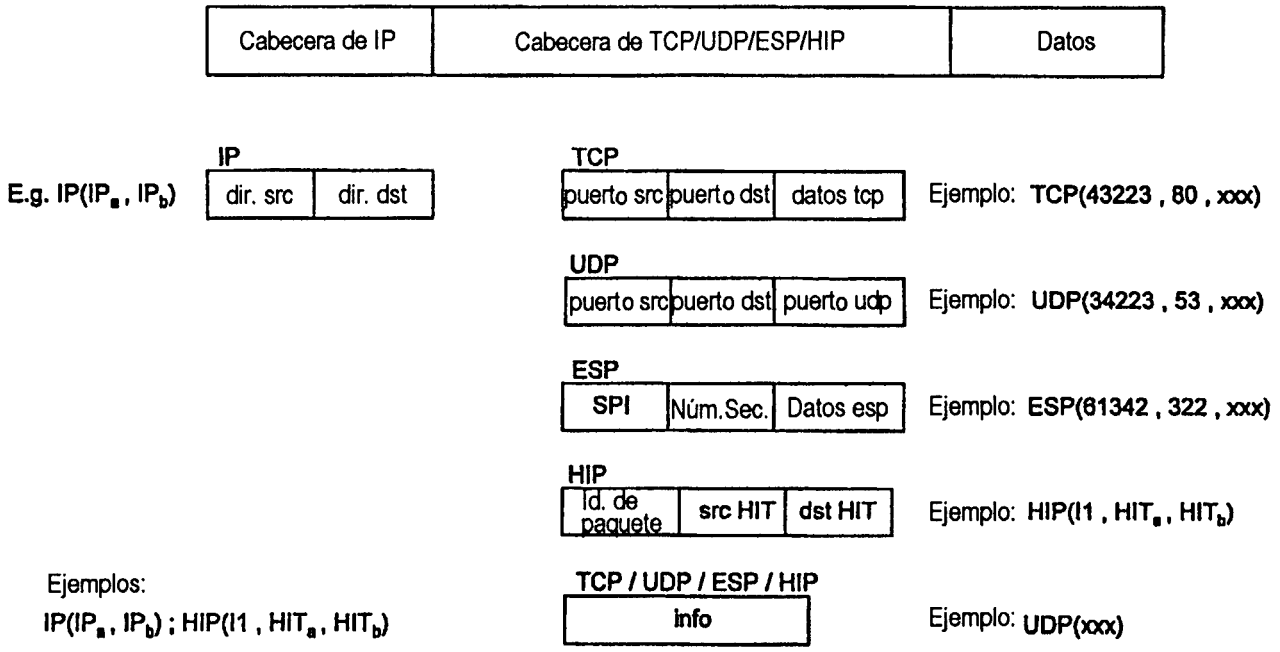

IP: 3ffe:201::10
IP: 3ffe:200::1
IP (ext): 3ffe:300::1
IP (in): 3ffe:400::1
IP: 3ffe:400::50
Pregunta de DNS
Respuesta de DNS
I1 (HIT_hip ; HIT_fepres)
R1 (HIT_hip ; HIT_fepres)
I2 (HIT_hip ; HIT_fepres)
R2 (HIT_hip ; HIT_fepres)
Pregunta de DNS: hip.foo.com
Respuesta de DNS: 3ffe:401::5
TCP SYN: dst = 3ffe:401::5
TCP ACK: dst = 3ffe:400::50

FIG. 7



ES 2 287 697 T3

FIG. 8

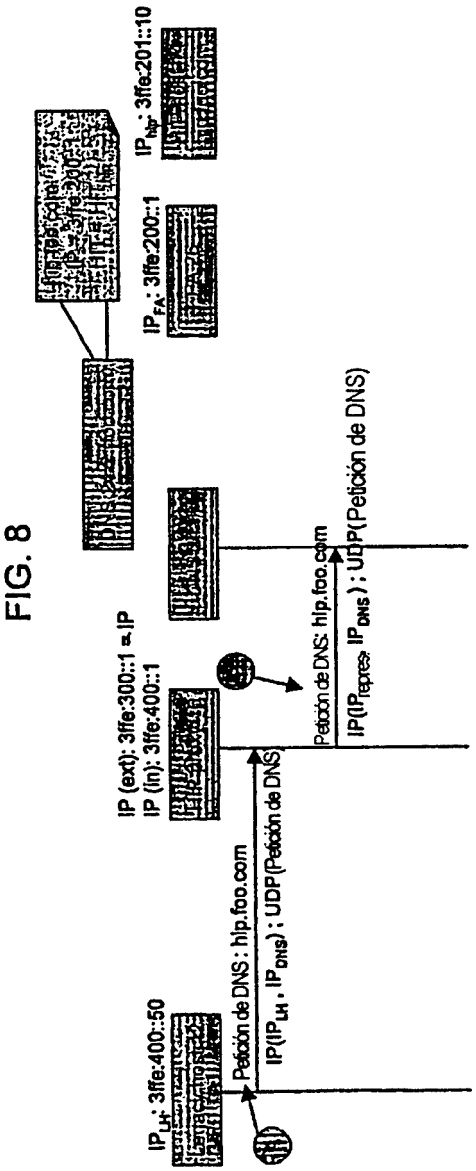

IP_LH: 3ffe:400::50
IP (ext): 3ffe:300::1 = IP
IP (in): 3ffe:400::1
IP_FA: 3ffe:200::1
IP_hip: 3ffe:201::10
Petición de DNS: hip.foo.com
IP(IP_LH, IP_DNS); UDP(Petición de DNS)
Petición de DNS: hip.foo.com
IP(IP_fapres, IP_DNS); UDP(Petición de DNS)

FIG. 9

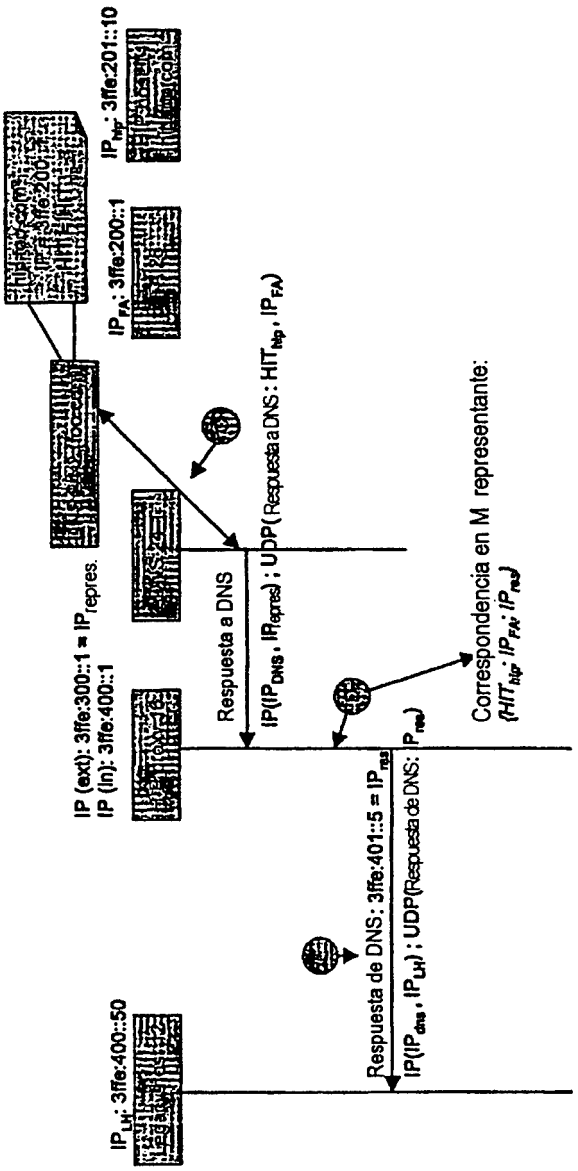

IP (ext): 3ffe:300::1 = IP repres.
IP (in): 3ffe:400::1
Respuesta a DNS
IP(IP DNS , IRepres) ; UDP(Respuesta a DNS : HIT hip , IP FA)
Correspondencia en M representante:
(HIT hip ; IP FA ; IP nat)
Respuesta de DNS: 3ffe:401::5 = IP nat
IP(IP dns , IP LH) ; UDP(Respuesta de DNS: IP nat)
IP LH: 3ffe:400::50
IP FA: 3ffe:200::1
IP hip: 3ffe:201::10

FIG. 10

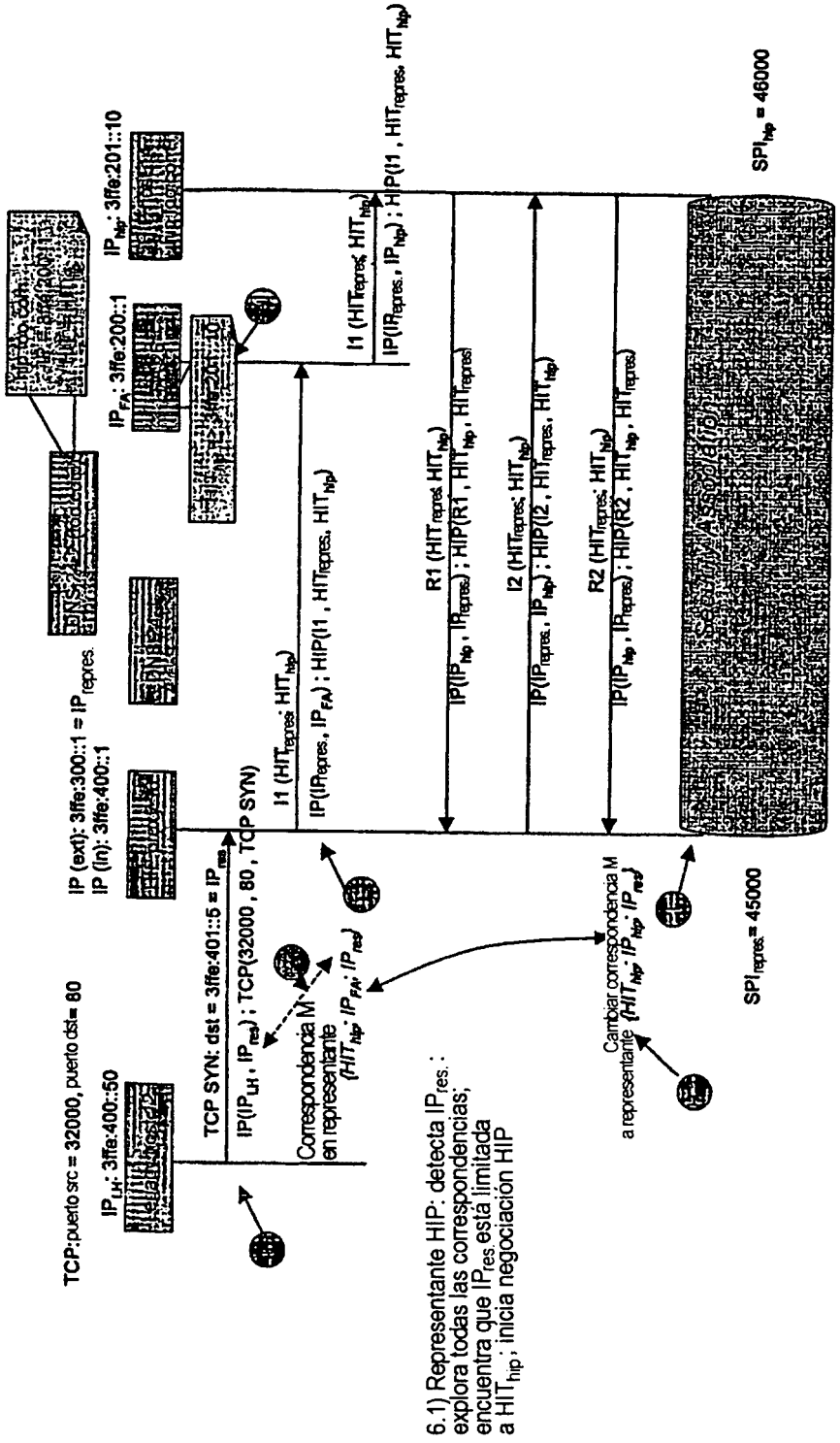

TCP:puerto src = 32000, puerto dst= 80
IP_LH: 3ffe:400::50
IP (ext): 3ffe:300::1 = IP_repres.
IP (in): 3ffe:400::1
IP_hip: 3ffe:201::10
IP_FA: 3ffe:200::1
TCP SYN: dst = 3ffe:401::5 = IP_hip
IP(IP_LH , IP_res) ; TCP(32000 , 80 , TCP SYN)
I1 (HIT_repres; HIT_hip)
IP(IP_repres , IP_FA) ; HIP(I1 , HIT_repres, HIT_hip)
I1 (HIT_repres; HIT_hip)
IP(IP_repres , IP_hip) ; HIP(I1 , HIT_repres, HIT_hip)
R1 (HIT_repres; HIT_hip)
IP(IP_hip , IP_repres) ; HIP(R1 , HIT_hip , HIT_repres)
I2 (HIT_repres; HIT_hip)
IP(IP_repres , IP_hip) ; HIP(I2 , HIT_repres, HIT_hip)
R2 (HIT_repres; HIT_hip)
IP(IP_hip , IP_repres) ; HIP(R2 , HIT_hip , HIT_repres)
Correspondencia M en representante (HIT_hip ; IP_FA ; IP_res)
Cambiar correspondencia M a representante (HIT_hip ; IP_hip ; IP_res)
SPI_repres = 45000
SPI_hip = 46000
6.1) Representante HIP: detecta IP_res. : explora todas las correspondencias; encuentra que IP_res. está limitada a HIT_hip ; inicia negociación HIP

FIG. 11

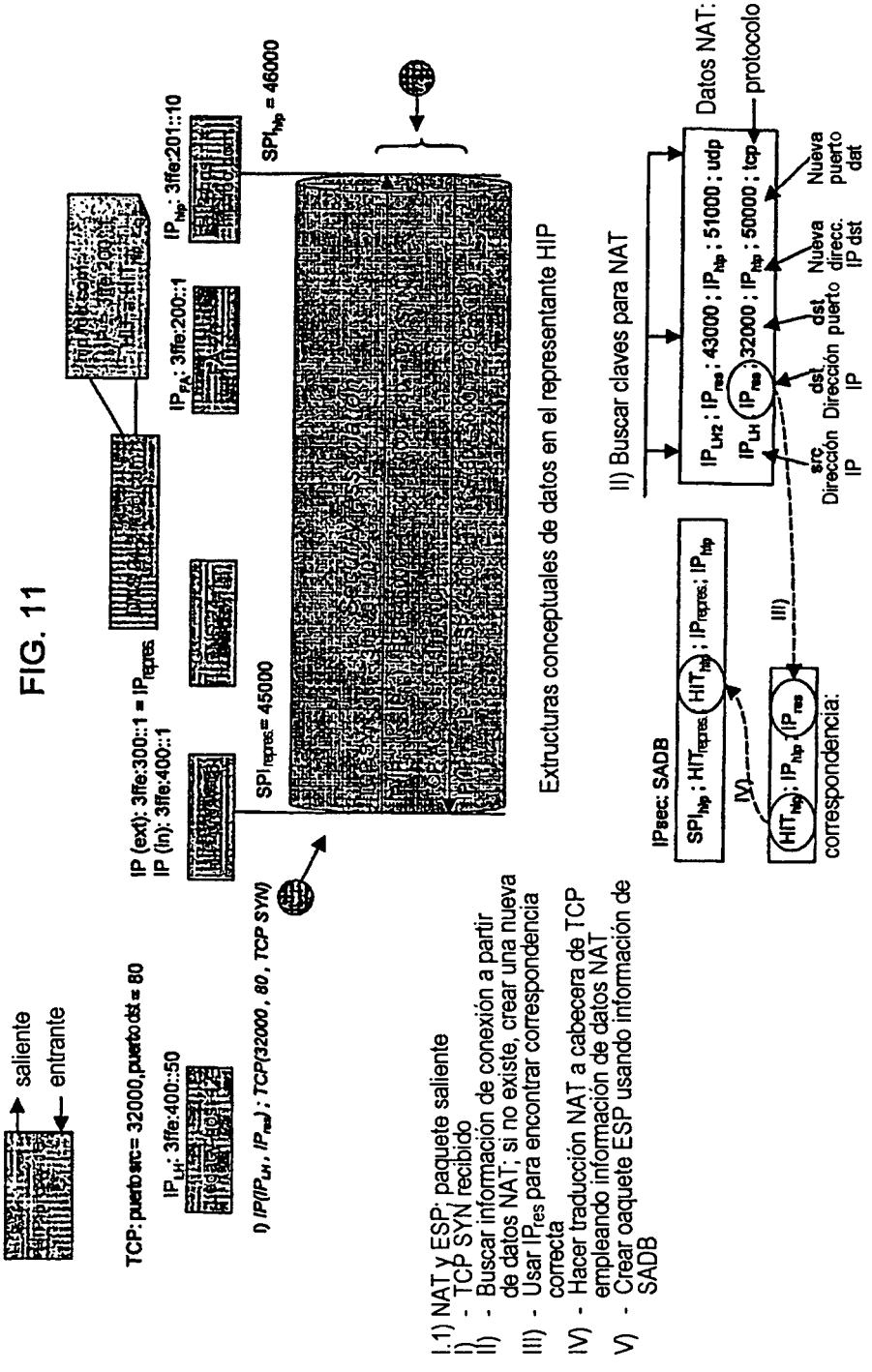
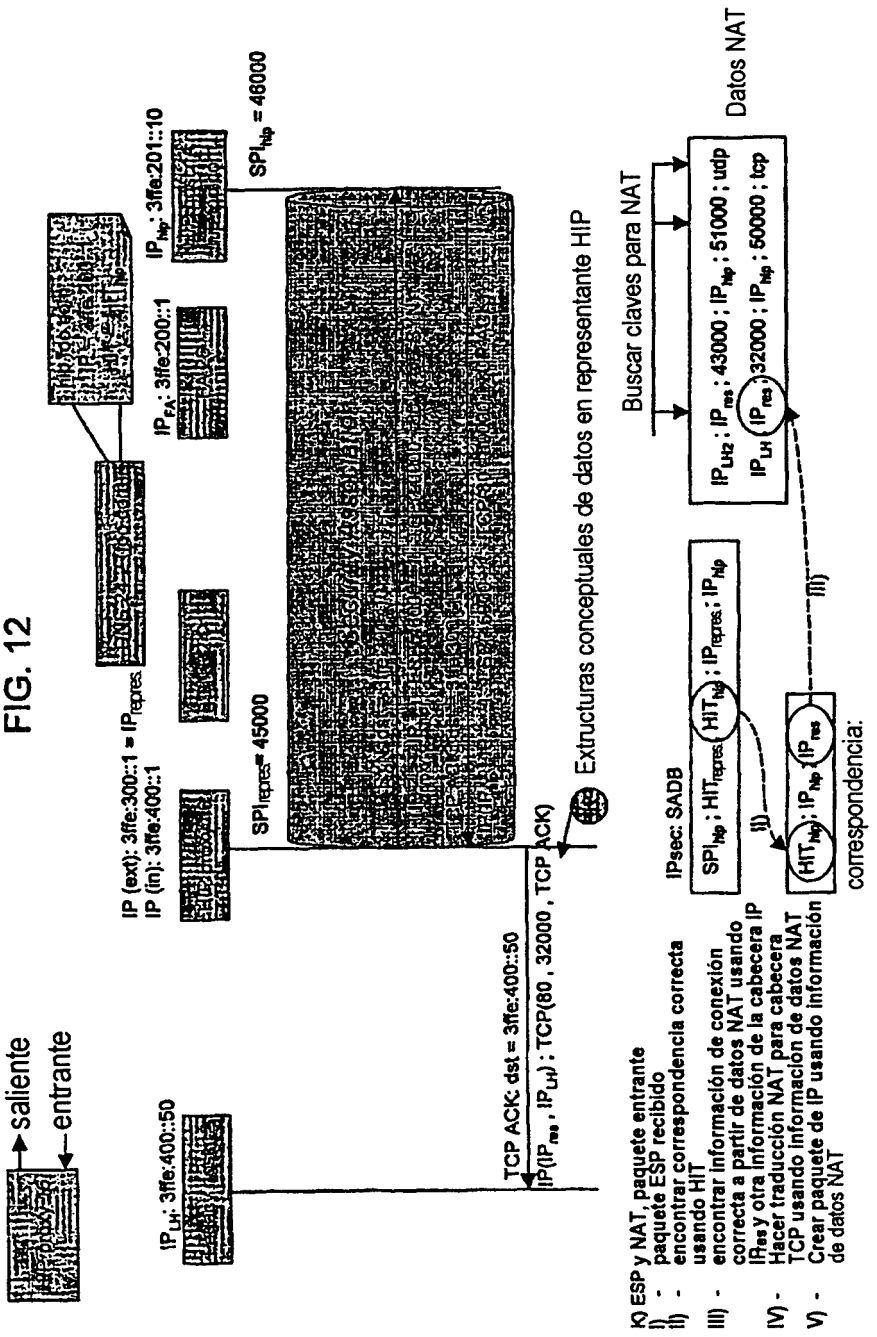

saliente
entrante
TCP: puerto src= 32000,puerto dst = 80
IP_LH: 3ffe:400::50
IP (ext): 3ffe:300::1 = IP_repres
IP (in): 3ffe:400::1
IP_PA: 3ffe:200::1
IP_hip: 3ffe:201::10
SPI_repres= 45000
SPI_hip = 46000
I) IP(IP_LH, IP_res) ; TCP(32000 , 80 , TCP SYN)
Extructuras conceptuales de datos en el representante HIP
I.1) NAT y ESP: paquete saliente
I) - TCP SYN recibido
II) - Buscar información de conexión a partir de datos NAT; si no existe, crear una nueva
III) - Usar IP_res para encontrar correspondencia correcta
IV) - Hacer traducción NAT a cabecera de TCP empleando información de datos NAT
V) - Crear oaquete ESP usando información de SADB
II) Buscar claves para NAT
IPsec: SADB
SPI_hip ; HIT_repres ; HIT_hip ; IP_repres ; IP_hip
IV)
III)
(HIT_hip) ; IP_hip ; (IP_res)
correspondencia:
Datos NAT:
protocolo
IP_LH2 ; IP_res : 43000 ; IP_hip : 51000 ; udp
IP_LH (IP_res) :32000 ; IP_hip : 50000 ; tcp
src Dirección IP
dst Dirección IP
dst puerto
Nueva direcc. IP dst
Nueva puerto dst

FIG. 12


saliente
entrante
IP (ext): 3ffe:300::1 = IP repres
IP (in): 3ffe:400::1
IP LH: 3ffe:400::50
IP FA: 3ffe:200::1
IP hip: 3ffe:201::10
SPI repres = 45000
SPI hip = 46000
TCP ACK: dst = 3ffe:400::50
IP(IP ms , IP LH) ; TCP(80 , 32000 , TCP ACK)
Extructuras conceptuales de datos en representante HIP
Buscar claves para NAT
IPsec: SADB
SPI hip ; HIT repres (HIT hip) ; IP repres ; IP hip
IP LH2 ; IP ms ; 43000 ; IP hip ; 51000 ; udp
IP LH (IP ms) ; 32000 ; IP hip ; 50000 ; tcp
Datos NAT
(HIT hip) ; IP hip (IP ms)
correspondencia:
IV) ESP y NAT, paquete entrante
I) - paquete ESP recibido
II) - encontrar correspondencia correcta usando HIT
III) - encontrar información de conexión correcta a partir de datos NAT usando IPms y otra información de la cabecera IP
IV) - Hacer traducción NAT para cabecera TCP usando información de datos NAT
V) - Crear paquete de IP usando información de datos NAT
II)
III)