(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 429 121**

(51) Int. CI.:

H04L 29/12 (2006.01)
H04L 12/46 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.03.2009 E 09721670 (9)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2013 EP 2253123**

(54) Título: **Método y aparato para comunicación de paquetes de datos entre redes locales**

(30) Prioridad:

20.03.2008 US 38192

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.11.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

KÖLHI, JOHAN;
GOTARE, CHRISTIAN;
THYNI, TOMAS y
WELIN, ANNIKKI

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y aparato para comunicación de paquetes de datos entre redes locales

Campo técnico

La invención se refiere de manera general a un método, un programa de ordenador y aparato para comunicación de paquetes de datos en un túnel VPN (Red Privada Virtual) entre dispositivos de comunicación situados dentro de diferentes redes locales que podrían usar espacios de dirección superpuestos.

Antecedentes

La transmisión basada en paquetes de información codificada digitalmente entre diferentes partes sobre redes IP (Protocolo de Internet) se usa para una variedad de servicios de comunicación, tales como mensajería de correo electrónico, transferencia de ficheros, navegación en Internet, telefonía de voz y vídeo, difusión en forma continua de contenido, juegos, etcétera. La información codificada digitalmente se dispone en paquetes de datos en una parte remitente que entonces transmite los paquetes hacia una parte de recepción objetivo sobre un trayecto de transmisión. Un paquete de datos está configurado básicamente con un campo de datos que contiene datos de carga útil y un campo de cabecera que contiene una dirección de destino de la parte de recepción y una dirección de fuente de la parte remitente.

Los paquetes de datos se pueden comunicar entre varios dispositivos de comunicación situados dentro de diferentes redes locales o privadas donde cada red emplea una pasarela para recibir paquetes para los dispositivos desde fuentes fuera de la red, y también para enviar paquetes desde los dispositivos a destinos fuera de la red. Los paquetes comunicados entre tales dispositivos en diferentes redes locales se transportan entonces entre las respectivas pasarelas de red sobre una red IP pública, tal como Internet.

En esta descripción, el término “red local” se usa para representar de manera general cualquier red que usa direccionamiento privado interno y una pasarela para comunicación externa con partes fuera de la red. Otros términos equivalentes usados comúnmente incluyen “red privada”, “red residencial” y “red doméstica”. Además, una “pasarela” podría ser una pasarela residencial (RGW), un encaminador IP o cualquier otro tipo de entidad de red capaz de comunicar paquetes de datos entre un dispositivo dentro de una red local y una entidad fuera de la red.

Dado que la comunicación sobre redes IP públicas se considera generalmente “inseguro” con respecto a protección de datos y privacidad, es deseable proteger los datos de la carga útil y otra información sensible en los paquetes de intercepción o manipulación ilícita. Una forma de superar este problema es establecer un túnel VPN (Red Privada Virtual) entre las partes que comunican sobre la red IP pública.

Una VPN puede ser vista básicamente como un túnel cifrado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores. Las VPN se usan comúnmente para comunicaciones seguras a través de Internet pública. Se pueden definir varios parámetros de QoS (Calidad de Servicio) para una VPN para lograr un comportamiento esperado entre un cliente VPN y un proveedor de servicios VPN. Generalmente, se puede establecer una VPN para dos o más dispositivos de comunicación en una comunidad de usuarios para proporcionar una cierta funcionalidad que es en algún aspecto relevante para esa comunidad.

Según crece la popularidad y el uso de Internet, llega a ser cada vez más deseable extender las redes privadas y locales a través de Internet también. Por ejemplo, muchas compañías y empresas que tienen una red local establecen sus propias VPN para permitir a sus empleados acceder a la red local de manera remota.

Una VPN puede de esta manera ser vista como una red local lógica y “distribuida” que se ejecuta sobre una infraestructura de red pública. Estas redes hacen uso de una gama de tecnologías para obtener privacidad de tráfico, separación de tráfico y QoS de los datos. Se puede establecer una VPN sobre una intranet, Internet o una infraestructura de red del proveedor de servicios. Hay generalmente dos tipos básicos de servicios VPN disponibles conocidos como “VPN de Acceso” y “VPN de LAN (Red de Área Local) a LAN”, el primero que se usa para acceso remoto y el último cuando se interconectan diferentes redes locales para proporcionar una intranet o extranet.

No obstante, establecer una VPN entre dispositivos en redes locales puede provocar varios problemas. Un problema es que los dispositivos dentro de las redes locales usan típicamente direcciones IP de un espacio de dirección privado, donde tales direcciones IP privadas se pueden asignar libremente a dispositivos internamente por un administrador local o similar. Las direcciones IP privadas usadas son básicamente desconocidas de esta manera para otros usuarios, a menos que se diga explícitamente, y también para el proveedor de servicios de Internet que proporciona las direcciones IP públicas a los abonados.

Otro problema es que las direcciones IP privadas usadas por diferentes redes locales para sus dispositivos se superponen generalmente unas con otras, en particular los espacios de direcciones privadas basados en IPv4 usados comúnmente que se reutilizan en múltiples redes locales. Por ejemplo, la dirección IP privada usada por un dispositivo en una red local puede ser la misma dirección que la usada por otro dispositivo en la red local opuesta, provocando direccionamiento ambiguo en los paquetes de datos comunicados entre estas dos redes. Esto hace una

tarea incómoda conectar diferentes redes locales juntas por medio de un túnel VPN. Debido a tales espacios de direcciones reutilizadas o superpuestas, las direcciones IP privadas son “inencaminables” de manera efectiva en la Internet pública, y las direcciones IP públicas por lo tanto se deben usar también en los paquetes.

La US-2007/195800-A1 describe un sistema y método para usar direcciones IP privadas para designar dispositivos centrales en diferentes redes. Las realizaciones abordan el problema de una escasez de direcciones IP públicas bajo una arquitectura IPv4 y en una realización se proporcionan capacidades de penetración NAT dinámicas.

La US-2004/148439-A1 describe un sistema y método para crear una red entre iguales interconectando redes privadas a través de una pasarela residencial direccionable públicamente. Se establece un túnel entre una pasarela de una primera red privada y una pasarela de una segunda red privada y la dirección de un dispositivo en una de las redes privadas se correlaciona en la otra red privada.

La US-2007/180139-A1 describe una conversión de direcciones en el caso de direcciones de red duplicadas cuando se hace una comunicación a través de dos pasarelas.

Compendio

Es un objeto de la presente invención abordar al menos algunos de los problemas perfilados anteriormente. También es un objeto proporcionar un mecanismo para permitir un direccionamiento no ambiguo para paquetes de datos incluso cuando comunican dispositivos en dos redes locales diferentes usando espacios de dirección superpuestos potencialmente.

Según diferentes aspectos que se define en las reivindicaciones independientes, se proporcionan un método, una adaptación en una pasarela y un programa de ordenador para abordar los problemas perfilados anteriormente.

Cada uno del método, adaptación de pasarela y programa de ordenador anteriores pueden comprender además rasgos y funciones configurados según las siguientes realizaciones.

Cuando el paquete entrante también tiene una cabecera IP externa que incluye las direcciones IP públicas de la primera y segunda pasarelas como direcciones de destino y de fuente externas, respectivamente, se elimina la cabecera IP externa del paquete entrante por la primera pasarela.

En otra realización, la primera pasarela además recibe un paquete de datos saliente desde el primer dispositivo, el paquete saliente que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la primera red local para el segundo dispositivo y una dirección de fuente interna usada en la primera red local para el primer dispositivo. El paquete entonces se encapsula con una cabecera IP externa que incluye las direcciones IP públicas de las pasarelas como direcciones de destino y de fuente externas, respectivamente. El túnel VPN correcto se puede determinar para el paquete saliente en base a la dirección de destino interna, y el paquete saliente entonces se envía a la segunda pasarela a través de un túnel VPN.

Se puede determinar entonces un túnel VPN para cada paquete saliente en base al número único en una dirección de destino interna en el paquete saliente, y entonces se envía el paquete a través del túnel VPN determinado. El establecimiento de los túneles VPN puede incluir añadir en la pasarela para cada red local un nombre de DNS registrado y una clave PKI pública correspondiente de cada pasarela opuesta. La clave PKI pública y una clave PKI privada correspondiente también se pueden generar para cada pasarela y las claves PKI públicas se almacenan en un servidor PKI accesible para las pasarelas.

En realizaciones adicionales, el túnel VPN se puede admitir además para el establecimiento si la red local candidata está asociada indirectamente con la primera parte en la lista de confianza que está asociada con una segunda parte presente en una lista de confianza de la primera parte. Por ejemplo, el túnel VPN se puede admitir para el establecimiento dependiendo de un número predeterminado de niveles de confianza aprobados para la primera red local.

La red local candidata se podría evaluar para el establecimiento de un túnel VPN en respuesta a una petición de túnel VPN desde la red local candidata. Un túnel VPN establecido entre dos redes locales también se podría terminar automáticamente si se modifica una lista de confianza asociada con cualquiera de las dos redes para inhabilitar el túnel VPN.

Llegarán a ser evidentes rasgos y beneficios posibles adicionales de la invención a partir de la descripción detallada de más adelante.

Breve descripción de los dibujos

La invención se describirá ahora en más detalle por medio de realizaciones ejemplares y con referencia a los dibujos anexos, en los que:

- La Fig. 1 es un diagrama de bloques esquemático que ilustra un escenario de comunicación que implica un túnel VPN, según algunas realizaciones ejemplares.

- La Fig. 2 es un esquema de transmisión esquemático que ilustra cómo se modifica la cabecera de un paquete de datos en pasarelas opuestas, según realizaciones adicionales.

- La Fig. 3 es un diagrama de flujo con pasos en un procedimiento realizado por una pasarela en una red local para manejar un paquete de datos entrante, según aún una realización.

- La Fig. 4 es un diagrama de bloques esquemático que ilustra una pasarela en más detalle, según realizaciones adicionales.

- La Fig. 5 es otro diagrama de flujo con pasos en un procedimiento realizado por la pasarela para manejar un paquete de datos saliente, según aún una realización.

- La Fig. 6 es otro diagrama de flujo con pasos en un procedimiento realizado por la pasarela para manejar una petición VPN, según aún una realización.

Descripción detallada

La invención proporciona un mecanismo para obtener un direccionamiento no ambiguo para paquetes de datos incluso cuando comunican dispositivos en dos redes locales diferentes usando espacios de dirección superpuestos. Brevemente descrito, se establece inicialmente un túnel VPN entre pasarelas en las dos redes locales dónde se ha asignado una dirección IP pública a cada pasarela. Además, se define un espacio de dirección IP interno seleccionado en cada red local a ser usado en la presente red para dispositivos en la red local opuesta, y que está separado de, es decir no se superpone con, un espacio de dirección IP interno usado en la presente red local para sus propios dispositivos.

Cuando se recibe cualquier paquete de datos entrante desde un dispositivo en una red opuesta en la pasarela de una red local presente, la cabecera de ese paquete tiene una cabecera IP interna con direcciones de destino y de fuente IP privadas superpuestas potencialmente con el espacio de dirección usado en la presente red para sus propios dispositivos. La cabecera es entonces modificada en la pasarela de recepción cambiando las direcciones de destino y de fuente en las direcciones que pertenecen a los espacios de dirección anteriores usados en la presente red para los dos dispositivos, respectivamente. En particular, la dirección fuente del dispositivo remitente se toma a partir del espacio de dirección IP interno definido anteriormente para dispositivos en la red opuesta. Por ello, la dirección fuente en la cabecera IP interna del paquete entrante no se puede confundir con las direcciones IP privadas de cualesquiera dispositivos en la presente red.

Un ejemplo de cómo se puede consumar lo anterior se describirá ahora con referencia a un escenario de comunicación mostrado en la Fig. 1. De esta manera, se supone que usuarios de dos redes locales diferentes A y B han acordado establecer un túnel VPN entre las redes para permitir una comunicación “segura” de paquetes de datos sobre una red IP pública 100, en este ejemplo Internet, entre dispositivos en las redes opuestas, por ejemplo debido a las razones presentadas anteriormente.

En la Fig. 1, se muestran una primera pasarela 102 y una segunda pasarela 104 que sirven a las primera y segunda redes A y B, respectivamente, donde una pluralidad de dispositivos E1A, E2A, E3A… están presentes en la primera red y una pluralidad de dispositivos E1B, E2B, E3B… están presentes en la segunda red. Se usa un espacio de dirección privado en cada red local para comunicación interna, los espacios de direcciones superpuestos potencialmente uno con otro dado que tales espacios de dirección se reutilizan ampliamente en numerosas redes locales, de manera general. Se supone además que cada pasarela 102, 104 comprende una función para traducir direcciones de red privadas de una manera que se describe más adelante, la cual se puede conocer como una función “NAT” (Traducción de Direcciones de Red).

Antes del establecimiento del túnel VPN, cada pasarela 102, 104 registrará primero sus nombres y direcciones IP públicas con un DNS (Servidor de Nombres de Dominio), en este caso un DDNS 106 (DNS Dinámico) que permite tanto direcciones IP dinámicas como estáticas, que se hace típicamente cuando se activa la pasarela. Las pasarelas 102, 104 también generan sus claves públicas y privadas o certificados para cifrado según el mecanismo PKI (Infraestructura de Claves Públicas) bien conocido, y las claves públicas se registran en un servidor PKI 108. Un primer paso 1:1 ilustra esquemáticamente el registro de DNS y el establecimiento de claves hecho por ambas pasarelas, como se muestra por las flechas de dos direcciones en la figura. Este paso se puede ejecutar de esta manera según procedimientos habituales que no son necesarios describir aquí más para explicar este ejemplo.

Los siguientes **pasos 1:2A** y **1:2B** ilustran que el túnel VPN está establecido entre las pasarelas, y también que cada pasarela define un espacio de dirección IP para dispositivos en la red local opuesta, que se han seleccionado para evitar superposición con el espacio de dirección IP usado internamente para sus propios dispositivos. De esta manera, la pasarela 102 define un espacio de dirección IP para dispositivos de red B en el **paso 1:2A**, mientras que la pasarela 104 define un espacio de dirección IP para dispositivos de red A en el **paso 1:2B**. El establecimiento de la VPN incluye, entre otras cosas, almacenar en cada pasarela el espacio de dirección IP definido anteriormente, o al menos una identificación del mismo, así como el nombre y la dirección IP pública asociada de la pasarela opuesta, que están disponibles y se recuperan a partir del DDNS 106.

En este sentido, una pasarela en una red local puede establecer múltiples túneles VPN con pasarelas de otras redes locales, y se puede crear una tabla de traducción o similar en la pasarela, que contiene al menos una identidad de túnel y un espacio de dirección IP no superpuesto usado en la red para cada red local opuesta. Ninguno de estos espacios de dirección IP no debería superponerse de esta manera con ningún otro espacio de dirección IP usado en esa red. Siempre que se recibe un paquete de datos entrante desde un dispositivo en cualquiera de las redes locales opuestas, se identifica el túnel VPN entrante y una dirección IP local, tomada a partir del espacio de dirección IP asociado con ese túnel en la tabla, se usa en la red de recepción para el dispositivo de la red remitente, que se describirá en más detalle más adelante.

Como se mencionó anteriormente, la tabla de traducción puede contener una identificación del espacio de dirección IP definido asociado con cada identidad de túnel. Por ejemplo, si los espacios de dirección IP incluyen direcciones basadas en IPv4 (IP versión cuarta), se puede asignar un número único en un segundo o tercer octeto de cada dirección IP para representar la red local opuesta correspondiente. Ese número único puede ser entonces suficiente para identificar la red en la tabla. Por ejemplo, si se usa el espacio de dirección de 10.0.0.0/24 para dispositivos dentro de la presente red, los espacios de dirección IP ejemplares siguientes se pueden definir para redes opuestas diferentes: 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24…, usando el tercer octeto como una identificación de red.

Por ello, también se puede determinar el túnel VPN correcto para un paquete saliente en base al número único en la dirección de destino interna de ese paquete, de manera que el paquete se puede enviar entonces a través del túnel VPN determinado. Se supone que el dispositivo remitente puede obtener conocimiento del espacio de dirección IP que fue definido para dispositivos en la red local opuesta y que la dirección de destino en el paquete es la asignada al dispositivo de recepción.

Volviendo a la Fig. 1, se envía un paquete de datos desde un dispositivo E1B en la red local B, dirigido a otro dispositivo E3A en la red local A. El paquete tiene una cabecera interna con direcciones IP de destino y de fuente locales, y se recibe en primer lugar en la pasarela 104 en un siguiente paso 1:3. En la cabecera interna, las direcciones IP de destino y de fuente de E3A y E1B, respectivamente, son direcciones usadas en la red remitente B, pero no en la red de recepción A. Por lo tanto, es necesaria una traducción de estas direcciones para obtener direccionamiento no ambiguo en la red de recepción A, que se hará por la pasarela 102 de la red de recepción A. Esto asegurará de esta manera que el paquete alcance el dispositivo de destino previsto.

Antes de enviar fuera el paquete, la pasarela 104 identifica el túnel VPN con la red A en base a la dirección IP de destino privada en la cabecera interna a partir del segundo o tercer octeto de la manera descrita anteriormente, y añade una cabecera externa con las direcciones IP públicas de las pasarelas 102 y 104 como direcciones IP de destino y de fuente, respectivamente, en un siguiente **paso 1:4**. El paquete se transmite entonces sobre la red IP pública 100 a la pasarela 102 de la red A, en un siguiente **paso 1:5**. La dirección IP de destino pública en la cabecera externa se puede usar entonces para encaminar el paquete hacia la pasarela 102 a través de la red IP pública 100 de una manera convencional.

Cuando se recibe el paquete de datos, la pasarela 102 elimina la cabecera externa, que ha cumplido su propósito, mientras que la red remitente se puede deducir desde el túnel VPN usado para transmitir el paquete. Se debería recordar que el paquete recibido contiene direcciones de destino y de fuente privadas que eran válidas en la red remitente B, pero no en la red de recepción A. La pasarela 102 cambia por lo tanto las direcciones de destino y de fuente en la cabecera interna del paquete, en un **paso 1:6** adicional, traduciéndolas en direcciones usadas en la red de recepción A.

En más detalle, se cambia la dirección de destino a una dirección de destino usada en la red A para el dispositivo E3A, y la dirección de fuente se cambia a una dirección de fuente interna del espacio de dirección seleccionado usado en la red A para el dispositivo E1B, esta última dirección que se toma del espacio de dirección IP interno definido previamente en el paso 1:2A por la pasarela 102 para los dispositivos en la red B. Esta última dirección se ha asignado al dispositivo E1B, junto con las asignaciones de dirección de otros dispositivos, durante el establecimiento del túnel VPN y esta información se ha almacenado en cada pasarela 102, 104 para permitir la traducción de direcciones para paquetes entrantes. Las asignaciones de direcciones se pueden hacer según un esquema predeterminado, por ejemplo por medio de un contador que asigna “1” en el tercer octeto a una primera red local opuesta, “2” en el tercer octeto a una segunda red local opuesta, y así sucesivamente. Las asignaciones de direcciones pueden ser además estáticas o dinámicas.

La Fig. 2 ilustra un ejemplo de cómo se puede configurar la cabecera del paquete de datos tratada anteriormente en más detalle en diferentes etapas de la transmisión de paquete descrita para la Fig. 1. El lado izquierdo de la Fig. 2 representa de esta manera el dispositivo remitente E1B, las pasarelas 104 y 102 de las redes B y A, respectivamente, y el dispositivo de recepción E3A.

En este ejemplo, la red B usa el espacio de dirección 10.0.0.0/24 para sus propios dispositivos y el espacio de dirección 10.0.1.0/24 se ha definido para dispositivos de la red opuesta A. El tercer octeto en estos espacios de direcciones indica de esta manera la red del dispositivo, es decir en la red B “0” indica la red B y “1” indica la red A. En el lado opuesto, la red A también usa el espacio de dirección 10.0.0.0/24 para sus propios dispositivos y el espacio de dirección 10.0.1.0/24 se ha definido igualmente para dispositivos de la red opuesta B. De esta manera en

la red A “0” indica la red A y “1” indica la red B, al contrario de la situación en la red B.

Cuando el paquete enviado desde el dispositivo E1B se recibe en primer lugar en la pasarela 104 según el paso 1:3 anterior, tiene una cabecera interna válida en la red B con una dirección de destino 10.0.1.11 que es válida para el dispositivo E3A, y una dirección de fuente 10.0.0.4 que es válida para el dispositivo E1B. Según el paso 1:4 anterior, la pasarela 104 añade una cabecera externa con una dirección de destino pública IPA de la pasarela 102 y una dirección de fuente pública IPB de la pasarela 104. La pasarela 104 entonces identifica el túnel VPN correcto a partir de la indicación de red de “1” que apunta a la red A, y envía el paquete a través del túnel a la pasarela 102, según el paso 1:5 anterior.

Habiendo recibido el paquete, la pasarela 102 entonces elimina la cabecera externa y cambia la cabecera interna traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de fuente a 10.0.1.4, que son válidas en la red A para los dispositivos E1B y E3A, respectivamente. El paquete con la cabecera interna modificada entonces es reenviado finalmente al dispositivo E3A, según el paso 1:7 anterior. Por lo tanto, incluso si se usan espacios de dirección superpuestos en las redes A y B como se describió anteriormente, las direcciones de destino y de fuente en la cabecera interna identificarán los dispositivos respectivos adecuadamente y sin riesgo de confusión en la red de recepción A.

Además, el dispositivo E3A puede enviar un paquete de datos como una respuesta al dispositivo E1B usando la dirección de fuente recibida como la dirección de destino y su propia dirección privada como dirección de fuente, las cuales son ambas válidas en la red A. En ese caso, el procedimiento anterior se repetirá en la dirección inversa y la pasarela de recepción 104 cambiará de esta manera la cabecera interna traduciendo las direcciones de destino y de fuente de vuelta a las válidas en la red B, es decir 10.0.0.4 (fuente) y 10.0.1.11 (destino).

Un procedimiento para comunicar paquetes de datos entre un primer dispositivo de comunicaciones en una primera red local y un segundo dispositivo de comunicaciones en una segunda red local opuesta, que se ejecuta por una pasarela de la primera red local, se describirá ahora con referencia al diagrama de flujo en la Fig. 3. Se supone que las direcciones IP privadas usadas en las primera y segunda redes locales para sus propios dispositivos respectivos se superponen potencialmente unas con otras, por ejemplo perteneciendo a un espacio de dirección que se reutiliza típicamente en redes locales plurales.

En un primer **paso 300**, se establece un túnel VPN con una pasarela en la segunda red local opuesta que incluye, entre otras cosas, almacenar un nombre y la dirección IP pública asociada de la pasarela opuesta, que está disponible y se puede recuperar a partir de un DDNS. En un siguiente **paso 302**, se define un espacio de dirección IP privado para la segunda red que se ha seleccionado para no estar superpuesto con el espacio de dirección IP privado usado en la primera red para sus propios dispositivos. Se supone además que la segunda pasarela opuesta define igualmente un espacio de dirección IP privado no superpuesto para la primera red también. Los pasos 300 y 302 se pueden ejecutar básicamente como se describió anteriormente para los pasos 1:2A y 1:2B.

En algún punto posterior en un paso adicional 304, se recibe un paquete de datos entrante a través del túnel VPN, cuyo paquete ha sido enviado desde el segundo dispositivo y que tiene una cabecera interna con direcciones de destino y de fuente usadas en la segunda red para los primer y segundo dispositivos, respectivamente. La primera pasarela entonces cambia las direcciones de destino y de fuente en la cabecera interna, en un siguiente **paso 306**, a unas direcciones de destino y de fuente usadas en una primera red para los primer y segundo dispositivos, respectivamente. En un último **paso 308** mostrado, el paquete se reenvía con la cabecera interna modificada al primer dispositivo. El primer dispositivo entonces es capaz de responder enviando un paquete de datos al segundo dispositivo usando la dirección de fuente recibida como dirección de destino que se traducirá de nuevo por la primera pasarela de recepción, de la manera descrita anteriormente.

Una adaptación en una primera pasarela 400 se describirá ahora en más detalle con referencia al diagrama de bloques en la Fig. 4. Se supone que la pasarela 400 está sirviendo a una primera red local, y es capaz de comunicar paquetes de datos entre un primer dispositivo de comunicaciones en la primera red local y un segundo dispositivo de comunicaciones en una segunda red local servida por una segunda pasarela. Se supone que se ha establecido un túnel VPN entre la primera pasarela y la segunda pasarela, se ha asignado una dirección IP pública a cada pasarela, y que se usan direcciones IP privadas superpuestas potencialmente para dispositivos en cada red local.

La pasarela 400 comprende medios de definición de direcciones IP 400a adaptados para definir un espacio de dirección IP interno seleccionado a ser usado en la primera red local para dispositivos en la segunda red local. El espacio de dirección IP seleccionado está separado, es decir no se superpone con, un espacio de dirección IP interno usado en la primera red local para dispositivos en la primera red local.

La pasarela 400 además comprende medios de recepción 400b adaptados para recibir un paquete de datos entrante P desde el segundo dispositivo. El paquete entrante P tiene cabeceras IP externas e internas, estas últimas que incluyen una dirección de destino interna usada en la segunda red local para el primer dispositivo y una dirección de fuente interna usada en la segunda red local para el segundo dispositivo.

La pasarela 400 también comprende medios de cambio de dirección IP 400c adaptados para cambiar la dirección de destino interna a una dirección de destino interna usada en la primera red local para el primer dispositivo, y para

cambiar la dirección de fuente interna a una dirección de fuente interna del espacio de dirección seleccionado usado en la primera red local para el segundo dispositivo y que está dentro del espacio de dirección IP interno seleccionado. Los medios de cambio de dirección IP 400c también están adaptados para eliminar la cabecera IP externa del paquete recibido.

La pasarela 400 también comprende medios de reenvío 400d adaptados para reenviar el paquete entrante P' al segundo dispositivo con una cabecera IP interna modificada que incluye las direcciones de destino y de fuente internas cambiadas. Por ello, las direcciones en la cabecera del paquete están separadas de y no pueden ser confundidas con ninguna dirección de otros dispositivos válidos en la segunda red local.

Hasta ahora, se ha descrito básicamente qué se hace en el lado de recepción de una transmisión de un paquete de datos, por ejemplo los procedimientos y funciones en la pasarela 102 en la red A en la Fig. 1 y por medio del diagrama de flujo en la Fig. 3. Ahora también se describirá con referencia al diagrama de flujo en la Fig. 5 qué se realiza por la pasarela en el lado remitente de la transmisión de un paquete de datos, por ejemplo, los procedimientos y funciones en la pasarela 104 en la red B en la Fig. 1. Usando la misma situación que para la Fig. 3, se puede ejecutar el siguiente procedimiento adicional por la primera pasarela cuando se recibe un paquete de datos saliente desde el primer dispositivo dirigido al segundo dispositivo en la segunda red opuesta.

Un primer **paso 500** ilustra de esta manera que se recibe un paquete de datos saliente que viene desde el primer dispositivo. El paquete saliente tiene una cabecera IP interna que incluye una dirección de destino interna usada en la primera red local para el segundo dispositivo y una dirección de fuente interna usada en la primera red local para el primer dispositivo. En un **paso 502** adicional, se determina el túnel VPN correcto para el paquete saliente en base a la dirección de destino interna. Por ejemplo, si los espacios de dirección IP usados incluyen direcciones basadas en IPv4, se puede asignar un número único en un segundo o tercer octeto de cada dirección IP para representar la red local opuesta correspondiente, y entonces se determina el túnel VPN correcto a partir de ese número.

En un siguiente **paso 504**, se encapsula el paquete con una cabecera IP externa que incluye las direcciones IP públicas de la primera y segunda pasarelas como direcciones de destino y de fuente externas, respectivamente, permitiendo encaminar sobre la red IP pública. En un último **paso 506**, se envía el paquete saliente a la segunda pasarela sobre la red IP pública a través del túnel VPN determinado.

Es posible establecer túneles VPN entre la primera red local y una pluralidad de redes locales opuestas. En ese caso, se define un espacio de dirección IP interno seleccionado para cada red opuesta a ser usado en la primera red local para dispositivos en cada red opuesta respectiva. Cada espacio de dirección IP seleccionado entonces debería estar separado de, es decir no superpuesto con, cualquier otro espacio de dirección usado en la primera red local.

Se puede asignar además un número único en un segundo o tercer octeto de cada dirección IP para representar cada red local opuesta correspondiente. En ese caso, se puede determinar un túnel VPN correcto para cada paquete saliente en base a ese número único en una dirección de destino interna en el paquete saliente, y el paquete se enviará entonces a través del túnel VPN determinado. Además, establecer los túneles VPN incluye añadir en la pasarela de cada red local un nombre de DNS registrado y una clave PKI pública correspondiente de cada pasarela opuesta.

Según realizaciones posibles adicionales ilustradas en la Fig. 4, se puede crear una lista de confianza 400e con partes de confianza para la primera red local en la primera pasarela 400. Cuando se recibe una petición o similar para establecer un túnel VPN con una pasarela de una red candidata 402, el túnel VPN se puede admitir para el establecimiento si la red local candidata está asociada con una primera parte presente en la lista de confianza 400e. Adicionalmente, se puede configurar la pasarela 400 de manera que el túnel VPN también se pueda admitir para el establecimiento si la red local candidata 402 está asociada indirectamente con la primera parte en la lista de confianza que está asociada con una segunda parte presente en una lista de confianza de la primera parte. La pasarela 400 se puede configurar además de manera que se pueda admitir el túnel VPN para el establecimiento dependiendo de un número predeterminado de niveles de confianza aprobados para la primera red local.

Como se mencionó anteriormente, se puede evaluar la red local candidata 402 para el establecimiento de un túnel VPN, en base a la lista de confianza 400e, en respuesta a una petición de túnel VPN R desde la red local candidata. La pasarela 400 se puede configurar además de manera que un túnel VPN establecido entre dos redes locales se termine automáticamente si se modifica una lista de confianza asociada con cualquiera de las dos redes para inhabilitar el túnel VPN.

Un procedimiento ejemplar para usar una lista de confianza de la manera anterior en una primera pasarela para peticiones de túnel VPN, se describirá ahora brevemente con referencia al diagrama de flujo en la Fig. 6. En primer lugar, se crea una lista de confianza con partes de confianza para la primera red local, como se ilustra esquemáticamente por un primer **paso 600**. Cuando se recibe una petición para el establecimiento de un túnel VPN con una pasarela en la red candidata en algún punto según un siguiente **paso 602**, la red candidata se evalúa en base a la lista de confianza creada en un siguiente **paso 604**.

Entonces se determina si se puede admitir el túnel VPN solicitado en un **paso 606**, que se puede deducir a partir de la lista de confianza como se describió anteriormente, por ejemplo considerando múltiples niveles de listas de

confianza de partes ya de confianza. Si es así, el túnel VPN se establece, como se muestra por un **paso 608** final, y se pueden comunicar paquetes de datos según la descripción anterior. Si la lista de confianza no permite el túnel VPN, se rechaza la petición o simplemente se ignora, en un **paso 610**.

Como se ilustra además en la Fig. 4, se pueden implementar las unidades funcionales en la pasarela 400 descrita anteriormente como módulos de programa de un programa informático 404 que comprende medios de código los cuales cuando se ejecutan en la primera pasarela 400 hacen a la primera pasarela realizar las funciones y los pasos anteriormente descritos de la primera pasarela. En esta realización, el programa de ordenador 4004 se transporta por un producto de programa de ordenador 406 que comprende un medio legible por ordenador en el cual se almacena el programa de ordenador.

Los módulos de programa del programa de ordenador 404 incluyen al menos un espacio de dirección que define el módulo 404a y un módulo de cambio de dirección 404b. El espacio de dirección que define el módulo 404a es capaz de definir un espacio de dirección IP interno seleccionado a ser usado en la primera red local para dispositivos en la segunda red local, el espacio de dirección IP seleccionado que está separado de, es decir no superpuesto con, un espacio de dirección IP interno usado en la primera red local para dispositivos en la primera red local.

El módulo de cambio de dirección 404b es capaz de, cuando se recibe desde el segundo dispositivo a través del túnel VPN un paquete entrante que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la segunda red local para el primer dispositivo y una dirección de fuente interna usada en la segunda red local para el segundo dispositivo, cambiar la dirección de destino interna a una dirección de destino interna usada en la primera red local para el primer dispositivo, y cambiar la dirección de fuente interna a una dirección de fuente interna del espacio de dirección seleccionado usado en la primera red local para el segundo dispositivo y que está dentro del espacio de dirección IP interno seleccionado. El paquete entrante entonces se puede reenviar al primer dispositivo con una cabecera IP interna modificada que incluye las direcciones de destino y de fuente internas cambiadas.

Los medios de código del programa de ordenador 404 y el producto de programa de ordenador 406 también pueden hacer a la primera pasarela realizar las siguientes funciones.

Cuando el paquete entrante tiene una cabecera IP externa que incluye direcciones IP públicas de la primera y segunda pasarelas como direcciones de destino y de fuente externas, respectivamente, los medios de código pueden hacer a la primera pasarela eliminar la cabecera IP externa del paquete entrante.

Cuando se recibe un paquete de datos saliente desde el primer dispositivo, el paquete saliente que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la primera red local para el segundo dispositivo y una dirección de fuente interna usada en la primera red local para el primer dispositivo, los medios de código también pueden hacer a la primera pasarela:

- encapsular el paquete con una cabecera IP externa incluyendo las direcciones IP públicas de las pasarelas como direcciones de destino y de fuente externas, respectivamente, y

- determinar el túnel VPN correcto para el paquete saliente en base a la dirección de destino interna,

antes de que se envíe el paquete saliente a la segunda pasarela a través del túnel VPN.

Los medios de código también pueden hacer a la primera pasarela establecer túneles VPN entre la primera red local y una pluralidad de redes locales opuestas, y definir un espacio de dirección IP interno seleccionado para cada red opuesta a ser usada en la primera red local para dispositivos en cada red opuesta respectiva, cada espacio de dirección IP seleccionado que está separado de, es decir no se solapa con, cualquier otro espacio de dirección usado en la primera red local.

Los espacios de direcciones IP seleccionados pueden incluir direcciones basadas en IPv4, y se puede asignar entonces un número único en un segundo o tercer octeto de cada dirección IP para representar la red local opuesta correspondiente. En ese caso, los medios de código también pueden hacer a la primera pasarela determinar un túnel VPN para cada paquete saliente en base al número único en una dirección de destino interna en el paquete saliente, en donde el paquete se envía entonces a través del túnel VPN determinado.

Los medios de código también pueden hacer a la primera pasarela establecer los túneles VPN añadiendo un nombre de DNS registrado y una clave PKI pública correspondiente de cada pasarela opuesta. La clave PKI pública y una clave PKI privada correspondiente pueden haber sido generadas para cada pasarela y las claves PKI públicas se almacenan en un servidor PKI accesible para las pasarelas.

Cuando se ha creado una lista de confianza con partes de confianza para la primera red local, los medios de código pueden hacer a la primera pasarela admitir un túnel VPN para establecimiento entre la primera red local y una red local candidata si la red local candidata está asociada con una primera parte presente en la lista de confianza.

Los medios de código también pueden hacer a la primera pasarela admitir el túnel VPN para establecimiento si la

red local candidata está asociada indirectamente con la primera parte en la lista de confianza que está asociada con una segunda parte presente en una lista de confianza de la primera parte.

Los medios de código también pueden hacer a la primera pasarela admitir el túnel VPN para establecimiento dependiendo de un número predeterminado de niveles de confianza aprobados para la primera red local.

Los medios de código también pueden hacer a la primera pasarela evaluar la red local candidata para el establecimiento de un túnel VPN en respuesta a una petición de túnel VPN desde la red local candidata.

Los medios de código también pueden hacer a la primera pasarela terminar un túnel VPN establecido entre dos redes locales automáticamente si se modifica una lista de confianza asociada con cualquiera de las dos redes para inhabilitar el túnel VPN.

Se debería señalar que la Fig. 4 ilustra meramente diversas unidades funcionales y módulos de programa ejemplares en la pasarela 400 en un sentido lógico, mientras que los expertos son libres de implementar las funciones descritas en la práctica usando cualesquiera medios de software y hardware adecuados. De esta manera, la invención no está limitada de manera general a la estructura mostrada de la pasarela 400. Por ejemplo, el producto de programa de ordenador puede ser una memoria instantánea, ROM (Memoria Solamente de Lectura) o una EEPROM (ROM Programable Borrable Eléctricamente), y los módulos de programa de ordenador descritos anteriormente podrían en realizaciones alternativas estar distribuidos en diferentes productos de programa de ordenador en forma de memorias dentro de la pasarela 400.

Aunque la invención se ha descrito con referencia a realizaciones ejemplares específicas, la descripción solamente se prende de manera genera que ilustre el concepto inventivo y no se debería tomar como limitante del alcance de la invención. La invención se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de comunicación de paquetes de datos entre un primer dispositivo de comunicaciones (E3A) en una primera red local y un segundo dispositivo de comunicaciones (E1B) en una segunda red local, en donde se usan direcciones IP privadas superpuestas potencialmente para dispositivos en las primera y segunda redes locales, que comprende los pasos de:

- establecer un túnel VPN, Red Privada Virtual, entre una primera pasarela (A) que sirve a la primera red local y una segunda pasarela (B) que sirve a la segunda red local, en donde se ha asignado una dirección IP pública a cada pasarela,

- definir, en la primera pasarela, un espacio de dirección IP interno seleccionado a ser usado en la primera red local para dispositivos en la segunda red local, el espacio de dirección IP seleccionado que está separado de, es decir no se superpone con, un espacio de dirección IP interno usado en la primera red local para dispositivos en la primera red local,

- recibir, en la primera pasarela, un paquete de datos entrante desde el segundo dispositivo (E1B) a través de dicho túnel VPN, el paquete entrante que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la segunda red local para el primer dispositivo y una dirección fuente interna usada en la segunda red local para el segundo dispositivo,

- cambiar, en la primera pasarela (A), dicha dirección de destino interna a una dirección de destino interna usada en la primera red local para el primer dispositivo,

- cambiar, en la primera pasarela (A), dicha dirección de fuente interna a una dirección de fuente interna del espacio de dirección seleccionado usado en la primera red local para el segundo dispositivo y que está dentro de dicho espacio de dirección IP interno seleccionado, y

- reenviar el paquete entrante al primer dispositivo (E3A) con una cabecera IP interna modificada que incluye el destino interno cambiado y las direcciones de fuente, **caracterizado porque** el método además comprende:

- crear una lista de confianza con partes de confianza para la primera red local, y

- admitir un túnel VPN para el establecimiento entre la primera red local y una red local candidata si la red local candidata está asociada con una primera parte presente en dicha lista de confianza.

2. Un método según la reivindicación 1, el paquete entrante que además tiene una cabecera IP externa que incluye las direcciones IP públicas de dicha primera y segunda pasarelas como direcciones de destino y de fuente externas, respectivamente, en donde la cabecera IP externa se elimina del paquete entrante por la primera pasarela.

3. Un método según la reivindicación 1 o 2, que comprende los siguientes pasos adicionales:

- recibir, en la primera pasarela, un paquete de datos saliente desde el primer dispositivo, el paquete saliente que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la primera red local para el segundo dispositivo y una dirección de fuente interna usada en la primera red local para el primer dispositivo,

- encapsular el paquete con una cabecera IP externa incluyendo las direcciones IP públicas de dichas pasarelas como direcciones de destino y de fuente externas, respectivamente,

- determinar el túnel VPN correcto para el paquete saliente en base a dicha dirección de destino interna, y

- enviar el paquete saliente a la segunda pasarela a través del túnel VPN.

4. Un método según cualquiera de las reivindicaciones 1-3, en donde los túneles VPN se establecen entre la primera red local y una pluralidad de redes locales opuestas, y se define un espacio de dirección IP interno seleccionado para cada red opuesta a ser usada en la primera red local para dispositivos en cada red opuesta respectiva, cada espacio de dirección IP seleccionado que está separado de, es decir no se superpone con, ningún otro espacio de dirección usado en la primera red local.

5. Un método según la reivindicación 1-4, en donde se admite el túnel VPN para establecimiento si la red local candidata está asociada indirectamente con dicha primera parte en la lista de confianza que está asociada con una segunda parte presente en una lista de confianza de la primera parte.

6. Un método según la reivindicación 5, en donde se evalúa la red local candidata para el establecimiento de un túnel VPN en respuesta a una petición de túnel VPN desde la red local candidata.

7. Un método según cualquiera de las reivindicaciones 5 o 6, en donde un túnel VPN establecido entre dos redes locales se termina automáticamente si se modifica una lista de confianza asociada con cualquiera de las dos redes para inhabilitar el túnel VPN.

8. Una adaptación en una primera pasarela (A) que sirve a una primera red local, capaz de comunicar paquetes de datos entre un primer dispositivo de comunicaciones (E1A) en la primera red local y un segundo dispositivo de comunicaciones (E3B) en una segunda red local servida por una segunda pasarela (B), la primera pasarela que está adaptada para establecer un túnel VPN entre la primera pasarela y la segunda pasarela en donde se ha asignado una dirección IP pública a cada pasarela, y las direcciones IP privadas superpuestas potencialmente se usan para dispositivos en cada red local, que comprende:

- medios de definición de dirección IP (400a) adaptados para definir un espacio de dirección IP interno seleccionado a ser usado en la primera red local para dispositivos en la segunda red local, el espacio de dirección IP seleccionado que está separado de, es decir no se superpone con, un espacio de dirección IP interno usado en la primera red local para dispositivos en la primera red local,

- medios de recepción (400b) adaptados para recibir un paquete de datos entrante desde el segundo dispositivo a través de dicho túnel VPN, el paquete entrante que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la segunda red local para el primer dispositivo y una dirección de fuente interna usada en la segunda red local para el segundo dispositivo,

- medios de cambio de dirección IP (400c) adaptados para cambiar dicha dirección de destino interna a una dirección de destino interna usada en la primera red local para el primer dispositivo, y para cambiar dicha dirección de fuente interna a una dirección de fuente interna del espacio de dirección seleccionado usado en la primera red local para el segundo dispositivo y que está dentro de dicho espacio de dirección IP interno seleccionado, y

- medios de reenvío (400d) adaptados para reenviar el paquete entrante al segundo dispositivo con una cabecera IP interna modificada que incluye las direcciones de destino y de fuente internas cambiadas,

en donde la adaptación se **caracteriza porque** está adaptada además para crear una lista de confianza con partes de confianza para la primera red local, y para admitir un túnel VPN para el establecimiento entre la primera red local y una red local candidata si la red local candidata está asociada con una primera parte presente en dicha lista de confianza.

9. Una adaptación según la reivindicación 8, el paquete entrante que además tiene una cabecera IP externa que incluye las direcciones IP públicas de dichas primera y segunda pasarelas como direcciones de destino y de fuente externas, respectivamente, en donde los medios de cambio de dirección IP están adaptados además para eliminar la cabecera IP externa del paquete entrante por la primera pasarela.

10. Una adaptación según la reivindicación 8 o 9, adaptada además para:

- recibir un paquete de datos saliente desde el primer dispositivo, el paquete saliente que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la primera red local para el segundo dispositivo y una dirección de fuente interna usada en la primera red local para el primer dispositivo,

- encapsular el paquete con una cabecera IP externa incluyendo las direcciones IP públicas de dichas pasarelas como direcciones de destino y de fuente externas, respectivamente,

- determinar el túnel VPN correcto para el paquete saliente en base a dicha dirección de destino interna, y

- enviar el paquete saliente a la segunda pasarela a través del túnel VPN.

11. Una adaptación según cualquiera de las reivindicaciones 8-10, en donde los túneles VPN se establecen entre la primera red local y una pluralidad de redes locales opuestas, y se define un espacio de dirección IP interno seleccionado para cada red opuesta a ser usada en la primera red local para dispositivos en cada red opuesta respectiva, cada espacio de dirección IP seleccionado que está separado de, es decir no se superpone con, ningún otro espacio de dirección usado en la primera red local.

12. Una adaptación según la reivindicación 11, en donde los espacios de direcciones IP seleccionados incluyen direcciones basadas en IPv4, y se asigna un número único en un segundo o tercer octeto de cada dirección IP para representar la red local opuesta correspondiente.

13. Una adaptación según la reivindicación 12, adaptada además para determinar un túnel VPN para cada paquete saliente en base a dicho número único en una dirección de destino interna en el paquete saliente, y entonces envía el paquete a través del túnel VPN determinado.

14. Una adaptación según la reivindicación 13, en donde el establecimiento de los túneles VPN incluye añadir en la pasarela de cada red local un nombre de DNS registrado y una clave PKI pública correspondiente de cada pasarela opuesta.

15. Una adaptación según la reivindicación 14, en donde se ha generado dicha clave PKI pública y una clave PKI privada correspondiente para cada pasarela y las claves PKI públicas están almacenadas en un servidor PKI

accesible para las pasarelas.

16. Una adaptación según la reivindicación 8, adaptada además para admitir el túnel VPN para el establecimiento si la red local candidata está asociada indirectamente con dicha primera parte en la lista de confianza estando asociada con una segunda parte presente en una lista de confianza de la primera parte.

17. Una adaptación según la reivindicación 16, adaptada además para admitir el túnel VPN para el establecimiento dependiendo de un número predeterminado de niveles de confianza aprobados para la primera red local.

18. Una adaptación según la reivindicación 16 o 17, adaptada además para evaluar la red local candidata para el establecimiento del túnel VPN en respuesta a una petición de túnel VPN desde la red local candidata.

19. Una adaptación según cualquiera de las reivindicaciones 16-18, adaptada además para terminar un túnel VPN establecido entre dos redes locales automáticamente si se modifica una lista de confianza asociada con cualquiera de las dos redes para inhabilitar el túnel VPN.

20. Un producto de programa de ordenador (400e) configurado para una primera pasarela (A) que sirve a una primera red local y es capaz de comunicar paquetes de datos entre un primer dispositivo de comunicaciones (E1A) en la primera red local y un segundo dispositivo de comunicaciones (E3B) en una segunda red local servida por una segunda pasarela (B), en donde un túnel VPN se establece entre la primera pasarela (a) y la segunda pasarela (B), una dirección IP pública se ha asignado a cada pasarela, y se usan direcciones IP privadas superpuestas potencialmente para dispositivos en cada red local, en donde el programa de ordenador comprende medios de código que cuando se ejecutan en la primera pasarela hacen a la primera pasarela:

- definir un espacio de dirección IP interno seleccionado a ser usado en la primera red local para dispositivos en la segunda red local, el espacio de dirección IP seleccionado que está separado de, es decir no se superpone con, un espacio de dirección IP interno usado en la primera red local para dispositivos en la primera red local, y

cuando se recibe desde el segundo dispositivo (E1B) a través de dicho túnel VPN un paquete entrante que tiene una cabecera IP interna que incluye una dirección de destino interna usada en la segunda red local para el primer dispositivo y una dirección de fuente interna usada en la segunda red local para el segundo dispositivo,

- cambiar dicha dirección de destino interna a una dirección de destino interna usada en la primera red local para el primer dispositivo,

- cambiar dicha dirección de fuente interna a una dirección de fuente interna del espacio de dirección seleccionado usado en la primera red local para el segundo dispositivo y que está dentro de dicho espacio de dirección IP interno seleccionado,

antes de que se reenvíe el paquete entrante al primer dispositivo (E3A) con una cabecera IP interna modificada que incluye las direcciones de destino y de fuente internas cambiadas,

en donde el programa de ordenador se **caracteriza porque** además hace a la primera pasarela:

- crear una lista de confianza con partes de confianza para la primera red local, y

- admitir un túnel VPN para el establecimiento entre la primera red local y una red local candidata si la red local candidata está asociada con una primera parte presente en dicha lista de confianza.

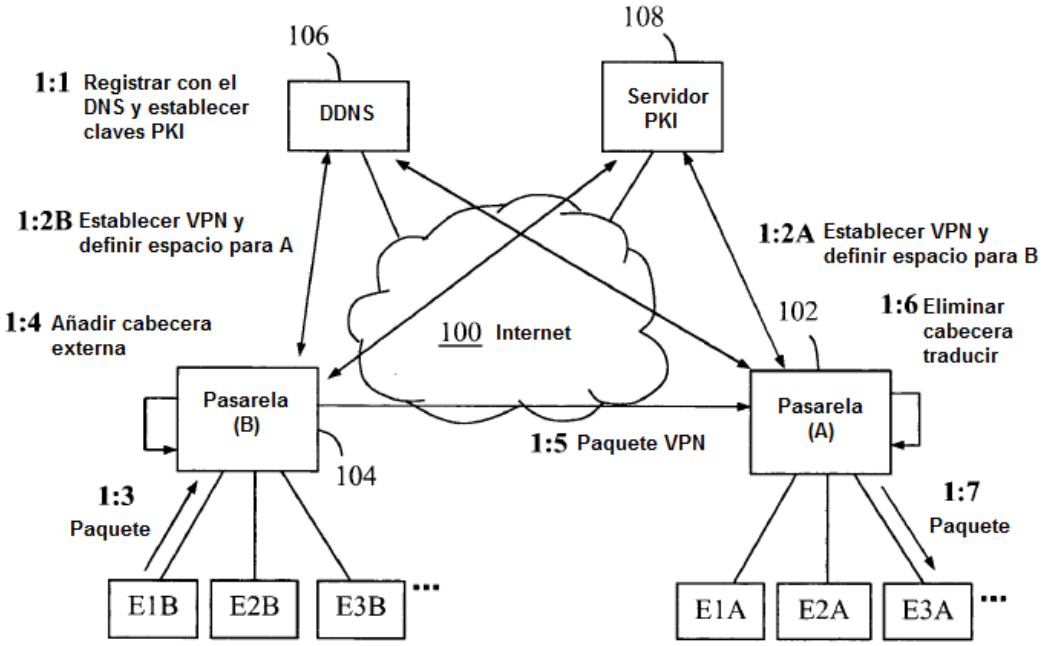
106
108
1:1 Registrar con el DNS y establecer claves PKI
DDNS
Servidor PKI
1:2B Establecer VPN y definir espacio para A
1:2A Establecer VPN y definir espacio para B
1:4 Añadir cabecera externa
100 Internet
102
1:6 Eliminar cabecera traducir
Pasarela (B)
Pasarela (A)
1:5 Paquete VPN
104
1:3 Paquete
1:7 Paquete
E1B
E2B
E3B
E1A
E2A
E3A

Fig.1

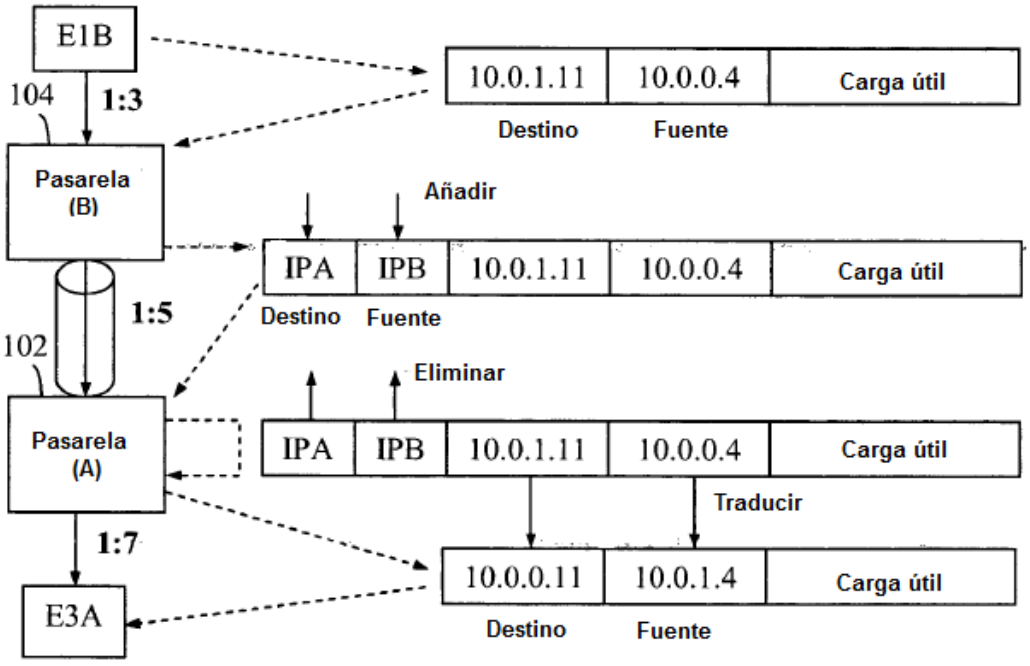
E1B
104
1:3
10.0.1.11
10.0.0.4
Carga útil
Destino
Fuente
Pasarela (B)
Añadir
IPA
IPB
10.0.1.11
10.0.0.4
Carga útil
Destino
Fuente
1:5
102
Eliminar
Pasarela (A)
IPA
IPB
10.0.1.11
10.0.0.4
Carga útil
Traducir
1:7
10.0.0.11
10.0.1.4
Carga útil
E3A
Destino
Fuente

Fig.2

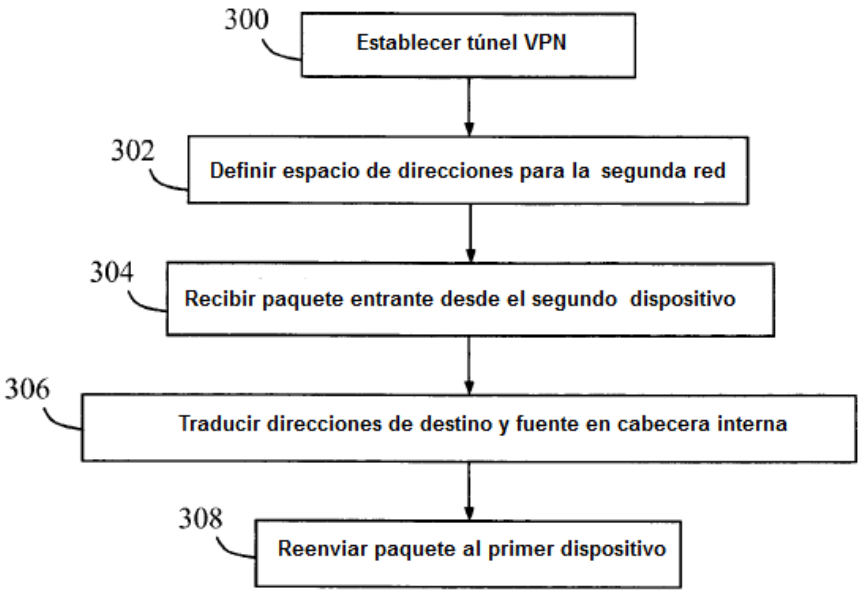
300
Establecer túnel VPN
302
Definir espacio de direcciones para la segunda red
304
Recibir paquete entrante desde el segundo dispositivo
306
Traducir direcciones de destino y fuente en cabecera interna
308
Reenviar paquete al primer dispositivo

Fig.3

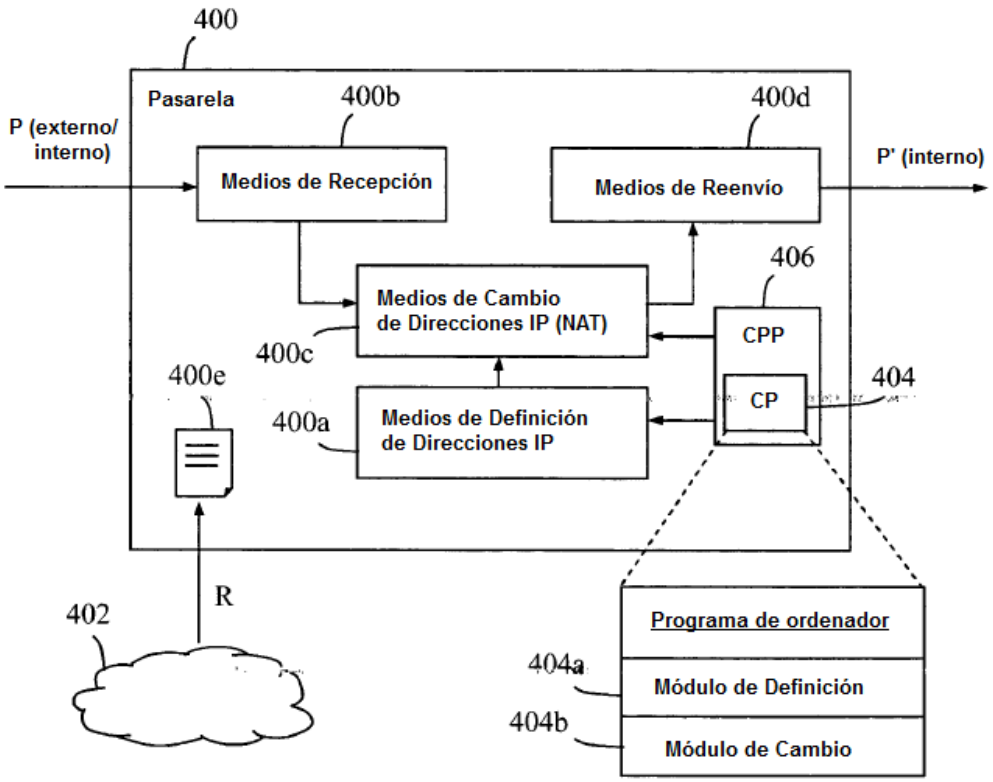
400
Pasarela
400b
400d
P (externo/ interno)
Medios de Recepción
Medios de Reenvío
P' (interno)
406
Medios de Cambio de Direcciones IP (NAT)
CPP
400c
400e
CP
404
400a
Medios de Definición de Direcciones IP
R
402
Programa de ordenador
404a
Módulo de Definición
404b
Módulo de Cambio

Fig.4

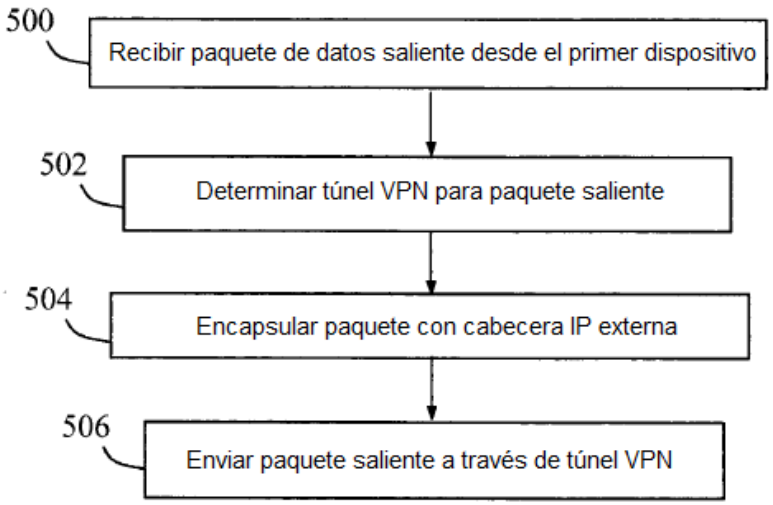
500
Recibir paquete de datos saliente desde el primer dispositivo
502
Determinar túnel VPN para paquete saliente
504
Encapsular paquete con cabecera IP externa
506
Enviar paquete saliente a través de túnel VPN

Fig.5

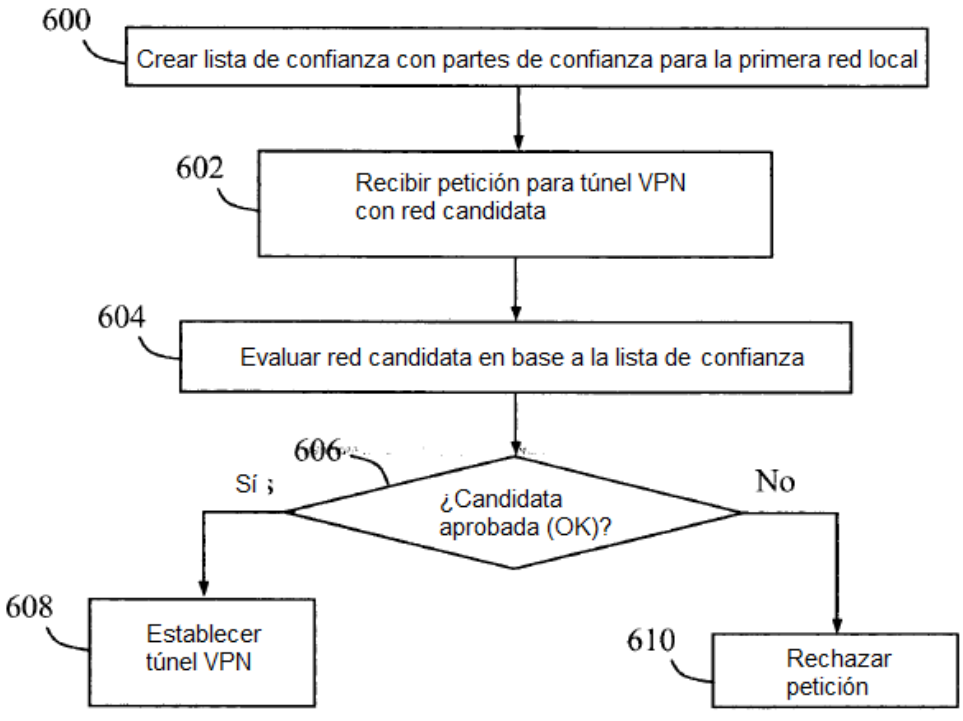
600
Crear lista de confianza con partes de confianza para la primera red local
602
Recibir petición para túnel VPN con red candidata
604
Evaluar red candidata en base a la lista de confianza
606
¿Candidata aprobada (OK)?
Sí
No
608
Establecer túnel VPN
610
Rechazar petición

Fig.6