(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 596 177**

(51) Int. CI.:

H04L 12/66 (2006.01)
H04L 12/46 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.03.2011 PCT/CN2011/071659**

(87) Fecha y número de publicación internacional: **23.02.2012 WO12022145**

(96) Fecha de presentación y número de la solicitud europea: **10.03.2011 E 11817673 (4)**

(97) Fecha y número de publicación de la concesión europea: **20.07.2016 EP 2590368**

(54) Título: **Método, equipo y sistema de red para hacer comunicar un terminal con un servidor de infraestructura de un subsistema multimedia IP (IMS) atravesando una red privada**

(30) Prioridad:

20.08.2010 CN 201010264191

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.01.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

CHEN, AIPING;
NIE, CHENGJIAO y
ZHANG, ZHANBING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, equipo y sistema de red para hacer comunicar un terminal con un servidor de infraestructura de un subsistema multimedia IP (IMS) atravesando una red privada

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de las tecnologías de comunicaciones y en particular, a un método, un aparato y un sistema de red para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura de subsistema multimedia de Protocolo Internet (IMS).

ANTECEDENTES DE LA INVENCIÓN

El subsistema multimedia de protocolo Internet (Internet Protocol Media Subsystem, IMS) es una arquitectura de red independiente del acceso basada en el protocolo IP. Es una red de infraestructura convergente que puede compartirse por una red móvil y una red fija, es decir, es capaz de proporcionar servicios convergentes para usuarios que utilizan diferentes maneras de acceso tales como una red de área local inalámbrica WLAN (Wireless Local Area Network) 2.5 G, 3 G, y una banda ancha fija y se considera como una red de la siguiente generación en el campo.

Para acceder a la red de infraestructura IMS, un terminal necesita atravesar una red privada (a modo de ejemplo, una red de empresa objeto de acceso por el terminal). Más concretamente, se utiliza una dirección IP de red privada dentro de la red de empresa, y un dispositivo de traducción de dirección de red (NAT) se desarrolla en la periferia de la red de empresa. Por lo tanto, el terminal necesita atravesar el dispositivo NAT y acceder a un servidor de la red de infraestructura IMS; o si un servidor proxy de capa de aplicación se desarrolla en la periferia de la red de empresa, el terminal necesita atravesar el servidor proxy de capa de aplicación y acceder al servidor de la red de infraestructura IMS.

La técnica anterior da a conocer un método para atravesar una red privada. Más concretamente, una pasarela de red privada virtual de Seguridad del protocolo Internet (Internet Protocol Security VPN, IPSec VPN) es desarrolla en una red de empresa y una red IMS respectivamente, con el fin de establecer un túnel IPSec VPN entre la red de empresa y la red IMS utilizando la pasarela IPSec VPN desarrollada; y rutas de terminales en la red de empresa convergen en la pasarela IPSec VPN en la red de empresa, y la pasarela IPSec VPN en la red de empresa realiza operaciones tales como encapsulación/desencapsulación sobre los datos de servicio. Más concretamente, cuando un terminal envía datos de servicio a la red de infraestructura IMS, una ruta de los datos de servicio enviados por el terminal se modifica y los datos de servicio se enrutan a la pasarela IPSec VPN en la red de empresa, en primer lugar. La pasarela IPSec VPN encapsula los datos de servicio, y luego, transmite los datos de servicio a través del túnel IPSec VPN a la pasarela IPSec VPN en la red de infraestructura IMS. La pasarela IPSec VPN en la red de infraestructura desencapsula los datos de servicio y los envía al servidor en la red de infraestructura IMS.

En la técnica anterior, la pasarela IPSec VPN necesita desarrollarse en la red de empresa, con la necesidad de modificar la ruta de datos del terminal y se requiere una importante modificación de la red de empresa.

El documento US 2008/198861 A1 da a conocer un método para el enrutamiento u control de tráfico de datos de paquetes en un sistema de comunicaciones. El método incluye: iniciar el establecimiento de una asociación de seguridad entre un nodo de cliente y un nodo de pasarela. Una dirección autorizada se proporciona al nodo del cliente desde la pasarela. El nodo del cliente transmite un paquete a la pasarela, incluyendo dicho paquete la dirección autorizada como dirección origen. La autorización se comprueba por el nodo de pasarela para permitir que paquetes salientes sean enviados a destinos específicos.

El documento US 2005/0008006 A1 da a conocer un método para utilizar un terminal vocal conectado a una centralita automática privada distante. El terminal vocal se asigna a una subred que tiene un primer espacio de dirección IP, funcionando la centralita automática privada distante en un segundo espacio de dirección IP. La dirección IP del primer espacio de dirección IP no es válida en el segundo espacio de dirección IP. El método incluye: determinar una dirección IP desde el primer espacio de direcciones para el terminal vocal; determinar un servidor VPN para el terminal vocal; establecer una conexión VPN entre el terminal vocal VoIP y el servidor VPN con la asignación de una dirección IP adicional, tomada a partir del segundo espacio de dirección IP, por el servidor VPN; e intercambiar información y/o información de señalización entre el terminal vocal y la centralita automática privada distante a través de dicha conexión de VPN.

El documento EP 1768343 A2 da a conocer un método y un aparato para la activación de protocolos de red privada virtual alternativos. El método permite a los clientes de empresa detectar el bloqueo del protocolo VPN por la red de acceso y proporcionar software de VPN del cliente con instrucciones para activar otro protocolo VPN tal como el protocolo de Capa de Conexión Segura (SSL) que es menos probable que sea bloqueado por su proveedor, se dan a conocer en este documento. A modo de ejemplo, si el proveedor de la red de acceso bloquea el protocolo IPSec VPN, el software VPN del cliente se conmutará a un protocolo VPN alternativo, tal como un Protocolo de Tunelización de Capa 2 de protocolo SSL (L2TP) o un Protocolo de Tunelización Punto a Punto (PPTP) para la

conexión a la red de VoIP.

SUMARIO DE LA INVENCIÓN

La presente invención da a conocer un método, un aparato y un sistema de red para un terminal que le permite atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS, de modo que el terminal sea capaz de atravesar la red privada para comunicarse con un servidor en una red pública (es decir, la red de infraestructura IMS) sin necesidad de modificar una red de empresa.

En consecuencia, la presente invención da a conocer las soluciones siguientes:

En conformidad con el primer aspecto de la presente invención, un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura de subsistema multimedia de protocolo Internet (IMS), incluye:

establecer, por el terminal, una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establecer una dirección de destino de los datos de servicio a enviarse como una dirección del servidor para obtener un primer paquete de servicio, en donde el terminal está situado en la red privada, siendo la dirección IP virtual una dirección asignada por la red de infraestructura IMS al terminal;

encapsular el primer paquete de servicio en un primer paquete de túnel, en donde una dirección IP origen del primer paquete de túnel es una dirección IP real del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de una pasarela de túnel de seguridad, estando la pasarela de túnel de seguridad situada en la periferia de la red de infraestructura IMS; y

enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través de un túnel de red privada virtual (VPN) entre el terminal y la pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel al servidor;

en donde el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel de Protocolo de Datagrama de Usuario, UDP; y cuando un túnel de Security Socket Layer, SSL, existe entre el terminal y la pasarela de túnel de seguridad de forma adicional,

el método comprende, además:

enviar, por el terminal, una primera información de control de servicio a la pasarela de túnel de seguridad a través del túnel SSL, siendo la primera información de control de servicio una demanda de asignación de la dirección IP virtual;

recibir, por el terminal, una segunda información de control de servicio enviada por la pasarela de túnel de seguridad a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

En una forma de realización preferida, el método para permitir a un terminal atravesar a una red privada para comunicarse con un servidor en una red de infraestructura IMS incluye:

recibir, por una pasarela de túnel de seguridad, un primer paquete de túnel a través de un túnel VPN entre la pasarela de túnel de seguridad y el terminal, en donde la pasarela de túnel de seguridad está situada en la periferia de la red de infraestructura IMS, estando el terminal situado en la red privada, siendo una dirección IP origen del primer paquete de túnel una dirección IP real del terminal y siendo una dirección IP de destino del primer paquete de túnel una dirección IP de la pasarela de túnel de seguridad;

desencapsular el primer paquete de túnel para obtener un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección del servidor, siendo la dirección IP virtual una dirección asignada por la red de infraestructura IMS al terminal; y

enviar el primer paquete de servicio al servidor;

en donde el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel UDP; y cuando un túnel SSL existe entre el terminal y la pasarela de túnel de seguridad de forma adicional, el método comprende, además:

recibir, por la pasarela de túnel de seguridad, una primera información de control de servicio enviada por el terminal a través del túnel SSL, siendo la primera información de control de servicio una demanda para la asignación de la dirección IP virtual;

enviar, por la pasarela de túnel de seguridad, una segunda información de control de servicio al terminal a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

En conformidad el segundo aspecto de la idea inventiva, un terminal incluye una componente de capacidad de comunicaciones, en donde el terminal está situado en una red privada, incluyendo la componente de capacidad de comunicaciones:

un primer módulo de convergencia de datos, configurado para establecer una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establecer una dirección de destino de los datos de servicio a enviarse como una dirección de un servidor situado en una red de infraestructura de subsistema multimedia de protocolo Internet, IMS, y obtener un primer paquete de servicio, en donde la dirección IP virtual es una dirección asignada por la red de infraestructura IMS al terminal; y

un primer módulo de transmisión de túnel, configurado para encapsular el primer paquete de servicio en un primer paquete de túnel, en donde una dirección IP origen de primer paquete de túnel es una dirección IP real del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de una pasarela de túnel de seguridad, estando la pasarela de túnel de seguridad situada en la periferia de la red de infraestructura IMS; y para enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través de túnel VPN entre el terminal y la pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel al servidor;

en donde el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel UDP; y en donde el terminal comprende, además:

un tercer módulo de transmisión de túnel, configurado para enviar una primera información de control de servicio a pasarela de túnel de seguridad de servicio a través un túnel SSL adicional entre el terminal y la pasarela de túnel de seguridad, siendo la primera información de control de servicio una demanda para la asignación de la dirección IP virtual;

un cuarto módulo de transmisión de túnel, configurado para recibir una segunda información de control de servicio enviada por la pasarela de túnel de seguridad de servicio a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

En conformidad con el tercer aspecto de la idea inventiva, una pasarela de túnel de seguridad situada en la periferia de una red de infraestructura de Subsistema Multimedia de Protocolo Internet, IMS, la pasarela de túnel de seguridad incluye:

un primer módulo de recepción, configurado para recibir un primer paquete de túnel a través de un túnel VPN entre la pasarela de túnel de seguridad y un terminal, en donde el terminal está situado en una red privada, siendo una dirección IP origen del primer paquete de túnel una dirección IP real del terminal, y siendo una dirección IP de destino del primer paquete de túnel una dirección IP de la pasarela de túnel de seguridad;

un módulo de desencapsulación, configurado para desencapsular el primer paquete de túnel; y

un primer módulo de envío, configurado para enviar un primer paquete de servicio obtenido como un resultado de la desencapsulación por el módulo de desencapsulación a un servidor situado en la red de infraestructura IMS, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección del servidor, y la dirección IP virtual es una dirección asignada por la red de infraestructura IMS al terminal;

en donde el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel UDP; y

en donde la pasarela de túnel de seguridad comprende, además:

un cuarto módulo de recepción, configurado para recibir una primera información de control de servicio enviada por el terminal a través de un túnel SSL adicional entre el terminal y la pasarela de túnel de seguridad, siendo la primera información de control de servicio es una demanda para la asignación de la dirección IP virtual; y

un tercer módulo de envío, configurado para enviar una segunda información de control de servicio al terminal a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

En conformidad con el cuarto aspecto de la idea inventiva, un sistema de red incluye una pasarela de túnel de seguridad y un servidor, estando el servidor situado en una red de infraestructura IMS, y estando la pasarela de túnel de seguridad situada en la periferia de la red de infraestructura IMS, en donde

La pasarela de túnel de seguridad está configurada para:

recibir un primer paquete de túnel a través de un túnel VPN entre la pasarela de túnel de seguridad y un terminal, en donde una dirección IP origen del primer paquete de túnel es una dirección IP real del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de la pasarela de túnel de seguridad, estando el terminal situado en una red privada;

desencapsular el primer paquete de túnel para obtener un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección del servidor, siendo la dirección IP virtual una dirección asignada por la red de infraestructura IMS al terminal; para enviar el primer paquete de servicio al servidor;

recibir un segundo paquete de servicio enviado por el servidor, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor y una dirección de destino del segundo paquete de servicio es la dirección IP virtual; para encapsular el segundo paquete de servicio en un segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es la dirección IP real del terminal; y

enviar el segundo paquete de túnel al terminal a través del túnel VPN entre la pasarela de túnel de seguridad y el terminal;

en donde el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel UDP; y en donde la pasarela de túnel de seguridad está configurada, además, para:

recibir una primera información de control de servicio enviada por el terminal a través de un túnel SSL adicional entre el terminal y la pasarela de túnel de seguridad, siendo la primera información de control de servicio una demanda para la asignación de la dirección IP virtual; enviar una segunda información de control de servicio al terminal a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

El servidor de red interna está configurado para recibir el primer paquete de servicio enviado por la pasarela de túnel de seguridad y para enviar el segundo paquete de servicio a la pasarela de túnel de seguridad.

En la presente invención, el terminal utiliza la dirección IP virtual asignada por la red de infraestructura IMS como una dirección de comunicación entre el terminal y servidor de red interno, establece la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, establece la dirección de destino de los datos de servicio a enviarse como una dirección del servidor de red interno, y encapsula los datos de servicio en un paquete de túnel, y luego transmite el paquete de túnel a la pasarela de túnel de seguridad a través del túnel entre el terminal y la pasarela de túnel de seguridad. De esta forma, la pasarela de túnel de seguridad es capaz de enviar el paquete de servicio que tiene la dirección IP virtual como la dirección origen y que tiene la dirección del servidor de red interno como la dirección de destino al servidor de red interno; los datos de servicio se transmiten entre el servidor de red interno y el terminal utilizando la pasarela de túnel de seguridad; y el terminal es capaz de atravesar la red privada para comunicarse con el servidor en la red pública sin necesidad de modificar la red de empresa que cubre el terminal.

En la presente invención, la pasarela de túnel de seguridad sirve como un dispositivo intermedio y desencapsula el paquete de túnel desde el terminal y envía el paquete de túnel desencapsulado al servidor de red interno, con el fin de facilitar la transmisión de datos de servicio entre el terminal y el servidor en la red de infraestructura IMS. De esta forma, el terminal es capaz de atravesar la red privada para comunicarse con el servidor en la red pública sin modificar la red de empresa que cubre el terminal.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1A es un diagrama de flujo de un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS en conformidad con una forma de realización de la presente invención;

La Figura 1B es otro diagrama de flujo de un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS en conformidad con una forma de realización de la presente invención;

La Figura 2A es otro diagrama de flujo de un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS en conformidad con un forma de realización de la presente invención;

La Figura 2B es otro diagrama de flujo de un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS en conformidad con una forma de realización de la presente invención;

La Figura 3 es un diagrama de flujo de establecimiento de túnel VPN en conformidad con una forma de realización de la presente invención;

La Figura 4 es un diagrama de flujo de autenticación de identidad de terminal en conformidad con una forma de realización de la presente invención;

La Figura 5 es un diagrama de flujo de transmisión transversal segura de datos de servicio de IMS en conformidad con una forma de realización de la presente invención;

La Figura 6 es otro diagrama de flujo de transmisión transversal segura de datos de servicio de IMS en conformidad con una forma de realización de la presente invención;

La Figura 7 es un diagrama estructural de un terminal en conformidad con una forma de realización de la presente invención;

La Figura 8 es un diagrama estructural de una pasarela de túnel de seguridad en conformidad con una forma de realización de la presente invención; y

La Figura 9 es un diagrama estructural de un sistema de red en conformidad con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

Haciendo referencia a la Figura 1A, una forma de realización de la presente invención da a conocer un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS. El método describe la solución técnica dada a conocer en la forma de realización de la presente invención desde la perspectiva de un lado de terminal. El método incluye:

101. El terminal establece una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establece una dirección de destino de datos de servicio a enviarse como una dirección de un servidor de red interno, y obtiene un primer paquete de servicio, en donde la dirección IP virtual es una dirección asignada por la red de infraestructura IMS al terminal.

En esta forma de realización, el proceso de obtención del primer paquete de servicio por el terminal incluye: establecer la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, establecer la dirección de destino de los datos de servicio que han de enviase como la dirección del servidor de red interno, establecer un puerto origen de los datos de servicio a enviarse como un puerto de servicio del terminal y establecer un puerto de destino de los datos de servicio a enviarse como un puerto de servicio del servidor de red interno.

Esta forma de realización y todas las formas de realización posteriores de la presente invención son aplicables al entorno operativo siguiente: el terminal está situado en una red privada tal como una red de empresa, y el terminal desea comunicarse con el servidor en la red de infraestructura IMS, por lo tanto, el terminal necesita atravesar la red privada para comunicarse con el servidor de red interno en la red de infraestructura IMS.

La dirección IP virtual se asigna por una pasarela de túnel de seguridad (Security Tunnel Gateway, STG). La pasarela de túnel de seguridad está situada en la periferia de la red de infraestructura IMS. La pasarela de túnel de seguridad (Security Tunnel Gateway, STG) puede ser una pasarela red de empresa de red privada virtual (Virtual Private Network, VPN) descrita en las formas de realización posteriores. Un túnel entre el terminal y la pasarela de túnel de seguridad puede ser un túnel de protocolo de datagrama de usuario (User Datagram Protocol, UDP), un túnel VPN de capa de conexión segura (Security Socket Layer, SSL) o un túnel VPN de protocolo de transferencia de hipertexto (HyperText Transfer Protocol, HTTP) túnel VPN.

La dirección IP virtual puede asignar por un servidor de Protocolo de configuración de host dinámico (Dynamic Host Configuration Protocol, DHCP) de la red de infraestructura IMS.

El túnel UDP VPN incluye un túnel de seguridad de capa de transporte de datagrama (Datagram Transport Layer Security, DTLS) túnel VPN.

102. Encapsular el primer paquete de servicio en un primer paquete de túnel, en donde una dirección IP virtual IP origen del primer paquete de túnel es una dirección IP del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de una pasarela de túnel de seguridad.

El proceso detallado de encapsular el primer paquete de túnel incluye: establecer la dirección IP origen del primer paquete de servicio como una dirección IP del terminal, en donde la dirección IP es una dirección IP real del terminal; establecer la dirección IP de destino del primer paquete de servicio como una dirección IP de la pasarela de túnel de seguridad; establecer un puerto origen del primer paquete de servicio como un puerto de servicio del terminal; y establecer un puerto de destino del primer paquete de servicio como un puerto de túnel de la pasarela de túnel de seguridad.

103. Enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través de un túnel VPN entre el terminal y le pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel al servidor de red interno.

La Figura 1B es otro diagrama de flujo de un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS en conformidad con una forma de realización de la presente invención. La forma de realización ilustrada en la Figura 1B describe cómo el terminal atraviesa la red privada para recibir los datos de servicio enviados por el servidor en la red de infraestructura IMS cuando el terminal necesita recibir los datos de servicio de un servidor de red interno. Según se ilustra en la Figura 1B, el método incluye:

104. El terminal recibe un segundo paquete de túnel a través de un túnel, en donde una dirección IP origen del segundo paquete de túnel es una dirección IP de una pasarela de túnel de seguridad, y una dirección IP de destino del segundo paquete de túnel es una dirección IP del terminal.

105. Desencapsular el segundo paquete de túnel para obtener un segundo paquete de servicio, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor de red interno, y una dirección de destino del segundo paquete de servicio es la dirección IP virtual.

106. Obtener los datos de servicio en el segundo paquete de servicio.

En una aplicación práctica, el método para permitir al terminal atravesar la red privada para comunicarse con el servidor en la red de infraestructura IMS en la forma de realización ilustrada en la Figura 1A puede utilizarse junto con el método en la forma de realización ilustrada en la Figura 1B. La forma de realización ilustrada en la Figura 1A describe un proceso que permite al terminal atravesar la red privada para enviar los datos de servicio al servidor en la red de infraestructura IMS. La forma de realización ilustrada en la Figura 1B describe un proceso para permitir al terminal atravesar la red privada para recibir los datos de servicio desde el servidor en la red de infraestructura IMS.

Cuando un túnel UDP VPN y un túnel SSL VPN coexisten en el túnel VPN entre el terminal y la pasarela de túnel de seguridad, los datos de servicio se transmiten través del túnel UDP VPN y la información de control de servicio se transmite a través del túnel SSL VPN. Más concretamente, el método incluye, además: enviar, por el terminal, una primera información de control de servicio a la pasarela de túnel de seguridad a través del túnel SSL VPN, a modo de ejemplo, enviar, por el terminal, información a la pasarela de túnel de seguridad como una demanda para asignar una dirección IP virtual; o bien, cuando el terminal necesita liberar un túnel VPN, enviar por el terminal, información de indicación de liberación del túnel VPN a la pasarela de túnel de seguridad a través del túnel SSL VPN; o bien, recibir, por el terminal, una segunda información de control de servicio enviada por la pasarela de túnel de seguridad a través del túnel SSL VPN. A modo de ejemplo, a través del túnel SSL VPN, el terminal recibe la dirección IP virtual asignada por la pasarela de túnel de seguridad después de que la pasarela de túnel de seguridad asigne la dirección IP virtual al terminal.

En la forma de realización de la presente invención, el terminal utiliza la dirección IP virtual asignada por la red de infraestructura IMS como una dirección de comunicación entre el terminal y el servidor de red interno, establece la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, establece la dirección de destino de los datos de servicio a enviarse como la dirección del servidor de red interno, y encapsula los datos de servicio en un paquete de túnel, y luego transmite paquete de túnel a la pasarela de túnel de seguridad entre el terminal y la pasarela de túnel de seguridad. De esta forma, la pasarela de túnel de seguridad es capaz de enviar el paquete de servicio que tiene la dirección IP virtual como la dirección origen y que tiene la dirección del servidor de red interno como la dirección de destino al servidor de red interno. Cuando los datos de servicio del servidor de red interno necesitan recibirse, el paquete de túnel recibido se desencapsula en un paquete de servicio que tiene la dirección del servidor de red interno como la dirección origen y tiene la dirección IP virtual como la dirección de destino. De esta forma, utilizando la pasarela de túnel de seguridad, los datos de servicio se transmiten entre el servidor de red interno y el terminal, y el terminal es capaz de atravesar la red privada para comunicarse con el servidor en una red pública sin necesidad de modificar una red de empresa que cubre el terminal.

Haciendo referencia a la Figura 2A, una forma de realización de la presente invención da a conocer un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS. El método describe la solución técnica dada a conocer en la forma de realización de la presente invención desde la perspectiva de un lado de pasarela de túnel de seguridad. El método incluye:

201. La pasarela de túnel de seguridad recibe un primer paquete de túnel a través de un túnel entre la pasarela de túnel de seguridad y el terminal, en donde una dirección IP origen del primer paquete de túnel es una dirección IP del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de la pasarela de túnel de seguridad.

La dirección IP virtual se asigna por la pasarela de túnel de seguridad. El túnel entre la pasarela de túnel de seguridad y el terminal puede ser un túnel de protocolo de datagrama de usuario (User Datagram Protocol, UDP), un túnel de capa de conexión segura (Security Socket Layer, SSL) o un túnel de protocolo de transferencia de hipertexto (HyperText Transfer Protocol, HTTP).

202. La pasarela de túnel de seguridad desencapsula el primer paquete de túnel para obtener un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección de un servidor de red interno.

203. La pasarela de túnel de seguridad envía el primer paquete de servicio al servidor de red interno.

La Figura 2B es otro diagrama de flujo de un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS en conformidad con otra forma de realización de la presente invención. La forma de realización ilustrada en la Figura 2B describe cómo transmitir un paquete de servicio enviado por un servidor de red interno al terminal a través un túnel VPN desde la perspectiva de un lado de pasarela de túnel de seguridad. Según se ilustra en la Figura 2B, el método incluye:

204. La pasarela de túnel de seguridad recibe un segundo paquete de servicio enviado por el servidor de red interno, en donde una dirección origen del segundo paquete de servicio es una dirección del servidor de red interno y una dirección de destino del segundo paquete de servicio es una dirección IP virtual.

205. Encapsular el segundo paquete de servicio en un segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es una dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es una dirección IP del terminal.

206. Enviar el segundo paquete de túnel al terminal a través de un túnel entre la pasarela de túnel de seguridad y el terminal.

Las formas de realización ilustradas en la Figura 2A y la Figura 2B describen un método para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS desde la perspectiva de un lado de pasarela de túnel de seguridad. La forma de realización ilustrada en la Figura 2A describe un proceso para transmitir el paquete de servicio enviado por el terminal a través un túnel VPN al servidor en la red de infraestructura IMS desde la perspectiva de un lado de pasarela de túnel de seguridad. La forma de realización ilustrada en la Figura 2B describe un proceso de transmisión del paquete de servicio enviado por el servidor en la red de infraestructura IMS al terminal a través de un túnel VPN desde la perspectiva de un lado de pasarela de túnel de seguridad. En una aplicación práctica, el método en esta forma de realización ilustrado en la Figura 2A puede utilizarse junto con el método en la forma de realización ilustrado en la Figura 2B.

Cuando un túnel UDP VPN y un túnel SSL VPN coexisten en el túnel VPN entre el terminal y la pasarela de túnel de seguridad, los datos de servicio se transmiten a través de un túnel UDP VPN y la información de control de servicio se transmite a través del túnel SSL VPN. Más concretamente, el método incluye, además: enviar, por la pasarela de túnel de seguridad, una segunda información de control de servicio al terminal a través del túnel SSL VPN, a modo de ejemplo, después de que la pasarela de túnel de seguridad asigne la dirección IP virtual al terminal, enviar, por la pasarela de túnel de seguridad, la dirección IP virtual al terminal a través del túnel SSL VPN; o bien, recibir, por la pasarela de túnel de seguridad, una primera información de control de servicio enviada por el terminal a través del túnel SSL VPN, a modo de ejemplo, cuando el terminal necesita liberar un túnel VPN, enviar, por el terminal, información de indicación de liberación del túnel VPN a la pasarela de túnel de seguridad a través del túnel SSL VPN.

En la forma de realización de la presente invención, la pasarela de túnel de seguridad sirve como un dispositivo intermedio, desencapsula el paquete de túnel desde el terminal y lo envía al servidor de red interno, y encapsula el paquete de servicio procedente del servidor de red interno en un paquete de túnel y lo envía al terminal, con el fin de facilitar la transmisión de datos de servicio entre el terminal y el servidor en la red de infraestructura IMS. De este modo, el terminal es capaz de atravesar la red privada para comunicarse con el servidor en una red pública sin necesidad de modificar una red de empresa que cubre el terminal.

A continuación se proporcionan detalles sobre las soluciones técnicas dadas a conocer en las formas de realización de la presente invención.

La Figura 3 es un diagrama de flujo de configuración de túnel VPN en conformidad con una forma de realización de la presente invención. El proceso de configurar un túnel VPN incluye concretamente:

301. Un terminal determina si la información pertinente de un servidor proxy de capa de aplicación está configurada; si la respuesta es afirmativa, el terminal envía un mensaje de demanda de configuración de conexión proxy al servidor proxy de capa de aplicación; si la respuesta es negativa, se realiza la etapa 303.

Más concretamente, un módulo de servicio del terminal solicita una interfaz de un módulo de transmisión de túnel en una componente de capacidad de comunicaciones en el terminal, e inicia operativamente el módulo de transmisión de túnel para determinar si la información pertinente del servidor proxy de capa de aplicación está configurada o no lo está. Si el resultado de la determinación es afirmativo, se envía un mensaje de demanda de configuración de conexión proxy y si el resultado de la determinación es negativo, una demanda de configuración de túnel VPN se envía directamente a una pasarela de túnel de seguridad de VPN. La componente de capacidad de comunicaciones en las formas de realización de la presente invención incluye tres módulos: un módulo de transmisión túnel, un módulo de encriptación y desencapsulación y un módulo de convergencia de datos. Más concretamente, esta etapa se realiza por el módulo de transmisión de túnel.

La información pertinente del servidor proxy de capa de aplicación incluye un tipo, una dirección IP y un puerto del servidor proxy de capa de aplicación; y el tipo del servidor proxy de capa de aplicación incluye, a modo de ejemplo, un servidor proxy HTTP, un servidor proxy HTTPS (Protocolo de Transferencia de Hipertexto Seguro) y un servidor proxy SOCKS (Socket Secure). Antes de esta etapa, en conformidad con la condición de la red entre una red de empresa y una pasarela de VPN (es decir, la pasarela de túnel de seguridad), un usuario decide si el terminal necesita, o no, la conexión a la pasarela de VPN por intermedio del servidor proxy de capa de aplicación. Si el terminal necesita la conexión a la pasarela de VPN por intermedio del servidor proxy de capa de aplicación, es necesario configurar el tipo, la dirección IP y el puerto del servidor proxy de capa de aplicación en el terminal.

302. El servidor proxy de capa de aplicación reenvía un mensaje de respuesta de establecimiento de conexión proxy al terminal.

Más concretamente, en esta etapa, el servidor proxy de capa de aplicación puede reenviar el mensaje de respuesta de establecimiento de conexión proxy al módulo de transmisión de túnel en el terminal.

El proceso de establecer una conexión proxy entre el terminal y un tipo de servidores proxy de capa de aplicación es diferente del proceso de establecer una conexión proxy entre el terminal y otro tipo de servidores proxy de capa de aplicación, y el número de tiempos de interacción requeridos puede variar a este respecto. Sin embargo, en el momento de establecer una conexión proxy, ningún requisito especial se impone sobre un dispositivo NAT. Por lo tanto, el mensaje de demanda de establecimiento de conexión proxy y el mensaje de respuesta de establecimiento de conexión proxy pueden atravesar todos los dispositivos NAT normales.

303. El terminal envía un mensaje de demanda de establecimiento de túnel VPN a la pasarela de VPN.

Más concretamente, el módulo de transmisión de túnel en el terminal envía el mensaje de demanda de establecimiento de túnel VPN a la pasarela de VPN.

304. La pasarela de VPN reenvía un mensaje de respuesta de establecimiento de túnel VPN al terminal.

Los tipos de túneles VPN en esta forma de realización incluyen: SSL VPN, HTTP VPN y UDP VPN. Más concretamente, la pasarela de VPN reenvía el mensaje de respuesta de establecimiento de túnel VPN al módulo de transmisión de túnel en el terminal.

Cuando el terminal necesita la conexión a la pasarela de VPN por intermedio del servidor proxy de capa de aplicación, en la etapa 303, el mensaje de demanda de establecimiento de túnel VPN necesita enviarse a la pasarela de VPN por intermedio del servidor proxy de capa de aplicación. En correspondencia, y en la etapa 304, la pasarela de VPN envía el mensaje de respuesta de establecimiento de túnel VPN al terminal por intermedio del servidor proxy de capa de aplicación.

305. El terminal envía un paquete de demanda de información de configuración a través del túnel VPN a la pasarela de VPN después de que se configure satisfactoriamente el túnel VPN.

Más concretamente el módulo de transmisión de túnel en el terminal envía el paquete de demanda de información de configuración a la pasarela de VPN.

306. La pasarela de VPN reenvía una información de configuración al terminal a través del túnel VPN.

La información de configuración incluye: una dirección IP/una máscara de un servidor de red interno y un dirección IP virtual/una máscara asignada por la pasarela de VPN al terminal. La dirección IP del servidor de red interno puede ser algunas direcciones IP específicas o puede ser segmentos de direcciones IP múltiples. En este caso, el servidor de red interno existe dentro de múltiples segmentos de red.

Más concretamente, la pasarela de VPN reenvía la información de configuración al módulo de transmisión de túnel en el terminal. El módulo de transmisión de túnel realiza un análisis sintáctico de la información de configuración y envía la información de configuración al módulo de convergencia de datos. El módulo de convergencia de datos configura una dirección del terminal como una dirección IP virtual/máscara en conformidad con la información de la configuración, y configura la dirección/máscara del servidor de red interno que se comunica con el terminal y luego, notifica al módulo de transmisión de túnel que las configuraciones están completas. El módulo de transmisión de túnel envía información de indicación de realización del establecimiento de túnel al módulo de servicio en el terminal.

Las etapas 303-304 pueden ponerse en práctica concretamente en las maneras siguientes:

1. El terminal intenta primero establecer un túnel UDP: El terminal envía una demanda de configuración de túnel UDP a la pasarela de VPN, en donde el mensaje de demanda puede incluir información de identidad del terminal; la pasarela de VPN puede realizar la autenticación de la identidad del terminal mediante la interacción informativa con un servidor de autenticación, y reenviar un resultado de la autenticación al terminal; si la identidad del terminal está autorizada y una protección firewall de la red de empresa abre un puerto UDP específico, ello indica que el túnel UDP está satisfactoriamente configurado; de no ser así, ello indica que falla la configuración del túnel UDP. El túnel UDP descrito en este apartado incluye un túnel de texto simple UDP, un túnel cifrado UDP y un túnel de DTLS (Seguridad de Capa de Transporte de Datagrama) basado en UDP. Es comprensible que cuando coexisten un servidor proxy SOCKS V5, un servidor proxy HTTP y un servidor proxy HTTPS, si el túnel UDP necesita establecerse utilizando el servidor proxy de capa de aplicación, el túnel UDP necesita establecerse utilizando el servidor proxy SOCK5 VS. En comparación con un túnel HTTP y un túnel SSL, el túnel UDP puede mejorar la calidad de la voz.

2. El terminal intenta establecer un túnel SSL: el terminal envía una demanda de establecimiento de túnel SSL a la pasarela de VPN, en donde el mensaje de demanda puede incluir información de identidad; la pasarela de VPN puede realizar la autenticación de la identidad mediante la interacción informativa con un servidor de autenticación, y reenviar un reducción de la autenticación al terminal. Si la identidad del terminal es legal y la protección firewall de la red de empresa abre un puerto SSL específico, ello indica que el túnel SSL está satisfactoriamente configurado, de no ser así, ello indica que falla la configuración del túnel SSL. Después de que el túnel SSL se configure de forma satisfactoria, un túnel UDP puede configurarse adicionalmente. Más concretamente, una demanda de configuración de conexión de UDP puede enviarse primero para detectar si una ruta está habilitada entre el terminal y la pasarela de VPN. Si la ruta está habilitada, el subsistema IMS y la pasarela de VPN negocian una clave de túnel UDP a través del túnel SSL, con el fin de configurar el túnel UDP. El túnel UDP descrito en este apartado incluye un túnel de texto simple UDP, un túnel cifrado UDP y un túnel DTLS (Datagram Transport Layer Security) basado en UDP. De forma comprensible, si el túnel SSL necesita establecerse utilizando el servidor proxy de capa de aplicación, el túnel SSL necesita establecerse utilizando un servidor proxy HTTPS.

3. El terminal intenta establecer un túnel HTTP: El terminal envía una demanda de configuración de túnel HTTP a la pasarela de VPN, en donde el mensaje de demanda puede incluir información de identidad; la pasarela de VPN puede realizar la autenticación de la identidad mediante la interacción informativa con un servidor de autenticación, y reenviar un resultado de la autenticación al terminal. Si la identidad del terminal es legal y la protección firewall de la red de empresa abre un puerto HTTP, el túnel HTTP se configura de forma satisfactoria. Después de que el túnel se configure de forma satisfactoria, el subsistema IMS y la pasarela de VPN negocian una clave de túnel SSL utilizando el túnel HTTP y la clave del túnel SSL se utiliza posteriormente para la encriptación de los datos de servicio transmitidos en el túnel HTTP. De forma entendible, si el túnel HTTP necesita configurarse utilizando el servidor proxy de capa de aplicación, el túnel HTTP necesita configurarse utilizando el servidor proxy HTTP.

Conviene señalar que si un servicio en curso requiere baja seguridad pero alto rendimiento, puede establecerse un túnel UDP y si el servicio en curso requiere alta seguridad, puede establecerse un túnel SSL.

De modo opcional, terminal puede intentar primero configurar directamente una conexión de servicio con el servidor de red interno en la red de infraestructura IMS en una manera ya existente. Puesto que un servicio IMS requiere numerosos puertos UDP a abrirse en una protección firewall desarrollada en la red de empresa y la red IMS, y si el desarrollo de puertos de la protección firewall no cumple los requisitos del servicio IMS, falla el intento de establecer directamente la conexión de servicio entre el terminal y el servidor de red interno. Después de que se produzca el fallo del establecimiento de la conexión de servicio, se pueden adoptar las maneras operativas anteriores dadas a conocer en las formas de realización de la presente invención para demandar el establecimiento de un túnel UDP VPN, un túnel SSL VPN o un túnel HTTP VPN. Las maneras operativas anteriores dadas a conocer en las formas de realización de la presente invención pueden también adoptarse directamente para demandar el establecimiento del túnel UDP VPN, el túnel SSL VPN o el túnel HTTP VPN.

La Figura 4 es un diagrama de flujo de autenticación de identidad del terminal a través de un túnel VPN en conformidad con una forma de realización de la presente invención. En la forma de realización de la invención, el proceso de autenticación de identidad a través del túnel VPN incluye:

401. Un terminal envía un identificador de terminal a una pasarela de VPN a través un túnel VPN.

402. La pasarela de VPN determina, en conformidad con los registros de suscripción externos o locales y el identificador del terminal, si permitir, o no, al terminal establecer un túnel VPN y envía un resultado de la autenticación al terminal, es decir, un resultado que indica si al terminal le está permitido, o no, establecer un túnel VPN.

403. Si al terminal le está permitido establecer un túnel VPN, el terminal envía información de identidad de usuario a la pasarela de VPN a través del túnel VPN.

La información de identidad del usuario incluye un nombre de usuario y una contraseña.

404. La pasarela de VPN realiza la autenticación de la identidad del usuario en conformidad con la información de identidad del usuario y reenvía un resultado de la autenticación.

Más concretamente, la identidad del usuario puede ser objeto de autenticación en conformidad con la información del abonado localmente memorizada o la información de abonado en un servidor externo.

En la forma de realización de la invención, el terminal envía también un mensaje a través del túnel VPN para demandar a la pasarela de VPN la autenticación de un solicitador de componentes, es decir, para demandar a la pasarela de VPN que determine si al terminal le está permitido, o no, utilizar un componente de capacidad de comunicación y poner en práctica la función del componente de capacidad de comunicación, es decir, si al terminal le está permitido, o no, establecer un túnel VPN y realizar la convergencia de datos.

En la forma de realización de la invención, la entidad para realizar las etapas ilustradas en la Figura 4 es un módulo de transmisión de túnel en el terminal.

La Figura 5 es un diagrama de flujo de una forma de atravesar segura de los datos de servicio de IMS en conformidad con una forma de realización de la presente invención. En este método, un terminal se comunica con un servidor de red interno en una red de infraestructura IMS de forma proactiva. Más concretamente, el proceso para realizar una operación de atravesar con seguridad los datos de servicio de IMS incluye:

501-502. El terminal establece una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establece una dirección de destino de los datos de servicio a enviarse como una dirección del servidor de red interno, establece un puerto origen de los datos de servicio a enviarse como un puerto de servicio del terminal, establece un puerto de destino de los datos de servicio a enviarse como un puerto de servicio del servidor de red interno, obtiene un primer paquete de servicio y realiza la encriptación del primer paquete de servicio, establece una dirección IP origen del paquete encriptado como una dirección IP real del terminal, establece una dirección IP de destino del paquete encriptado como una dirección IP de una pasarela de VPN, establece un puerto origen del paquete encriptado como un puerto de túnel de terminal, establece un puerto de destino del paquete encriptado como un puerto de túnel de la pasarela de VPN y obtiene el primer paquete de túnel y luego, envía el primer paquete de túnel a la pasarela de VPN a través de un túnel entre el terminal y la pasarela de VPN.

Según se describió con anterioridad, el terminal incluye un componente de capacidad de comunicaciones y el componente de capacidad de comunicaciones e incluye tres módulos: un módulo de convergencia de datos, un módulo de encriptación y desencriptación y un módulo de transmisión de túnel. Más concretamente, el módulo de convergencia de datos incluye un primer módulo de convergencia de datos y un segundo módulo de convergencia de datos; el módulo de encriptación y desencriptación incluye un módulo de encriptación y un módulo de desencriptación; y el módulo de transmisión de túnel incluye un primer módulo de transmisión de túnel y un segundo módulo de transmisión de túnel.

El terminal puede obtener el primer paquete de servicio de dos maneras. La primera manera es: Un módulo de servicio del terminal solicita una interfaz proporcionada por el primer módulo de convergencia de datos en el terminal e inicia operativamente el primer módulo de convergencia de datos para establecer la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, establece la dirección de destino de los datos de servicio a enviarse como la dirección del servidor de red interno, establece puerto origen de los datos de servicio a enviarse como el puerto de servicio del terminal y establece el puerto de destino de los datos de servicio a enviarse como el puerto de servicio del servidor de red interno. La segunda manera consiste en: el primer módulo de convergencia de datos en el terminal captura los datos de servicio a enviarse en una interfaz de comunicaciones proporcionada por un sistema operativo, establece la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, establece la dirección de destino de los datos de servicio a enviarse como la dirección del servidor de red interno, establece puerto origen de los datos de servicio a enviarse como el puerto de servicio del terminal y establece el puerto de destino de los datos de servicio a enviarse como el puerto de servicio del servidor de red interno. La interfaz de comunicaciones proporcionada por el sistema operativo puede ser una interfaz de controlador de adaptador de red virtual o una interfaz de controlador de transporte (Transport Driver Interface, TDI).

Más adelante, el módulo de encriptación en el terminal realiza la encriptación del primer paquete de servicio; el primer módulo de transmisión de túnel en el terminal establece la dirección IP origen del paquete encriptado como la dirección IP real del terminal, establece la dirección IP de destino del paquete encriptado como la dirección IP de la pasarela de VPN, establece el puerto origen del paquete encriptado como el puerto de túnel del terminal, establece el puerto de destino del paquete encriptado como el puerto de túnel de la pasarela de VPN, y obtiene el primer paquete de túnel y luego, envía el primer paquete de túnel a la pasarela de VPN a través del túnel entre el terminal y la pasarela de VPN. Más concretamente, si el túnel VPN adoptado es un túnel HTTP VPN, el módulo de encriptación en el terminal en esta etapa utiliza una clave de túnel SSL para encriptar el primer paquete de servicio.

503-504. Después de recibir el primer paquete de túnel, la pasarela de VPN desencapsula y desencripta el primer paquete de túnel para obtener el primer paquete de servicio que tiene la dirección IP virtual como la dirección origen y tiene la dirección IP del servidor de red interno como la dirección de destino, y envía el primer paquete de servicio al servidor de red interno.

Si se adopta un túnel HTTP, la pasarela de VPN en esta etapa, utiliza la clave de túnel SSL para desencriptar el primer paquete de túnel.

505. Después de que el servidor de red interno reciba el primer paquete de servicio, si necesita reenviarse un paquete de respuesta al terminal, el servidor de red interno envía un segundo paquete de servicio a la pasarela de VPN, en donde una dirección origen del segundo paquete de servicio es la dirección IP del servidor de red interno, una dirección de destino del segundo paquete de servicio es la dirección IP virtual, un puerto origen del segundo paquete de servicio es el puerto origen del servidor de red interno y un puerto de destino del segundo paquete de servicio es el puerto de servicio del terminal.

Más concretamente, el servidor de red interno difunde un mensaje de protocolo de resolución de dirección (Address Resolution Protocol, ARP) que incluye la dirección IP virtual para consultar una pasarela de VPN a la que pertenece la dirección IP virtual. La pasarela de VPN que ha asignado, una vez, esta dirección IP virtual envía un mensaje de respuesta de ARP al servidor de red interno, en donde el mensaje de respuesta de ARP incluye una dirección MAC (control de acceso al soporte, MAC) de la pasarela de VPN. El servidor de red interno envía el segundo paquete de servicio a la pasarela de VPN en conformidad con la dirección MAC.

506-507. La pasarela de VPN realiza la encriptación del segundo paquete de servicio recibido, lo encapsula en un segundo paquete de túnel y envía el segundo paquete de túnel al terminal a través del túnel entre la pasarela de VPN y el terminal.

Si se adopta un túnel HTTP, la pasarela de VPN en esta etapa utiliza una clave de túnel SSL para la encriptación del segundo paquete de túnel.

508. Después de recibir el segundo paquete de túnel enviado por la pasarela de VPN, el terminal desencapsula y desencripta el segundo paquete de túnel recibido para obtener el segundo paquete de servicio, y extrae los datos de servicio desde el segundo paquete de servicio.

Más concretamente, el segundo módulo de transmisión de túnel en el terminal recibe el segundo paquete de túnel enviado por la pasarela de VPN, desencapsula el segundo paquete de túnel, y elimina la dirección IP origen (dirección IP de la pasarela de VPN), la dirección IP de destino (dirección IP real del terminal), el puerto origen (puerto de túnel de la pasarela de VPN) y el puerto de destino (puerto de túnel del terminal) en el segundo paquete de túnel. Más adelante, el módulo de desencriptación en el terminal desencripta el paquete desencapsulado para obtener el segundo paquete de servicio. El segundo módulo de convergencia de datos elimina la dirección IP origen (dirección IP del servidor de red interno), la dirección IP de destino (dirección IP virtual), el puerto origen (el puerto de servicio del servidor de red interno) y el puerto de destino (puerto de servicio del terminal) en el segundo paquete de servicio desencriptado y extrae los datos de servicio desde el segundo paquete de servicio.

El módulo de servicio situado en una capa superior del terminal puede obtener los datos de servicio en el segundo paquete de servicio en dos maneras. La primera manera operativa es: El módulo de servicio del terminal obtiene los datos de servicio en el segundo paquete de servicio a partir del segundo módulo de convergencia de datos en el terminal. La segunda manera consiste en: El segundo módulo de convergencia de datos en el terminal inserta los datos de servicio extraídos en la interfaz de comunicaciones proporcionada por el sistema operativo y el módulo de servicio en el terminal obtiene los datos de servicio en el segundo paquete de servicio desde la interfaz de comunicaciones proporcionada por el sistema operativo.

Los datos de servicio en la forma de realización de la presente invención se transmiten a través de un túnel VPN (a modo de ejemplo, el túnel UDP VPN anteriormente descrito, el túnel SSL VPN y el túnel HTTP VPN). Dichos túneles pueden atravesar dispositivos NAT tales como enrutadores, protecciones firewalls y conmutadores que tengan la función NAT. Por lo tanto, pueden evitarse operaciones tales como control del acceso y modificación de dirección, realizadas por los dispositivos NAT sobre los datos de servicio y el fallo de la comunicación entre el terminal y el servidor de red interno debido a operaciones realizadas por los dispositivos NAT se pueden evitar de esta manera.

Además, el túnel UDP VPN puede atravesar un servidor proxy SOCKS V5, el túnel SSL VPN puede atravesar un servidor proxy HTTPS y el túnel HTTP VPN puede atravesar un servidor proxy HTTP. Por lo tanto, cuando el terminal se comunica con el servidor de red interno, se pueden impedir operaciones tales como control del acceso y modificación de dirección, realizadas por un servidor proxy de capa de aplicación correspondiente sobre los datos de servicio y puede evitarse el fallo de la comunicación entre el terminal y el servidor de red interno debido a las operaciones realizadas por el servidor proxy de capa de aplicación. Además, en esta forma de realización, la dirección IP virtual se utiliza como una dirección de comunicación entre el terminal y el servidor de red interno y el terminal se comunica con el servidor de red interno a través de la pasarela de VPN, sin requerir que una red de empresa realice una conversión de ruta adicional o la modificación de la red de empresa.

La Figura 6 es un diagrama de flujo para permitir la seguridad en atravesar los datos de servicio de IMS en conformidad con una forma de realización de la presente invención. En este método, un servidor de red interno en una red de infraestructura IMS se comunica con un terminal de forma proactiva. Más concretamente, este proceso de atravesamiento seguro de los datos de servicio IMS incluye:

601. El servidor de red interno envía un paquete de servicio a una pasarela de VPN, en donde la dirección origen del paquete de servicio es la dirección IP del servidor de red interno, la dirección de destino del paquete de servicio es la dirección IP virtual, el puerto origen del paquete de servicio es el puerto de servicio del servidor de red interno y el puerto de destino del paquete de servicio es el puerto de servicio del terminal.

Más concretamente, cuando el servidor de red interno necesita enviar datos de servicio al terminal correspondiente a una dirección IP virtual específica, el servidor de red interno difunde un mensaje ARP que incluye la dirección IP virtual para consultar una pasarela de VPN a la que pertenece la dirección IP virtual. La pasarela de VPN que ha asignado, una vez, esta dirección IP virtual envía un mensaje de respuesta de ARP al servidor de red interno, en donde el mensaje de respuesta de ARP incluye una dirección IP de la pasarela de VPN. En conformidad con la dirección IP, el servidor de red interno envía el paquete de servicio a la pasarela de VPN, en donde la dirección origen del paquete de servicio es la dirección IP del servidor de red interno y la dirección de destino del paquete de servicio es la dirección IP virtual.

602-603. La pasarela de VPN realiza la encriptación del paquete de servicio recibido, lo encapsula en un paquete de túnel y envía el paquete de túnel al terminal a través de un túnel que ha establecido.

Para la manera de puesta en práctica específica de esta etapa, puede hacerse referencia a la descripción contenida en las etapas 506-507, por lo que no se repite aquí de nuevo.

604. Después de recibir el paquete de túnel enviado por la pasarela de VPN, el terminal desencapsula y desencripta el paquete de túnel recibido para obtener el paquete de servicio y extrae los datos de servicio a partir del paquete de servicio.

Para la manera de puesta en práctica específica de esta etapa, puede hacerse referencia a la descripción contenida en la etapa 508 por lo que no se repite aquí de nuevo.

Los datos de servicio en la forma de realización de la presente invención se transmiten a través de un túnel VPN (a modo de ejemplo, el túnel UDP VPN, el túnel SSL VPN y el túnel HTTP VPN, anteriormente descritos). Dichos túneles pueden atravesar dispositivos NAT tales como enrutadores, protecciones firewall y conmutadores que tienen la función NAT. Por lo tanto, se pueden impedir las operaciones tales como control del acceso y modificación de dirección, realizadas por los dispositivos NAT sobre los datos de servicio y se puede evitar el fallo de la comunicación entre el terminal y el servidor de red interno debido a las operaciones realizadas por los dispositivos NAT. Además, el túnel UDP VPN puede atravesar un servidor proxy SOCKS V5, el túnel SSL VPN puede atravesar un túnel proxy HTTPS y el túnel HTTP VPN puede atravesar un túnel proxy HTTP. Por lo tanto, cuando el terminal se comunica con el servidor de red interno, se pueden impedir operaciones tales como control del acceso y modificación de dirección, realizadas por un servidor proxy de capa de aplicación correspondiente sobre los datos de servicio y se puede evitar el fallo de la comunicación entre el terminal y el servidor de red interno debido a las operaciones realizadas por el servidor proxy de capa de aplicación. Además, en esta forma de realización, la dirección IP virtual se utiliza como una dirección de comunicación entre el terminal y el servidor de red interno, y el terminal se comunica con el servidor de red interno a través de la pasarela de VPN, sin requerir a una red de empresa que realice una conversión de ruta adicional o la modificación de la red de empresa.

Conviene señalar que, en la forma de realización anterior, después de que se establezca el túnel UDP VPN, el túnel SSL VPN o el túnel HTTP VPN, el terminal envía un paquete de presencia activa a la pasarela de VPN de forma periódica o envía el paquete de presencia activa a la pasarela de VPN en un tiempo establecido, con el fin de mantener el túnel que se ha configurado.

Conviene señalar que, si existen dos túneles VPN, es decir, un túnel UDP VPN y un túnel SSL VPN, entre el terminal y la pasarela de VPN, los datos de servicio pueden transmitirse a través del túnel UDP VPN. La manera de transmisión específica se describe en la forma de realización anterior. El terminal puede utilizar, además, el túnel

SSL VPN para transmitir información de control de servicio. Más concretamente, después de la encriptación de la primera información de control de servicio a enviarse, el terminal establece una dirección IP origen de la información de control encriptada como una dirección IP real del terminal, establece una dirección IP de destino de la información de control encriptada como la dirección IP de la pasarela de VPN y luego, envía la información de control encriptada a la pasarela de VPN; y después de recibir la información de control encriptada, la pasarela de VPN desencapsula y desencripta la información de control encriptada para obtener la primera información de control. De modo similar, la pasarela de VPN puede enviar una segunda información de control al terminal a través del túnel SSL VPN. De esta forma, los datos de servicio se transmiten a través del túnel UDP VPN con más baja seguridad y la información de control de servicio se transmite a través del túnel SSL VPN con más alta seguridad.

Haciendo referencia a la Figura 7, una forma de realización de la presente invención da a conocer un terminal, que incluye:

un primer módulo de convergencia de datos 701, configurado para establecer una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establece una dirección de destino de los datos de servicio a enviarse como una dirección de un servidor de red interno, y para obtener un primer paquete de servicio, en donde la dirección IP virtual es una dirección asignada por una red infraestructura IMS de subsistema multimedia IP al terminal; y

un primer módulo de transmisión de túnel 702, configurado para encapsular el primer paquete de servicio en un primer paquete de túnel, en donde una dirección IP origen del primer paquete de túnel es una dirección IP del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de una pasarela de túnel de seguridad; y para enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través de un túnel VPN de red privada virtual entre el terminal y la pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel al servidor de red interno.

Además, en otra forma de realización de la presente invención, para recibir los datos de servicio enviados por el servidor de red interno, el terminal puede incluir, además:

un segundo módulo de transmisión de túnel 703, configurado para: cuando el terminal necesita recibir los datos de servicio del servidor de red interno, recibir un segundo paquete de túnel a través del túnel y desencapsular el segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad, y una dirección IP de destino del segundo paquete de túnel es la dirección IP del terminal; y

un segundo módulo de convergencia de datos 704, configurado para extraer datos de servicio a partir de un segundo paquete de servicio obtenido como un resultado de la desencapsulación por el segundo módulo de transmisión de túnel, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor de red interno, y una dirección de destino del segundo paquete de servicio es la dirección IP virtual.

Además, en otra forma de realización de la presente invención, el terminal puede incluir, además:

un módulo de servicio 705, configurado concretamente para: cuando el terminal necesita enviar los datos de servicio, solicitando una interfaz proporcionada por el primer módulo de convergencia de datos, iniciar operativamente al primer módulo de convergencia de datos para establecer la dirección origen de los datos de servicio a enviarse como la dirección IP virtual y establecer la dirección de destino de los datos de servicio a enviarse como la dirección del servidor de red interno; y cuando el terminal necesita recibir los datos de servicio del servidor de red interno, obtener los datos de servicio en el segundo paquete de servicio a partir del segundo módulo de convergencia de datos.

Más concretamente, el primer módulo de convergencia de datos 701 está configurado para: cuando el terminal necesita enviar los datos de servicio, capturar los datos de servicio a enviarse en una interfaz de comunicaciones proporcionada por un sistema operativo, establecer la dirección origen de los datos de servicio a enviarse como la dirección IP virtual y establecer la dirección de destino de los datos de servicio a enviarse como la dirección del servidor de red interno, en donde los datos de servicio a enviarse se envían por el módulo de servicio 705 a la interfaz de comunicaciones proporcionada por el sistema operativo. De este modo, el módulo de servicio no está necesariamente acoplado estrechamente con un componente de capacidad de comunicaciones.

El segundo módulo de convergencia de datos 704 está configurado para: cuando el terminal necesita recibir los datos de servicio del servidor de red interno, extraer los datos de servicio a partir del segundo paquete de servicio, e insertar los datos de servicio extraídos en la interfaz de comunicaciones proporcionada por el sistema operativo, de modo que el módulo de servicio en el terminal obtenga los datos de servicio en el segundo paquete de servicio a partir de la interfaz de comunicaciones proporcionada por el sistema operativo.

Para garantizar la seguridad del paquete transmitido a través del túnel VPN, el terminal puede incluir, además:

un módulo de encriptación 706, configurado para utilizar una clave de túnel SSL para encriptar el primer paquete de servicio cuando el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel HTTP VPN; y

un módulo de desencriptación 707, configurado para utilizar la clave de túnel SSL para desencriptar el paquete obtenido como un resultado de desencapsulación por el segundo módulo de transmisión de túnel cuando el túnel VPN entre en el terminal y la pasarela de túnel de seguridad es el túnel HTTP VPN.

La clave de túnel SSL es previamente negociada entre el terminal y la pasarela de túnel de seguridad a través del túnel HTTP. En este caso, el primer módulo de transmisión de túnel 701 está concretamente configurado para encapsular el primer paquete de servicio, que se encripta por el módulo de encriptación 706, en el primer paquete de túnel, y para enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través del túnel VPN entre el terminal y la pasarela de túnel de seguridad. El segundo módulo de convergencia de datos 704 está concretamente configurado para extraer los datos de servicio a partir del paquete desencriptado por el módulo de desencriptación 707.

Cuando dos túneles VPN, tales como un túnel UDP VPN y un túnel SSL VPN, existen entre el terminal y la pasarela de túnel de seguridad, en otra forma de realización de la presente invención, el terminal puede utilizar el primer módulo de convergencia de datos 701, el primer módulo de transmisión de túnel 702, el segundo módulo de transmisión de túnel 703 y el segundo módulo de convergencia de datos 704 para procesar y transmitir los datos de servicio; y puede utilizar un tercer módulo de transmisión de túnel 708 y/o un cuarto módulo de transmisión de túnel 709 para procesar y transmitir información de control de servicio.

El tercer módulo de transmisión de túnel 708 está configurado para enviar una primera información de control de servicio a la pasarela de túnel de seguridad de servicio a través del túnel SSL VPN; y/o

el cuarto módulo de transmisión de túnel 709 está configurado para recibir una segunda información de control de servicio enviada por la pasarela de túnel de seguridad de servicio a través del túnel SSL VPN.

Para establecer los dos túneles VPN anteriormente mencionados, en otra forma de realización de la presente invención, se incluyen además, las unidades siguientes:

una primera unidad de configuración de túnel 710, configurada para configurar un túnel UDP VPN; y

una segunda unidad de configuración de túnel 711, configurada para negociar una clave de túnel UDP con la pasarela de túnel de seguridad a través del túnel SSL que ha sido establecido, con el fin de configurar un túnel UDP.

En la forma de realización de la presente invención, el terminal utiliza la dirección IP virtual asignada por la red de infraestructura IMS como una dirección de comunicaciones entre el terminal y el servidor de red interno, establece la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, establece la dirección de destino de los datos de servicio a enviarse como una dirección del servidor de red interno, y encapsula los datos de servicio en un paquete de túnel, y luego transmite el paquete de túnel a la pasarela de túnel de seguridad a través de un túnel entre el terminal y la pasarela de túnel de seguridad. De este modo, la pasarela de túnel de seguridad es capaz de enviar el paquete de servicio que tiene la dirección IP virtual como la dirección origen y que tiene la dirección del servidor de red interno como la dirección de destino al servidor de red interno. Cuando el terminal recibe los datos de servicio del servidor de red interno, el paquete de túnel recibido se desencapsula en un paquete de servicio que tiene la dirección del servidor de red interno como la dirección origen y tiene la dirección IP virtual como la dirección de destino. De este modo, los datos de servicio se transmiten entre el servidor de red interno y el terminal por intermedio de la pasarela de túnel de seguridad; y el terminal es capaz de atravesar una red privada para comunicarse con el servidor en una red pública sin necesidad de modificar una red de empresa que cubre el terminal.

Haciendo referencia a la Figura 8, una forma de realización de la presente invención da a conocer una pasarela de túnel de seguridad, que incluye un primer módulo de transmisión de túnel 80. El primer módulo de transmisión de túnel 80 incluye un primer módulo de recepción 801 un módulo de desencapsulación 802 y un primer módulo de envío 803.

El primer módulo de recepción 801 está configurado para recibir un primer paquete de túnel a través de un túnel entre la pasarela de túnel de seguridad y un terminal, en donde una dirección IP origen del primer paquete de túnel es una dirección IP del terminal y una dirección IP de destino del primer paquete de túnel es la dirección IP de la pasarela de túnel de seguridad.

El módulo de desencapsulación 802 está configurado para desencapsular el primer paquete de túnel; y

El primer módulo de envío 803 está configurado para enviar un primer paquete de servicio obtenido como un resultado de la desencapsulación por el módulo de desencapsulación a un servidor de red interno, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual y una dirección de destino del primer

paquete de servicio es una dirección del servidor de red interno.

Además, en otra forma de realización de la presente invención, para transmitir al terminal es paquete de servicio enviado por el servidor de red interno, un primer módulo de transmisión de túnel 90 puede incluirse además. El primer módulo de transmisión de túnel 90 incluye concretamente:

un segundo módulo de recepción 804, configurado para recibir un segundo paquete de servicio enviado por el servidor de red interno, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor de red interno, y una dirección de destino del segundo paquete de servicio es la dirección IP virtual;

un módulo de encapsulación 805, configurado para encapsular el segundo paquete de servicio en un segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es la dirección IP del terminal; y

una segunda unidad de envío 806, configurada para enviar el segundo paquete de túnel al terminal a través del túnel entre la pasarela de túnel de seguridad y el terminal.

Para garantizar la seguridad del paquete transmitido en un túnel VPN, la pasarela de túnel de seguridad puede incluir, además:

un módulo de encriptación 807, configurado para utilizar una clave de túnel SSL para encriptar el segundo paquete de servicio cuando el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel HTTP VPN; y

un módulo de desencriptación 808, configurado para utilizar la clave de túnel SSL para desencriptar el paquete obtenido como resultado de la desencapsulación por el módulo de desencriptación para obtener el primer paquete de servicio cuando el túnel VPN entre el terminal y la pasarela de túnel de seguridad es el túnel HTTP VPN.

La clave de túnel SSL es previamente negociada entre el terminal y la pasarela de túnel de seguridad a través del túnel HTTP; el módulo de encapsulación 805 está concretamente configurado para encapsular el segundo paquete de servicio encriptado en el segundo paquete de túnel; y el primer módulo de envío 803 está concretamente configurado para enviar el primer paquete de servicio desencriptado por el módulo de desencriptación 808 al servidor de red interno.

Cuando dos túneles VPN, tales como un túnel UDP VPN y un túnel SSL VPN, coexisten entre el terminal y la pasarela de túnel de seguridad, el terminal puede transmitir un paquete de servicio a través del túnel UDP VPN y transmitir información de control de servicio a través del túnel SSL VPN. Por lo tanto, en otra forma de realización de la presente invención, los siguientes módulos están incluidos además:

un tercer módulo de envío 809, configurado para enviar una segunda información de control de servicio al terminal a través del túnel SSL VPN; y un cuarto módulo de recepción 810, configurado para recibir una primera información de control de servicio enviada por el terminal a través del túnel SSL VPN.

Para establecer los dos túneles anteriormente mencionados, en otra forma de realización de la presente invención, los siguientes módulos están incluidos, además:

un primer módulo de configuración de túnel 811, configurado para establecer un túnel SSL con el terminal; y

un segundo módulo de configuración de túnel 812, configurado para negociar una clave de túnel UDP con el terminal a través del túnel SSL que ha sido configurado, con el fin de establecer un túnel UDP.

En la forma de realización de la presente invención, la pasarela de túnel de seguridad sirve como un dispositivo intermedio, desencapsula el paquete de túnel desde el terminal y lo envía al servidor de red interno y encapsula el paquete de servicio desde el servidor de red interno en un paquete de túnel y lo envía al terminal con el fin de facilitar la transmisión de datos de servicio entre el terminal y el servidor en la red de infraestructura IMS. De este modo, el terminal es capaz de atravesar una red privada para comunicarse con el servidor en una red pública sin necesidad de modificar una red de empresa que cubre el terminal.

Haciendo referencia a la Figura 9, una forma de realización de la presente invención da a conocer un sistema de red. El sistema de red incluye principalmente una pasarela de túnel de seguridad 901 y un servidor de red interno 902 descritos en las formas de realización anteriores. Las funciones y la estructura de la pasarela de túnel de seguridad son similares a las que se describen en las formas de realización anteriores, por lo que no se repiten aquí de nuevo.

El sistema de red dado a conocer en la forma de realización de la presente invención utiliza la pasarela de túnel de seguridad como un dispositivo intermedio, desencapsula un paquete de túnel desde un terminal y lo envía al servidor de red interno, y encapsula un paquete de servicio desde el servidor de red interno en un paquete de túnel y lo envía

al terminal, con el fin de facilitar la transmisión de datos de servicio entre el terminal y el servidor en una red de infraestructura IMS. De este modo, el terminal es capaz de atravesar una red privada para comunicarse con el servidor en una red pública sin necesidad de modificar una red de empresa que cubre el terminal.

Conviene señalar que, para mayor brevedad, las formas de realización de los métodos anteriores se representan como una serie de acciones. Pero los expertos en esta técnica deben apreciar que la presente invención no está limitada al orden de las acciones descritas, puesto que, en conformidad con la presente invención, algunas etapas pueden adoptar otro orden o realizarse de forma simultánea. Debe entenderse, además, por los expertos en esta técnica que las formas de realización descritas pertenecen todas ellas a formas de realización a modo de ejemplo y las acciones y módulos implicados no son necesariamente requeridas por la presente invención.

En las formas de realización anteriores, la descripción de cada forma de realización tiene su propio énfasis y algunas formas de realización pueden no estar detalladas. Puede hacerse referencia a la descripción pertinente de otras formas de realización.

Los expertos en esta técnica deben entender que la totalidad o una parte de los procesos de los métodos en las formas de realización anteriores pueden ponerse en práctica mediante un programa que proporcione instrucciones a un hardware pertinente. El programa puede memorizarse en un soporte de memorización legible por ordenador. Cuando se ejecuta el programa, se realizan los procesos de los métodos descritos en las formas de realización. El soporte de memorización puede ser un disco magnético, un disco óptico, una memoria de solamente lectura (Read-Only Memory, ROM), una memoria de acceso aleatorio (Random Access Memory, RAM) y similares.

Lo que anteriormente fue detallado son un método, un aparato y un sistema de red para permitir a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura IMS dada a conocer por la presente invención. Resulta evidente para los expertos en esta técnica que se pueden realizar modificaciones a las maneras de puesta en práctica específicas de la presente invención. En conclusión, el contenido en la especificación no debe interpretarse como una limitación para la presente invención, que se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método que permite a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura de subsistema multimedia de protocolo Internet, IMS, que comprende:

establecer (101), por el terminal, una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establecer una dirección de destino de los datos de servicio a enviarse como una dirección del servidor para obtener un primer paquete de servicio en donde el terminal está situado en la red privada, siendo la dirección IP virtual una dirección asignada por la red de infraestructura IMS al terminal;

encapsular (102), por el terminal, el primer paquete de servicio en un primer paquete de túnel, en donde una dirección IP origen del primer paquete de túnel es una dirección IP real del terminal, y una dirección IP de destino del primer paquete de túnel es una dirección IP de una pasarela de túnel de seguridad, estando la pasarela de túnel de seguridad situada en la periferia de la red de infraestructura IMS; y

enviar (103), por el terminal, el primer paquete de túnel a la pasarela de túnel de seguridad a través de un túnel de red privada virtual, VPN, entre el terminal y la pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel al servidor; estando el método caracterizado por cuanto que:

el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel de Protocolo de Datagrama de Usuario, UDP; y por cuanto que un túnel de Capa de Conexión Segura, SSL, existe entre el terminal y la pasarela de túnel de seguridad de forma adicional,

comprendiendo el método, además:

enviar, por el terminal, una primera información de control de servicio a la pasarela de túnel de seguridad a través del túnel SSL, siendo la primera información de control de servicio una demanda para asignar la dirección IP virtual;

recibir, por el terminal, una segunda información de control de servicio enviada por la pasarela de túnel de seguridad a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

2. El método según la reivindicación 1, en donde:

la etapa que consiste en establecer (101) una dirección origen de datos de servicio a enviarse como una dirección IP virtual, y en establecer una dirección de destino de los datos de servicio a enviarse como una dirección del servidor comprenden:

solicitar, por un módulo de servicio del terminal, una interfaz proporcionada por un primer módulo de convergencia de datos en el terminal, e iniciar operativamente el primer módulo de convergencia de datos para establecer la dirección origen de los datos de servicio a enviarse como la dirección IP virtual y establecer la dirección de destino de los datos de servicio a enviarse como la dirección del servidor;

o

capturar, por el primer módulo de convergencia de datos del terminal, los datos de servicio a enviarse en una interfaz de comunicaciones proporcionada por un sistema operativo, establecer la dirección origen de los datos de servicio a enviarse como la dirección IP virtual, y establecer la dirección de destino de los datos de servicio a enviarse como la dirección del servidor.

3. El método según la reivindicación 1, que comprende, además:

recibir (104), por el terminal, un segundo paquete de túnel a través del túnel cuando el terminal necesita recibir datos de servicio del servidor, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es la dirección IP real del terminal;

desencapsular (105) el segundo paquete de túnel para obtener un segundo paquete de servicio, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor y una dirección de destino del segundo paquete de servicio es la dirección IP virtual; y

obtener (106) los datos de servicio en el segundo paquete de servicio.

4. El método según la reivindicación 1, en donde:

el método comprende, además: configurar, primero, por el terminal, el túnel SSL con la pasarela de túnel de seguridad, y negociar operativamente una clave de túnel UDP con la pasarela de túnel de seguridad a través del túnel SSL que ha sido configurado, con el fin de configurar el túnel UDP.

5. Un método que permite a un terminal atravesar una red privada para comunicarse con un servidor en una red de infraestructura de Subsistema Multimedia de Protocolo Internet, IMS, que comprende:

recibir (201), por una pasarela de túnel de seguridad, un primer paquete de túnel a través de un túnel de red privada virtual, VPN, entre la pasarela de túnel de seguridad y el terminal, en donde la pasarela de túnel de seguridad está situada en la periferia de la red de infraestructura IMS, estando el terminal situado en la red privada, siendo una dirección IP origen del primer paquete de túnel una dirección IP real del terminal y siendo una dirección IP de destino del primer paquete de túnel una dirección IP de la pasarela de túnel de seguridad;

desencapsular (202), por la pasarela de túnel de seguridad, el primer paquete de túnel para obtener un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y siendo una dirección de destino del primer paquete de servicio una dirección del servidor, con la dirección IP virtual siendo una dirección asignada por la red de infraestructura IMS al terminal; y

enviar (203), por la pasarela de túnel de seguridad, el primer paquete de servicio al servidor;

estando caracterizado el método por cuanto que el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel de Protocolo de Datagrama de Usuario, UDP y por cuanto que un túnel de Capa de Conexión Segura, SSL, existe entre el terminal y la pasarela de túnel de seguridad de forma adicional,

comprendiendo el método, además:

recibir, por la pasarela de túnel de seguridad, una primera información de control de servicio enviada por el terminal a través del túnel SSL, siendo la primera información de control de servicio una demanda para asignar la dirección IP virtual;

enviar, por la pasarela de túnel de seguridad, una segunda información de control de servicio al terminal a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

6. El método según la reivindicación 5 que comprende, además:

recibir (204), por la pasarela de túnel de seguridad, un segundo paquete de servicio enviado por el servidor, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor y siendo una dirección de destino del segundo paquete de servicio la dirección IP virtual;

encapsular (205) el segundo paquete de servicio en un segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es una dirección IP de la pasarela de túnel de seguridad y siendo una dirección IP de destino del segundo paquete de túnel una dirección IP real del terminal; y

enviar (206) el segundo paquete de túnel al terminal a través del túnel entre la pasarela de túnel de seguridad y el terminal.

7. Un terminal que comprende una componente de capacidad de comunicación, en donde el terminal está situado en una red privada, comprendiendo la componente de capacidad de comunicación:

un primer módulo de convergencia de datos (701), configurado para: establecer una dirección origen de datos de servicio a enviarse como una dirección de protocolo Internet, IP, virtual, establecer una dirección de destino de los datos de servicio a enviarse como una dirección de un servidor situado en una red de infraestructura de Subsistema Multimedia de Protocolo Internet, IMS, y obtener un primer paquete de servicio, en donde la dirección IP virtual es una dirección asignada por la red de infraestructura IMS al terminal;

un primer módulo de transmisión de túnel (702) configurado para encapsular el primer paquete de servicio en un primer paquete de túnel, en donde una dirección IP origen del primer paquete de túnel es una dirección IP real del terminal y siendo una dirección IP de destino del primer paquete de túnel una dirección IP de la pasarela de túnel de seguridad, estando la pasarela de túnel de seguridad situada en la periferia de la red de infraestructura IMS; y enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través de un túnel de Red Privada Virtual, VPN, entre el terminal y la pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel al servidor;

caracterizado por cuanto que el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel de Protocolo de Datagrama de Usuario, UDP y por cuanto que el terminal comprende, además:

un tercer módulo de transmisión (708), configurado para enviar una primera información de control de servicio a la pasarela de túnel de seguridad de servicio a través de un túnel de Capa de Conexión Segura, SSL, adicional entre el terminal y la pasarela de túnel de seguridad, siendo la primera información de control de servicio una demanda para asignar la dirección IP virtual;

un cuarto módulo de transmisión de túnel (709), configurado para recibir una segunda información de control de servicio enviada por la pasarela de túnel de seguridad de servicio a través del túnel SSL, siendo la segunda información de control de servicio una dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

8. El terminal según la reivindicación 7, en donde:

un segundo módulo de transmisión de túnel (703) configurado para: cuando el terminal necesita recibir los datos de servicio del servidor, recibir un segundo paquete de túnel a través del túnel VPN, y desencapsular el segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es la dirección IP real del terminal;

un segundo módulo de convergencia de datos (704), configurado para extraer los datos de servicio desde un segundo paquete de servicio obtenido como un resultado de la desencapsulación por el segundo módulo de transmisión de túnel, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor y una dirección de destino del segundo paquete de servicio es la dirección IP virtual; o

cuando el terminal necesita recibir los datos de servicio del servidor, extraer los datos de servicio desde el segundo paquete de servicio e insertar los datos de servicio extraídos en una interfaz de comunicación proporcionada por un sistema operativo, de modo que el módulo de servicio en el terminal obtenga los datos de servicio en el segundo paquete de servicio a partir de la interfaz de comunicación proporcionada por el sistema operativo.

9. El terminal según la reivindicación 7, que comprende, además:

una primera unidad de configuración de túnel (710), configurada para configurar el túnel SSL; y

una segunda unidad de configuración de túnel (711), configurada para negociar una clave de túnel UDP con la pasarela de túnel de seguridad a través del túnel SSL que ha sido configurado, con el fin de configurar un túnel UDP.

10. Una pasarela de túnel de seguridad situada en la periferia de una red de infraestructura de Subsistema Multimedia de Protocolo Internet, IMS, comprendiendo la pasarela de túnel de seguridad:

un primer módulo de recepción (801), configurado para recibir un primer paquete de túnel a través de un túnel de red privada virtual, VPN, entre la pasarela de túnel de seguridad y un terminal, en donde el terminal está situado en una red privada, una dirección IP origen del primer paquete de túnel es una dirección IP real del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de la pasarela de túnel de seguridad;

un módulo de desencapsulación (802), configurado para desencapsular el primer paquete de túnel; y

un primer módulo de envío (803), configurado para enviar el primer paquete de servicio obtenido como un resultado de la desencapsulación por el módulo de desencapsulación a un servidor situado en la red de infraestructura IMS, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección del servidor y la dirección IP virtual es una dirección asignada por la red de infraestructura IMS al terminal;

caracterizado por cuanto que el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel de Protocolo de Datagrama de Usuario, UDP, y por cuanto que la pasarela de túnel de seguridad comprende, además:

un cuarto módulo de recepción (810), configurado para recibir una primera información de control de servicio enviada por el terminal a través de un túnel de Capa de Conexión Segura, SSL, adicional entre el terminal y la pasarela de túnel de seguridad, siendo la primera información de control de servicio una demanda para la asignación de la dirección IP virtual; y

un tercer módulo de envío (809), configurado para enviar una segunda información de control de servicio al terminal a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal.

11. La pasarela de túnel de seguridad según la reivindicación 10, que comprende, además:

un segundo módulo de recepción (804), configurado para recibir un segundo paquete de servicio enviado por el servidor, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor y una dirección

de destino del segundo paquete de servicio es la dirección IP virtual;

un módulo de encapsulación (805), configurado para encapsular el segundo paquete de servicio en un segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es la dirección IP real del terminal; y

una segunda unidad de envío (806), configurada para enviar el segundo paquete de túnel al terminal a través del túnel VPN entre la pasarela de túnel de seguridad y el terminal.

12. Un sistema de red, que comprende una pasarela de túnel de seguridad y un servidor, estando el servidor situado en una red de infraestructura de Subsistema Multimedia de Protocolo Internet, IMS, estando la pasarela de túnel de seguridad situada en la periferia de la red de infraestructura IMS, en donde

la pasarela de túnel de seguridad está configurada para:

recibir un primer paquete de túnel a través de un túnel de red privada virtual, VPN, entre la pasarela de túnel de seguridad y un terminal, en donde una dirección IP origen del primer paquete de túnel es una dirección IP real del terminal y una dirección IP de destino del primer paquete de túnel es una dirección IP de la pasarela de túnel de seguridad, estando el terminal situado en una red privada;

desencapsular el primer paquete de túnel para obtener un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección del servidor, siendo la dirección IP virtual una dirección asignada por la red de infraestructura IMS al terminal;

enviar el primer paquete de servicio al servidor; recibir un segundo paquete de servicio enviado por el servidor, en donde una dirección origen del segundo paquete de servicio es la dirección del servidor y una dirección de destino del segundo paquete de servicio es la dirección IP virtual;

encapsular el segundo paquete de servicio en un segundo paquete de túnel, en donde una dirección IP origen del segundo paquete de túnel es la dirección IP de la pasarela de túnel de seguridad y una dirección IP de destino del segundo paquete de túnel es la dirección IP real del terminal; y

enviar el segundo paquete de túnel al terminal a través del túnel VPN entre la pasarela de túnel de seguridad y el terminal;

caracterizado por cuanto que el túnel VPN entre el terminal y la pasarela de túnel de seguridad es un túnel de Protocolo de Datagrama de Usuario, UDP, y por cuanto que la pasarela de túnel de seguridad está configurada, además, para:

recibir una primera información de control de servicio enviada por el terminal a través de un túnel de Capa de Conexión Segura, SSL, adicional entre el terminal y la pasarela de túnel de seguridad, siendo la primera información de control de servicio una demanda para la asignación de la dirección IP virtual;

enviar una segunda información de control de servicio al terminal a través del túnel SSL, siendo la segunda información de control de servicio la dirección IP virtual asignada por la pasarela de túnel de seguridad al terminal, y

el servidor está configurado para recibir el primer paquete de servicio enviado por la pasarela de túnel de seguridad y para enviar el segundo paquete de servicio a la pasarela de túnel de seguridad.

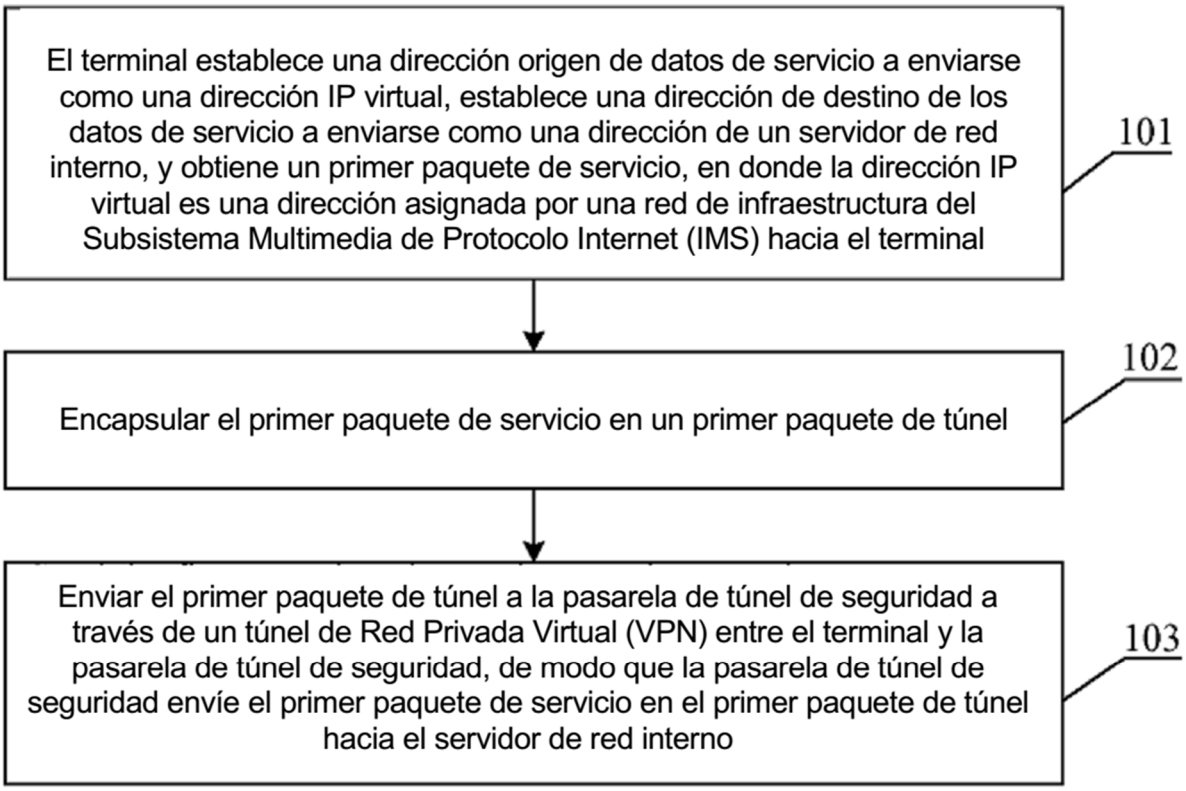
El terminal establece una dirección origen de datos de servicio a enviarse como una dirección IP virtual, establece una dirección de destino de los datos de servicio a enviarse como una dirección de un servidor de red interno, y obtiene un primer paquete de servicio, en donde la dirección IP virtual es una dirección asignada por una red de infraestructura del Subsistema Multimedia de Protocolo Internet (IMS) hacia el terminal
101
Encapsular el primer paquete de servicio en un primer paquete de túnel
102
Enviar el primer paquete de túnel a la pasarela de túnel de seguridad a través de un túnel de Red Privada Virtual (VPN) entre el terminal y la pasarela de túnel de seguridad, de modo que la pasarela de túnel de seguridad envíe el primer paquete de servicio en el primer paquete de túnel hacia el servidor de red interno
103

FIG. 1A

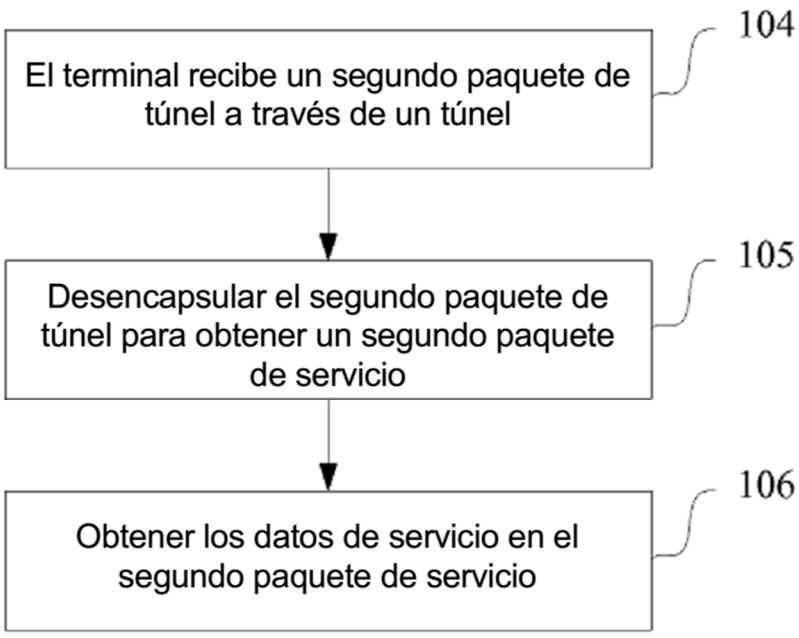
El terminal recibe un segundo paquete de túnel a través de un túnel
104
Desencapsular el segundo paquete de túnel para obtener un segundo paquete de servicio
105
Obtener los datos de servicio en el segundo paquete de servicio
106

FIG. 1B

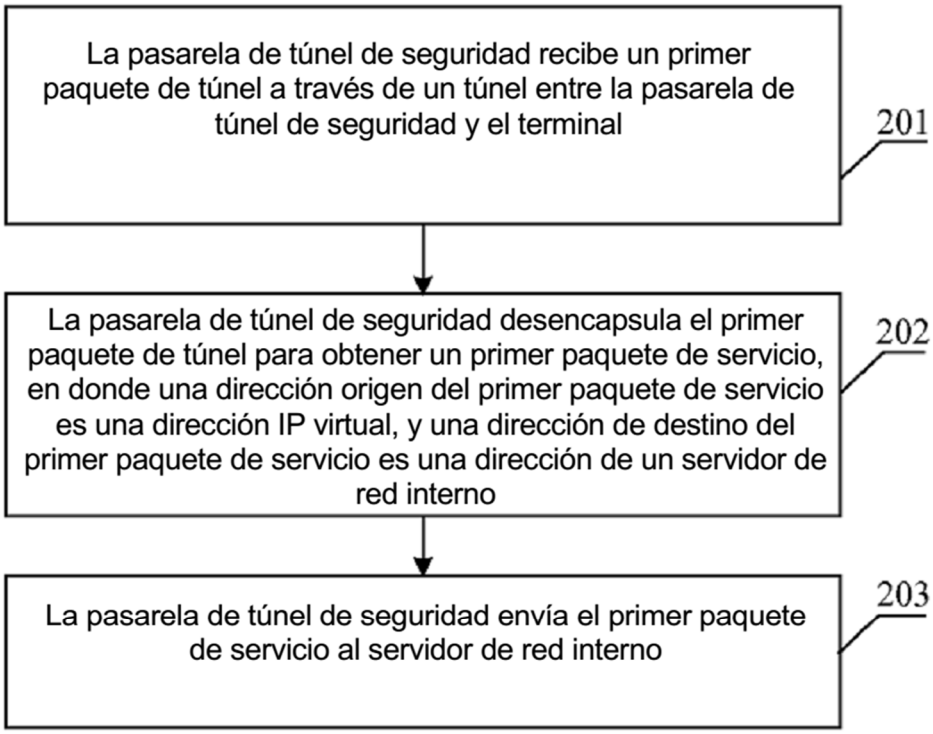
La pasarela de túnel de seguridad recibe un primer paquete de túnel a través de un túnel entre la pasarela de túnel de seguridad y el terminal
201
La pasarela de túnel de seguridad desencapsula el primer paquete de túnel para obtener un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es una dirección IP virtual, y una dirección de destino del primer paquete de servicio es una dirección de un servidor de red interno
202
La pasarela de túnel de seguridad envía el primer paquete de servicio al servidor de red interno
203

FIG. 2A

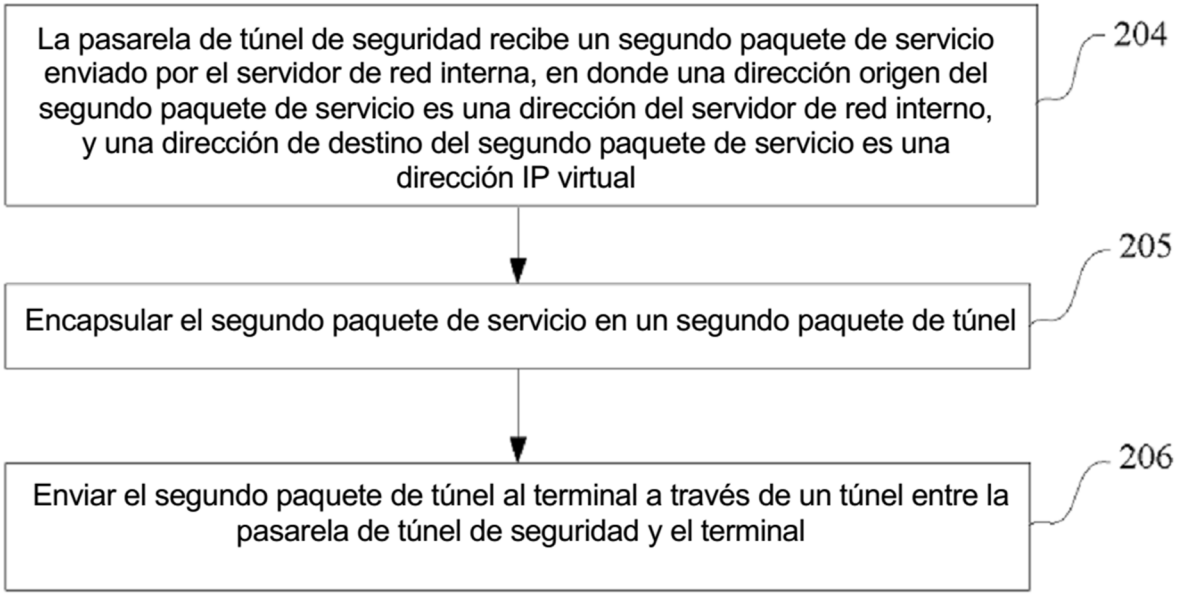
La pasarela de túnel de seguridad recibe un segundo paquete de servicio enviado por el servidor de red interna, en donde una dirección origen del segundo paquete de servicio es una dirección del servidor de red interno, y una dirección de destino del segundo paquete de servicio es una dirección IP virtual
204
Encapsular el segundo paquete de servicio en un segundo paquete de túnel
205
Enviar el segundo paquete de túnel al terminal a través de un túnel entre la pasarela de túnel de seguridad y el terminal
206

FIG. 2B

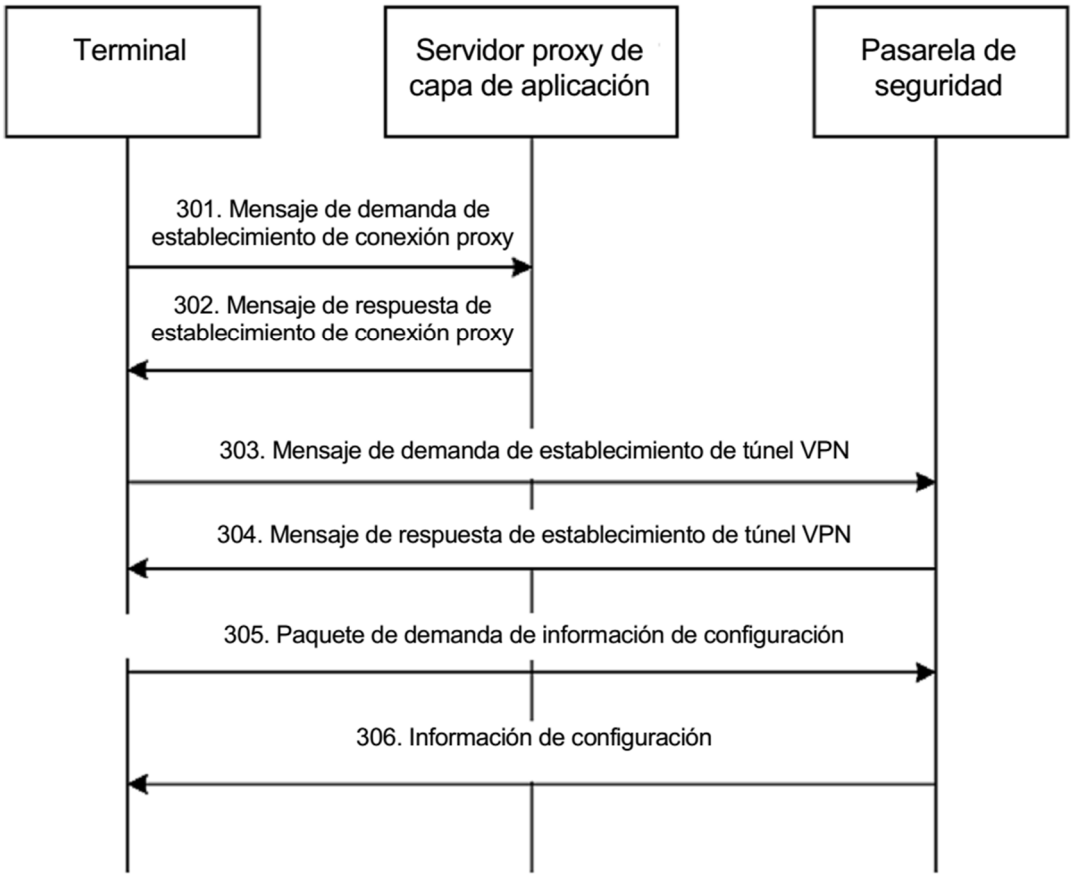
Terminal
Servidor proxy de capa de aplicación
Pasarela de seguridad
301. Mensaje de demanda de establecimiento de conexión proxy
302. Mensaje de respuesta de establecimiento de conexión proxy
303. Mensaje de demanda de establecimiento de túnel VPN
304. Mensaje de respuesta de establecimiento de túnel VPN
305. Paquete de demanda de información de configuración
306. Información de configuración

FIG. 3

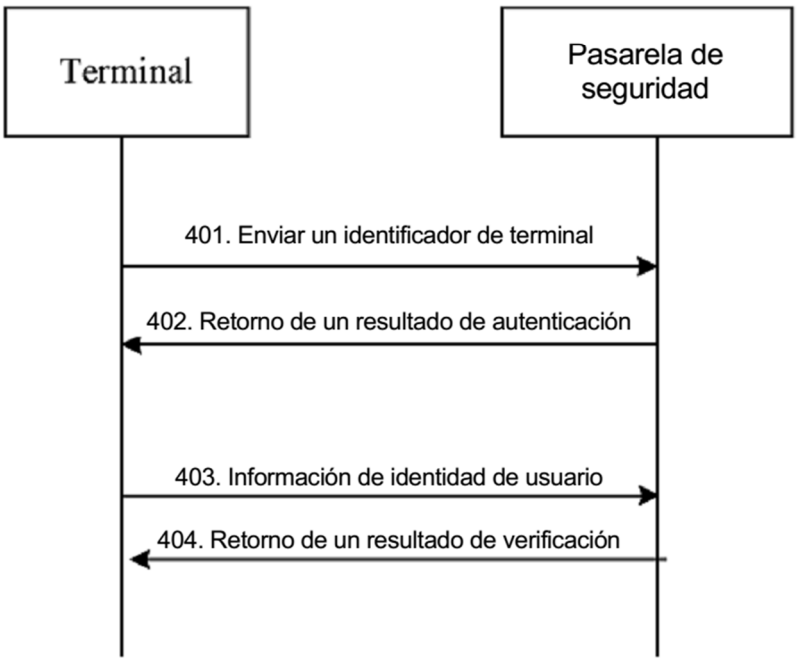
Terminal
Pasarela de seguridad
401. Enviar un identificador de terminal
402. Retorno de un resultado de autenticación
403. Información de identidad de usuario
404. Retorno de un resultado de verificación

FIG. 4

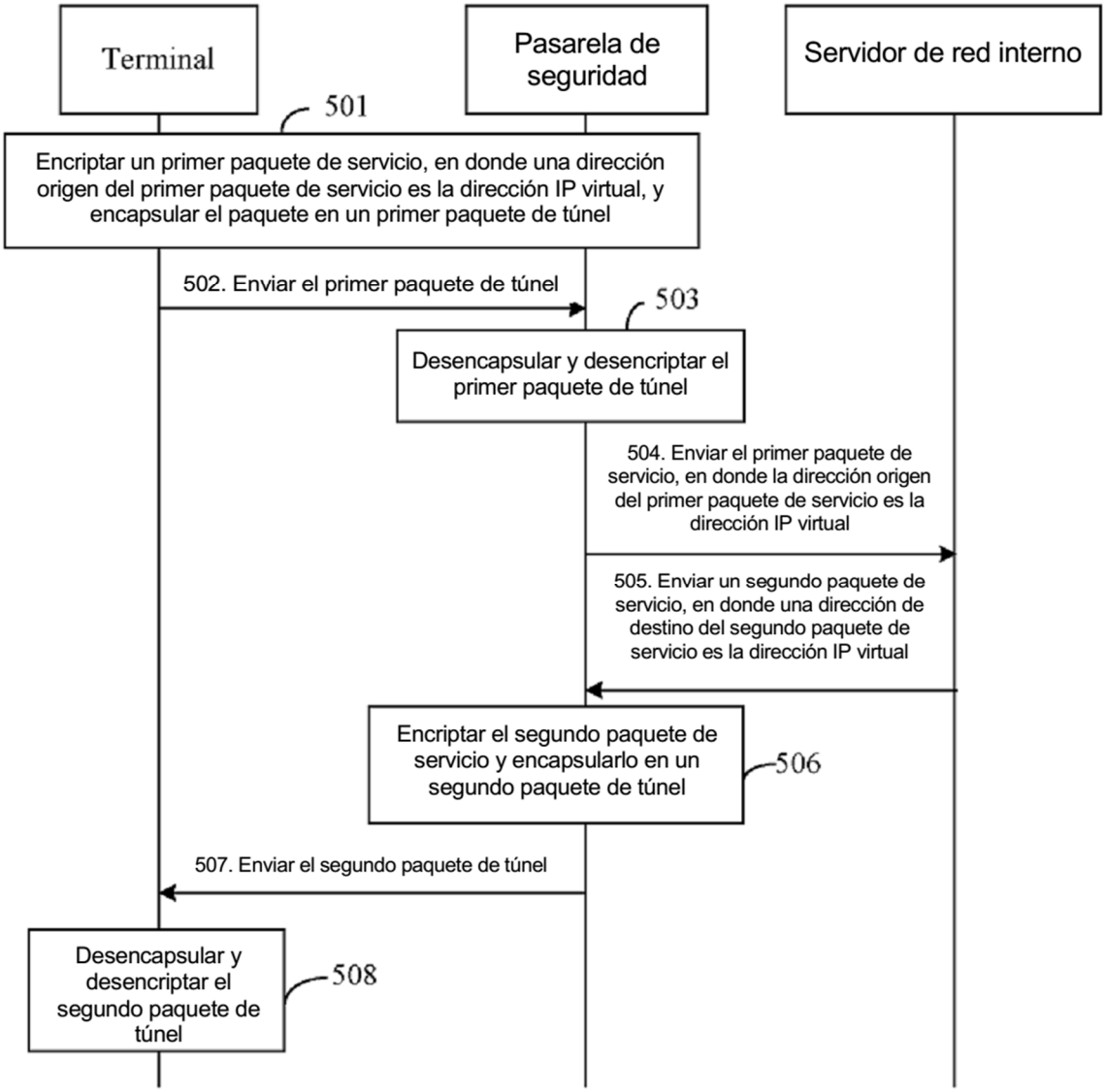
Terminal
Pasarela de seguridad
Servidor de red interno
501
Encriptar un primer paquete de servicio, en donde una dirección origen del primer paquete de servicio es la dirección IP virtual, y encapsular el paquete en un primer paquete de túnel
502. Enviar el primer paquete de túnel
503
Desencapsular y desencriptar el primer paquete de túnel
504. Enviar el primer paquete de servicio, en donde la dirección origen del primer paquete de servicio es la dirección IP virtual
505. Enviar un segundo paquete de servicio, en donde una dirección de destino del segundo paquete de servicio es la dirección IP virtual
Encriptar el segundo paquete de servicio y encapsularlo en un segundo paquete de túnel
506
507. Enviar el segundo paquete de túnel
Desencapsular y desencriptar el segundo paquete de túnel
508

FIG. 5

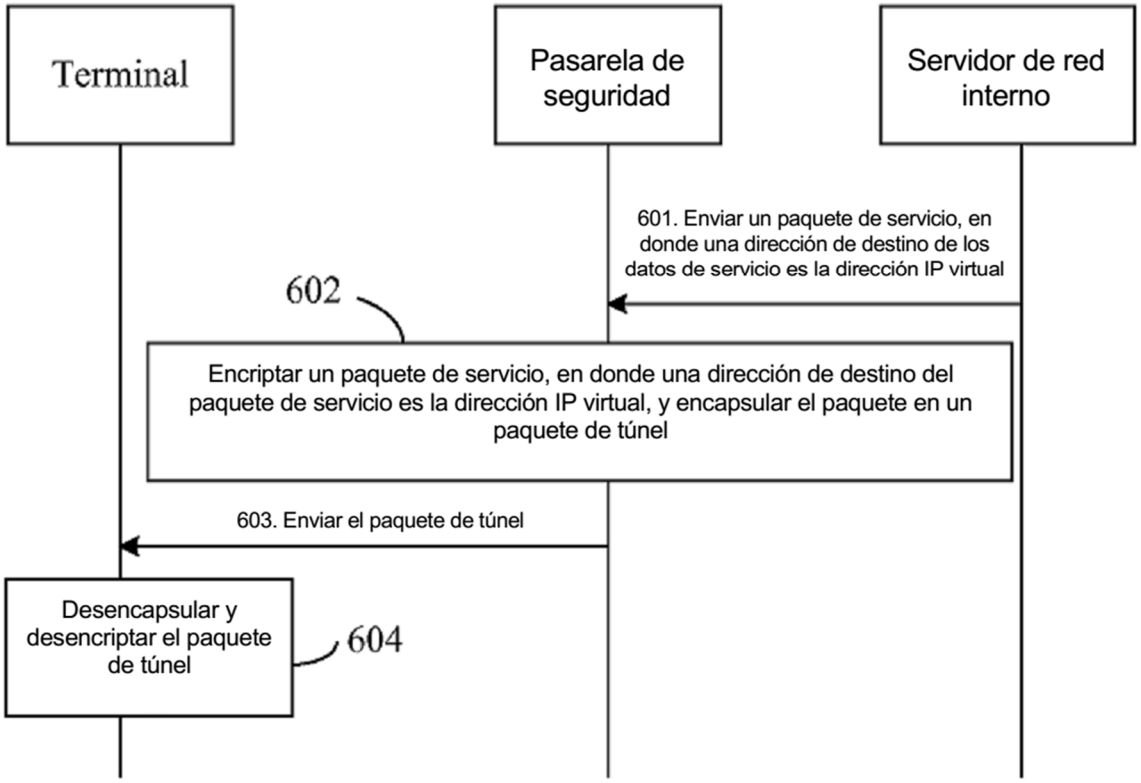
Terminal
Pasarela de seguridad
Servidor de red interno
601. Enviar un paquete de servicio, en donde una dirección de destino de los datos de servicio es la dirección IP virtual
602
Encriptar un paquete de servicio, en donde una dirección de destino del paquete de servicio es la dirección IP virtual, y encapsular el paquete en un paquete de túnel
603. Enviar el paquete de túnel
Desencapsular y desencriptar el paquete de túnel
604

FIG. 6

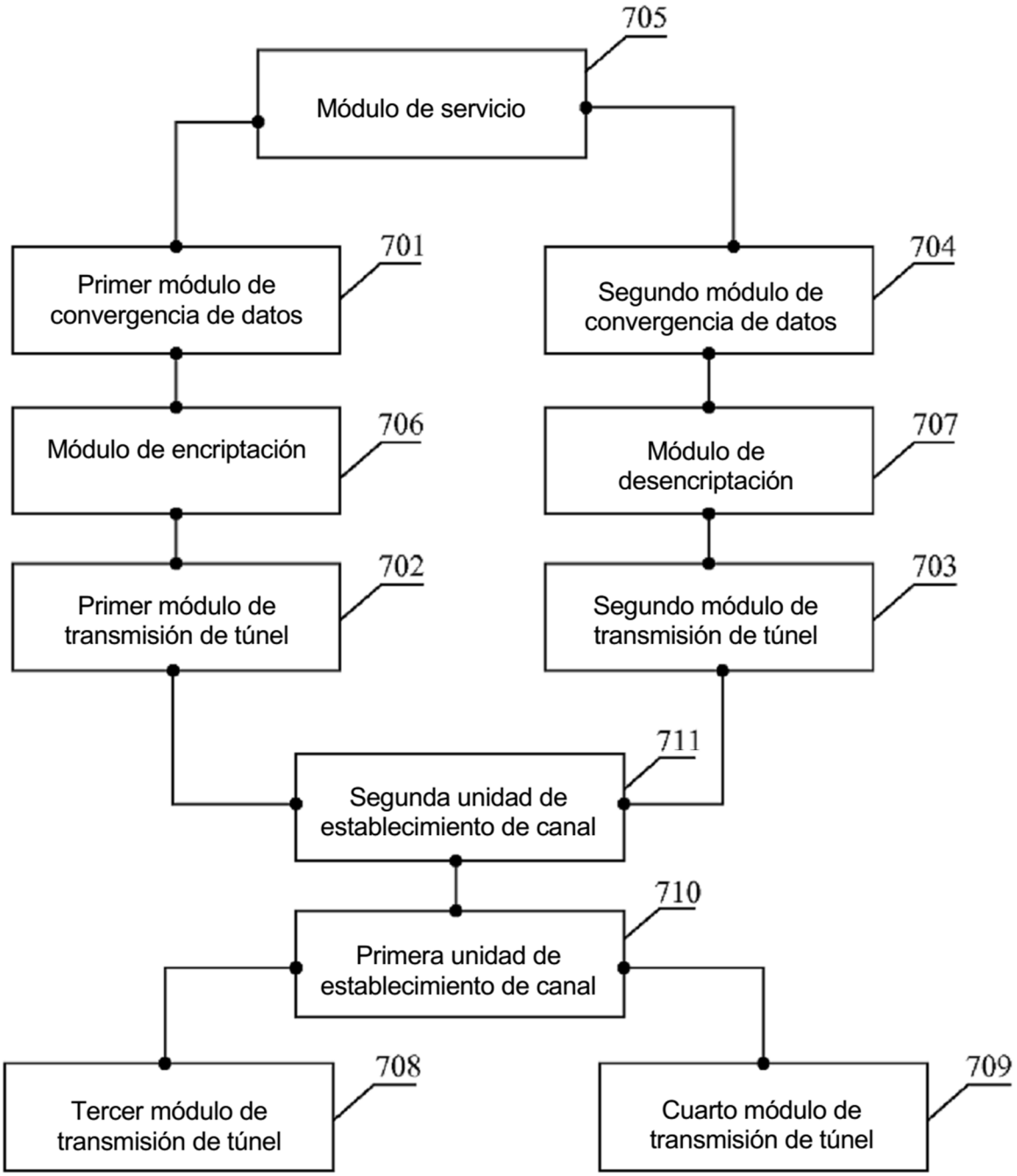
705
Módulo de servicio
701
Primer módulo de convergencia de datos
704
Segundo módulo de convergencia de datos
706
Módulo de encriptación
707
Módulo de desencriptación
702
Primer módulo de transmisión de túnel
703
Segundo módulo de transmisión de túnel
711
Segunda unidad de establecimiento de canal
710
Primera unidad de establecimiento de canal
708
Tercer módulo de transmisión de túnel
709
Cuarto módulo de transmisión de túnel

FIG. 7

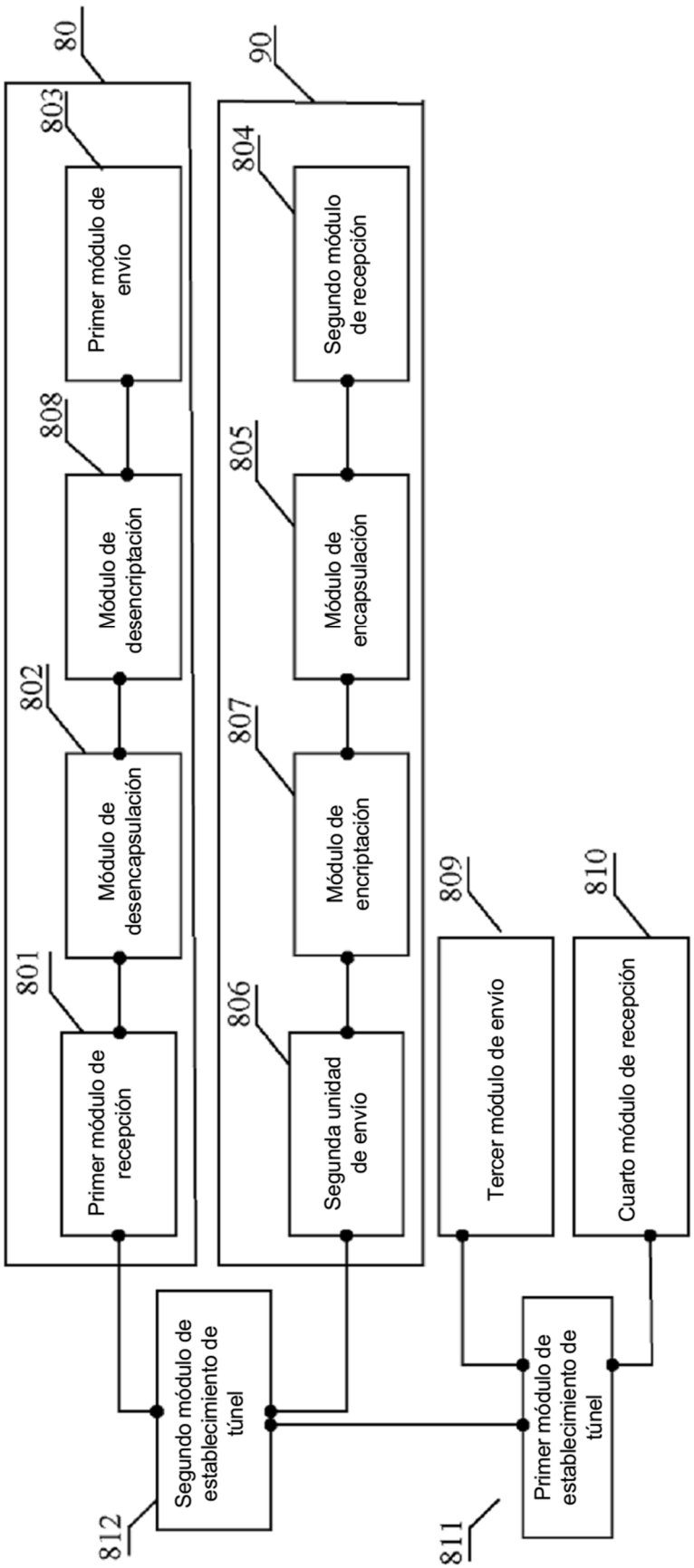
80
90
803
804
Primer módulo de envío
Segundo módulo de recepción
808
805
Módulo de desencriptación
Módulo de encapsulación
802
807
Módulo de desencapsulación
Módulo de encriptación
801
806
809
810
Primer módulo de recepción
Segunda unidad de envío
Tercer módulo de envío
Cuarto módulo de recepción
812
811
Segundo módulo de establecimiento de túnel
Primer módulo de establecimiento de túnel

FIG. 8

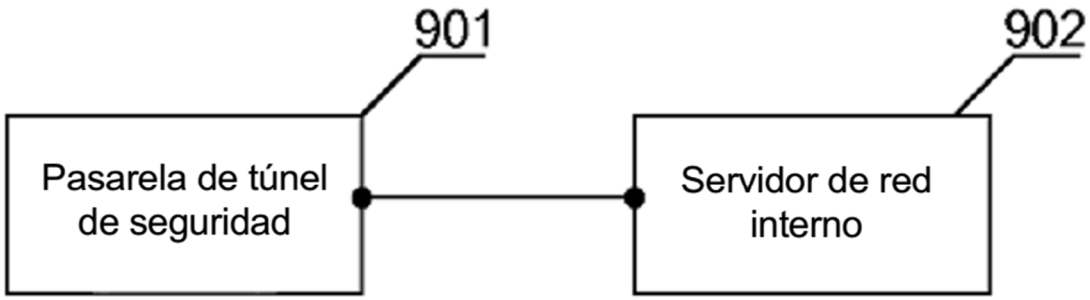
901
902
Pasarela de túnel de seguridad
Servidor de red interno

FIG. 9