(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 251**

(51) Int. CI.:

***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.12.2010 PCT/CN2010/079593**

(87) Fecha y número de publicación internacional: **04.08.2011 WO11091688**

(96) Fecha de presentación y número de la solicitud europea: **09.12.2010 E 10844465 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.04.2017 EP 2530883**

(54) Título: **Método, dispositivo y sistema de red para transmitir datagrama**

(30) Prioridad:

**27.01.2010 CN 201010104324**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**24.07.2017**

(73) Titular/es:

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

(72) Inventor/es:

**LIU, BING;**
**XU, YEJIAN;**
**XU, MENG y**
**NIE, CHENGJIAO**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Método, dispositivo y sistema de red para transmitir datagrama.

Campo de la invención

La presente invención se refiere al campo de las tecnologías de la comunicación y, en particular, a un método, aparato y sistema de red de transmisión de paquetes.

Antecedentes de la invención

En una red privada virtual (VPN, por su sigla en inglés) del protocolo de capa de zócalos seguros (SSL, por su sigla en inglés), un cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN. Por lo tanto, para los paquetes de ciertos servicios públicos, el cliente puede transmitirlos, de forma directa, a la intranet; para los paquetes de ciertos servicios protegidos, el cliente necesita transmitir los paquetes de los servicios protegidos en SSL VPN a la intranet.

La estructura topológica de la red provista en la técnica anterior se muestra en la Figura 1. Después de que el cliente inicia sesión en SSL VPN, para un paquete (es decir, un paquete de un servicio púbico) que no necesita transmitirse en SSL VPN, el cliente lo envía directamente sin añadir una dirección IP de túnel o mediante el uso de un túnel VPN. La dirección IP de origen del paquete es una dirección IP de red externa (por ejemplo, la dirección IP de red externa del paquete enviado por el Puerto B en la Figura 1 es 50.1.1.1). Para un paquete (un paquete de un servicio protegido) que necesita transmitirse en SSL VPN, el software del cliente lo envía en el túnel VPN después de añadir una dirección IP de túnel. En el presente caso, la dirección IP de origen del paquete enviado es una dirección IP de red externa (por ejemplo, la dirección IP de red externa del paquete enviado por el Puerto A en la Figura 1 es 50.1.1.1). El cortafuegos envía el paquete a SSL VPN según la dirección IP de túnel. SSL VPN asigna una dirección IP virtual (por ejemplo, 192.168.0.X en la Figura 1) a dicho cliente y cambia la dirección IP de origen (es decir, la dirección IP de red externa, por ejemplo, 50.1.1.1 en la Figura 1) a la dirección IP virtual (por ejemplo, 192.168.0.X en la Figura 1) para implementar la comunicación entre la red externa y la intranet. Por consiguiente, un segmento de la red privada correspondiente a la dirección IP virtual se asigna en la intranet y se dedica para la comunicación con la red externa en SSL VPN.

En la técnica anterior, dado que un segmento dedicado de la red privada para la comunicación con la red externa en SSL VPN necesita asignarse en la intranet, la estructura topológica de la intranet cambiará. Además, dado que una red privada se asigna en la intranet, la directiva de administración de la intranet también cambiará. Especialmente cuando múltiples clientes necesitan acceder a la intranet en SSL VPN, un gran número de direcciones IP virtuales necesitan asignarse y múltiples redes privadas necesitan asignarse en la intranet, cambiando, por consiguiente, la estructura topológica de la intranet.

El documento WO 2006/012612 A1 se refiere a un método para asegurar el acceso remoto a redes privadas, incluidas las etapas de interceptar desde una capa de enlace de datos un paquete en una primera pluralidad de paquetes destinados a un primer sistema en una red privada. Un paquete en una segunda pluralidad de paquetes transmitidos desde un segundo sistema en la red privada destinada a un sistema en una segunda red se intercepta desde la capa de enlace de datos. Una traducción de dirección de red se lleva a cabo en al menos un paquete interceptado y el al menos un paquete interceptado se transmite a un destino, que responde a una aplicación de una directiva al paquete interceptado. Un paquete interceptado se puede transmitir a una aplicación de cliente, que responde a una tabla de filtrado o tabla de enrutamiento modificado, para la transmisión a un sistema de destino, que responde a una aplicación de una directiva. La aplicación de cliente puede residir en un dispositivo informático de puerta de enlace, en un dispositivo informático del cliente o en un dispositivo periférico.

El documento US 2003/140142 A1 se refiere al acceso a dispositivos privados que se separan de la red pública por cortafuegos y NATs sin reconfigurar los cortafuegos y NATs. Un dispositivo privado que desea proveer acceso a dispositivos externos establece una tubería privada virtual hasta un concentrador seguro, el cual incluye la funcionalidad de terminar tuberías virtuales y conmutar comunicaciones entre dichas tuberías y la red pública. El concentrador seguro asigna una dirección IP secundaria al dispositivo/concentrador privado y, por consiguiente, provee al dispositivo privado una apariencia de red que ahora se encuentra más allá del cortafuegos/NAT. Los dispositivos externos acceden al dispositivo privado dirigiendo las comunicaciones a la dirección IP secundaria, cuyas comunicaciones se encaminan al concentrador seguro y se envían por túnel a través de la tubería al dispositivo privado. El dispositivo privado puede también restringir el acceso a través de una lista de control de acceso que ejecuta el concentrador seguro.

Compendio de la invención

Las realizaciones de la presente invención proveen un método, aparato y sistema de red de transmisión de paquetes, los cuales pueden transferir paquetes entre una red externa y una intranet en SSL VPN sin cambiar una estructura topológica de la intranet.

Según un aspecto, una realización de la presente invención provee un método:

un método de transmisión de paquetes aplicable a una red privada virtual, VPN, del protocolo de capa de zócalos seguros, SSL, en donde un cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN, que incluye:

recibir, por un servidor SSL VPN de la SSL VPN, mediante el uso de un túnel VPN, un paquete encriptado enviado por el cliente, donde el paquete encriptado se envía por el cliente después de que el cliente determina, según una directiva de control preestablecida, que la directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse y encripta el paquete a enviarse y la directiva de control incluye información sobre una dirección IP y un número de puerto de un servidor de intranet de la intranet;

descifrar, por el servidor SSL VPN, el paquete encriptado; y

enviar, por el servidor SSL VPN, el paquete descifrado a un servidor de intranet correspondiente, donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa.

Un método de transmisión de paquetes aplicable a una red privada virtual, VPN, del protocolo de capa de zócalos seguros, SSL, en donde un cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN, que incluye:

determinar, por un cliente, si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y un número de puerto de destino de un paquete a enviarse, donde la directiva de control preestablecida incluye información sobre una dirección IP y un número de puerto de un servidor de intranet de la intranet;

cuando la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar, por el cliente, mediante el uso de un túnel VPN, el paquete a enviarse después de la encriptación a un servidor SSL VPN de la SSL VPN; y

cuando la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y el número de puerto de destino del paquete a enviarse, enviar, por el cliente, el paquete a enviarse, donde el paquete a enviarse se envía sin usar el túnel VPN.

Un servidor SSL VPN de SSL VPN, que incluye:

un medio configurado para transferir una directiva de control a un cliente cuando el cliente inicia sesión en la SSL VPN, en donde el cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN, la directiva de control comprende información sobre una dirección IP y un número de puerto de un servidor de intranet de la intranet;

una primera unidad de recepción, configurada para recibir, mediante el uso de un túnel VPN, un paquete encriptado enviado por el cliente;

una unidad de descifrado, configurada para descifrar el paquete encriptado; y

una primera unidad de envío, configurada para enviar el paquete descifrado al servidor de intranet, donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa, una dirección IP de destino del paquete descifrado es la dirección IP del servidor de intranet y un número de puerto de destino del paquete descifrado es el número de puerto de un servidor de intranet;

en donde el servidor SSL VPN además comprende:

una segunda unidad de recepción, configurada para recibir un paquete de respuesta del servidor de intranet;

una unidad de determinación, configurada para determinar si una directiva de control preestablecida comprende una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta;

una primera unidad de encriptación, configurada para: cuando un resultado de la decisión de la unidad de determinación es que la directiva de política de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, encriptar el paquete de respuesta; y

una segunda unidad de envío, configurada para: cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida no comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, transmitir, de forma transparente, el paquete de respuesta al cliente; y cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, enviar el paquete de respuesta encriptado por la primera unidad de encriptación al cliente.

Un cliente, que incluye:

una unidad de determinación, configurada para determinar si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse, donde la directiva de control preestablecida incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor SSL VPN;

una unidad de encriptación, configurada para: cuando un resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, encriptar el paquete a enviarse; y

una unidad de envío, configurada para: cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar, mediante el uso de un túnel VPN, el paquete encriptado por la unidad de encriptación; y cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar directamente el paquete a enviarse, donde el paquete a enviarse se envía sin usar el túnel VPN.

Un sistema de red, que incluye: el servidor SSL VPN y el cliente.

Según la presente realización, la dirección IP y el número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet correspondiente al servidor SSL VPN y el paquete del cliente recibido por el servidor SSL VPN desde el túnel VPN se envía por el cliente después de que el cliente determina que la directiva de control incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse y encripta el paquete a enviarse. Dado que el servidor SSL VPN puede aprender el segmento de red del servidor de intranet que procesa dicho paquete (en este momento, el paquete es un paquete de un servicio protegido) según la dirección IP de destino y el número de puerto de destino del paquete, la dirección IP virtual no necesita asignarse, pero la dirección IP de origen del paquete permanece sin cambios, es decir, la dirección IP de origen del paquete es aún una dirección IP de red externa. Como tal, el segmento dedicado de red privada para la comunicación con la red externa en SSL VPN no necesita asignarse en el servidor de intranet. Por lo tanto, la topología de la red no necesita cambiarse.

Breve descripción de los dibujos

Con el fin de ilustrar las soluciones técnicas en las realizaciones de la presente invención de forma más clara, a continuación se describen brevemente los dibujos anexos requeridos para describir las realizaciones de la presente invención. De manera aparente, los dibujos anexos en la siguiente descripción muestran simplemente algunas realizaciones de la presente invención y las personas con experiencia ordinaria en la técnica pueden derivar otros dibujos a partir de dichos dibujos anexos sin esfuerzos creativos.

La Figura 1 es un diagrama esquemático de una transmisión de paquete en la técnica anterior;

la Figura 2 es un diagrama de flujo de un método de transmisión de paquetes según una realización de la presente invención;

la Figura 3 es un diagrama de flujo de un método de transmisión de paquetes según otra realización de la presente invención;

la Figura 4A es un diagrama de flujo de un método de transmisión de paquetes según otra realización de la presente invención;

la Figura 4B es un diagrama esquemático de una transmisión de paquetes según otra realización de la presente invención;

la Figura 5A, que se muestra como las Figuras 5A-A y 5A-B, es un diagrama de flujo de un método de transmisión de paquetes según otra realización de la presente invención;

la Figura 5B es un diagrama esquemático de una transmisión de paquetes según otra realización de la presente invención;

la Figura 6A es un diagrama esquemático estructural de un servidor SSL VPN según una realización de la presente invención;

la Figura 6B es un diagrama esquemático estructural de otro servidor SSL VPN según una realización de la presente invención;

la Figura 7 es un diagrama esquemático estructural de un cliente según una realización de la presente invención;

la Figura 8A es un diagrama esquemático estructural de un sistema de red según una realización de la presente invención; y

la Figura 8B es un diagrama esquemático estructural de un sistema de red según otra realización de la presente invención.

Descripción detallada de las realizaciones

A continuación se describen, de forma clara y completa, las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos anexos en las realizaciones de la presente invención.

La Figura 2 es un diagrama de flujo de un método de transmisión de paquetes según una realización de la presente invención. El método incluye lo siguiente:

201: recibir, mediante el uso de un túnel VPN, un paquete encriptado enviado por un cliente.

El paquete encriptado se envía por el cliente después de que el cliente determina, según una directiva de control preestablecida, que la directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse y encripta el paquete a enviarse, la directiva de control incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor de red privada virtual con protocolo de capa de zócalos seguros SSL VPN y la dirección IP y el número de puerto del servidor de intranet pueden identificar un segmento de red específico del servidor de intranet.

202: descifrar el paquete encriptado.

203: enviar el paquete descifrado a un servidor de intranet correspondiente.

El paquete descifrado incluye la dirección IP de destino y el número de puerto de destino y una dirección IP de origen del paquete descifrado es una dirección IP de red externa.

El sujeto de ejecución de cada etapa en el método puede ser un servidor SSL VPN.

El servidor SSL VPN en la presente realización se puede conectar a un dispositivo de enrutamiento y el servidor de intranet o el servidor SSL VPN se pueden conectar solamente al dispositivo de enrutamiento pero no al servidor de intranet. El dispositivo de enrutamiento puede ser un cortafuegos o un enrutador.

Cuando el servidor SSL VPN se conecta al dispositivo de enrutamiento y al servidor de intranet, un paquete enviado por el cliente (incluido un paquete enviado por el cliente mediante el uso del túnel VPN y un paquete enviado directamente sin usar el túnel VPN) se intercepta por el dispositivo de enrutamiento. El dispositivo de enrutamiento transmite, de forma transparente, el paquete interceptado al servidor SSL VPN. El servidor SSL VPN transmite, de forma transparente, el paquete recibido que se envía sin usar el túnel VPN a un servidor de intranet correspondiente. Asimismo, el servidor SSL VPN puede además recibir un paquete de respuesta del servidor de intranet, enviar el paquete de respuesta después de la encriptación al cliente mediante el uso del túnel VPN cuando la directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta y transmitir, de forma transparente, el paquete de respuesta al cliente cuando la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta.

Cuando el servidor SSL VPN se conecta al dispositivo de enrutamiento únicamente pero no al servidor de intranet, un paquete descifrado enviado por SSL VPN al servidor de intranet se intercepta por el dispositivo de enrutamiento. El dispositivo de enrutamiento envía el paquete interceptado al servidor de intranet. El servidor SSL VPN recibe además un paquete de respuesta del servidor de intranet reenviado por el dispositivo de enrutamiento y envía el paquete de respuesta después de la encriptación al cliente mediante el uso del túnel VPN. El paquete de respuesta se reenvía al servidor SSL VPN después de que el dispositivo de enrutamiento determina que la directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta.

Según la presente realización, la dirección IP y el número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet correspondiente al servidor SSL VPN y el paquete del cliente recibido por el servidor SSL VPN del túnel VPN se envía por el cliente después de que el cliente determina que la directiva de control incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse y encripta el paquete a enviarse. Dado que el servidor SSL VPN puede aprender el segmento de red del servidor de intranet que procesa dicho paquete (en este momento, el paquete es un paquete de un servicio protegido) según la dirección IP de destino y el número de puerto de destino del paquete, la dirección IP virtual no necesita asignarse, pero la dirección IP de origen del paquete permanece sin cambios, es decir, la dirección IP de origen del paquete es aún una dirección IP de red externa. Como tal, el segmento dedicado de red privada para la comunicación con la red externa en SSL VPN necesita asignarse en el servidor de intranet. Por lo tanto, la topología de la red no necesita cambiarse.

La Figura 3 es un diagrama de flujo de un método de transmisión de paquetes según una realización de la presente invención. El método incluye lo siguiente:

301: determinar si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse, donde la directiva de control preestablecida incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor SSL VPN; cuando la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, ejecutar la etapa 302; y cuando la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, ejecutar la etapa 303.

El sujeto de ejecución de cada etapa en la presente realización puede ser un cliente. La directiva de control del cliente se descarga por el cliente desde el servidor SSL VPN cuando el cliente inicia sesión en SSL VPN. La directiva de control en la presente realización incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor SSL VPN, y la dirección IP y el número de puerto del servidor de intranet pueden identificar un segmento de red específico del servidor de intranet.

302: enviar, mediante el uso de un túnel VPN, el paquete a enviarse después de la encriptación. El procedimiento finaliza.

303: enviar el paquete a enviarse, donde el paquete a enviarse se envía sin usar el túnel VPN.

El cliente determina si la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse. La dirección IP y el

número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet que puede intercambiar paquetes con el servidor SSL VPN. Por lo tanto, si un resultado de la decisión es no, ello indica que el paquete a enviarse es un paquete de un servicio público. Dado que un paquete de un servicio público no necesita enviarse en SSL VPN, el paquete se puede enviar directamente. En el presente caso, el paquete se envía sin usar el túnel VPN. Si el resultado de la decisión es sí, ello indica que el paquete a enviarse es un paquete de un servicio protegido. Dado que los paquetes de servicios protegidos necesitan transmitirse en SSL VPN, el paquete a enviarse se encripta y encapsula en una dirección IP de túnel antes de enviarse mediante el uso del túnel VPN.

Según la presente realización, la dirección IP y el número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet correspondiente al servidor SSL VPN y el cliente envía, mediante el uso del túnel VPN, el paquete a enviarse después de determinar que la directiva de control incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse y de encriptar el paquete de modo que el servidor SSL VPN puede aprender el segmento de red del servidor de intranet que procesa el paquete según la dirección IP de destino y el número de puerto de destino del paquete. Por lo tanto, la dirección IP virtual no necesita asignarse, pero la dirección IP de origen del paquete permanece sin cambios, es decir, la dirección IP de origen del paquete es aún una dirección IP de red externa. Como tal, el segmento dedicado de red privada para la comunicación con la red externa en SSL VPN no necesita asignarse en el servidor de intranet. Por lo tanto, la topología de la red no necesita cambiarse.

Con el fin de ilustrar las soluciones técnicas provistas en la presente invención de forma más clara, las siguientes dos realizaciones describen las soluciones técnicas provistas en la presente invención en detalle.

Como se muestra en la Figura 4A y la Figura 4B, una realización de la presente invención provee un método de transmisión de paquetes. En la presente realización, SSL VPN se conecta a un dispositivo de enrutamiento y a un servidor de intranet y el dispositivo de enrutamiento es un cortafuegos. El método de transmisión de paquetes incluye lo siguiente:

401A: un cliente determina si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse; si no es así, envía directamente el paquete (es preciso remitirse al paquete enviado desde el Puerto B en la Figura 4B) al servidor de intranet sin usar un túnel VPN; y si es así, encripta el paquete a enviarse (es preciso remitirse al paquete enviado desde el Puerto A en la Figura 4B), encapsula una dirección IP de túnel y luego envía, mediante el uso del túnel VPN, el paquete a un servidor SSL VPN.

Se debe notar que, antes de esta etapa, cuando el cliente inicia sesión en SSL VPN, el cliente necesita descargar la directiva de control del servidor SSL VPN.

402A: un cortafuegos intercepta un paquete del cliente y envía el paquete interceptado al servidor SSL VPN.

403A: el servidor SSL VPN descifra el paquete recibido del túnel VPN, envía el paquete descifrado al servidor de intranet, donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa, almacena una dirección IP de destino y un número de puerto de destino del paquete descifrado y una relación de mapeo entre la dirección IP de destino y el número de puerto de destino y el túnel VPN (el túnel VPN es el túnel VPN para recibir el paquete) y transmite, de forma directa y transparente, un paquete recibido sin usar el túnel VPN al servidor de intranet.

404A: el servidor de intranet recibe el paquete producido por el servidor SSL VPN y devuelve un paquete de respuesta en respuesta al paquete recibido, donde una dirección IP de origen y un número de puerto de origen del paquete de respuesta son la dirección IP de destino y el número de puerto de destino del paquete recibido, respectivamente.

405A: el servidor SSL VPN recibe el paquete de respuesta del servidor de intranet y determina si la directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta; si es así, determina un túnel VPN correspondiente a la dirección IP de origen y al número de puerto de origen según la relación de mapeo almacenada en la etapa 403A y encripta el paquete de respuesta (por ejemplo, el paquete enviado desde el Puerto 1 en la Figura 4B) antes de enviar, mediante el uso del túnel VPN, el paquete al cliente; si no es así, transmite, de forma directa y transparente, el paquete de respuesta (por ejemplo, el paquete enviado desde el Puerto 2 en la Figura 4B).

En la presente etapa, el servidor SSL VPN determina si la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta. Si la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a

la dirección IP de origen y al número de puerto de origen del paquete de respuesta, ello indica que el paquete de respuesta es un paquete de un servicio público. Dado que un paquete de un servicio público no necesita enviarse en SSL VPN, el paquete se puede transmitir de forma directa y transparente. En el presente caso, el paquete de respuesta se transmite de forma directa y transparente. Si la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, ello indica que el paquete de respuesta es un paquete de un servicio protegido. Dado que los paquetes de servicios protegidos necesitan transmitirse mediante el uso del túnel VPN, el paquete del servicio protegido se encripta y encapsula en una dirección IP de túnel antes de enviarse mediante el uso del túnel VPN.

406A: el cortafuegos intercepta un paquete del servidor SSL VPN y envía el paquete interceptado al cliente.

Según la presente realización, el cliente determina si el paquete a enviarse se envía mediante el uso del túnel VPN determinando si la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse. El servidor SSL VPN determina si el paquete de respuesta se envía mediante el uso del túnel VPN determinando si la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta. Dado que tanto el paquete a enviarse como el paquete de respuesta incluyen la dirección IP y el número de puerto del servidor de intranet, lo cual permite al servidor SSL VPN aprender el segmento de red del servidor de intranet que intercambia paquetes consigo mismo, el servidor SSL VPN no necesita convertir la dirección IP cuando el cliente accede al servidor de intranet en SSL VPN, implementando la función de proveer protección de acceso SSL VPN sin cambiar la topología de la red del servidor de intranet.

Como se muestra en la Figura 5A y la Figura 5B, otra realización de la presente invención provee un método de transmisión de paquetes. En la presente realización, SSL VPN se conecta a un dispositivo de enrutamiento únicamente pero no a un servidor de intranet. El dispositivo de enrutamiento en la presente realización es un cortafuegos. El método de transmisión de paquetes incluye, específicamente, lo siguiente:

501A: un cliente determina si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse; si no es así, envía directamente el paquete (es preciso remitirse al paquete enviado desde el Puerto B en la Figura 5B) al servidor de intranet sin usar un túnel VPN; y, si es así, encripta el paquete a enviarse (es preciso remitirse al paquete enviado desde el Puerto A en la Figura 4B), encapsula una dirección IP de túnel y luego envía, mediante el uso del túnel VPN, el paquete a un servidor SSL VPN y es preciso dirigirse a 502A.

Se debe notar que, antes de esta etapa, cuando inicia sesión en SSL VPN, el cliente necesita descargar la directiva de control del servidor SSL VPN.

502A: el cortafuegos intercepta el paquete del cliente. Cuando se determina que el paquete interceptado se encapsula en una dirección IP de túnel (es decir, el paquete interceptado del cliente es un paquete enviado por el cliente mediante el uso del túnel VPN), es preciso dirigirse a 503A; cuando se determina que el paquete interceptado no se encapsula en una dirección IP de túnel (es decir, el paquete interceptado del cliente es un paquete enviado por el cliente sin usar el túnel VPN), es preciso dirigirse a 506A.

503A: el cortafuegos envía el paquete interceptado al servidor SSL VPN. Es preciso dirigirse a 504A.

504A: el servidor SSL VPN envía el paquete recibido desde el túnel VPN después del descifrado, donde la dirección IP de origen del paquete descifrado es una dirección IP de red externa y almacena una relación de mapeo entre una dirección IP de destino y un número de puerto de destino del paquete descifrado y el túnel VPN (el túnel VPN es el túnel VPN para recibir el paquete). Es preciso dirigirse a 505A.

505A: el cortafuegos intercepta el paquete enviado por el servidor SSL VPN y lo envía al servidor de intranet. Es preciso dirigirse a 507A.

506A: el cortafuegos envía directamente el paquete interceptado al servidor de intranet. Es preciso dirigirse a 507A.

507A: el servidor de intranet recibe el paquete del cliente y envía un paquete de respuesta en respuesta al paquete recibido, donde la dirección IP de origen y un número de puerto de origen del paquete de respuesta son la dirección IP de destino y el número de puerto de destino del paquete recibido, respectivamente. Es preciso dirigirse a 508A.

508A: el cortafuegos intercepta el paquete de respuesta del servidor de intranet y determina si la directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a la dirección IP de origen y al

número de puerto de origen del paquete de respuesta. Si es así, es preciso dirigirse a 509A; de lo contrario, es preciso dirigirse a 512A.

509A: el cortafuegos envía el paquete de respuesta al servidor SSL VPN. Es preciso dirigirse a 510A.

Para más detalles, es preciso remitirse al paquete enviado desde el Puerto 1 en la Figura 5B.

510A: el servidor SSL VPN determina un túnel VPN correspondiente a la dirección IP de origen y al número de puerto de origen según la dirección IP de origen y el número de puerto de origen del paquete de respuesta y la relación de mapeo almacenada, encripta el paquete de respuesta y lo encapsula con una dirección IP de túnel antes de enviar el paquete al cliente mediante el uso del túnel VPN determinado. Es preciso dirigirse a 511A.

511A: el cortafuegos intercepta un paquete de respuesta encriptado enviado por el servidor SSL VPN y envía el paquete interceptado al cliente. El procedimiento finaliza.

512A: el cortafuegos transmite, de forma transparente, el paquete de respuesta del servidor de intranet al cliente.

Para más detalles, es preciso remitirse al paquete enviado desde el Puerto 2 en la Figura 5B.

Según la presente realización, el cliente determina si el paquete a enviarse se envía mediante el uso del túnel VPN determinando si la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse. El cortafuegos determina si el paquete de respuesta se envía mediante el uso del túnel VPN determinando si la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta. Dado que tanto el paquete a enviarse como el paquete de respuesta incluyen la dirección IP y el número de puerto del servidor de intranet, lo cual permite al servidor SSL VPN aprender el segmento de red del servidor de intranet que intercambia paquetes consigo mismo, el servidor SSL VPN no necesita convertir la dirección IP cuando el cliente accede al servidor de intranet en SSL VPN, implementando la función de proveer protección de acceso SSL VPN sin cambiar la topología de la red del servidor de intranet. Además, según el presente método, el servidor SSL VPN se despliega en forma de desvío detrás del cortafuegos, de modo que el cortafuegos puede todavía enviar, de forma directa, paquetes de servicios públicos al servidor de intranet cuando el servidor SSL VPN es anormal y evitar así que dichos servicios públicos se interrumpan.

Como se muestra en la Figura 6A y la Figura 6B, una realización de la presente invención provee un servidor SSL VPN, donde el servidor SSL VPN puede incluir:

una primera unidad de recepción 601, configurada para recibir, mediante el uso de un túnel VPN, un paquete encriptado enviado por un cliente;

el paquete encriptado se envía por el cliente después de que el cliente determina, según una directiva de control preestablecida, que la directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse y encripta el paquete a enviarse, y la directiva de control incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor de red privada virtual con protocolo de capa de zócalos seguros SSL VPN;

una unidad de descifrado 602, configurada para descifrar el paquete encriptado; y

una primera unidad de envío 603, configurada para enviar el paquete descifrado a un servidor de intranet correspondiente, donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa.

De manera específica, la primera unidad de recepción 601 se configura además para recibir, sin usar el túnel VPN, un paquete enviado por un cliente; la primera unidad de envío 603 se configura además para transmitir, de forma transparente, el paquete recibido sin usar el túnel VPN a un servidor de intranet correspondiente.

Asimismo, en un caso, como se muestra en la Figura 6A, el servidor SSL VPN según la presente realización puede además incluir:

una segunda unidad de recepción 604, configurada para recibir un paquete de respuesta del servidor de intranet;

una unidad de determinación 605, configurada para determinar si la directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta;

una primera unidad de encriptación 606, configurada para encriptar el paquete de respuesta cuando un resultado de la decisión de la unidad de determinación 605 es que la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta; y

una segunda unidad de envío 607, configurada para transmitir, de forma transparente, el paquete de respuesta al cliente cuando el resultado de la decisión de la unidad de determinación 605 es no; y enviar el paquete de respuesta encriptado por la primera unidad de encriptación 606 al cliente cuando el resultado de la decisión de la unidad de determinación 605 es sí.

Asimismo, la presente realización puede además incluir:

una unidad de almacenamiento 608, configurada para almacenar una relación de mapeo entre la dirección IP de destino y el número de puerto de destino del paquete descifrado y el túnel VPN.

De manera específica, la segunda unidad de envío 607 envía el paquete de respuesta encriptado por la primera unidad de encriptación 606 al cliente mediante el uso del túnel VPN correspondiente a la dirección IP de origen y al número de puerto de origen según la relación de mapeo almacenada por la unidad de almacenamiento 608 cuando el resultado de la decisión de la unidad de determinación 605 es sí.

Asimismo, en otro caso, como se muestra en la Figura 6B, el servidor SSL VPN según la presente realización puede además incluir:

una unidad de almacenamiento 608, configurada para almacenar una relación de mapeo entre la dirección IP de destino y el número de puerto de destino del paquete descifrado y el túnel VPN;

una tercera unidad de recepción 609, configurada para recibir un paquete de respuesta del servidor de intranet reenviado por un dispositivo de enrutamiento, donde el paquete de respuesta se reenvía al servidor SSL VPN por el dispositivo de enrutamiento después de que el dispositivo de enrutamiento determina, según una directiva de control preestablecida, que la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta;

una segunda unidad de encriptación 610, configurada para encriptar el paquete de respuesta; y

una tercera unidad de envío 611, configurada para enviar el paquete de respuesta encriptado por la segunda unidad de encriptación 610 al cliente.

De manera específica, la tercera unidad de envío 611 puede enviar el paquete de respuesta encriptado por la segunda unidad de encriptación 610 al cliente mediante el uso del túnel VPN correspondiente a la dirección IP de origen y al número de puerto de origen según la relación de mapeo almacenada por la unidad de almacenamiento 608.

Según la presente realización, la dirección IP y el número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet correspondiente al servidor SSL VPN y el paquete del cliente recibido por el servidor SSL VPN desde el túnel VPN se envía por el cliente después de que el cliente determina que la directiva de control incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse y encripta el paquete a enviarse. Dado que el servidor SSL VPN puede aprender el segmento de red del servidor de intranet que procesa dicho paquete (en este momento, el paquete es un paquete de un servicio protegido) según la dirección IP de destino y el número de puerto de destino del paquete, la dirección IP virtual no necesita asignarse, pero la dirección IP de origen del paquete permanece sin cambios, es decir, la dirección IP de origen del paquete es aún una dirección IP de red externa. Como tal, el segmento dedicado de red privada para la comunicación con la red externa en SSL VPN no necesita asignarse en el servidor de intranet. Por lo tanto, la topología de la red no necesita cambiarse.

Como se muestra en la Figura 7, una realización de la presente invención provee un cliente, el cual incluye:

una unidad de determinación 701, configurada para determinar si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse, donde la directiva de control preestablecida incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor SSL VPN;

una unidad de encriptación 702, configurada para: cuando un resultado de la decisión de la unidad de determinación 701 es que la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, encriptar el paquete a enviarse; y

una unidad de envío 703, configurada para: enviar, mediante el uso de un túnel VPN, el paquete encriptado por la unidad de encriptación 702; o cuando el resultado de la decisión de la unidad de determinación 701 es que la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar directamente el paquete a enviarse, donde el paquete a enviarse se envía sin usar el túnel VPN.

El cliente determina si la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse. La dirección IP y el número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet que puede intercambiar paquetes con el servidor SSL VPN. Por lo tanto, si un resultado de la decisión es no, ello indica que el paquete a enviarse es un paquete de un servicio público. Dado que un paquete de un servicio público no necesita enviarse en SSL VPN, el paquete se puede enviar directamente. En el presente caso, el paquete se envía sin usar el túnel VPN. Si el resultado de la decisión es sí, ello indica que el paquete a enviarse es un paquete de un servicio protegido. Dado que los paquetes de servicios protegidos necesitan transmitirse en SSL VPN, el paquete a enviarse se encripta y encapsula en una dirección IP de túnel antes de enviarse mediante el uso del túnel VPN.

Según la presente realización, la dirección IP y el número de puerto de la directiva de control son la dirección IP y el número de puerto del servidor de intranet correspondiente al servidor SSL VPN y el cliente envía el paquete a enviarse usando el túnel VPN después de determinar que la directiva de control incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse y de encriptar el paquete de modo que el servidor SSL VPN puede aprender el segmento de red del servidor de intranet que procesa el paquete según la dirección IP de destino y el número de puerto de destino del paquete. Por lo tanto, la dirección IP virtual no necesita asignarse, pero la dirección IP de origen del paquete permanece sin cambios, es decir, la dirección IP de origen del paquete es aún una dirección IP de red externa. Como tal, el segmento dedicado de red privada para la comunicación con la red externa en SSL VPN necesita asignarse en el servidor de intranet. Por lo tanto, la topología de la red no necesita cambiarse.

Como se muestra en la Figura 8A y la Figura 8B, una realización de la presente invención provee un sistema de red, que incluye un cliente 81 y un servidor SSL VPN 82.

El cliente 81 se configura para: determinar si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse, donde la directiva de control preestablecida incluye información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor SSL VPN; cuando la directiva de control preestablecida incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar, mediante el uso de un túnel VPN, el paquete a enviarse después de la encriptación; y cuando la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar directamente el paquete a enviarse, donde el paquete a enviarse directamente enviado no se envía usando el túnel VPN.

El servidor SSL VPN 82 se configura para: recibir un paquete encriptado enviado por el cliente usando el túnel VPN, donde el paquete encriptado se envía por el cliente después de que el cliente determina, según la directiva de control preestablecida, que la directiva de control incluye la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse y encripta el paquete a enviarse, y la directiva de control comprende información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar paquetes con un servidor SSL VPN de red privada virtual de protocolo de capa de zócalos de seguridad; enviar el paquete descifrado a un servidor de intranet correspondiente, donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa; recibir sin usar un túnel VPN el paquete enviado por el cliente; y transmitir, de forma transparente, el paquete recibido sin usar el túnel VPN a un servidor de intranet correspondiente.

Como se muestra en la Figura 8A, el sistema de red incluye además un servidor de intranet 83 y un dispositivo de enrutamiento 84. En el presente caso, el servidor SSL VPN 82 se despliega entre el dispositivo de enrutamiento 84 y el servidor de intranet 83 en una manera de trayecto directo.

El dispositivo de enrutamiento se puede configurar para interceptar un paquete del cliente y enviar el paquete interceptado al servidor SSL VPN 82.

El paquete interceptado incluye el paquete enviado por el cliente 81 mediante el uso del túnel VPN y el paquete enviado sin usar el túnel VPN.

El servidor SSL VPN 82 se configura además para recibir un paquete de respuesta del servidor de intranet 83, enviar, mediante el uso del túnel VPN, el paquete de respuesta después de la encriptación al cliente cuando la directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta y transmitir, de forma transparente, el paquete de respuesta al cliente cuando la directiva de control preestablecida no incluye la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta.

O, como se muestra en la Figura 8B, el sistema de red incluye además un servidor de intranet 93 y un dispositivo de enrutamiento 94. En el presente caso, el servidor SSL VPN 82 se conecta únicamente al dispositivo de enrutamiento 94 pero no a un servidor de intranet 93.

El dispositivo de enrutamiento 94 se configura para: interceptar un paquete del cliente; cuando el paquete interceptado es un paquete enviado por el cliente usando el túnel VPN, enviar el paquete interceptado al servidor SSL VPN e interceptar un paquete descifrado enviado por el servidor SSL VPN y enviarlo al servidor de intranet.

El dispositivo de enrutamiento se configura además para interceptar un paquete de respuesta del servidor de intranet y determinar si una directiva de control preestablecida incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta; si es así, reenviar el paquete de respuesta al servidor SSL VPN; de lo contrario, transmitir, de forma transparente, el paquete de respuesta al cliente.

El servidor SSL VPN se configura además para recibir el paquete de respuesta del servidor de intranet reenviado por el dispositivo de enrutamiento y enviar, mediante el uso del túnel VPN, el paquete de respuesta después de la encriptación al cliente.

El dispositivo de enrutamiento en la presente realización puede ser un cortafuegos o un enrutador.

Según la presente realización, el cliente determina si el paquete a enviarse se envía mediante el uso del túnel VPN determinando si la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse. El servidor SSL VPN o el dispositivo de enrutamiento determinan si el paquete de respuesta se envía mediante el uso del túnel VPN determinando si la directiva de control incluye una dirección IP y un número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta. Dado que tanto el paquete a enviarse como el paquete de respuesta incluyen la dirección IP y el número de puerto del servidor de intranet, lo cual permite al servidor SSL VPN aprender el segmento de red del servidor de intranet que intercambia paquetes consigo mismo, el servidor SSL VPN no necesita convertir la dirección IP cuando el cliente accede al servidor de intranet mediante el uso de SSL VPN, implementando la función de proveer protección de acceso SSL VPN sin cambiar la topología de la red del servidor de intranet. Además, según el presente método, el servidor SSL VPN se despliega en forma de desvío detrás del cortafuegos, de modo que el cortafuegos puede todavía enviar, de manera directa, paquetes de servicios públicos al servidor de intranet cuando el servidor SSL VPN es anormal y evitar así que dichos servicios públicos se interrumpan.

Las personas con experiencia ordinaria en la técnica pueden comprender que todas o una parte de las etapas del método provisto en las realizaciones de más arriba se pueden implementar por un programa que ordena el hardware relevante. El programa se puede almacenar en un medio de almacenamiento legible por ordenador, por ejemplo, una memoria de solo lectura, un disco magnético o un disco óptico.

**REIVINDICACIONES**

1. Un método de transmisión de paquetes aplicable a una red privada virtual, VPN, del protocolo de capa de zócalos seguros, SSL, en donde un cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN, que comprende:

recibir (201), por un servidor SSL VPN de SSL VPN, mediante el uso de un túnel de Red Privada Virtual, VPN, un paquete encriptado enviado por el cliente, en donde el paquete encriptado se envía por el cliente después de que el cliente determina, según una directiva de control preestablecida, que la directiva de control comprende una dirección de Protocolo de Internet, IP, y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse y encripta el paquete a enviarse y la directiva de control comprende información sobre una dirección IP y un número de puerto de un servidor de intranet de la intranet; descifrar (202), por el servidor SSL VPN, el paquete encriptado; y

enviar (203), por el servidor SSL VPN, el paquete descifrado a un servidor de intranet correspondiente, en donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa.

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

recibir, sin usar el túnel VPN, un paquete enviado por el cliente; y

transmitir, de forma transparente, el paquete recibido sin usar el túnel VPN a un servidor de intranet correspondiente.

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

recibir un paquete de respuesta del servidor de intranet;

cuando la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta, enviar, mediante el uso del túnel VPN, el paquete de respuesta después de la encriptación al cliente; y

cuando la directiva de control preestablecida no comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, transmitir, de forma transparente, el paquete de respuesta al cliente.

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

recibir un paquete de respuesta del servidor de intranet reenviado por un dispositivo de enrutamiento, en donde el paquete de respuesta se reenvía al servidor SSL VPN por el dispositivo de enrutamiento después de que el dispositivo de enrutamiento determina, según una directiva de control preestablecida, que la directiva de control comprende una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta; y

enviar, mediante el uso del túnel VPN, el paquete de respuesta después de la encriptación al cliente.

5. El método según la reivindicación 3 o 4, que además comprende:

almacenar una relación de mapeo entre la dirección IP de destino y el número de puerto de destino del paquete descifrado y el túnel VPN;

enviar, mediante el uso del túnel VPN, el paquete de respuesta después de la encriptación al cliente, que comprende:

según la dirección IP de origen y el número de puerto de origen del paquete de respuesta y la relación de mapeo almacenada, enviar el paquete de respuesta después de la encriptación al cliente usando el túnel VPN correspondiente a la dirección IP de origen y al número de puerto de origen.

6. Un servidor de Red Privada Virtual, VPN, del Protocolo de Capa de Zócalos Seguros, SSL, SSL VPN, que comprende:

un medio configurado para transferir una directiva de control a un cliente cuando el cliente inicia sesión en SSL VPN, en donde el cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN, la directiva de control comprende información sobre una dirección IP y un número de puerto de un servidor de intranet de la intranet;

una primera unidad de recepción (601), configurada para recibir, mediante el uso de un túnel VPN, un paquete encriptado enviado por el cliente;

una unidad de descifrado (602), configurada para descifrar el paquete encriptado; y

una primera unidad de envío (603), configurada para enviar el paquete descifrado al servidor de intranet, en donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa, una dirección IP de destino del paquete descifrado es la dirección IP del servidor de intranet y un número de puerto de destino del paquete descifrado es el número de puerto de un servidor de intranet;

en donde el servidor SSL VPN además comprende:

una segunda unidad de recepción (604), configurada para recibir un paquete de respuesta del servidor de intranet;

una unidad de determinación (605), configurada para determinar si una directiva de control preestablecida comprende una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta;

una primera unidad de encriptación (606), configurada para: cuando un resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número puerto de origen del paquete de respuesta, encriptar el paquete de respuesta; y

una segunda unidad de envío (607), configurada para: cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida no comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, transmitir, de forma transparente, el paquete de respuesta al cliente; y cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de origen y al número de puerto de origen del paquete de respuesta, enviar el paquete de respuesta encriptado por la primera unidad de encriptación al cliente.

7. El servidor SSL VPN según la reivindicación 6, en donde:

la primera unidad de recepción se configura además para recibir, sin usar el túnel VPN, un paquete enviado por el cliente; y

la primera unidad de envío se configura además para transmitir, de forma transparente, el paquete recibido sin usar el túnel VPN a un servidor de intranet correspondiente.

8. El servidor SSL VPN según la reivindicación 6, que además comprende:

una tercera unidad de recepción (609), configurada para recibir un paquete de respuesta del servidor de intranet reenviado por un dispositivo de enrutamiento, en donde el paquete de respuesta se reenvía al servidor SSL VPN por el dispositivo de enrutamiento después de que el dispositivo de enrutamiento determina, según la directiva de control preestablecida, que la directiva de control comprende una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta;

una segunda unidad de encriptación (610), configurada para encriptar el paquete de respuesta; y

una tercera unidad de envío (611), configurada para enviar el paquete de respuesta encriptado por la segunda unidad de encriptación al cliente.

9. El servidor SSL VPN según la reivindicación 8 o 9, que además comprende:

una unidad de almacenamiento (608), configurada para almacenar una relación de mapeo entre la dirección IP de destino y el número de puerto de destino del paquete descifrado por la unidad de descifrado y el túnel VPN;

en donde, el paquete de respuesta encriptado se envía usando el túnel VPN correspondiente a la dirección IP de origen y al número de puerto de origen del paquete de respuesta encriptado al cliente según la relación de mapeo almacenada por la unidad de almacenamiento.

10. Un método de transmisión de paquetes aplicable a una red privada virtual, VPN, del protocolo de capa de zócalos seguros, SSL, en donde un cliente puede acceder a una intranet mediante el uso de una función de extensión de red después de iniciar sesión en SSL VPN, que comprende:

determinar (301), por un cliente, si una directiva de control preestablecida comprende una dirección de Protocolo de Internet, IP, y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse, en donde la directiva de control preestablecida comprende información sobre una dirección IP y un número de puerto de un servidor de intranet de la intranet;

cuando la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar (302), por el cliente, mediante el uso de un túnel VPN, el paquete a enviarse después de la encriptación a un servidor SSL VPN de SSL VPN; y

cuando la directiva de control preestablecida no comprende la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar (303), por el cliente, el paquete a enviarse, en donde el paquete a enviarse se envía sin usar el túnel VPN.

11. El método de transmisión de paquetes según la reivindicación 10, que además comprende:

descargar la directiva de control del servidor SSL VPN cuando se inicia sesión en SSL VPN.

12. Un cliente, que comprende:

una unidad de determinación (701), configurada para determinar si una directiva de control preestablecida comprende una dirección de Protocolo de Internet, IP, y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse, en donde la directiva de control preestablecida comprende información sobre una dirección IP y un número de puerto de un servidor de intranet que puede intercambiar un paquete con un servidor de Red Privada Virtual, VPN, del Protocolo de Capa de Zócalos Seguros, SSL;

una unidad de encriptación (702), configurada para: cuando un resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, encriptar el paquete a enviarse; y

una unidad de envío (703), configurada para: cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida comprende la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar, mediante el uso de un túnel VPN, el paquete encriptado por la unidad de encriptación; y cuando el resultado de la decisión de la unidad de determinación es que la directiva de control preestablecida no comprende la dirección IP y el número de puerto que son iguales a la dirección IP de destino y al número de puerto de destino del paquete a enviarse, enviar directamente el paquete a enviarse, en donde el paquete a enviarse se envía sin usar el túnel VPN.

13. Un sistema de red, que comprende: el servidor SSL VPN según cualquiera de las reivindicaciones 6 a 9 y el cliente según la reivindicación 12.

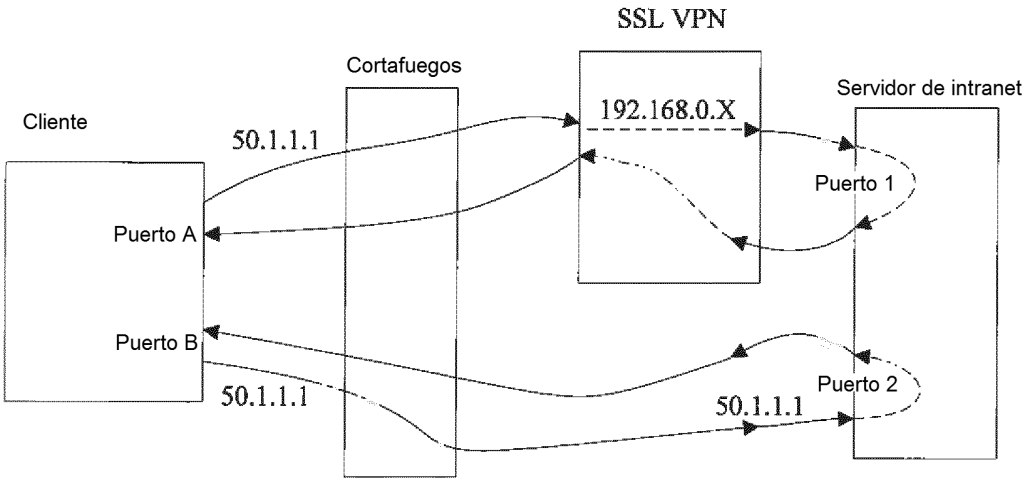
SSL VPN
Cortafuegos
Servidor de intranet
Cliente
192.168.0.X
50.1.1.1
Puerto 1
Puerto A
Puerto B
50.1.1.1
Puerto 2
50.1.1.1

FIG. 1

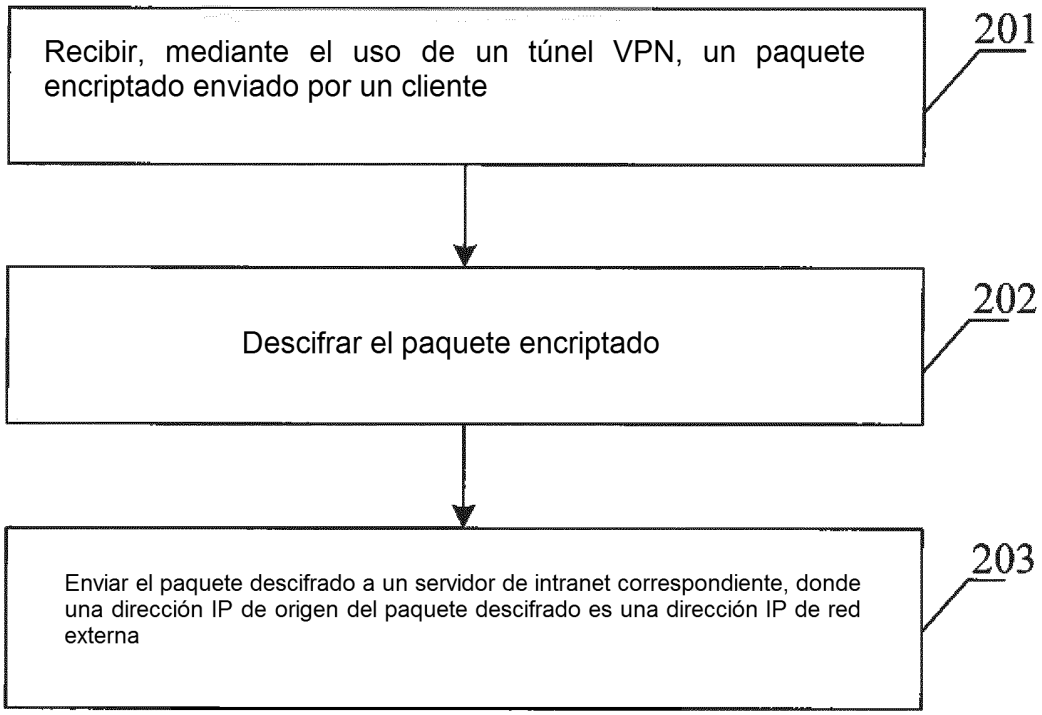
Recibir, mediante el uso de un túnel VPN, un paquete encriptado enviado por un cliente
201
Descifrar el paquete encriptado
202
Enviar el paquete descifrado a un servidor de intranet correspondiente, donde una dirección IP de origen del paquete descifrado es una dirección IP de red externa
203

FIG. 2

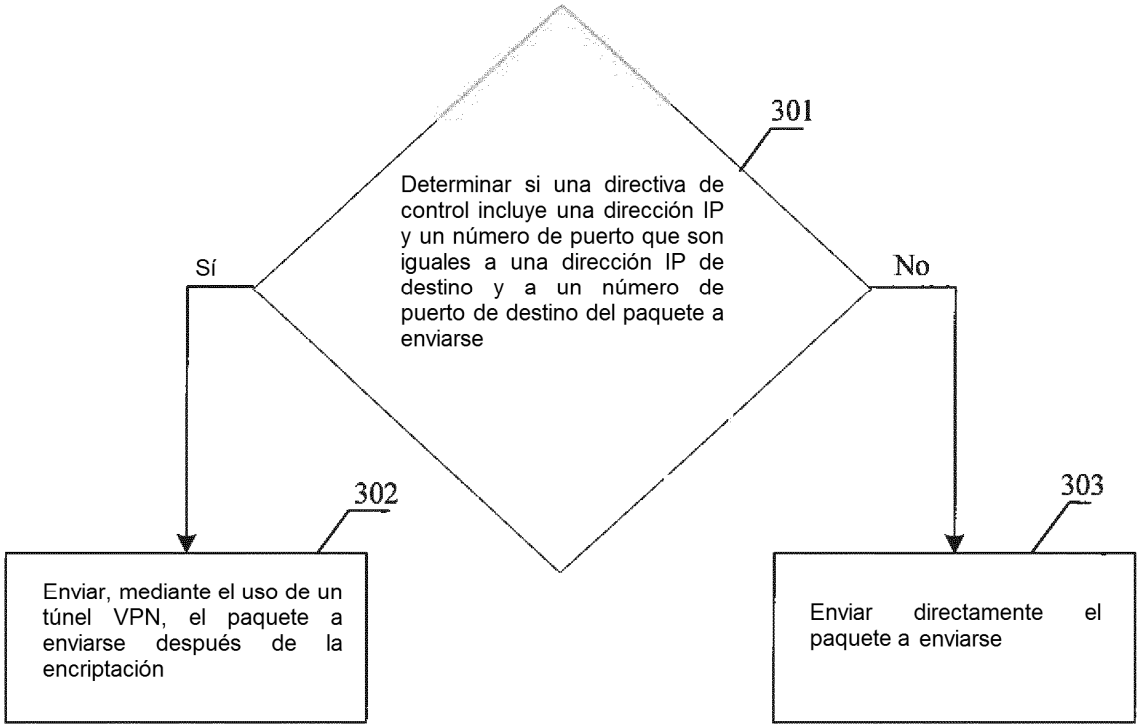
301
Determinar si una directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino del paquete a enviarse
Sí
No
302
Enviar, mediante el uso de un túnel VPN, el paquete a enviarse después de la encriptación
303
Enviar directamente el paquete a enviarse

FIG. 3

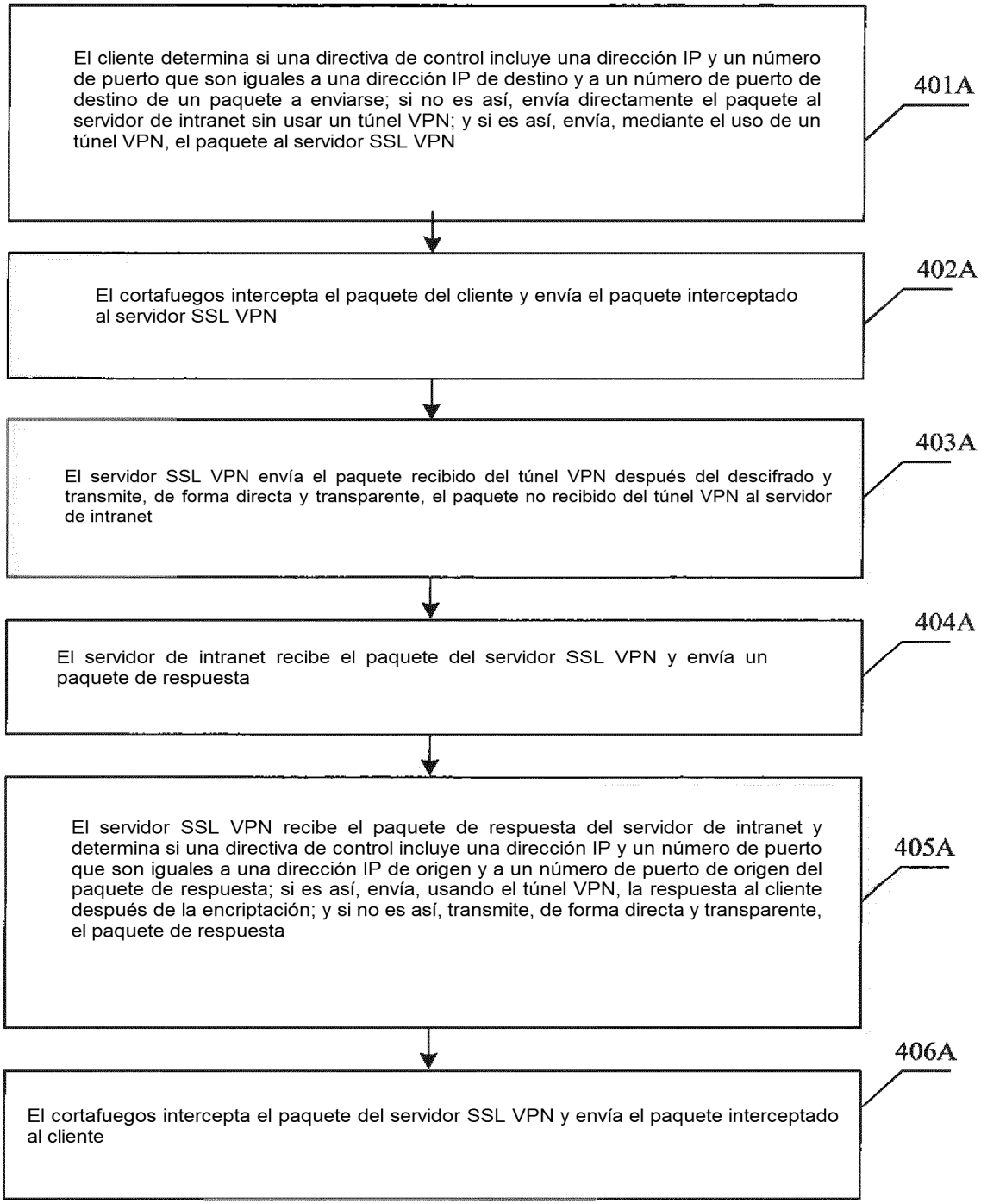
El cliente determina si una directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de destino y a un número de puerto de destino de un paquete a enviarse; si no es así, envía directamente el paquete al servidor de intranet sin usar un túnel VPN; y si es así, envía, mediante el uso de un túnel VPN, el paquete al servidor SSL VPN
401A
El cortafuegos intercepta el paquete del cliente y envía el paquete interceptado al servidor SSL VPN
402A
El servidor SSL VPN envía el paquete recibido del túnel VPN después del descifrado y transmite, de forma directa y transparente, el paquete no recibido del túnel VPN al servidor de intranet
403A
El servidor de intranet recibe el paquete del servidor SSL VPN y envía un paquete de respuesta
404A
El servidor SSL VPN recibe el paquete de respuesta del servidor de intranet y determina si una directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta; si es así, envía, usando el túnel VPN, la respuesta al cliente después de la encriptación; y si no es así, transmite, de forma directa y transparente, el paquete de respuesta
405A
El cortafuegos intercepta el paquete del servidor SSL VPN y envía el paquete interceptado al cliente
406A

FIG. 4A

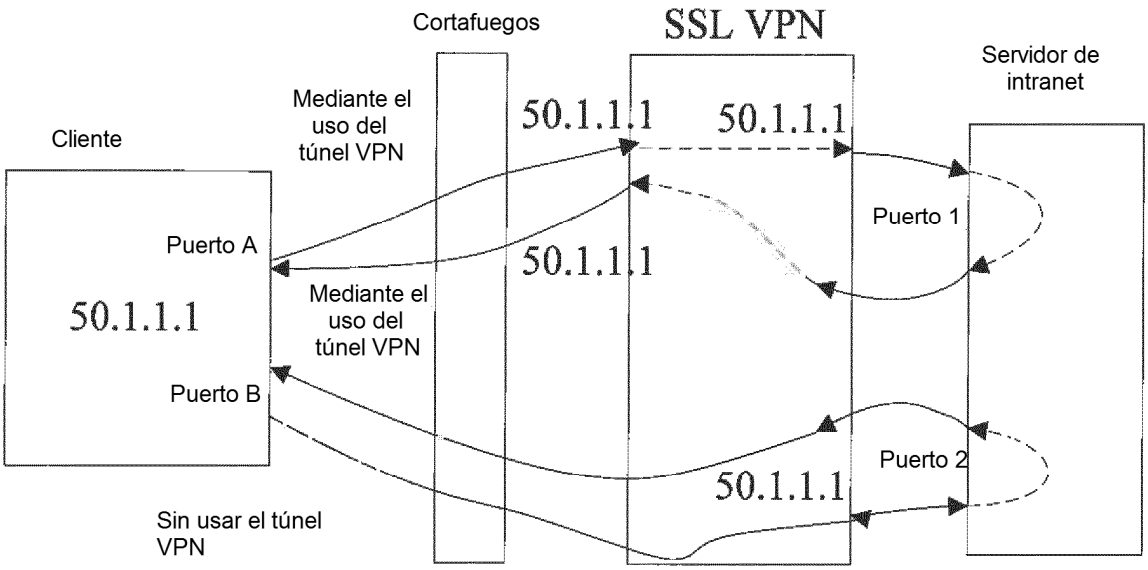
Cortafuegos
SSL VPN
Servidor de intranet
Cliente
Mediante el uso del túnel VPN
50.1.1.1
50.1.1.1
Puerto 1
Puerto A
50.1.1.1
50.1.1.1
Mediante el uso del túnel VPN
Puerto B
Puerto 2
50.1.1.1
Sin usar el túnel VPN

FIG. 4B

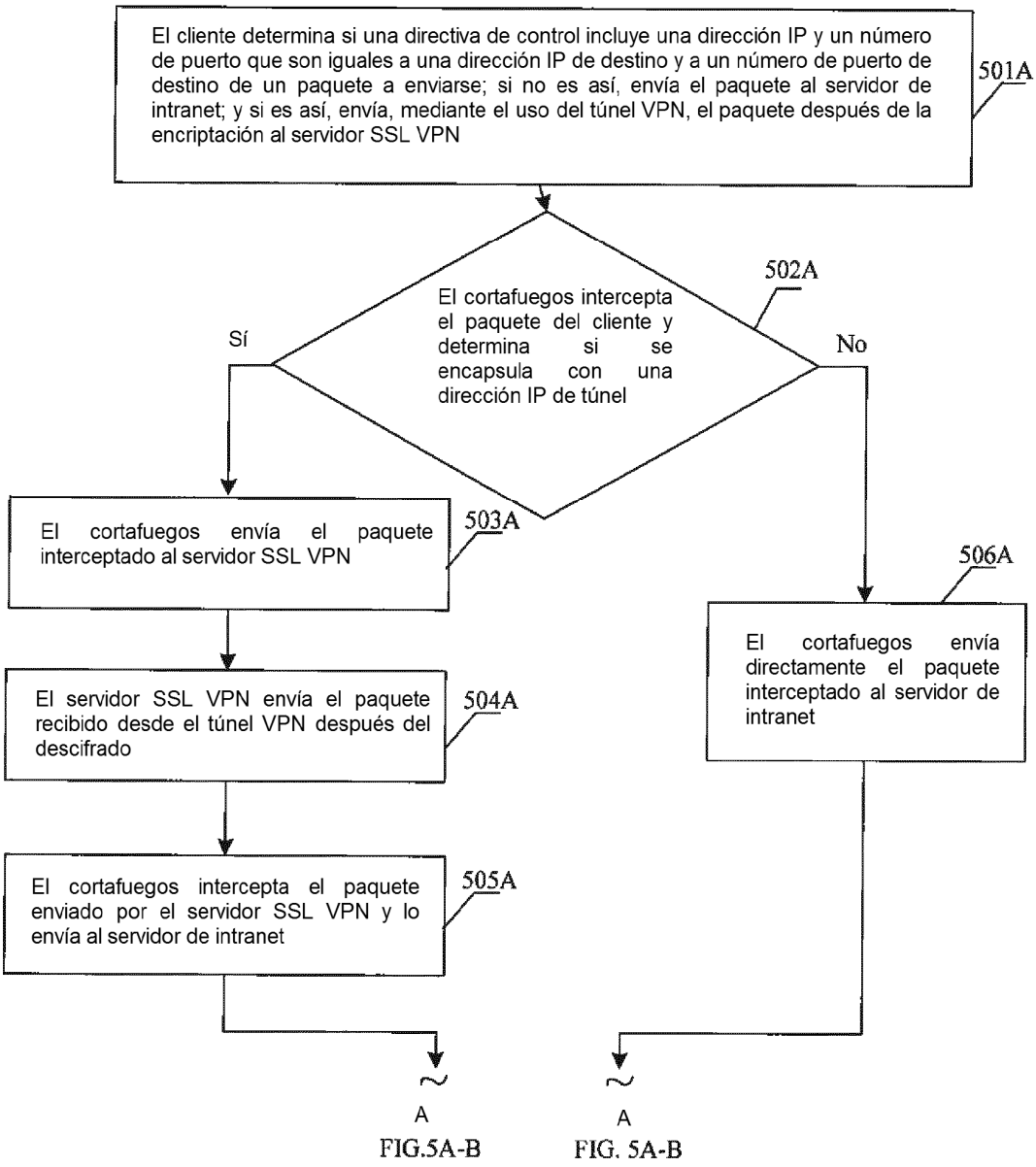


FIG.5A-B FIG. 5A-B

FIG. 5A-A

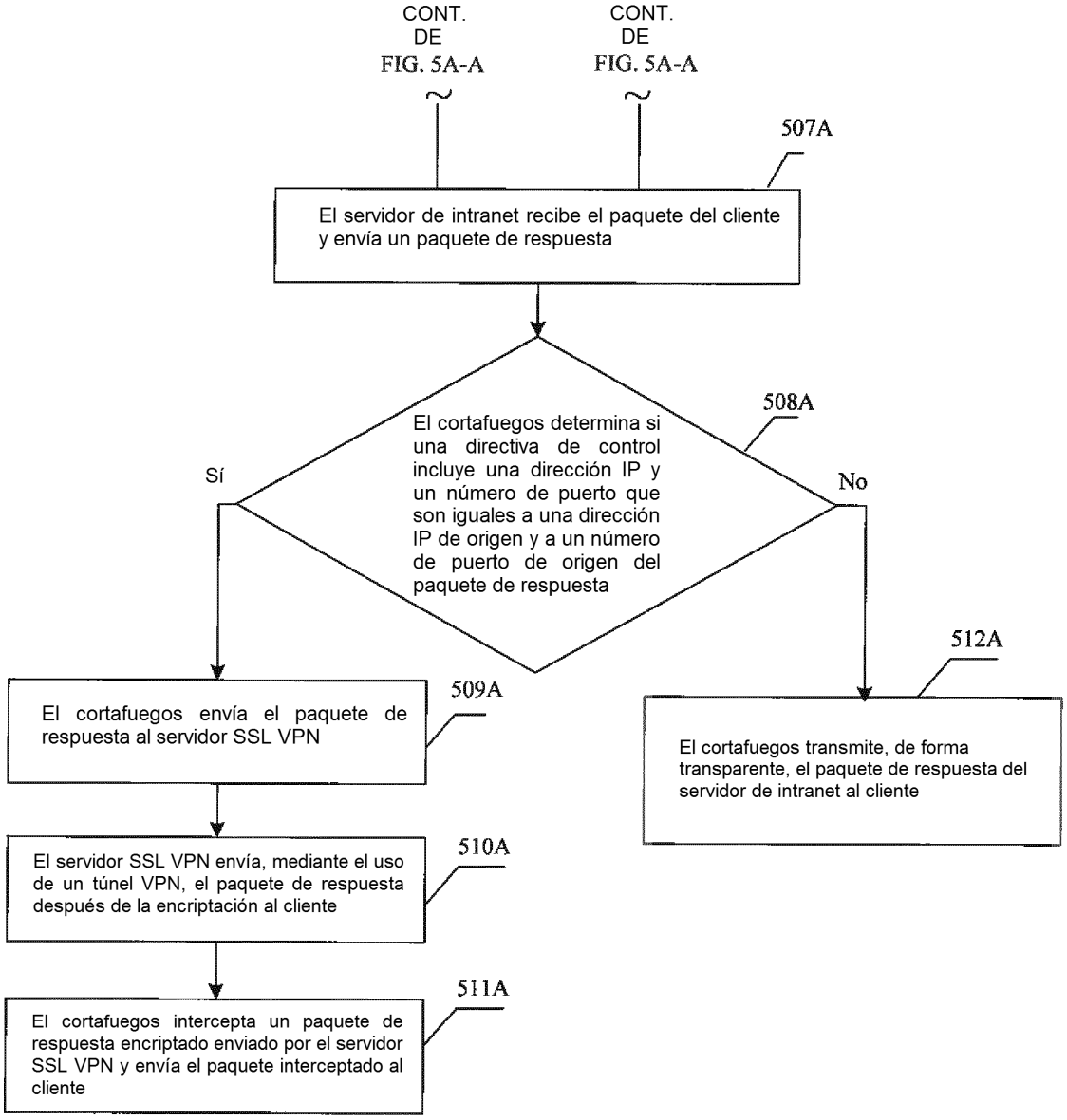
CONT. DE FIG. 5A-A
CONT. DE FIG. 5A-A
507A
El servidor de intranet recibe el paquete del cliente y envía un paquete de respuesta
508A
El cortafuegos determina si una directiva de control incluye una dirección IP y un número de puerto que son iguales a una dirección IP de origen y a un número de puerto de origen del paquete de respuesta
Sí
No
509A
El cortafuegos envía el paquete de respuesta al servidor SSL VPN
510A
El servidor SSL VPN envía, mediante el uso de un túnel VPN, el paquete de respuesta después de la encriptación al cliente
511A
El cortafuegos intercepta un paquete de respuesta encriptado enviado por el servidor SSL VPN y envía el paquete interceptado al cliente
512A
El cortafuegos transmite, de forma transparente, el paquete de respuesta del servidor de intranet al cliente

FIG. 5A-B

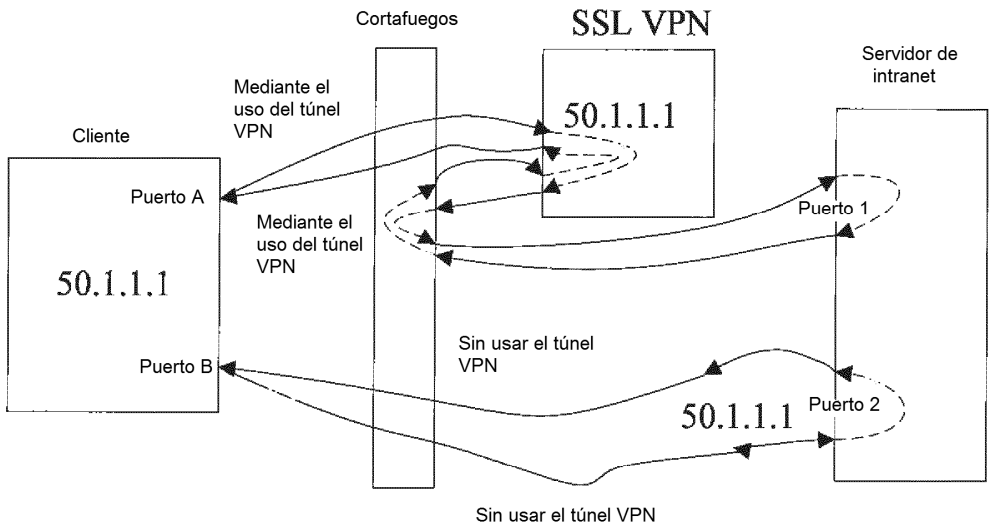
Cortafuegos
SSL VPN
Servidor de intranet
Mediante el uso del túnel VPN
50.1.1.1
Cliente
Puerto A
Puerto 1
Mediante el uso del túnel VPN
50.1.1.1
Sin usar el túnel VPN
Puerto B
50.1.1.1
Puerto 2
Sin usar el túnel VPN

FIG. 5B

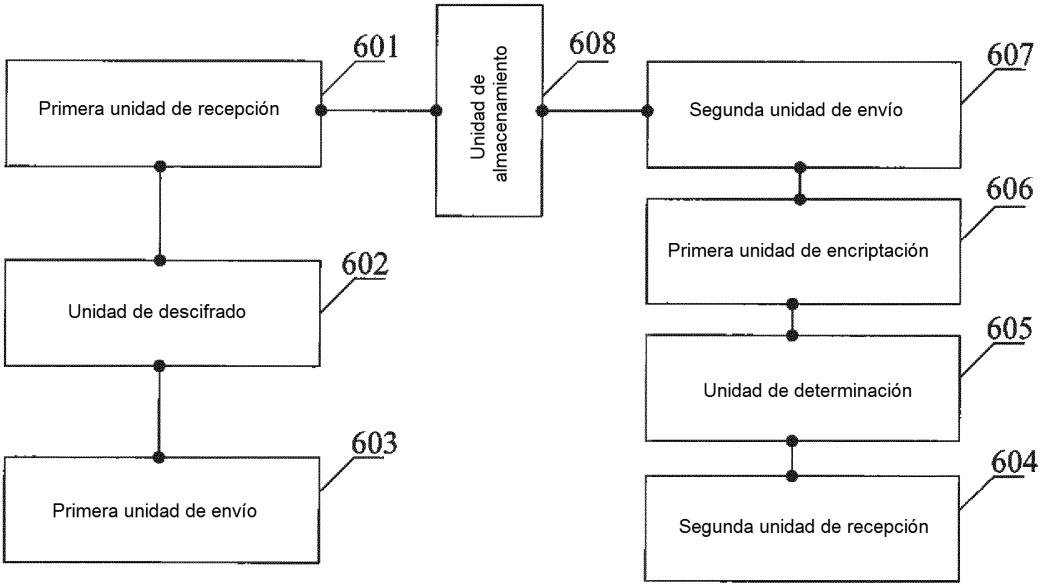
601
Primera unidad de recepción
608
Unidad de almacenamiento
607
Segunda unidad de envío
606
Primera unidad de encriptación
602
Unidad de descifrado
605
Unidad de determinación
603
Primera unidad de envío
604
Segunda unidad de recepción

FIG. 6A

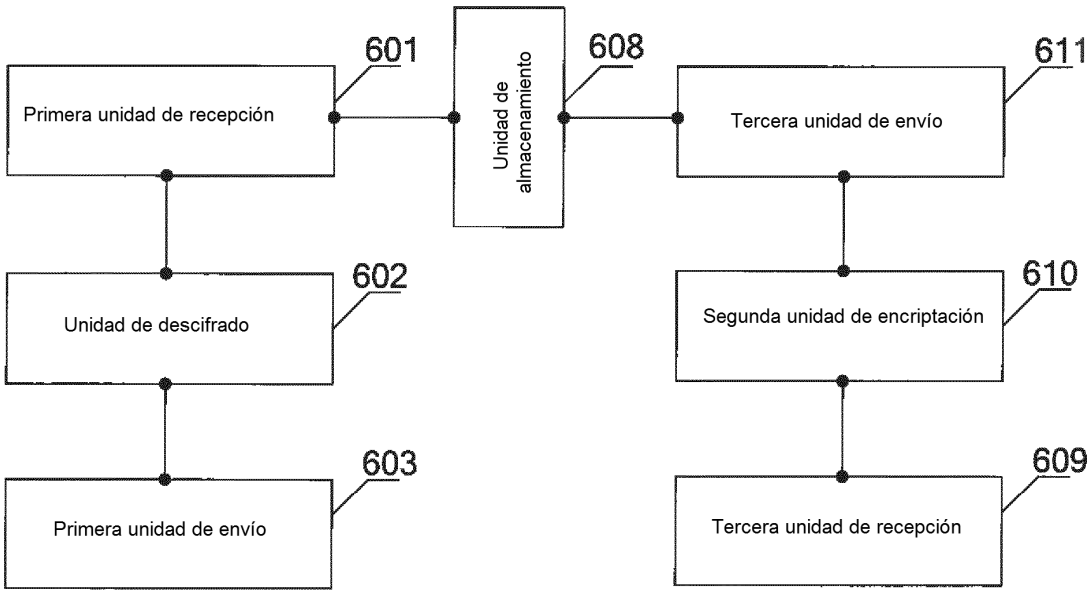
601
Primera unidad de recepción
Unidad de almacenamiento
608
611
Tercera unidad de envío
602
Unidad de descifrado
610
Segunda unidad de encriptación
603
Primera unidad de envío
609
Tercera unidad de recepción

FIG. 6B

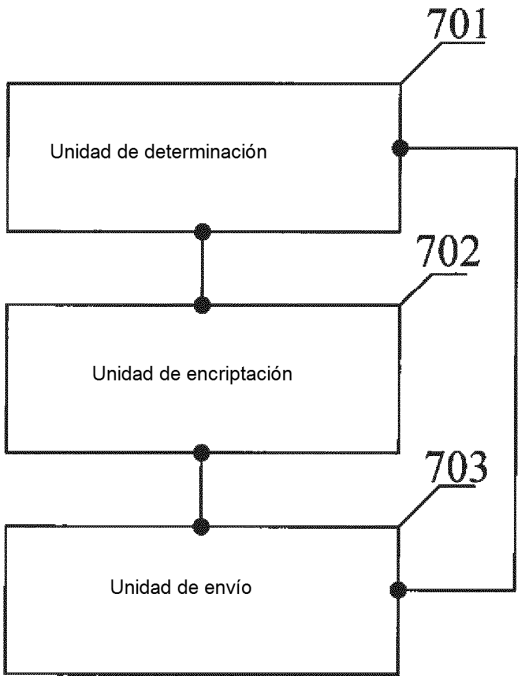
701
Unidad de determinación
702
Unidad de encriptación
703
Unidad de envío

FIG. 7

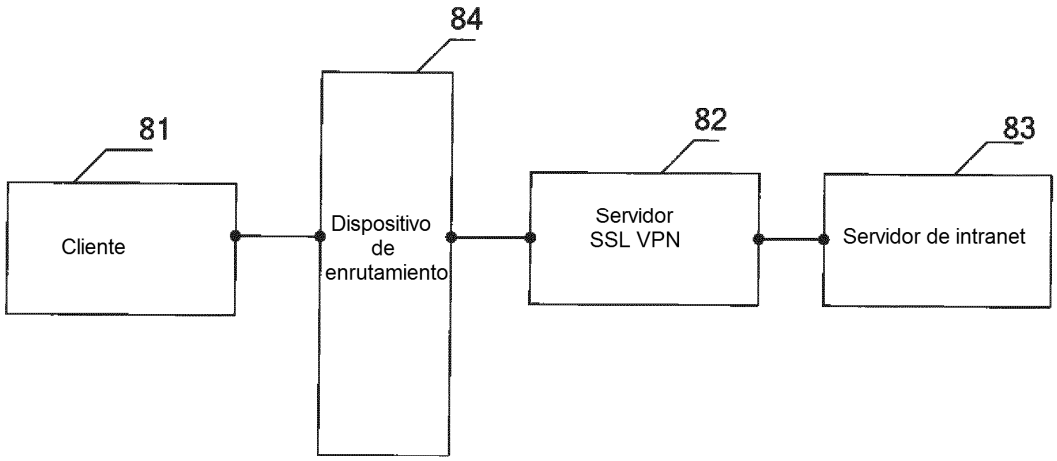
84
81
82
83
Cliente
Dispositivo de enrutamiento
Servidor SSL VPN
Servidor de intranet

FIG. 8A

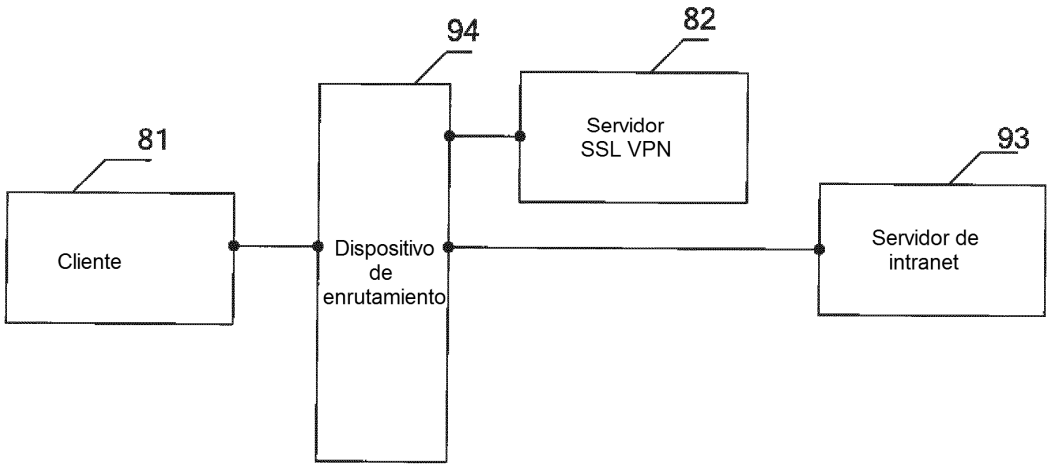
94
82
81
93
Servidor SSL VPN
Cliente
Dispositivo de enrutamiento
Servidor de intranet

FIG. 8B