(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 580 677**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.05.2010 E 10736596 (7)**

(97) Fecha y número de publicación de la concesión europea: **23.03.2016 EP 2436166**

(54) Título: **Interfaz de servicio**

(30) Prioridad:

28.05.2009 DE 102009022977

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.08.2016

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

ALBRECHT, ROBERT MANFRED y
BRANDT, RONALD

(74) Agente/Representante:

MORGADES MANONELLES, Juan Antonio

DESCRIPCIÓN

Interfaz de servicio

La invención se refiere a un sistema para permitir acceso a servicios u ordenadores de una primera red local a una segunda red, en donde ambas redes están conectadas a través de una red intermedia / red desmilitarizada (DMZ) común.

Campo de la invención:

En el sector del mantenimiento de ordenadores y software, existe una serie de formas de acceder a una red local de clientes potenciales. Normalmente se usa una conexión VPN (Red Privada Virtual), en la que un usuario se conecta a una red a través de una conexión encriptada al cortafuegos de la red de clientes, desde allí accediendo a los recursos correspondientes. Sin embargo, este enfoque presenta una serie de desventajas, puesto que, frecuentemente, la red privada virtual no está sujeta a ninguna restricción de modo que se tiene acceso a toda la red y, además, tiene el problema de que el cortafuegos que proporciona acceso VPN debe ser accesible directamente desde internet.

El objeto de la presente invención es ofrecer una prestación alternativa de servicios a usuarios que trabajan en una primera red privada y que requieren los servicios de una segunda red privada. Tal escenario puede producirse cuando un empleado que trabaja con la empresa A está también contratado por la empresa B y desea consultar sus correos electrónicos almacenados en la empresa B. Con este objeto, normalmente tendría que conectarse a la empresa B a través de una conexión VPN de la red de la empresa B para poder leer los mensajes de correo en su ordenador. Sin embargo, esto supone que el ordenador en el que está trabajando tiene instalado el software de cliente necesario y que cuenta con los derechos de acceso necesarios en el cortafuegos de la red A de la empresa A.

Desde la “Guía del Administrador de Citrix Access Gateway Enterprise Edition” de noviembre de 2008, se conoce la configuración de una puerta de enlace según esa especificación. Desde “Firewalls for Dummies”, 2003, Wiley Publishing, se conoce la configuración de los cortafuegos. La memoria US2005/198380A1 también se refiere al control de acceso a redes.

Resumen de la invención:

El objeto de la presente invención es proporcionar acceso a servicios en una primera red local A desde una segunda red local B, en donde ambas redes están protegidas por un cortafuegos, y ambas redes están conectadas a través de una red situada entre los cortafuegos. Por lo tanto, podrían determinarse derechos de acceso y podría aplicarse la limitación a ciertos servicios.

El objeto se consigue mediante un método con las características de las reivindicaciones independientes.

Debe tenerse en cuenta que una red A, protegida por un cortafuegos Fa, está conectada por una red Nab en una posible realización como una DMZ, a una red B, que a su vez está protegida por un cortafuegos Fb. En detalle, la presente memoria trata acerca de una red A en la que un usuario U1 trabaja con su ordenador C1. Esto requiere acceso a una red B para que pueda usar los servicios S1. Un posible servicio S1 podría ser, por ejemplo, el acceso al servidor de correo o al servidor de terminales. Otros servicios también son posibles, tales como servidores de archivos, bases de datos u otros similares.

Para permitirlo, el usuario U1/C1 accede mediante una autenticación adecuada en el cortafuegos Fa. En la realización preferida se utilizan tarjetas inteligentes. Según la autenticación, puede fijarse una norma para que ese usuario pueda acceder solo a un servidor SNab específico dentro de la red Nab, es decir, dentro de la DMZ. Dicho servidor, también llamado servidor de salto, gestiona las aplicaciones. En una realización preferida, un servidor de terminales o un servidor de transmisión de aplicaciones, tal y como ofrece, por ejemplo, Citrix, o un servidor Unix/Linux que administre y proporcione aplicaciones. Las aplicaciones, como programas de correo que funcionan en este servidor SNab, a su vez acceden a través del cortafuegos Fb a la red B para recuperar datos allí almacenados. En caso de un servidor de correo, se facilita al usuario el programa Outlook<(R)> o Lotus Notes<(R)> en el servidor de salto para que pueda acceder a dicha aplicación. Sin embargo, los datos del correo personal están en un servidor de correo que funciona en la red B. Así, debe determinarse que el servidor SNab también puede acceder a la red B. Esto se consigue asignado a un usuario que haya accedido al servidor SNab una dirección IP única. Esto requiere un gran rango de direcciones IP, que se seleccionan preferiblemente del grupo de direcciones IP privadas. También es posible que se asignen a un usuario múltiples direcciones IP. A los usuarios se les asigna direcciones IP desde un directorio central (por ej. LDAP).

Cuando el usuario se ha autenticado en el servidor SNab y ha lanzado su aplicación, se le asigna una dirección única del rango de direcciones asignadas. Con esta dirección la aplicación puede acceder a la red B a través del cortafuegos Fb. Desde la dirección IP, el cortafuegos Fb reconoce al usuario y puede, en función de normas

específicas, determinar a qué servidor SNb de la red B puede acceder el usuario. Por ejemplo, un usuario que solo desea comprobar sus mensajes de correo electrónico, simplemente accede al servidor de correo electrónico de la red B. Según la dirección IP, el cortafuegos Fb puede acceder a reglas a través del servicio de directorio que determina a qué servidor SNb puede acceder el usuario. Debe tenerse en cuenta que en otra realización el usuario también debe autentificarse en el cortafuegos Fb.

En la realización preferida las reglas se administran en un LDAP. Se trata de un directorio que gestiona centralmente las reglas y la autenticación de usuarios.

Además, en una realización preferida se escoge un enfoque con un inicio de sesión único. Según la presente memoria, el usuario inicia su sesión o se autentica solo una vez y luego puede acceder a diferentes servicios sin tener que repetir la autenticación. Además, los servicios realizan consultas de fondo para comprobar si la persona ya está registrada correctamente en otro sistema admisible. De no seleccionarse el enfoque de inicio de sesión único, normalmente son necesarias tres autenticaciones. La primera autenticación se produce en el cortafuegos Fa, la segunda en el servidor Sab y la tercera en el cortafuegos Fb.

En una realización preferida, la red HP es una DMZ. Una zona desmilitarizada (DMZ, también zona desmilitarizada) denota una red de ordenadores con opciones de acceso a servidores conectados controladas mediante seguridad. Los sistemas dispuestos en la DMZ están protegidos por uno o más cortafuegos contra otras redes (por ejemplo, Internet, LAN). Mediante esta separación se permite el acceso a servicios disponibles de difusión (servidores bastión, por ejemplo, correo electrónico, WWW, u otros parecidos) mientras que la red interna (LAN) está protegida del acceso no autorizado.

Los servidores de la DMZ acceden al servidor de la red B sobre la red B a través de una conexión segura. En otra realización posible, la conexión entre el ordenador del usuario y el servidor Sab también está encriptado, al igual que la conexión del servidor Sab a la red B. Esto puede realizarse desde el cortafuegos Fa o desde el ordenador del usuario.

En una realización alternativa, hay múltiples cortafuegos Fa, Fa1, …, Fan que están dispuestos de forma redundante, de modo que el acceso a un ordenador de la DMZ puede realizarse en cualquier momento. Así, también puede accederse a diferentes DMZ a través del cortafuegos cuando no puede alcanzarse una de las DMZ, o los servidores de la DMZ. Por ejemplo, si una DMZ está situada en Europa y la otra DMZ está en EE.UU., y resulta que una de las dos DMZ se cae, el cortafuegos Fa pasará automáticamente a otra DMZ, en la que, normalmente, también pueden encontrarse servidores alternativos (servicios de salto). También es posible que dentro de una DMZ se dispongan más de un servidor de salto, a los que puede accederse en función de la carga de trabajo. El equilibrado de la carga, que garantiza una utilización razonable de los servidores, se realiza mediante un sistema de proxy ascendente, dispuesto antes del servidor, o a través del propio cortafuegos, que remite las solicitudes basadas en un algoritmo determinado, tal como Round-robin. Al utilizar servidores Citrix pueden usarse las técnicas para el equilibrado de la carga proporcionadas por el productor.

Descripción de las figuras:

A continuación, se describen brevemente las figuras. Las figuras y la siguiente descripción detallada no pretenden limitar la invención:

La Fig. 1 muestra la estructura básica de las diferentes redes con los servidores y los usuarios;

La Fig. 2 muestra la estructura de un enfoque redundante de los servidores de salto y cortafuegos.

Descripción de una realización preferente de la invención:

La Fig. 1 muestra la parte frontal de un primer cortafuegos 7, también referido como Fb, un servidor de salto 1, que permite a los usuarios 2, 3 acceder a las aplicaciones de la red B. El servidor de salto remite las solicitudes al servidor 16 o al servidor 15. Debe tenerse en cuenta que en esta configuración el servidor de salto no está dispuesto detrás del cortafuegos 7, sino delante del cortafuegos. Se trata de una excepción fundamental al enfoque presentado.

En el cliente VPN, con un tubo dividido selectivo, el túnel dividido puede estar activo, en casos individuales.

El servidor de salto transmite la aplicación (transfiere el archivo de programa junto con algunos archivos de control) al ordenador del usuario. Allí se ejecuta en un entorno protegido (aislamiento de procesos, un tipo de máquina virtual). Las opciones de comunicación de la aplicación pueden limitarse a través de los archivos de control transmitidos. Estos regulan si se permite a la aplicación acceder a medios de almacenamiento local, si se les permite acceder a otros recursos de red, ...

Puesto que los archivos de control se transfieren individualmente para cada aplicación, es posible regular las opciones de comunicación de cada aplicación: el llamado túnel dividido selectivo.

Con tunelización dividida real el comportamiento es distinto.

El cliente VPN incluye la posibilidad de bloquear el túnel dividido al establecer el túnel VPN. Al establecer el túnel, el cliente VPN bloquea las comunicaciones con todas las redes excepto con su propio túnel.

Esta función del cliente VPN se controla a través de un archivo de control situado en el disco duro local del ordenador del usuario. Según la presente memoria el túnel dividido puede activarse o desactivarse.

Como función adicional, en el momento de establecer el túnel el cliente VPN ofrece la posibilidad de comprobar la configuración del ordenador del usuario en relación con determinadas características. Dichas características pueden ser, por ejemplo, fecha de archivo o la presencia de un archivo determinado o de su contenido. La presencia de determinados procesos o claves de registro también puede comprobarse,

Al establecer un túnel, el contenido del archivo de control se comprueba para activar/desactivar el túnel dividido. Si dicho archivo no satisface los requisitos, el túnel no se establecerá con éxito. Por lo tanto, un usuario con derechos de administración no puede también establecer el túnel con un túnel dividido activo. En cambio, sí que puede cambiar el contenido del archivo de control, aunque fallaría el establecimiento del túnel.

El usuario de la red B quiere acceder a una aplicación, como, por ejemplo, un servidor de correo 15, 16. En una primera alternativa, se accede al servidor de salto 1, que tiene la misma función que los servidores de salto 10 y 9, que están dispuestos, no obstante, en la DMZ detrás del cortafuegos 7. El servidor de salto envía entonces la solicitud a través de una conexión encriptada virtual (VPN) a los servidores 16, 15, 14, 13. Si el redireccionamiento se realiza a través de un servidor de salto dispuesto entre los cortafuegos 7 y 8, la información 18 se transmitirá al cortafuegos 7, donde tiene lugar una autenticación. Según la información utilizada en la autenticación, tal como reglas y derechos de acceso, la solicitud se remite al servidor de salto. A continuación, se lleva a cabo la autenticación en los servidores de salto 10, 9 de nuevo explícitamente o a través del enfoque de inicio de sesión único. Esto puede realizarse mediante diversos enfoques, según corresponda, a través de un servicio de directorio (LDAP). Tras establecer una conexión con este servidor de salto, las solicitudes 19 se dirigen a través del cortafuegos 8 o 7 a los correspondientes servidores 16, 15, 14 y 13, en los que se utilizan las direcciones IP únicas asignadas con este propósito a los usuarios por el servidor de salto. Cada usuario posee una dirección IP única, o un grupo de direcciones IP únicas, que permiten extraer conclusiones sobre la identidad del usuario. Estas direcciones IP se almacenan, por ejemplo, en el LDAP. Al utilizar estas direcciones IP únicas en el servidor de salto, se produce el acceso a los servidores 13-16. Para acceder al servidor 13, debe atravesarse el cortafuegos 8 Fa, que reconoce al usuario en base a la dirección IP y otra información de autenticación. Según un conjunto de reglas 20, entonces se determina a través de qué servidor 13 puede producirse el acceso a la red A. El mismo enfoque puede también realizarse por los usuarios 11 y 12 desde la red A. Además, la red A cuenta con un servidor local 23 que no participa en el acceso.

La Fig. 2 muestra un enfoque redundante. Aquí, hay una serie de cortafuegos, cada uno de los cuales permite acceso a un servidor de salto. En caso que uno de los servidores o cortafuegos fallara, las solicitudes se redireccionan a través de un cortafuegos distinto u otro servidor de salto del país que corresponda, garantizando la redundancia.

Lista de referencia

1 Servidor de salto
2 Usuario de la red B
3 Usuario de la red B
5 Excepción de túnel dividido
6 Túnel SSL
7 Cortafuegos del sistema T / puerta VPN
8 Cortafuegos A
9 Servidor de salto Unix
10 Servidor de salto Windows
11 Usuario de la red A
12 Usuario de la red A
13 DMZ descentralizada en ubicación A
14 DMZ física
15 Servidor VPN único
16 DMZ descentralizada en ubicación B
17
18 Conexión IP directa
19 Filtro de entrada al servidor de salto

20 Filtro de salida desde el servidor de salto
21 Límite entre la ubicación A y la ubicación B
22 Servidor en la ubicación B
23 Servidor en la ubicación A

REIVINDICACIONES

1. Un método para garantizar el acceso de un usuario U1 con su ordenador C1 a una primera red local A para acceder a servicios digitales (13, 15, 16) en una segunda red local B, en donde ambas redes están protegidas por un cortafuegos (7, 8), y en donde ambas redes están conectadas a través de una red Nab, dispuesta entre los cortafuegos, que comprende los pasos siguientes:

- Autenticación del usuario U1 en el primer cortafuegos (7, 8);
- Con la autenticación se determina una regla según la cual el usuario U1 puede acceder a un servidor de salto específico (13, 15, 16) dentro de la red Nab;
- Acceder al servidor de salto (9, 10) y autenticación del usuario U1 en el servidor de salto (9, 10), y asignar una dirección IP única en función de la autenticación;
- Acceder al servicio (13, 15, 16) de la segunda red B a través del servidor de salto (9, 10), en donde se produce la autenticación de la dirección IP en el segundo cortafuegos (7, 8);
- Determinar una regla en el segundo cortafuegos (7, 8) en base a la dirección IP para verificar si se permite acceso al servicio (13, 15, 16), si se permite un acceso, pasar la solicitud del servidor de salto (9, 10) a la segunda red B para acceder al servicio (13, 15, 16).

2. El segundo según la reivindicación anterior, en donde una o más direcciones IP utilizadas por el servidor de salto se asignan de forma exclusiva a un usuario.

3. El método según una o más de las reivindicaciones anteriores, en donde las reglas y/o las direcciones IP de un usuario se almacenan en un directorio central tal como LDAP.

4. El método según una o varias de las reivindicaciones anteriores, en donde se utiliza un método de inicio de sesión único para autenticarse en el primer cortafuegos y el segundo cortafuegos y/o al servidor de salto.

5. El método según una o más de las reivindicaciones anteriores, en donde la red Nab es una zona desmilitarizada, DMZ.

6. El método según una o más de las reivindicaciones anteriores, en donde las conexiones entre el cortafuegos, el servidor de salto y los servicios están encriptadas.

7. El método según una o más de las reivindicaciones anteriores, en donde hay una pluralidad de cortafuegos diseñados para redundancia, de modo que se puede acceder en cualquier momento a un servidor de salto en una o más DMZ.

8. El método según una o más de las reivindicaciones anteriores, en donde los cortafuegos se dirigen a diferentes DMZ, si alguna de las DMZ no fuera alcanzable o no pudieran alcanzarse los servidores de la DMZ.

9. El método según una o varias de las reivindicaciones anteriores, en donde se produce el equilibrado de la carga de una pluralidad de servidores de salto, para evitar la sobrecarga de un lado de los servidores de salto.

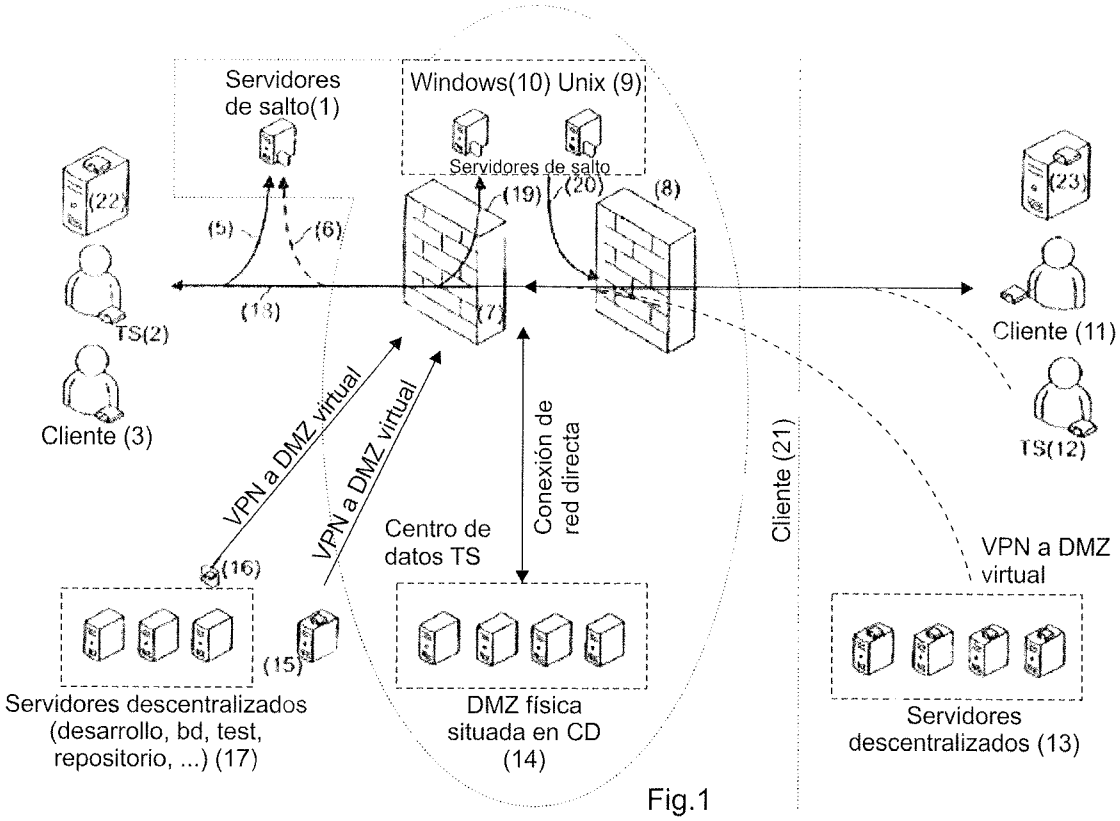
Servidores de salto(1)
Windows(10) Unix (9)
Servidores de salto
(22)
(5)
(6)
(19)
(20)
(8)
(23)
(13)
(7)
TS(2)
Cliente (3)
Cliente (11)
TS(12)
VPN a DMZ virtual
VPN a DMZ virtual
Conexión de red directa
Centro de datos TS
Cliente (21)
(16)
(15)
VPN a DMZ virtual
Servidores descentralizados (desarrollo, bd, test, repositorio, ...) (17)
DMZ física situada en CD (14)
Servidores descentralizados (13)

Fig.1

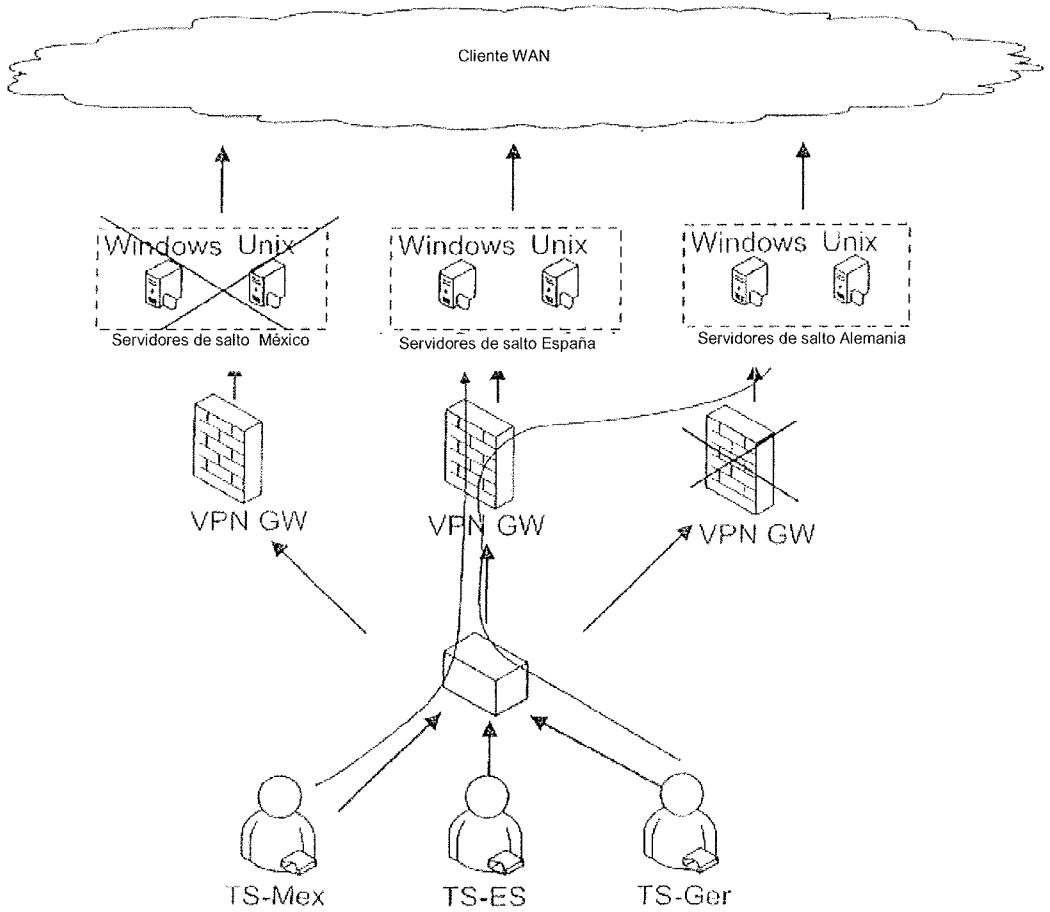
Cliente WAN
Windows Unix
Servidores de salto México
Windows Unix
Servidores de salto España
Windows Unix
Servidores de salto Alemania
VPN GW
VPN GW
VPN GW
TS-Mex
TS-ES
TS-Ger

Fig. 2