(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 596 528**

(51) Int. CI.:

***H04L 29/12*** (2006.01)
***H04L 29/06*** (2006.01)
***H04M 7/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.11.2004 PCT/IB2004/003850**

(87) Fecha y número de publicación internacional: **09.06.2005 WO05053275**

(96) Fecha de presentación y número de la solicitud europea: **24.11.2004 E 04798959 (5)**

(97) Fecha y número de publicación de la concesión europea: **10.08.2016 EP 1687958**

(54) Título: **Método y sistema para el filtrado de tráfico multimedia basados en enlaces de direcciones IP**

(30) Prioridad:

**25.11.2003 US 524640 P**
**13.04.2004 US 822874**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**10.01.2017**

(73) Titular/es:

**NOKIA TECHNOLOGIES OY (100.0%)**
**Karaportti 3**
**02610 Espoo, FI**

(72) Inventor/es:

**LE, FRANK y**
**FACCIN, STEFANO**

(74) Agente/Representante:

**VALLEJO LÓPEZ, Juan Pedro**

## DESCRIPCIÓN

Método y sistema para el filtrado de tráfico multimedia basados en enlaces de direcciones IP

La presente invención se refiere a la filtración de los flujos dinámicos, y más particularmente, a un nodo de filtrado, un nodo de anclaje utilizado en relación con el filtrado, un método para configurar dicho nodo de anclado, y un método correspondiente de comunicación de datos.

Recientemente, las redes de comunicación se han extendido ampliamente y se utilizan en la vida diaria de muchos usuarios. Entre dichas redes de comunicación, las denominadas redes de comunicación de conmutación de paquetes encuentran cada vez más atención. Las redes de conmutación de paquetes transmiten/reciben datos en unidades de paquetes. Un paquete consiste en una cabecera que lleva información de control tal como (entre otros), por ejemplo, una información de dirección de paquete (origen/destino), así como de una sección de carga útil transporta datos reales tales como la voz o similares.

Existen diversos protocolos para dicha comunicación de conmutación de paquetes. Para el propósito de la presente invención, sin embargo, como un ejemplo de tales protocolos, se describen el IPv4 y/o IPv6 (que son versiones IP Protocolo de Internet bien conocido). A pesar de esto, otros protocolos de conmutación de paquetes son utilizables en conexión con la presente invención. También los protocolos de no conmutación de paquetes se pueden utilizar en conexión con la presente invención, siempre y cuando la fuente/destino sean identificables por medio de direcciones.

Las redes de comunicación que normalmente forman parte de un sistema de red de comunicación donde las redes de una pluralidad de operadores cooperan entre sí. Además, una red individual puede consistir en una pluralidad de los llamados dominios de una red con la red, como tal, siendo operada por un operador de red, pero los dominios siendo, por ejemplo, controlados por una tercera parte respectiva (diferente al operador de red), siendo operados en un protocolo diferente, o teniendo una definición de espacio de direcciones diferente, o similares. Así, para el propósito de la presente invención, cuando se refiere a las redes de comunicación, no se distingue entre diferentes redes o dominios diferentes, pero las redes de comunicación pretenden cubrir todas las alternativas posibles de la constitución de la red que se describió anteriormente. Más bien, una red de comunicación puede ser considerada como un sistema de red de comunicación.

En relación con dichas redes de comunicación o sistemas de red, respectivamente, los problemas de seguridad se hacen más y más importantes.

Normalmente, se establece/está en curso una comunicación entre dos terminales. Un terminal de origen de comunicación se conoce como primer terminal o equipo de usuario UE, y un terminal de destino de comunicación se conoce como nodo correspondiente CN o segundo terminal. Por supuesto, en una comunicación bidireccional, el nodo correspondiente CN también actúa como un equipo de usuario UE cuando se responde al terminal de origen. Técnicamente, no es necesario que haya ninguna diferencia entre los terminales, pero, sin embargo, los terminales pueden ser diferentes desde un punto de vista técnico. Cualquier diferencia, sin embargo, no importa siempre que los terminales estén adaptados para comunicarse entre sí por medio de la red de comunicación intermedia.

En el caso en que una comunicación es o ha sido establecida entre dos terminales, la comunicación es identificada por las direcciones de origen y destino de los terminales. También, ya que la comunicación puede implicar diferentes contenidos o tipos de tráfico que se intercambiarán entre los terminales tales como el tráfico en tiempo real y el tráfico no en tiempo real, un tráfico respectivo está asociado a un puerto respectivo. Así, un puerto o número de puerto representa un refinamiento de la información de la dirección utilizada en la comunicación.

Las direcciones no utilizadas o incluso números de puerto, sin embargo, constituyen una posibilidad para los atacantes para establecer una comunicación fraudulenta o de mal comportamiento al terminal de un usuario que en realidad no desea tener dicha comunicación.

Por lo tanto, los problemas de seguridad en las redes de comunicación se vuelven más y más importantes. Los llamados cortafuegos FW juegan un papel importante para garantizar la seguridad en las redes de comunicación. Un cortafuego por lo tanto puede ser considerado como un nodo de filtrado en una red de comunicación que filtra el tráfico desautorizado y evita que este tipo de tráfico llegue a un terminal que no autoriza que se reciba este tipo de tráfico.

Esta invención se refiere a este tipo de problemas de seguridad y nodos de filtrado o cortafuegos, respectivamente. Se refiere más particularmente a la configuración dinámica de orificios en los cortafuegos y para el soporte de servicios en tiempo real en la comunicación. La expresión "orificio" tal como se utiliza en la presente invención se refiere a un permiso temporal válido para un tráfico específico para llegar a un terminal específico, dicho el permiso se concede o se rechaza por el cortafuego. Así, un orificio abierto representa el permiso concedido, mientras que un orificio cerrado representa el permiso rechazado.

En muchos marcos de las redes de comunicación, existe la necesidad de abrir y cerrar de forma dinámica los orificios de los cortafuegos. Por ejemplo, las comunicaciones SIP (protocolo de iniciación de sesión) establecidas requieren orificios que se crean de forma dinámica para el flujo de medios (es decir, UDP/RTP para servicios en tiempo real (protocolo de datagrama de usuario, protocolo de tiempo real), TCP (protocolo de control de transmisión) para la mensajería instantánea) para pasar a través del cortafuego y para los paquetes de datos que se intercambian entre los nodos de comunicación (terminal de origen y terminal de nodo correspondiente). Estos orificios se deben quitar (es decir, cerrar) a la terminación de la comunicación para evitar posibles ataques.

A continuación, la arquitectura y, más particularmente, las entidades de la red, así como las interfaces que han sido introducidas y adoptadas en las redes 3GPP (proyecto de participación de tercera generación) para la interoperabilidad de dominios IPv6 con IPv4 se describen brevemente con referencia a la figura 1. Esto demuestra que la presente invención como se describe en las siguientes secciones no introduce nuevas entidades, pero se reutiliza una arquitectura de red de comunicación existente y el marco así adoptado de una manera innovadora.

La arquitectura como se ilustra en la figura 1 ha sido recientemente aprobada en 3GPP para el interfuncionamiento de dominios IPv6 e IPv4. Sin embargo, esta descripción sirve como solo un ejemplo y la presente invención no se limita a los dominios IPv4/IPv6, pero se destina a cubrir también situaciones en las redes dentro de un único dominio. Además, la funcionalidad de las entidades e interfaces que se han introducido se describen brevemente.

Las secciones posteriores a continuación, explican cómo la presente invención reutiliza la infraestructura actualmente existente de una forma innovadora para resolver el problema transversal del cortafuego.

Ahora bien, como es derivable a partir de la figura 1:

La arquitectura de interfuncionamiento actual se basa en un traductor de portal: El TrGW es un portal de enlace que convierte las cabeceras IP como necesaria, más en general, convierte o traduce la información de dirección incluida en los paquetes a transmitir.

La arquitectura de interconexión actual también se basa en un IMS (Subsistema Multimedia IP) portal de capa de aplicación (ALG): la funcionalidad del IMS ALG es proporcionar la función de aplicación necesaria para pila de protocolos SIP/SDP con el fin de establecer la comunicación entre aplicaciones SIP IPv6 e IPv4 (protocolo de iniciación de sesión/protocolo de descripción de sesión).

El IMS ALG recibe un mensaje SIP entrante de nodos CSCF (función de control del estado de la llamada, se han definido una S-CSCF, CSCF de servicio y una I-CSCF, CSCF de interrogación) o desde un dominio de red IPv4 SIP (de CSCF como un (proxy) P-CSCF, S-CSCF, o I-CSCF también se conocen como servidor SIP en esta aplicación). Este dominio puede ser un dominio externo, pero también puede ser un dominio interno de la red de comunicación. El IMS ALG a continuación, cambia los parámetros SDP/SIP apropiados, traduciendo las direcciones IPv6 a direcciones IPv4 y viceversa. Ténganse en cuenta que, para la presente invención, los protocolos IPv4/IPv6 solo son ejemplos y otras transiciones de protocolo son concebibles.

El IMS ALG modifica los cuerpos de los mensajes SIP y los encabezados que incluyen la dirección IP. El IMS ALG solicitará la NA (P) T-PT (dirección de red (y puerto) de traducción-protocolo de traducción) para proporcionar los datos de enlace entre las diferentes direcciones IP (IPv6 a IPv4 y viceversa) al iniciar sesión, y dará a conocer los enlaces en la liberación de sesiones. La NA (P) T-PT es, pues, una especie de traductor de estado y mantiene una tabla de asignación de IPv6/IPv4.

También se ha introducido y adoptado una interfaz de Ix entre el TrGW y el IMS ALG. Dicha interfaz permitirá:

Que el IMS ALG solicite a la NA (P) T-PT proporcionar los datos de un enlace entre las diferentes direcciones IP (IPv6 a IPv4 y viceversa) al iniciar la sesión,
el TrGW para proporcionar los datos de enlace al IMS ALG, y
el IMS ALG para liberar los enlaces en la liberación de la sesión.

Por otra parte, la figura 1 representa un equipo de usuario operativo UE basado en IPv6 (que se comunica con un nodo correspondiente (no mostrado) CN operado basado en IPv4. Además, se ilustra un Proxy-CSCF (P-CSCF) que recibe un "primer salto" de información de señalización desde el equipo de usuario UE al iniciar una comunicación o de sesión. Las I-CSCF y S-CSCF pueden considerarse como un denominado CPS del servidor de procesamiento de llamadas que representa un ejemplo de un nodo de gestión de la comunicación. Además, un DNS de servidor de nombres de dominio y un servidor de abonado doméstico HSS forman parte de la arquitectura. Las entidades anteriormente descritas están principalmente involucradas en la gestión de señalización y comunicación como se indica por la línea de puntos que indica el tráfico de señalización, mientras que la carga útil de datos se transmite desde el equipo de usuario UE a través de la IP-CAN (red de acceso de conectividad IP) a través de la puerta de enlace de traductor TrGW hacia el interlocutor de comunicación, es decir, el nodo correspondiente (no mostrado), como se indica por la línea en negrita denotado como "portador" en la figura 1.

Como se considera que los expertos en la materia están familiarizados con la arquitectura general y las entidades/nodos con las funciones individuales de los mismos, se omite aquí una descripción adicional detallada.

Los cortafuegos filtran paquetes IP según las reglas de filtrado, por lo general teniendo en cuenta las direcciones IP de origen y destino, el tipo de protocolo y/o los números de puerto. Con el fin de evitar los ataques, los cortafuegos están configurados con las reglas de filtrado. Dichas normas incluyen reglas estáticas (por ejemplo, para detener las inundaciones de TCP o protocolos específicos) y las reglas dinámicas (orificios). Varias aplicaciones requieren una configuración dinámica del orificio en el cortafuego. A modo de ejemplo, las comunicaciones SIP requieren la creación/eliminación dinámica (es decir, apertura/cierre) de los orificios en el cortafuego para que el flujo de medios pase el cortafuego, mientras que bloquea los ataques (inundaciones UDP, etc.). Más en general, aplicaciones basadas en UDP (protocolo de datagrama de usuario) requieren orificios dinámicos para abrir/cerrar cuando la comunicación se inicia/se detiene. Ténganse en cuenta que la descripción de SIP sirve como solo un ejemplo y que otros protocolos también se puede usar en conexión con la presente invención, tal como por ejemplo WAP (protocolo de aplicación inalámbrica), o similares.

Hasta ahora, se han propuesto varias soluciones para el control del orificio dinámico en los cortafuegos, que se explican brevemente a continuación:

1. El uso de paquetes UDP falsos:

Según este enfoque, el equipo de usuario UE envía un paquete UDP simulado y el cortafuego FW abre el orificio sobre la base de tales paquetes. Sin embargo, no hay manera para que el cortafuegos FW determine cuando los orificios deben ser cerrados (ya que la comunicación UDP no tiene un establecimiento/desmontaje de sesión al igual que TCP). Por otra parte, el equipo de usuario UE puede enviar paquetes UDP ficticios para crear el orificio en el cortafuegos FW y mantendrá el envío de dichos paquetes UDP ficticios por una transmisión periódica de dichos paquetes. Dicho método, sin embargo, presenta dos problemas principales: (1) el equipo de usuario UE no tiene ningún conocimiento acerca de los temporizadores del estado creada en el cortafuego FW y (2) esto puede resultar en un alto número de bytes que se envían a través del enlace inalámbrico, desperdiciando así recursos.

2. El uso de un cortafuego FW que es consciente de, por ejemplo, SIP:

Un FW consciente del SIP que analizará la señalización SIP y abrirá/cerrará los orificios según se requiera. Esto, sin embargo, requiere que la señalización de SIP sea visible en el cortafuego, mientras que, sin embargo, la compresión SIP puede ser aplicada (por ejemplo, en 3GPP y 3GPP2 IMS) y el cortafuego FW puede no ser capaz de descomprimirlo. Además, esta solución da demasiado control al cortafuego FW, y el operador de red pierde el control al menos en parte (mientras que, por lo general, es preferible mantener el control en los propios productos y/o redes). Por último, esta solución no se puede aplicar cuando se aplica IPsec (seguridad de protocolo de internet (IP)) o TLS cifrado (seguridad de capa de transporte) para proteger el SIP.

3. El uso de una interfaz entre el cortafuegos FW y el servidor de aplicaciones (por ejemplo, servidor SIP en IMS):

A pesar de tales interfaces están siendo definidas (por ejemplo, MIDCOM en IETF (MIDCOM: Comunicación de caja intermedia, tal como bajo la definición del IETF, grupo de acción de ingeniería de Internet), que todavía están en una etapa de especificación temprana, el trabajo de estandarización puede requerir algún tiempo y su disponibilidad en los productos está muy lejos, mientras que los sistemas (por ejemplo, IMS) deben desplegarse antes de que el cortafuego FW soportará dichas interfaces. Por otra parte, si bien esta solución permite que el control esté en los productos del fabricante (por ejemplo, servidor SIP), el despliegue no es totalmente independiente de los productos de otras compañías.

4. Un protocolo de señalización desde el terminal UE al FW para llevar a cabo la configuración del FW:

El protocolo TIST (topología insensible transversal de servicio), el protocolo de CASP (protocolo de señalización de aplicación de cruz) y otras contribuciones sugiriendo un protocolo de señalización de la apertura y el cierre del terminal de los orificios necesarios en los cortafuegos en la red. Estos métodos son, sin embargo, borradores individuales y se necesitará mucho tiempo antes de que estas soluciones se conviertan en estandarizadas.

El documento "Middlebox communication architecture and framework", RFC 3303, de agosto de 2002 por Srisuresh et al. describe una arquitectura y el marco de comunicación middlebox. Específicamente, se da a conocer el marco subyacente de las comunicaciones de caja intermedia (MIDCOM) para habilitar aplicaciones complejas a través de un tercero. Hay varios dispositivos intermedios hoy en el Internet que requieren inteligencia de aplicaciones para su funcionamiento. Datagramas pertenecientes a las aplicaciones de transmisión en tiempo real, tales como SIP y H.323 y aplicaciones de igual a igual, como Napster y NetMeeting, no pueden ser identificadas por el mero examen de las cabeceras de paquetes. Cajas intermedias que implementan servicios de cortafuegos y de traductor de

direcciones de red normalmente incrustan inteligencia de las aplicaciones en el dispositivo para su funcionamiento. El documento especifica una arquitectura y un marco en los que terceros de confianza pueden ser delegados para asistir a los dispositivos intermedios para llevar a cabo su operación, sin recurrir a la incorporación de inteligencia de las aplicaciones. Hacer esto permitirá que una caja intermedia siga proporcionando los servicios, manteniendo mientras tanto la aplicación de caja intermedia agnóstica.

Por otra parte, el documento "IPv6-IPv4 Translators in 3GPP Networks", del 17 de junio de 2003 (2003-06-17) El Malki por K et al. da a conocer traductores IPv6-IPv4 en las redes 3GPP. En concreto, se ha debatido sobre las listas de correo v6ops en las reuniones del IETF sobre la idoneidad de los traductores (por ejemplo, NAT-PT) como mecanismos de transición de IPv4 a IPv6. A menudo se ha afirmado que el NAT-PT no es un mecanismo que se recomiende en general para resolver el problema de la transición IPv6-IPv4 y se han propuesto algunas modificaciones al NAT-PT. Sin embargo, también ha habido discusiones con respecto a escenarios especiales donde algunas formas de traductores podrían desplegarse si su uso está documentado apropiadamente. El objetivo de este proyecto es documentar la justificación del uso de traductores en las redes 3GPP, en particular para IPv6 solo IMS (Subsistema Multimedia IP) y describir las posibles soluciones al problema y las interacciones con SIP.

Por lo tanto, es un objetivo de la presente invención proporcionar una solución alternativa para los problemas asociados con orificios dinámicos, cuya solución permite una implementación a corto plazo y que esté libre de los inconvenientes asociados con las propuestas anteriormente expuestas.

Según la presente invención, este objeto se consigue por lo que se expone en las reivindicaciones independientes adjuntas. Modificaciones ventajosas se definen en las reivindicaciones dependientes adjuntas.

De este modo, se define un método para filtrar las comunicaciones IP de forma segura a través de un cortafuego en escenarios en los que los orificios dinámicos normalmente necesitan ser creados para garantizar un nivel adecuado de seguridad (por ejemplo, flujos UDP en las comunicaciones SIP). Esto se basa en la idea de crear un anclaje seguro y autorizado para las comunicaciones, donde todas las comunicaciones se dirigen antes de que un cortafuego realice el filtrado de paquetes.

Según ello, al menos se consiguen las siguientes ventajas aplicando la presente invención:

1. Esta invención, al menos, no requiere una interfaz de configuración de FW específica (desde un terminal al cortafuego), y también no requiere un ALG en un FW);
2. La presente invención se apoya firmemente las comunicaciones establecidas SIP (los usuarios están protegidos contra las amenazas IP comunes tales como el conocido "inundación TCP SYN", "desgarro", etc.);
3. La presente invención no tiene que ser estandarizada, por lo que la implementación de la misma es más rápida que con las soluciones a estandarizar;
4. Esta invención no requiere modificación sustancial de una implementación actual CPS (S-CSCF/I-CSCF), o a una implementación de servidor proxy SIP en el caso de que se adopte una solución de este tipo;
5. La presente invención no requiere ninguna modificación/actualización de la infraestructura actual (terminales, IMS (subsistema multimedia IP), etc.);
6. La presente invención tiene las ventajas adicionales de que no depende de ningún tercero externo ni foros de estandarización, y puede por lo tanto ser completamente desarrollada por un solo fabricante.

Como resultado de esta invención, todo el tráfico de datos pasa a través del nodo de anclaje como, por ejemplo, el traductor de puerta de enlace TrGW, pero esto no debería ser un problema, ya que todos los datos de todas formas también tienen que pasar a través del cortafuego. (Más bien, el TrGW podría estar configurado para ser físicamente ubicado cerca o dentro del cortafuego o viceversa).

De este modo, como se indicó anteriormente, la presente invención define un método para filtrar las comunicaciones, tales como las comunicaciones basadas en IP a través de cortafuegos en escenarios en los poros dinámicos necesitan ser creado para garantizar un nivel adecuado de seguridad (por ejemplo, UDP arroyos en las comunicaciones SIP). La invención se basa en la idea de crear un anclaje seguro y autorizado para las comunicaciones, donde todas las comunicaciones se dirigen antes de que un cortafuego realice el filtrado de paquetes. La invención no introduce nuevas entidades, sino que reutiliza un marco existente. La invención se basa en el TrGW (traductor de puerta de enlace), que es la funcionalidad para cambiar las direcciones IP en la cabecera IP según la tabla de asignación de IP almacenada y una interfaz entre el CPS (o un proxy SIP) y el TrGW.

Esta interfaz permitirá: al CPS solicitar el TrGW para proporcionar datos de un enlace entre las direcciones IP al iniciar la sesión, el TrGW para proporcionar los datos de un enlace al CPS y el CPS para liberar las fijaciones en el lanzamiento de sesión. El FW será uno susceptible de estado y, en la interfaz externa, únicamente aceptará los paquetes recibidos cuya dirección IP pertenece al conjunto de direcciones del TrGW. Así, cualquier paquete entrante que no corresponde a una llamada o sesión existente se caerá en el TrGW (impidiendo cualquier intento de inundación), y paquete válido irá a través del FW, el cual verificará que el paquete no es un mensaje incorrecto u otro ataque (por ejemplo, inundación TCP SYN, etc.)

Las ventajas anteriores y otras se harán más evidentes tras la referencia a la siguiente descripción en relación con los dibujos adjuntos en los que:

La figura 1 ilustra la arquitectura conocida adoptada en 3GPP para el interfuncionamiento de IPv6 con redes IPv4;

La figura 2 ilustra la invención propuesta en este documento en relación con la configuración de un nodo de anclaje;

La figura 3 describe el enrutamiento de paquetes IP cuando se aplica la invención propuesta en este documento en relación con la comunicación de los datos;

La figura 4 describe un método alternativo específico de implementación de la invención en relación con la configuración de un nodo de anclaje;

La figura 5 ilustra un nodo de anclaje en relación con la configuración del nodo de anclaje según la presente invención;

La figura 6 ilustra un nodo de anclaje en relación con la comunicación de datos según la presente invención;

La figura 7 ilustra un nodo de filtrado en relación con la comunicación de datos según la presente invención; y

La figura 8 ilustra una señalización en relación con la terminación de una sesión de comunicación.

La presente invención se describirá ahora en detalle con referencia a los dibujos adjuntos.

Para los fines de la ilustración de esta invención, se describe una llamada SIP con flujos en tiempo real. Sin embargo, el método descrito en este documento no se limita a los escenarios en los que se utiliza SIP (por ejemplo, 3GPP IMS) sino que también se puede aplicar, por ejemplo, en escenarios de WAP. Generalmente, también se puede aplicar en cualquier otro ambiente de trabajo donde necesitan ser creados orificios dinámicos pero las interfaces de configuración del cortafuego no están presentes.

Se reconocerá que la invención hace uso de un nodo de anclaje como un traductor de puerta de enlace (TrGW). La funcionalidad del nodo de anclaje es cambiar las direcciones como las direcciones IP en la cabecera IP según la tabla de asignación de IP almacenada; su funcionamiento es similar al de un traductor de direcciones de red NAT. Además, se verá que la invención hace uso de una interfaz entre el CPS (o un proxy SIP) y el TrGW. Esta interfaz permitirá: al CPS (o proxy SIP) solicitar el TrGW para proporcionar datos de un enlace entre las direcciones IP (véase más explicación más abajo) al iniciar la sesión, al TrGW proporcionar los datos de un enlace al CPS (o proxy SIP), y al CPS (o proxy SIP) liberar las fijaciones en el lanzamiento sesión.

En primer lugar, con referencia a la figura 2, se describe un método para configurar un nodo de anclaje en una red de comunicación.

La figura 2 ilustra un terminal UE como un terminal de comunicación de origen identificado por su dirección IP1, un servidor de procesamiento de llamadas CPS como un ejemplo de un nodo de gestión de la comunicación, una puerta de enlace del traductor TrGW como una instancia del nodo de anclaje, un cortafuegos FW (que se describirá más tarde ) para su uso en la comunicación una vez que el nodo de anclaje se ha configurado, y un terminal de comunicación de destino, es decir, un nodo correspondiente CN identificado por su dirección IP3.

En una comunicación entre los terminales, existe una asociación lógica entre los terminales que se puede denominar como una llamada. Dentro de una llamada de este tipo, los datos de los diferentes "contenidos" o tipos de tráfico, es decir, de diferente calidad de servicio QoS, se pueden comunicar como en tráfico tiempo real o en tiempo no real, o similares. Un tipo respectivo de datos/tráfico se comunica a continuación, en un así llamado formador de sesión de parte de la llamada como tal. Una sesión es precisada no solo por las direcciones del terminal sino, además, por un número de puerto del terminal respectivo, a través del cual el número puerto el tráfico es guiado/manipulado. La puerta de enlace del traductor mantiene/almacena una tabla de traducción o la tabla de asignación en la que una dirección IP de un terminal de comunicación iniciando (InitIP) está asociado a una dirección IP correspondiente CorrIP (que representa un alias para el terminal). Opcionalmente (no mostrado), la tabla de asignación no solo incluía direcciones de terminales, sino, además, también los puertos respectivos de un terminal respectivo.

A continuación, se describe el método para la configuración del nodo de anclaje TrGW. El método comprende las siguientes etapas:

En una primera etapa, 1., el UE envía un SIP Invite a su CPS, especificando la dirección IP IP1, así como el número de puerto donde se espera que el flujo de medios en el campo SDP (protocolo de descripción de sesión). A los efectos de este ejemplo, vamos a llamar IP1 y Puerto#1 a la dirección IP y al número de puerto donde el

UE espera el flujo de medios. Dicho en otras palabras, se produce una solicitud para iniciar una sesión de comunicación para un primer terminal UE a través de un nodo de CPS gestión de la comunicación de dicha red de comunicación. Además, dicha etapa de solicitud para la iniciación comprende una etapa de indicar, a dicho nodo CPS de gestión de la comunicación, como mínimo, las direcciones de los terminales UE, CN a participar en la sesión de comunicación, y dicha etapa de indicar comprende además informar de un número de puerto Puerto#1 para dicha sesión de comunicación de dicho primer terminal UE.

En una segunda etapa, 2., el CPS envía una solicitud al TrGW proporcionando la dirección IP de la UE, es decir IP_1. Esta solicitud solicita que se asocie una dirección IP a la dirección del terminal que solicita establecer con ello un enlace. El nodo de anclaje como el TrGW a continuación, realiza un primer establecimiento, en el nodo de anclaje (TrGW), de un enlace para el primer terminal UE ante la petición de dicho nodo de gestión de la comunicación CPS.

Esto significa que el TrGW asocia otra dirección IP (un alias), IP_2, a IP_1 y crea una entrada en su tabla de asignación para almacenar esta asociación. Opcionalmente, el CPS puede proporcionar el número de puerto Puerto#1 del equipo de usuario UE, y opcionalmente el TrGW puede asignar otro número de puerto Puerto#2. Esta información también se almacena en la tabla de asignación, y se puede utilizar para un mayor filtrado de granularidad de los paquetes de datos entrantes, ya que se explican en las secciones siguientes. Sobre la base del enlace proporcionado por el nodo de anclaje TrGW, el CPS modifica el campo SDP de la invitación SIP: sustituye más particularmente IP_1 y opcionalmente Puerto#1 con IP_2 y el Puerto#2.

El TrGW a continuación, envía una respuesta al CPS que proporciona IP_2 como la dirección de un enlace asociada a IP1. Esta respuesta de asociación se ilustra por la etapa 3 en la figura 2.

A partir de entonces, en la etapa 4., hay un reenvío de dicha solicitud de iniciación de dicho nodo de gestión de comunicaciones CPS basado en el enlace establecido hacia un segundo terminal de CN, cuando el CPS envía la invitación SIP al nodo correspondiente usando la dirección de un enlace IP IP2 asociada al equipo de usuario UE.

En respuesta a ello, (no mostrado en la figura 2) la parte llamada responde con, por ejemplo, un "SIP 200 OK" al nodo CPS de gestión de llamadas. Por lo tanto, hay un reconocimiento de dicha solicitud por dicho segundo terminal de CN a dicho nodo de gestión de la comunicación CPS.

Las capacidades de flujo de medios del destino se devuelven a lo largo de la ruta de señalización, en el mensaje "SIP 200 OK" en los flujos de señalización anteriormente. En realidad, también podrían ser devueltos en una denominada "respuesta provisional de progreso de sesión SIP 183", o incluso en otra respuesta.

Tras la recepción de, por ejemplo, el SIP 200 OK, el CPS solicita un nuevo enlace para la dirección IP, IP3 del nodo correspondiente (y, opcionalmente, el número de puerto Puerto#3) de la parte llamada especificada en el campo SDP en el TrGW del nodo de anclaje. Esto representa un segundo establecimiento, en dicho nodo de anclaje, de un enlace para el segundo terminal de CN a petición de dicho nodo de gestión de la comunicación.

El TrGW proporciona (en el segundo establecimiento) una dirección y, opcionalmente, un número de puerto, IP_4 y Puerto#4, que el CPS especificará en el campo SDP del mensaje SIP 200 OK que finalmente se devuelve al terminal UE.

Estas etapas se llevan a cabo de manera que la parte llamada CN "ve" una única dirección IP, es decir, IP_2, como la dirección IP del equipo de usuario de la parte llamante. En la comunicación, todos los paquetes se deben enrutar a través del nodo de anclaje TrGW que llevará a cabo las conversiones de direcciones requeridas. No tener las etapas anteriores para establecer un enlace para la dirección del terminal llamado, el UE enviará los paquetes de IP1 al CN, mientras que la señalización SIP indicará IP2 como la dirección de origen.

A continuación, el nodo de gestión de llamadas CPS reenvía el mensaje SIP al terminal UE. Desde el punto de vista del terminal UE, la parte llamada CN está esperando el flujo de medios en IP_4 y, opcionalmente, por ejemplo, Puerto#4. Por lo tanto, hay una etapa de notificar a dicho primer terminal UE de la iniciación de la sesión, con el enlace de dicho segundo terminal siendo utilizada en la notificación.

Enviando del flujo de medios en esta dirección IP y el número de puerto, los paquetes llegarán al TrGW que identificará el enlace asociado ese flujo.

Ambas de dichas etapas de establecer un enlace por lo tanto comprenden una etapa de asociar un alias a dicho terminal UE respectivo, CN; es decir, los terminales se vuelven "conocidos" en una dirección diferente (y opcionalmente el número de puerto) tal como IP2 en lugar de IP1 e IP4 en lugar de IP3.

Además, las etapas de establecer un enlace adicional comprenden la etapa de almacenar el alias asociado para el terminal respectivo en dicho nodo de anclaje, por ejemplo en una memoria del nodo de anclaje en forma de una tabla de búsqueda.

(Por otra parte, dicha etapa de reconocer, como una opción, comprende además una etapa de informar de un número de puerto Puerto#3 para dicha sesión de comunicación de dicho segundo terminal de CN.)

De este modo, una tabla de asignación se configura en el nodo de anclaje al momento de solicitar un inicio de una sesión de llamada o comunicación.

Se muestran en la figura 8 las etapas según la presente invención involucradas con la terminación de una sesión de comunicación. En este sentido, el método comprende además una etapa S81 de solicitar la terminación de una sesión de comunicación para el primer terminal UE a través de un nodo de gestión de la comunicación CPS de dicha red de comunicación (la petición de terminación igualmente puede ser originada por el nodo corresponsal que actúa entonces como el "primer terminal"). Esta solicitud de terminación se envía entonces, S82, desde dicho nodo de gestión de la comunicación CPS basada en el enlace establecido hacia el segundo terminal CN, que reconoce, S83, dicho solicitud a dicho nodo de gestión de la comunicación CPS. El nodo de administración CPS transmite, S84, dicha solicitud al nodo de anclaje TrGW.

A continuación, se produce una primera liberación, S85, en el nodo de anclaje TrGW, del enlace del primer terminal UE a petición (S84) por dicho nodo de gestión de la comunicación CPS, y una segunda liberación, S86, en dicho nodo de anclaje TrGW, del enlace del segundo terminal CN a petición (S84) por dicho nodo de gestión de la comunicación. Estas etapas de liberación comprenden una etapa de borrar el alias asociado al terminal respectivo en dicho nodo de anclaje. Esto significa que las entradas a la tabla de asignación (que se muestran en las figuras 2, 3 y 4) se borran de forma selectiva.

Hasta aquí, se ha descrito la configuración del nodo de anclaje. Posteriormente, se describirá la comunicación mediante un nodo de anclaje así configurado.

En general, el ejemplo de un método de comunicación de datos que se describe en lo siguiente se refiere a los datos en una sesión de comunicación establecida entre un primer UE, CN y un segundo terminal CN, UE en una red de comunicación. El método comprende las etapas de transmitir los datos a comunicar desde el primer UE, la terminal de CN a un nodo de anclaje TrGW, el nodo de anclaje estando configurado para almacenar una tabla de enlaces respectivos para los terminales. Entonces hay una retransmisión de los datos que se comunican desde el nodo de anclaje hacia un nodo de filtrado, tal como un cortafuego FW de dicha red mediante los enlaces configurados para los terminales. A continuación de esto hay una filtración, en dicho nodo de filtrado, dichos datos a comunicar basados en los enlaces para dichos terminales.

Más específicamente, el filtrado comprende además pasar dichos datos a comunicar a través de dicho nodo de filtrado hacia adelante al segundo terminal CN, UE basado en el enlace, si existe dicho enlace, entre los enlaces configurados. Además, el filtrado comprende además el bloqueo de dichos datos de que se comunican a través de dicho nodo de filtrado hacia adelante al segundo terminal de CN, UE basado en el enlace, si tal enlace no existe entre los enlaces configurados.

Con referencia a la figura 3 esto significa que una vez que el nodo de anclaje se ha configurado como se describe anteriormente, como una etapa siguiente, el tráfico entre el UE al CN y el CN al UE se enruta - basado en las enlaces configurados- como sigue:

Primer caso (aguas abajo desde el UE a CN):

Los datos se enrutan desde el UE al TrGW, a continuación, desde el TrGW al FW y de allí al CN como se describe en lo siguiente (no se muestra la figura 3).

Segundo caso (aguas arriba del CN al UE):

Los datos se enrutan desde el CN al TrGW, a continuación, desde el TrGW al FW y de allí al UE, como se describe en el siguiente (como se muestra la figura 3).

Esto se describe ahora con más detalle:

Los datos de carga útil que se originan en el equipo de usuario UE se enrutan de manera forzada al nodo de anclaje. En caso de que existan nodos plurales de anclaje en la red, esto se puede conseguir mediante la asociación de un nodo de anclaje a un terminal respectivo, por ejemplo, dependiente de la dirección y/o ubicación del terminal o dependiente de cualquier otro criterio, por ejemplo, dependiente del tipo de tráfico en cuestión.

El nodo de anclaje TrGW modifica la cabecera IP de los paquetes entrantes de tal manera que se diferencia de la cabecera de los paquetes de datos salientes de la siguiente manera:

- La dirección IP de origen se modifica de IP_1 a IP_2
- La dirección IP de destino se modifica de IP_4 a IP_3
- Opcionalmente, el número de puerto de origen es modificado desde Puerto#1 a Puerto#2
- Opcionalmente, el número de puerto de destino es una modificación de Puerto#4 a Puerto#3.

Y para los paquetes IP entrantes, la parte llamada, es decir, el CN, envía paquetes IP como una respuesta de su dirección IP_3 a la dirección alias IP_2 del equipo de usuario UE.

Además, estos paquetes IP llegan al nodo de anclaje TrGW que modifica los paquetes como sigue:

- La dirección IP de origen se modifica de IP_3 a IP_4,
- La dirección IP de destino se modifica de IP_2 a IP_1,
- Opcionalmente, el número de puerto de origen es una modificación del Puerto#3 al Puerto#4,
- Opcionalmente, el número de puerto de destino es una modificación del Puerto#2 al Puerto#1.

En cualquier caso, en la comunicación, los paquetes con la cabecera modificada se enrutan de manera forzada al nodo de filtrado, tal como un cortafuego. Es decir, los datos que emanan del nodo de anclaje TrGW se enruta de manera forzada al cortafuego. En caso de que existan cortafuegos plurales en la red, esto se puede conseguir mediante la asociación de un cortafuego a un nodo de anclaje respectivo, por ejemplo, dependiente de la dirección y/o ubicación del nodo de anclaje, o dependiente de cualquier otro criterio.

El cortafuego a su vez está configurado para permitir que los paquetes entrantes del grupo de las direcciones IP del nodo de anclaje TrGW pasen el cortafuegos y bloqueen otros. El cortafuego como un nodo de filtrado de este modo conoce el conjunto de direcciones de los enlaces existentes para las comunicaciones autorizadas.

Este conocimiento se obtiene, por ejemplo, informando al cortafuego mediante el nodo de anclaje de cada enlace recién creado o eliminado para el establecimiento o supresión del enlace en el nodo de anclaje. Alternativamente, en el caso de la recepción de paquetes, el cortafuego puede consultar al nodo de anclaje para saber si las direcciones en cuestión son parte del conjunto de direcciones del nodo de anclaje o no. Varias otras posibilidades son posibles con el fin de que el cortafuego obtenga el conocimiento del grupo de direcciones del nodo de anclaje.

Tal método de comunicación permite:

- que los paquetes de datos no válidos que llegan al cortafuego se caigan,
- que los paquetes de datos no válidos que llegan al nodo de anclaje TrGW se caigan, por ejemplo, un paquete IP entrante que no corresponde a una sesión existente ni siquiera se reenvía al cortafuego,
- que paquetes entrantes desde los nodos válidos sean entregados a los equipos de usuario UE
- que los paquetes entrantes desde los nodos válidos sean revisados por el cortafuegos contra las amenazas comunes IP (por ejemplo, TCP SYN, Ping de muerte, etc.)

Opcionalmente, en caso de que el CPS proporcione los números de puerto y la dirección IP del nodo corresponsal al configurar el nodo de anclaje, esta información también se podría utilizar cuando se filtran los paquetes IP entrantes.

Los únicos paquetes que pueden pasar a través del TrGW primero y luego el cortafuego son aquellos generados por un CN legítimo (es decir, del CNs en una llamada SIP con un UE en la red protegida por el FW, de lo contrario caerían del TrGW), dirigida a una dirección IP legítima de un UE, y que corresponde al tipo de protocolo permitido para el UE, y viceversa.

Con el fin de poner en práctica la invención, el nodo de anclaje TrGW está configurado como se ha descrito anteriormente. También la interfaz entre el TrGW y el CPS está configurada como se describe anteriormente. Esta interfaz puede estar basada en el Protocolo LDAP (protocolo de acceso de directorio en línea), o COPS (servicio de política abierta común).

La funcionalidad adicional del CPS (solicitudes enviadas por el CPS al TrGW, la modificación de los mensajes SIP) se puede añadir a las actuales implementaciones de CPS o se aplican en un servidor proxy SIP. El CPS remitirá toda la señalización SIP a este proxy SIP que llevará a cabo las operaciones descritas anteriormente.

Esta modificación se ilustra en la figura 4 de los dibujos. El flujo de método es similar al de la figura 2, pero la funcionalidad impartida al CPS en la figura 2 se transfiere en esta modificación al servidor proxy SIP situado entre el CPS y el nodo de anclaje. El CPS simplemente transmite la solicitud para iniciar una sesión de comunicación en adelante con el servidor proxy SIP como un nodo de gestión de la comunicación alternativa, y las respuestas respectivas respuestas/reconocimientos al UE. Una descripción más detallada de la misma, por lo tanto, se omite aquí.

Por lo tanto, una seguridad de comunicación se puede lograr mediante el análisis de la señalización SIP y los datos intercambiados entre los nodos de comunicación, más en particular mediante el análisis de las direcciones IP indicadas (y números de puerto opcionalmente) que sirven como las "reglas dinámicas" para el cortafuego.

En lo que antecede, la presente invención se ha descrito con referencia a los métodos implicados. Sin embargo, es de señalar que la presente invención se refiere también a los nodos adaptados correspondientemente.

Por lo tanto, se entenderá que, en relación con el método de la configuración de un nodo de anclaje, un nodo de anclaje está constituido de la siguiente manera.

El nodo de anclaje según la presente invención y como se muestra en la figura 5 comprende un receptor que recibe primero una petición de enlace para establecer un enlace por un primer terminal solicitante para la iniciación de la sesión de comunicación desde un nodo de gestión de la comunicación, un procesador que establece primero un enlace para dicho primer terminal UE en respuesta a dicha petición de enlace recibida y devolver dicho enlace a dicho nodo de gestión de la comunicación, y dicho receptor que recibe en segundo lugar una solicitud de enlace para establecer un enlace para un segundo terminal para participar en la sesión de comunicación, desde el nodo de gestión de la comunicación, y dicho procesador en segundo lugar estableciendo un enlace para el segundo terminal CN ante la petición por dicho nodo de gestión de la comunicación. Es de notar que el receptor es en realidad un receptor/transmisor y el transmisor devuelve parte de la información con respecto al enlace establecido al nodo de gestión de comunicaciones CPS (o Proxy-CSCF). Tenga en cuenta que, aunque la figura 5 muestra un recibo distinto de las solicitudes de enlace, esto es solo para fines ilustrativos y ambas solicitudes recibidas en diferentes momentos, por supuesto, pueden ser recibidas a través de la misma interfaz del nodo de anclaje hacia el nodo de gestión de la comunicación CPS (o proxy-CSCF).

Además, el procesador comprende un dispositivo de asignación que asocia un alias a dicho terminal respectivo cuando se establece el enlace, así, y el nodo de anclaje comprende una memoria que almacena el alias asociado para el terminal respectivo.

Además, se entenderá que, en relación con el ejemplo descrito anteriormente para un método o comunicación, un nodo de anclaje está, por ejemplo, constituido de la siguiente manera. A este respecto, aunque diferentes dibujos ilustran el nodo de anclaje, se tiene que tener en cuenta que esto es solo a efectos ilustrativos. En realidad, un nodo de anclaje según la presente invención puede estar equipado con todos los dispositivos/medios internos en cualquier momento, mientras que éstos se representan operativos selectivamente según el estado operativo del nodo de anclaje, es decir, al configurar el nodo de anclaje o en la comunicación a través del nodo de anclaje. Además, una configuración se puede llevar a cabo entre o durante la comunicación, cuando el dispositivo de procesamiento del nodo de anclaje se configura preferiblemente para permitir un procesamiento en paralelo para el procesamiento de configuración y comunicación. Además, algunos componentes del nodo de anclaje no se proporcionan dos veces, pero utilizan para ambos propósitos, la configuración y la comunicación (por ejemplo, receptor, memoria).

El nodo de anclaje como se muestra en la figura 6 comprende un receptor que recibe los datos a comunicar desde el primer terminal UE, CN a un segundo terminal CN, UE, una memoria que almacena una tabla de enlaces respectivos para los terminales, un procesador de transmisión de los datos a comunicar hacia un nodo de filtrado FW de dicha red utilizando los enlaces para los terminales. Por supuesto, el receptor es en realidad un receptor/transmisor y actúa como transmisor con el fin de transmitir los datos según los resultados de procesamiento del procesador. El procesador en cooperación con la memoria y los enlaces almacenados en la misma, modifica las cabeceras de los datos como se ha descrito antes en relación con el método de comunicación. Tenga en cuenta que el nodo de anclaje solo puede realizar selectivamente una retransmisión de los datos al cortafuego para los datos/direcciones para los que tiene una información de enlace, es decir, datos asociados a una dirección de terminal para el que ningún alias (enlace) se almacena en el nodo de anclaje puede ser impedido de ser enviado al cortafuego. Esto significa que el nodo de anclaje comprueba los enlaces y envía solo los paquetes válidos según los enlaces al nodo de filtrado, y en la medida en que ya constituye parte de la funcionalidad de cortafuego. Sin embargo, la misma funcionalidad se puede atribuir al propio cortafuego.

Además, se entenderá que, en relación con el ejemplo descrito anteriormente de un método de comunicación, un nodo de filtrado es, por ejemplo, constituido de la siguiente manera.

El nodo de filtrado como se muestra en la figura 7 comprende un receptor que recibe los datos a comunicar desde el primer terminal UE, CN a un segundo terminal CN, UE, desde un nodo de anclaje manteniendo fijaciones para los terminales, y un procesador de análisis de los enlaces para dichos terminales, y un filtro filtrando dichos datos

dependiente de los resultados de análisis.

En particular, dicho filtro pasa dichos datos a comunicar hacia adelante al segundo terminal CN, UE basado en el enlace, si existe dicho enlace entre los enlaces configurados en el nodo de anclaje, y dicho filtro bloquea que dichos datos puedan ser comunicados hacia adelante al segundo terminal CN, UE basado en el enlace, si tal enlace no existe entre los enlaces configurados en el nodo de anclaje. Los datos bloqueados no se entregan, sino más bien se eliminan o se descartan. El nodo de filtrado de este modo comprueba que los paquetes que llegan al nodo de filtrado desde el nodo de anclaje, y por lo tanto "parecen" ser válidos (por ejemplo, debido a haber pasado por el nodo de anclaje), no son de otra manera inválidos.

Hay que señalar que los diagramas de bloques del nodo de anclaje, así como del nodo filtrado se dan sin ningún tipo de detalles específicos de aplicación. Los nodos pueden ser implementados en hardware, tal como un procesador de señal digital DSP o como un ASIC (circuito integrado de aplicación específica), o en software. Cualquier implementación es posible, siempre y cuando el nodo realice las funcionalidades como se describe más arriba con referencia a los métodos específicos/etapas a realizar.

Según ello, como se ha descrito anteriormente en este documento, la presente invención define métodos y nodos correspondientes para filtrar las comunicaciones IP a través de cortafuegos en escenarios en que los orificios dinámicos deben crearse para garantizar un nivel adecuado de seguridad. La invención se basa en crear un anclaje seguro y autorizado para las comunicaciones, donde todas las comunicaciones se dirigen a través antes de que un cortafuego realice el filtrado de paquetes. La invención no introduce nuevas entidades sino una reutilización del marco existente. La invención se basa en un traductor de puerta de enlace TrGW que conmuta direcciones en la cabecera según una tabla de asignación almacenada y una interfaz entre un CPS (o un proxy SIP) y el TrGW. Esta interfaz permitirá: al CPS solicitar el TrGW para proporcionar datos de enlaces entre las direcciones IP al iniciar la sesión, al TrGW proporcionar los datos de enlaces al CPS y al CPS para liberar las fijaciones en el lanzamiento de sesión. El FW será susceptible de estado y, en la interfaz externa, únicamente aceptará los paquetes recibidos cuya dirección IP pertenece al conjunto de direcciones del TrGW. Por tanto, cualquier paquete entrante que no corresponde a una llamada existente será dado de baja en el TrGW, y el paquete válido pasará por el FW que se compruebe que el paquete no es un mensaje con formato incorrecto u otro ataque.

A pesar de que la presente invención se ha descrito con referencia a realizaciones específicas que se eligieron solo como ejemplos, debe entenderse que la descripción y figuras anteriores que acompañan están destinadas a ilustrar la presente invención a modo de ejemplo solamente. Las realizaciones preferidas de los métodos y los nodos pueden variar por lo tanto dentro del alcance de las reivindicaciones adjuntas.

**REIVINDICACIONES**

1. Un método para configurar un nodo de anclaje en una red de comunicación, comprendiendo el método las etapas de:

una primera solicitud de inicio de una sesión de comunicación para un primer terminal a través de un nodo de gestión de la comunicación de dicha red de comunicaciones;
un primer establecimiento, en un nodo de anclaje, de un enlace para el primer terminal a petición de dicho nodo de gestión de la comunicación;
reenviar dicha primera solicitud para iniciar desde dicho nodo de gestión de la comunicación basado en el enlace establecido hacia un segundo terminal;
reconocer dicha primera solicitud para iniciar mediante dicho segundo terminal de dicho nodo de gestión de la comunicación;
un segundo establecimiento, en dicho nodo de anclaje, de un enlace para el segundo terminal a petición de dicho nodo de gestión de la comunicación;
comunicar datos en una sesión de comunicación establecida entre el primer terminal y el segundo terminal en la red de comunicación, en donde la comunicación comprende las etapas de:

transmitir los datos a comunicar desde el primer terminal al nodo de anclaje, estando el nodo de anclaje configurado para almacenar una tabla de enlaces respectivos para los terminales; y
transmitir los datos a comunicar desde el nodo de anclaje hacia un nodo de filtrado de dicha red mediante los enlaces respectivos para los terminales en donde el nodo de filtrado filtra dichos datos a comunicar basándose en los enlaces para dichos terminales.

2. Un método según la reivindicación 1, en el que dicha etapa de solicitar para iniciar comprende una etapa de:

indicar a dicho nodo de gestión de la comunicación, al menos, las direcciones de los terminales que participarán en la sesión de comunicación.

3. Un método según la reivindicación 2, en el que dicha etapa de indicar comprende además informar de un número de puerto para dicha sesión de comunicación de dicho primer terminal.

4. Un método según la reivindicación 1, en el que dichas etapas de establecer los enlaces comprenden la etapa de asociar un alias a dicho terminal respectivo.

5. Un método según la reivindicación 4, en el que dichas etapas de establecer los enlaces adicionales comprenden la etapa de almacenar el alias asociado para el terminal respectivo en dicho nodo de anclaje.

6. Un método según la reivindicación 1, en el que dicha etapa de reconocimiento comprende además una etapa de informar de un número de puerto para dicha sesión de comunicación de dicho segundo terminal.

7. Un método según la reivindicación 1, que comprende además una etapa de notificar a dicho primer terminal de la iniciación de la sesión usando el enlace de dicho segundo terminal.

8. Un método según la reivindicación 1, que comprende además las etapas de
una segunda solicitud de terminar la sesión de comunicación al primer terminal a través del nodo de gestión de la comunicación de dicha red de comunicaciones,
reenviar dicha segunda solicitud para terminar desde dicho nodo de gestión de la comunicación basándose en el enlace establecido hacia el segundo terminal,
reconocer dicha segunda solicitud para terminar mediante dicho segundo terminal a dicho nodo de gestión de la comunicación,
una primera liberación, en el nodo de anclaje, del enlace al primer terminal a petición de dicho nodo de gestión de la comunicación, y
una segunda liberación, en dicho nodo de anclaje, del enlace al segundo terminal a petición de dicho nodo de gestión de la comunicación.

9. Un método según la reivindicación 8, en el que dichas etapas de liberación comprenden una etapa de borrar el alias asociado para el terminal respectivo en dicho nodo de anclaje.

10. Un método según la reivindicación 1, en el que dicha etapa de filtrado comprende además pasar dichos datos a comunicar a través de dicho nodo de filtrado hacia adelante al segundo terminal basado en el enlace, si existe dicho enlace, entre los enlaces respectivos.

11. Un método según la reivindicación 1, en el que dicha etapa de filtrar comprende además bloquear que dichos datos puedan ser comunicados a través de dicho nodo de filtrado al segundo terminal basado en el enlace, si tal enlace no existe, entre los enlaces respectivos.

12. Un método según la reivindicación 1, en el que dicha etapa de transmitir comprende una etapa de traducción de direcciones basada en los enlaces respectivos.

13. Un nodo de anclaje en una red de comunicación, que comprende:

un receptor configurado operativamente para recibir una primera petición de enlace para establecer un primer enlace para un primer terminal que solicita un inicio de sesión de comunicación desde un nodo de gestión de la comunicación; y
un procesador configurado operativamente para establecer el primer enlace para dicho primer terminal en respuesta a dicha solicitud de enlace recibida y devolver dicho enlace a dicho nodo de gestión de la comunicación;
en donde dicho receptor está además configurado operativamente para recibir una segunda petición de enlace para establecer un segundo enlace para un segundo terminal para participar en la sesión de comunicación desde el nodo de gestión de la comunicación; y
dicho procesador está adicionalmente configurado operativamente para establecer el segundo enlace para el segundo terminal a petición de dicho nodo de gestión de la comunicación;
comprendiendo el nodo de anclaje, además:

una memoria operable configurada para almacenar una tabla de enlaces respectivos para los terminales;
donde el receptor está además configurado operativamente para recibir datos a comunicar desde el primer terminal al segundo terminal; y
el procesador está configurado además de manera operativa para transmitir los datos a comunicar hacia un nodo de filtrado de dicha red mediante los respectivos enlaces para los terminales y en donde dicho nodo de filtrado filtra dichos datos para comunicar basándose en los enlaces para dichos terminales.

14. Un nodo de anclaje según la reivindicación 13, en el que dicho procesador comprende un dispositivo de asignación configurado operativamente para asociar un alias a dicho terminal respectivo cuando se establece el enlace.

15. Un nodo de anclaje según la reivindicación 13, en el que dicho procesador comprende un traductor de direcciones que realiza una traducción de dirección basándose en los enlaces configurados.

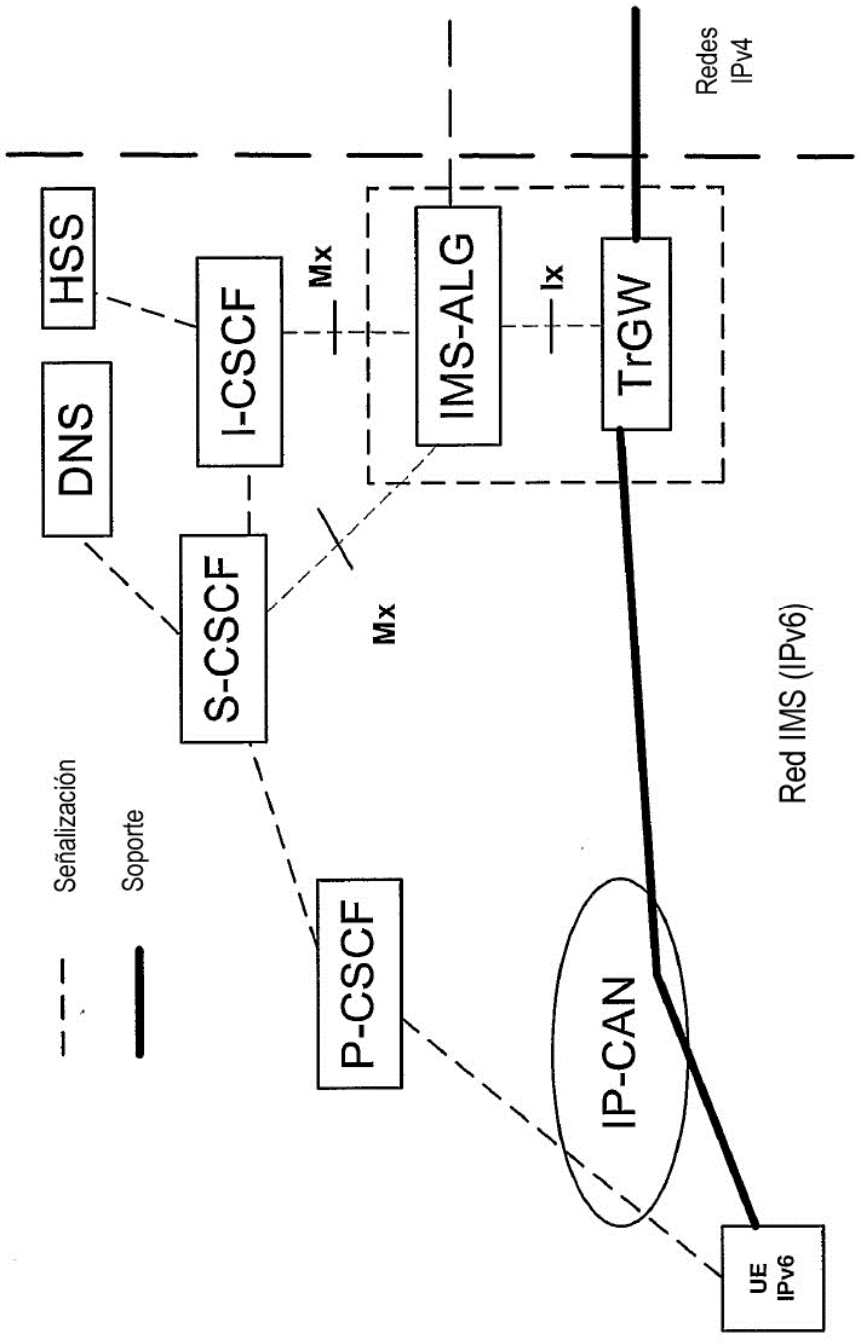


Fig. 1
(técnica anterior)

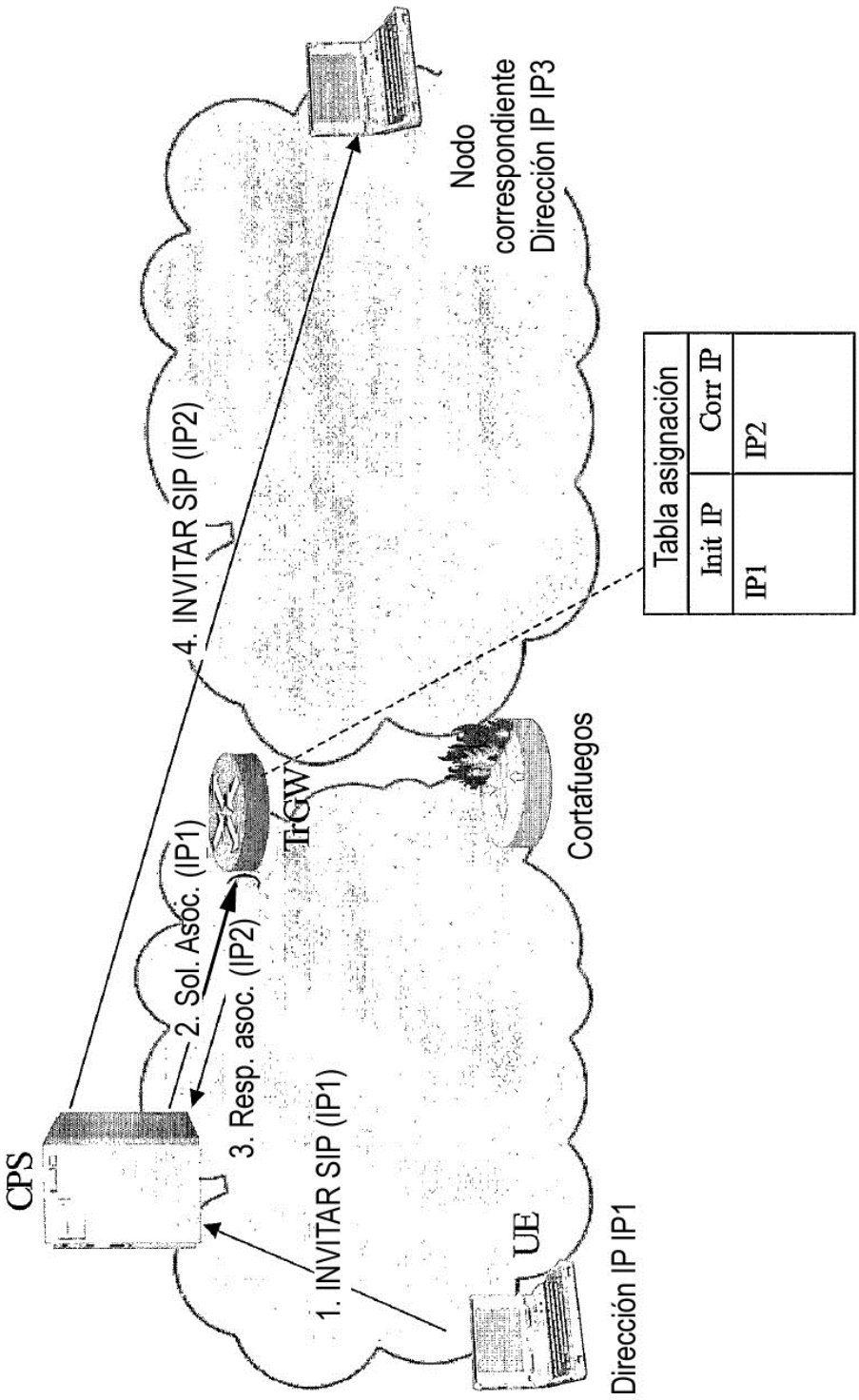
CPS
1. INVITAR SIP (IP1)
2. Sol. Asoc. (IP1)
3. Resp. asoc. (IP2)
4. INVITAR SIP (IP2)
TrGW
Cortafuegos
UE
Dirección IP IP1
Nodo correspondiente
Dirección IP IP3
Tabla asignación
Init IP
Corr IP
IP1
IP2

Fig. 2

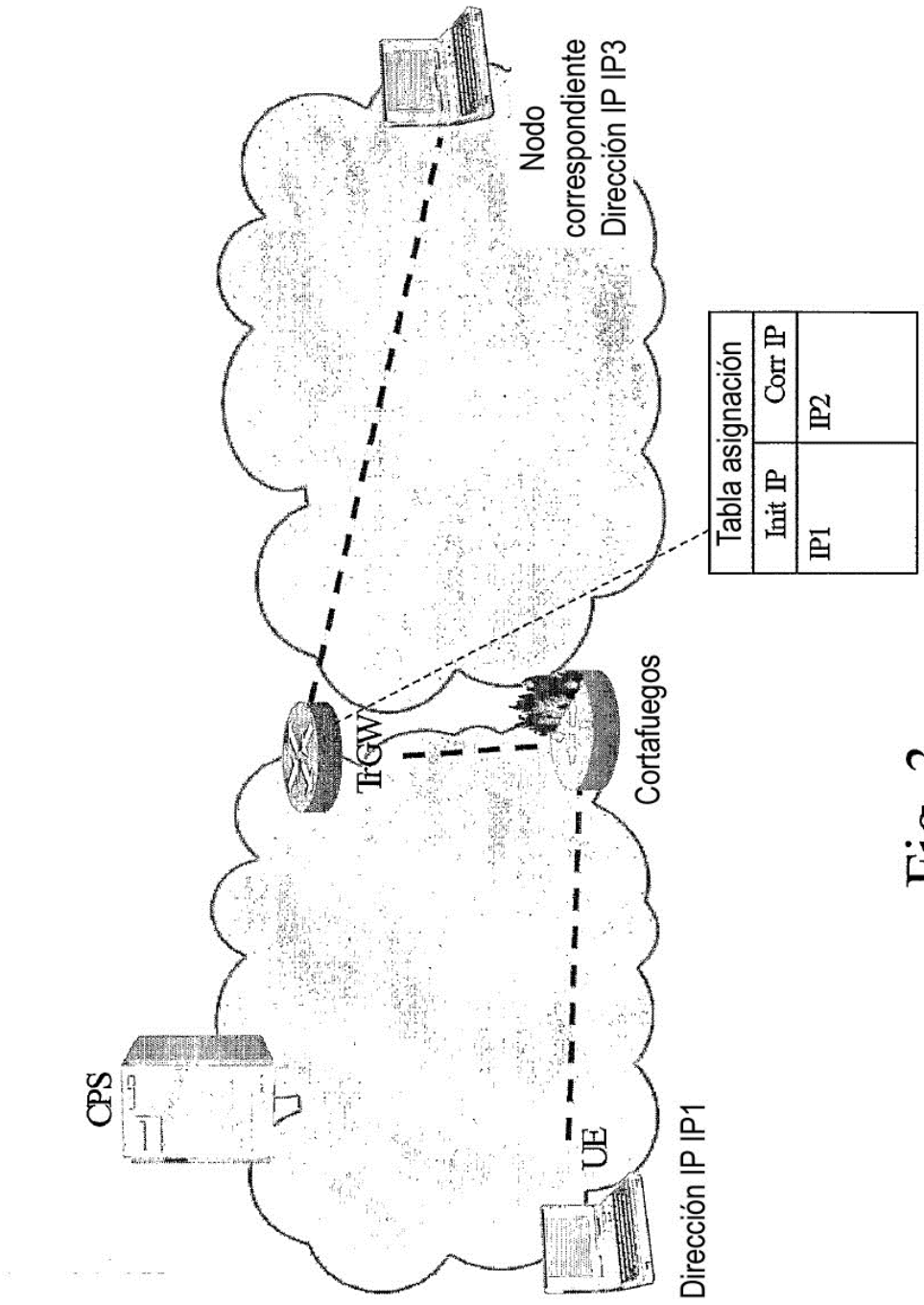
Nodo
correspondiente
Dirección IP IP3
Tabla asignación
Init IP
Corr IP
IP1
IP2
TrGW
Cortafuegos
CPS
UE
Dirección IP IP1

Fig. 3

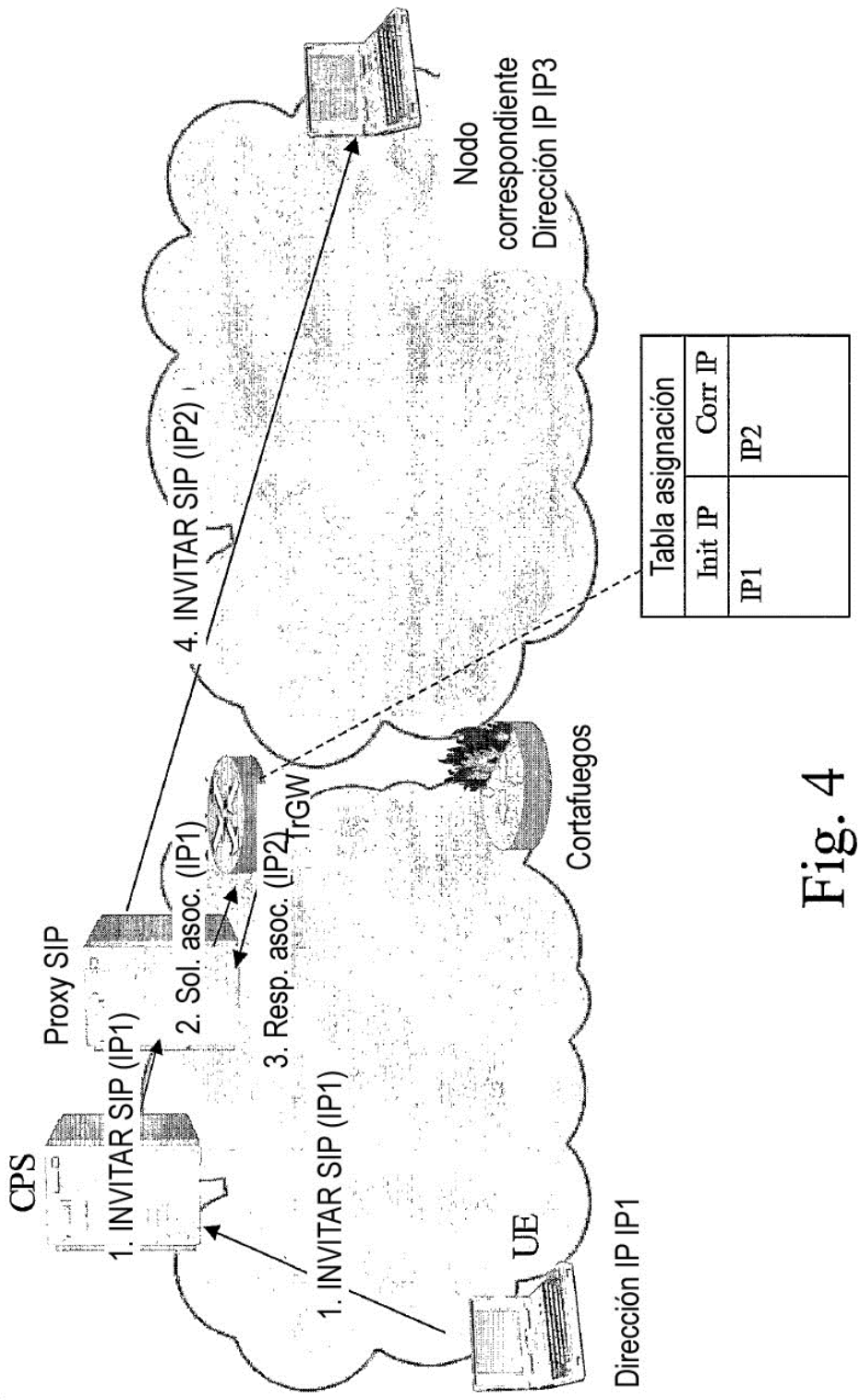
CPS
Proxy SIP
1. INVITAR SIP (IP1)
2. Sol. asoc. (IP1)
3. Resp. asoc. (IP2)
TrGW
4. INVITAR SIP (IP2)
Nodo correspondiente
Dirección IP IP3
1. INVITAR SIP (IP1)
UE
Dirección IP IP1
Cortafuegos
Tabla asignación
Init IP
Corr IP
IP1
IP2

Fig. 4

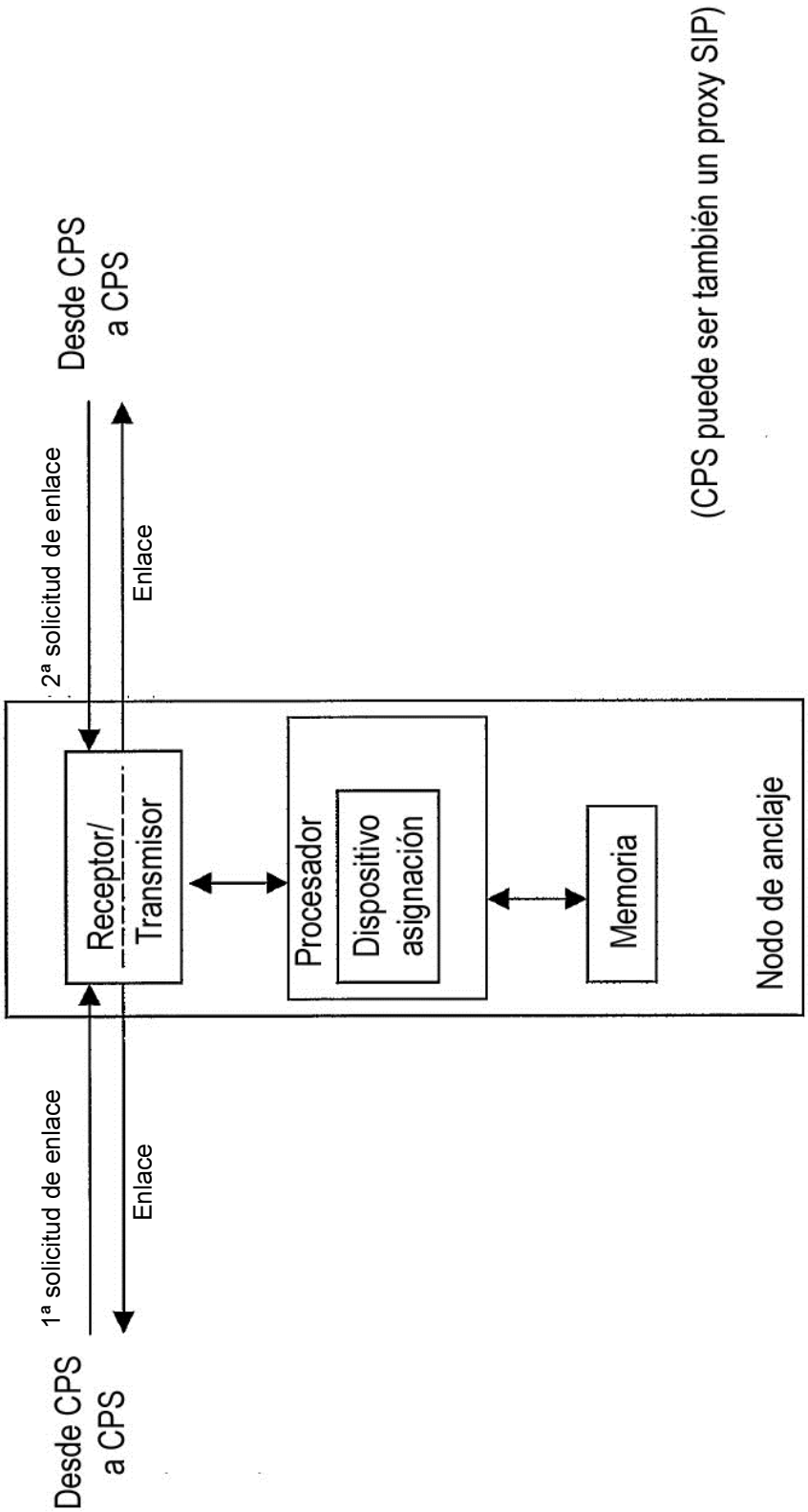
Desde CPS a CPS
1ª solicitud de enlace
Enlace
Desde CPS a CPS
2ª solicitud de enlace
Enlace
Receptor/ Transmisor
Procesador
Dispositivo asignación
Memoria
Nodo de anclaje
(CPS puede ser también un proxy SIP)

Fig. 5

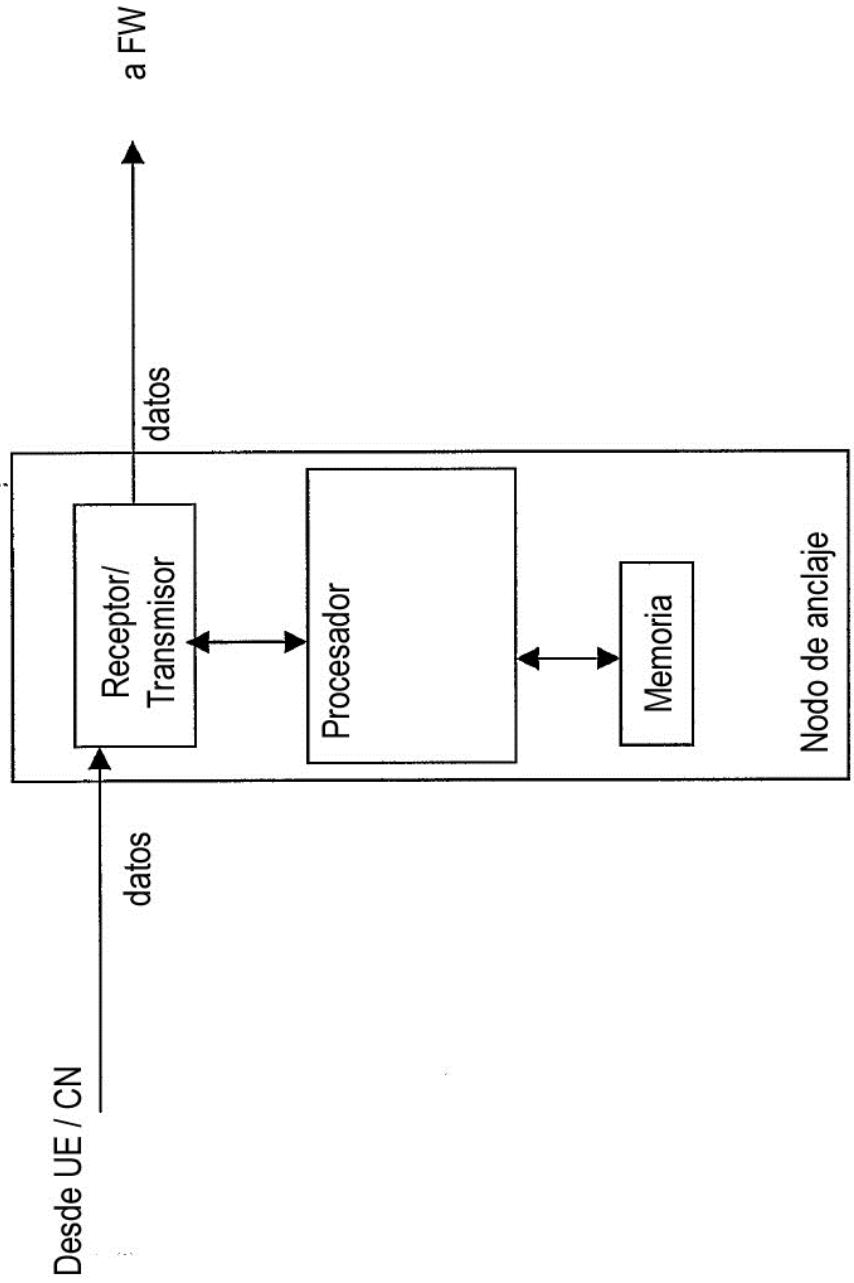
a FW
datos
Receptor/
Transmisor
Procesador
Memoria
Nodo de anclaje
datos
Desde UE / CN

Fig. 6

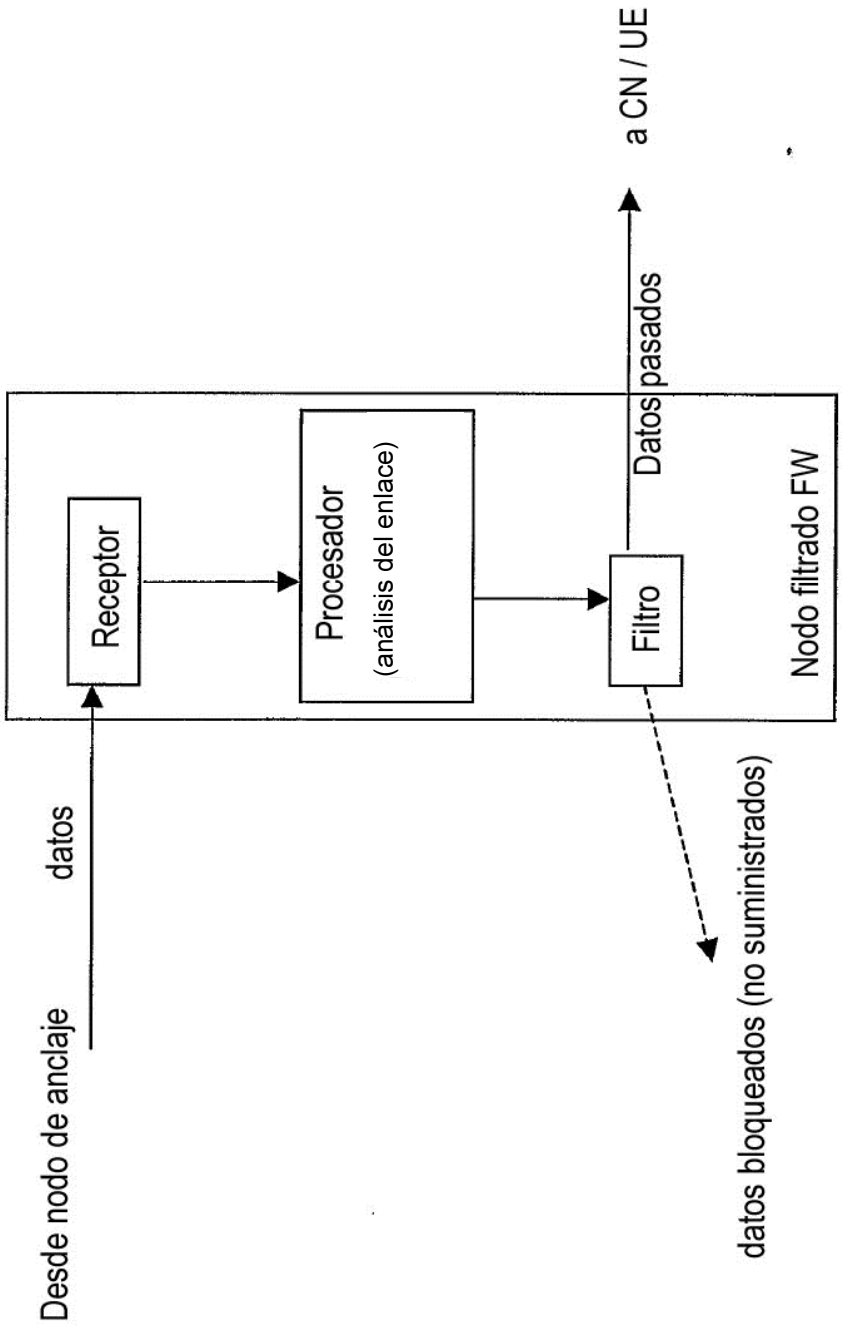
Desde nodo de anclaje
datos
Receptor
Procesador
(análisis del enlace)
Filtro
Datos pasados
a CN / UE
Nodo filtrado FW
datos bloqueados (no suministrados)

Fig. 7

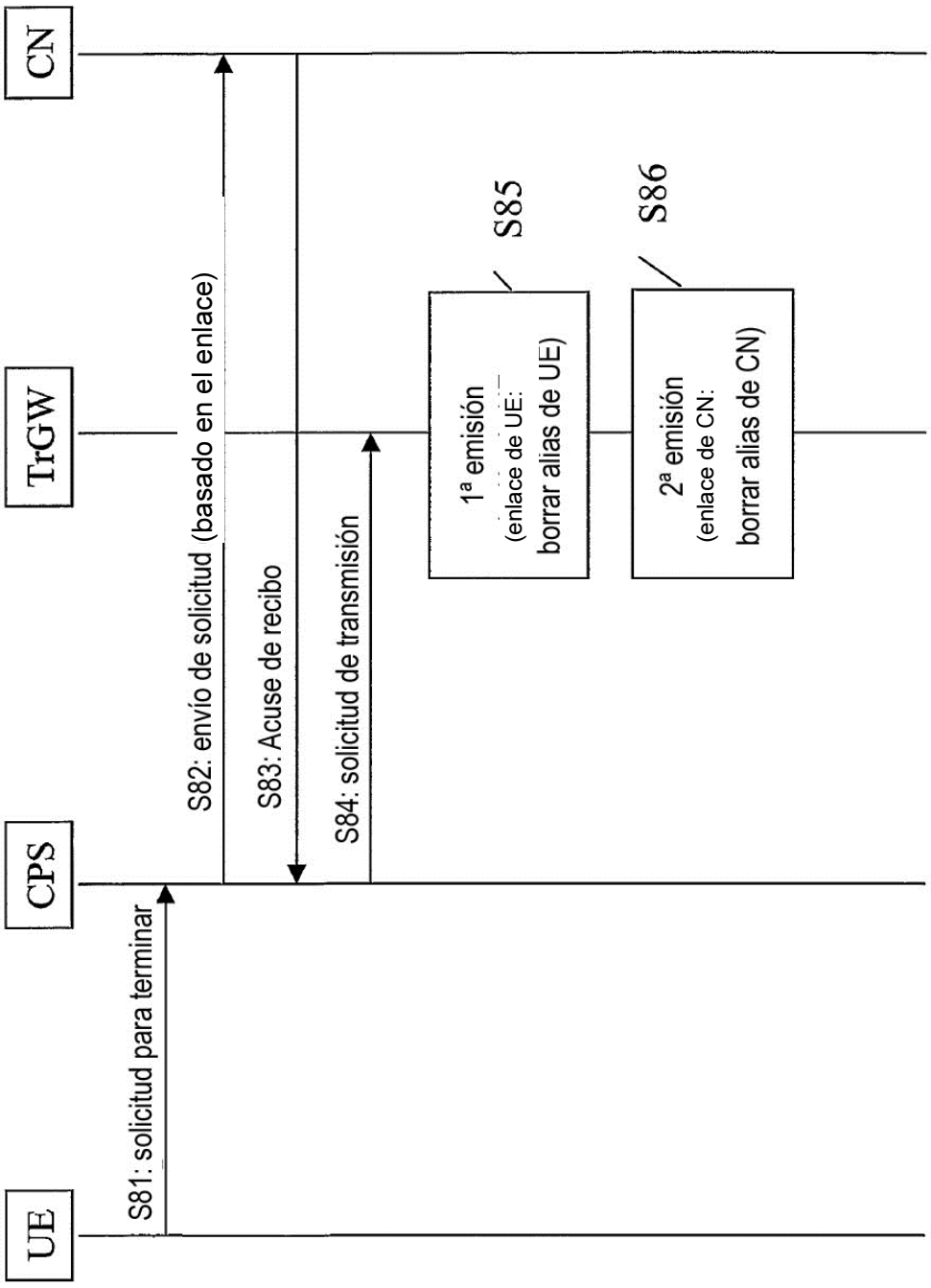
UE
CPS
TrGW
CN
S81: solicitud para terminar
S82: envío de solicitud (basado en el enlace)
S83: Acuse de recibo
S84: solicitud de transmisión
S85
1ª emisión
(enlace de UE:
borrar alias de UE)
S86
2ª emisión
(enlace de CN:
borrar alias de CN)

Fig. 8