(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 245**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.07.2005 E 05775366 (7)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 1782265**

(54) Título: **Sistema y procedimiento para conectividad de red segura**

(30) Prioridad:

30.07.2004 US 903941

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.01.2016

(73) Titular/es:

BARCLAYS CAPITAL INC. (100.0%)
200 PARK AVENUE
NEW YORK, NY 10166, US

(72) Inventor/es:

ENGLE, MICHAEL T.;
NWOKOBIA, FREDERICK;
NOACK, BRADLEY D. y
MAKOWIECKI, JERZY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Sistema y procedimiento para conectividad de red segura

Antecedentes de la invención

Muchas empresas permiten a los usuarios acceder a las redes y recursos corporativos internos externamente. Uno de estos procedimientos utiliza una conexión de red privada virtual (VPN). En un escenario típico, un usuario que trabaja en un ordenador remoto se conecta a Internet e inicia un programa VPN del lado del cliente. El programa VPN utiliza un protocolo de red aceptable para acceder al ordenador de puerta de enlace VPN de la empresa. El ordenador de puerta de enlace, por ejemplo, un servidor VPN, autentica al usuario y establece una sesión de trabajo en red remoto para el usuario remoto. Uno de los beneficios de una sesión VPN de este tipo, es que el ordenador del usuario remoto parece estar directamente en la red de la empresa.

Las redes corporativas internas suelen ser amortiguadas o aisladas de la red o de Internet externo, por razones de seguridad. El tráfico de Internet en, y fuera de la red interna se puede filtrar en base a la política de seguridad de la corporación. Las políticas de seguridad pueden restringir el acceso a archivos y bases de datos, o pueden limitar o prohibir el acceso a cualquier recurso de la empresa, para los ordenadores que tienen acceso ilimitado a Internet. Por ejemplo, sólo determinados usuarios u ordenadores, pueden ser autorizados para establecer conexiones de red externas y comunicarse con el mundo exterior; sin embargo, estos ordenadores pueden ser excluidos de acceder a bases de datos que almacenan los datos del cliente. Esto se hace para proteger los recursos de la empresa y los ordenadores de los virus y otras amenazas que existen. Otras políticas de seguridad pueden requerir la verificación y el cumplimiento de los controles de seguridad corporativos antes de iniciar una sesión en la red interna.

Esta forma de aislamiento interno suele ser adecuada cuando no hay usuarios remotos autorizados a conectarse a la red corporativa interna. Sin embargo, hay un problema fundamental con permitir a los usuarios remotos acceder a los recursos corporativos internos, mientras que se aplican los requisitos de la política de seguridad corporativa. Esto es evidente en que un ordenador remoto normalmente accede a Internet sin filtro, o simplemente un cortafuegos, en su lugar. En esta situación, cuando un ordenador remoto se conecta a un servidor de la empresa a través de una conexión VPN, la corporación no puede imponer su política de seguridad interna en el ordenador del cliente. De este modo, el ordenador remoto es capaz de acceder a datos críticos, es decir, que parece estar conectado directamente a la red interna, sin cumplir los mismos requisitos de seguridad interna, y sin ser amortiguado de las amenazas externas. Esta es una preocupación para la seguridad de la empresa en que los ordenadores remotos comprometidos ganarían acceso sin restricciones a la red corporativa.

Este peligro puede ser mitigado si el ordenador remoto está protegido adecuadamente y no es comprometido durante el uso de la VPN. Sin embargo, dado que el ordenador remoto no está bajo el control directo de la empresa, este no puede garantizarse con los procedimientos actuales de seguridad manejados por el cliente.

Varios intentos se han implementado para abordar estas cuestiones, sin embargo, ninguno proporciona plenamente el cumplimiento estricto de la política de seguridad corporativa. La mayoría de las soluciones dependen de las políticas de seguridad del ordenador del cliente, o la ejecución implementada por el cliente de una política de seguridad, antes de permitir el acceso a VPN. Por ejemplo, muchos programas de cliente VPN comprueban la presencia de un escáner de virus y, posiblemente, un cortafuegos personal en el ordenador del cliente remoto. Esta información puede ser útil para el servidor, pero no garantiza que un ordenador del cliente no se vea comprometido. Por otra parte, ciertos virus pueden eludir los detectores de virus y cortafuegos, o un ordenador remoto puede quedar comprometido durante una sesión VPN activa.

Otros controles de seguridad se pueden ejecutar en el ordenador del cliente, tales como la verificación a las definiciones de virus actualizadas, o asegurar que los programas de seguridad, como la familia de productos BlackICE™, están presentes. Sin embargo, estas soluciones todavía dependen de la verificación iniciada por el cliente, y la información del cliente verificado se presenta al servidor. En el caso de que el ordenador del cliente se vea comprometido, la información inexacta puede pasar al servidor.

Por lo tanto, sigue habiendo una necesidad de sistemas y procedimientos para verificar el estado de configuración de un ordenador remoto antes de permitir que el ordenador remoto acceda a la red interna.

El documento WO 02/03178 se refiere a un procedimiento y un aparato para la evaluación de la red y la autenticación. Durante un proceso de inicio de sesión local, una evaluación de ordenador principal local de la estación de trabajo de un usuario se lleva a cabo antes de solicitar las credenciales del usuario. La estación de trabajo incluye un servicio de evaluación de estación de trabajo local que genera credenciales de la estación de trabajo, completando una evaluación de vulnerabilidad de la estación de trabajo. Un cliente de red recupera las credenciales y las proporciona a un servicio de red a través de una red informática. El servicio de red determina si se debe dar servicio a una estación de trabajo junto a la red informática basada en las credenciales de la estación de trabajo.

El documento WO 2004/057834 se refiere a un sistema para la administración de la protección de datos accesibles por uno o más dispositivos móviles. El sistema tiene un módulo de autorización, un módulo de distribución de la

política, un módulo de gestión de la política y un módulo de diagnóstico remoto. El módulo de autorización autoriza un intercambio de comunicación entre un dispositivo móvil del cliente y los módulos de distribución o de gestión de la política.

Sumario de la invención

De acuerdo con la invención, se proporciona: un procedimiento para un servidor según la reivindicación 1; un procedimiento para un ordenador remoto según la reivindicación 17; un medio legible por ordenador según la reivindicación 23; un aparato según la reivindicación 24; y una red segura según la reivindicación 25.

Las realizaciones de la presente invención proporcionan un procedimiento para asegurar que un ordenador remoto que realiza una conexión VPN está protegido adecuadamente. Por consiguiente, una realización, se requiere un control de seguridad impulsado por el servidor de la máquina remota antes de permitir cualquier conexión VPN. Estos controles manejados por el servidor son preferentemente adaptables y configurables para proporcionar conexiones VPN seguras. Los controles de seguridad manejados por servidores se pueden configurar sobre qué verificar y cómo debe llevarse a cabo la verificación. Un servidor puede primero ser configurado con cualquier número de niveles de acceso de usuario remoto. Los controles de seguridad manejados por el servidor pueden ser configurados para verificar el cumplimiento de cada nivel de acceso antes de que se conceda el acceso a ese nivel, es decir, los controles de acceso limitado al servidor suelen ser menos estrictos que los controles de acceso ilimitado al servidor. De esta manera, tanto los recursos de cliente como del servidor se pueden utilizar de manera eficiente para otorgar el nivel de acceso requerido. Además, los controles de seguridad pueden requerir la verificación de nivel de acceso iterativo, en lugar de la verificación de todos los niveles a la vez. Además, los controles de seguridad pueden estar configurados de tal manera que cada comunicación con el cliente es tratada de forma independiente, y la información acumulada se incluye en cada ciclo de comunicación cliente-servidor.

En otra realización, los controles de seguridad se adaptan a la información recibida desde el ordenador remoto para determinar si se requiere información adicional antes de que se permita el acceso VPN. Por ejemplo, cuando un cliente transmite información de que un programa o proceso en particular está activo, el control de seguridad puede exigir de forma adaptativa que el cliente transmita entradas de registro o archivos .dll asociados en uso por el programa o proceso. Cuando el servidor está convencido de que el programa o proceso en particular es seguro, el servidor puede a continuación, comprobar de forma adaptativa otros programas, procesos, etc., en su lugar en el ordenador del cliente.

Sobre la base de los controles de seguridad configurados, y el análisis de seguridad adaptativo, se concede el acceso VPN a un ordenador remoto. En una realización, un testigo es proporcionado por un servidor a un ordenador cliente. El ordenador del cliente puede pasar a este testigo al programa cliente VPN, o la aplicación VPN, para su uso al iniciar la sesión en el servidor VPN. El servidor puede requerir que el testigo se actualice cada cierto intervalo de tiempo, por ejemplo, 10 segundos, 1 minuto y 1 hora, para asegurar que el ordenador remoto sigue cumpliendo con la política de seguridad corporativa. Por otra parte, el testigo puede contener información sobre el nivel de acceso a conceder al ordenador remoto basado en el análisis de los controles de seguridad manejados por el servidor.

Los beneficios de dicha verificación manejada por el servidor incluyen ser fácilmente configurable por el usuario y los perfiles de seguridad de grupo sin la necesidad de actualizar los ordenadores clientes. Además, uno de una pluralidad de niveles de acceso puede concederse sobre la base de pruebas de conformidad. Además, se pueden añadir pruebas de conformidad o modificarse para permitir una respuesta oportuna a las vulnerabilidades recién descubiertas y las contraseñas se pueden cambiar en cualquier intervalo para evitar ataques de repetición.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra una realización preferida del presente sistema y procedimiento;

La figura 2 es un diagrama de bloques que ilustra aspectos de la realización preferida de la figura 1 con más detalle;

La figura 3 es un diagrama de flujo que ilustra aspectos de la operación del sistema en una realización preferida del presente sistema y procedimiento;

La figura 4 es un diagrama de flujo que ilustra aspectos de la operación del sistema en otra realización preferida del presente sistema y procedimiento;

La figura 5 es una captura de pantalla ejemplar de selección de acceso de nivel de usuario en una realización del presente sistema y procedimiento.

La figura 6 es una lista de información de configuración que puede ser usada en algunas realizaciones de la presente invención; y

La figura 7 es una captura de pantalla ejemplar de un ciclo de la comunicación cliente-servidor en una realización del presente sistema y procedimiento; y

Descripción detallada de las realizaciones preferidas

La figura 1 ilustra una realización preferida del presente sistema y procedimiento. Se muestran en la figura 1 servidores 102A-102N adaptados para comunicarse con una pluralidad de ordenadores clientes 104A-104N a través de Internet 110. Un servidor de seguridad 114 también se pueden conectar entre cada ordenador del cliente e Internet como se muestra en la figura 1, o entre los servidores 102 e Internet (no mostrado).

También se muestra en la figura 1 son las redes internas corporativas (112A-112N) y bases de datos corporativas (108A-108N) conectadas a los servidores 102. Como se reconocerá por aquellos expertos en la materia, muchos servidores pueden estar presentes, incluyendo servidores de conmutación por fallos y equilibrio de carga. Además, cualquier conexión de red adecuada puede ser implementada en lugar de Internet 110, aunque se prefiere la conexión utilizando HTTP o HTTPS. Además, otros recursos de la empresa pueden ser accesibles a través de servidores 102, aunque estos recursos no se ilustran en la figura 1. Ejemplos de recursos de la empresa pueden ser, pero no se limitan a, impresoras, servidores de correo electrónico, servidores de aplicaciones, servidores proxy y escáneres.

La figura 2 ilustra aspectos del presente sistema y procedimiento en detalle. Los componentes 102, 104, y 110 corresponden a componentes idénticos mostrados en la figura 1. Un servidor 102 está conectado preferiblemente a Internet a través de la conexión 200. Como se describió anteriormente, cualquier conexión de red adecuada puede ser implementada para facilitar la comunicación entre servidores y clientes.

Se muestra además en la figura 2, los clientes 104. Cada uno de los clientes, o ordenador remoto, tiene un sistema operativo en ejecución, así como una pluralidad de aplicaciones 206. El sistema operativo puede incluir un registro que contiene la información de configuración del sistema operativo y de las aplicaciones. Estas aplicaciones pueden ser aplicaciones de procesamiento de documentos, navegadores de Internet, aplicaciones de audio o video, programas de correo electrónico, programas antivirus, juegos u otras aplicaciones que un usuario puede optar por instalar. Cada cliente comprende, preferiblemente, una aplicación de cliente VPN 204. La aplicación de cliente VPN facilita la comunicación entre el ordenador remoto y el servidor, y una vez que se establece una conexión VPN, proporciona a un usuario la capacidad de acceder a los recursos de la red corporativa. La aplicación cliente VPN está adaptada preferentemente para realizar los controles de seguridad requeridos por el servidor 102. Como se reconocerá, otras aplicaciones secundarias (206) se pueden utilizar para realizar la conexión VPN, tales como Cisco VPN Client®. El programa cliente VPN, o la aplicación secundaria VPN, se pueden configurar con una lista de servidores disponibles y una lista de localizaciones de puertas de enlace disponibles VPN (Nueva York, Londres, Tokio, etc., por ejemplo).

Tal como se describe en detalle a continuación, los servidores 102 pueden estar configurados con grupos de usuarios o perfiles, lo que permite diferentes niveles de acceso a los recursos corporativos. Como se describe en detalle a continuación, un perfil define un grupo web mediante los distintos niveles de acceso y restricciones de recursos corporativos, así como el nombre del grupo y contraseñas de grupo requeridos para conectarse a la VPN a un nivel de acceso particular. Como se reconocerá, niveles de acceso más bajos concedidos a un ordenador cliente normalmente representan menos peligro para la red corporativa.

En una realización, el ordenador remoto solicita un perfil particular desde el servidor 102. El servidor asigna preferiblemente el perfil solicitado al cliente después de que se verifica que el cliente cumple con la política de seguridad corporativa correspondiente a ese perfil. En otra realización, el servidor asigna al cliente un perfil basado en el nivel real de cumplimiento de las políticas de seguridad del cliente. En otra realización, el servidor puede asignar al cliente un perfil predeterminado según lo establecido por la política de seguridad configurada.

Cada grupo de usuarios también pueden ser protegidos por una contraseña. En consecuencia, un cliente puede ser obligado a proporcionar una contraseña antes de que el servidor asigne el ordenador remoto al grupo solicitado. Las contraseñas de grupo pueden ser cambiadas periódicamente, y los perfiles actualizados, para evitar que los usuarios capturen el perfil y lo utilicen para conectarse al servidor (repetición), evitando en su lugar así los controles de seguridad. Dado que las contraseñas se pueden cambiar mediante programación, una corporación puede actualizar las contraseñas de grupo en cualquier intervalo tal como, por ejemplo, 10 segundos, 1 minuto, o 1 hora, reduciendo así la eficacia de un ataque de repetición.

En una realización, el servidor 102 puede requerir un testigo con una solicitud de inicio de sesión. Este testigo comprende preferiblemente un perfil de servidor asignado. Estos testigos de inicio de sesión se pasan preferentemente desde el servidor al cliente después de que el servidor determina que el cliente cumple con un nivel de acceso determinado. En otra realización, el propio perfil se transmite al cliente, y se utiliza en el proceso de inicio de sesión. Como se reconocerá, el servidor puede requerir otros datos para un inicio de sesión de ordenador remoto, como un nombre de usuario y contraseña, número de identificación de seguridad, u otra información de validación de seguridad de usuario, como se conoce en la técnica. Por otra parte, el servidor puede requerir que el perfil o testigo se incluya en la solicitud de inicio de sesión, y también puede revalidar el cumplimiento de la política

de seguridad, la contraseña de grupo, asignación de perfiles de cliente, etc., en cualquier momento.

La figura 3 es un diagrama de flujo que ilustra una realización preferida que ilustra el funcionamiento del sistema de inicio de sesión para un ordenador remoto. En una realización preferida, un ordenador ejecutando un programa almacenado en un medio legible por ordenador mantiene el funcionamiento del sistema. Como se muestra en la figura 3, en la etapa 302, se inicia una instancia de cliente VPN 204 en el ordenador remoto. En una realización, el cliente VPN puede intentar iniciar la sesión en un servidor 102 y el funcionamiento fluiría directamente a la etapa 306. Sin embargo, como se ha descrito anteriormente, el servidor 102 puede requerir que el ordenador remoto presente un testigo con una solicitud de inicio de sesión. Por consiguiente, en una realización preferida, el cliente VPN solicita un testigo desde el servidor 102 (etapa 304). Además, en otras realizaciones, el ordenador remoto solicita un determinado servidor de puerta de enlace VPN, un servidor de perfiles en particular, o un punto de acceso VPN particular con su solicitud de testigo. Típicamente, la información del perfil relacionada está preconfigurada para cada usuario, pero estos parámetros pueden ser alterados, por ejemplo, cuando el usuario se desplaza.

Después de que el cliente VPN solicita un testigo, o intenta iniciar sesión en el servidor, el ordenador remoto recibe datos desde el servidor en la etapa 306. En la etapa 308, la aplicación del cliente VPN determina si un testigo (o perfil) está presente en los datos recibidos. Si un testigo (o perfil) está presente, la operación pasa a la etapa 314. Si hay un testigo (o perfil) presente, la aplicación del cliente procesa los datos recibidos desde el servidor.

En una realización, los datos comprenden una solicitud para que el cliente recoja datos relacionados con un grupo de usuarios solicitado o asignado. La solicitud de datos puede estar formateada en XML, HTML, u otro procedimiento de formato adecuado. La petición de datos puede requerir que el ordenador remoto recoja la información de seguridad u otra, y puede contener acciones que el ordenador remoto debe o tiene que realizar. En una realización, hay acciones ejecutables se incluyen en la solicitud de datos. En otras realizaciones, el servidor puede proporcionar un programa que se ejecute en el ordenador remoto. El programa puede ser, por ejemplo, una aplicación, guion, o un enlace a un programa en red. En algunas realizaciones, el programa puede residir en el ordenador remoto. En algunas realizaciones, el programa proporcionado por el servidor puede ejecutarse de forma automática en el ordenador remoto sin intervención directa del usuario.

La recopilación de datos solicitada por el servidor puede incluir, pero no se limita a: un chequeo de si existe una clave del registro (obtener las propiedades de esa clave); una lista de sub-claves de la clave de registro; una lista de valores en una clave de registro; un valor en una clave de registro; atributos de un directorio del disco; una lista de los archivos en un directorio; regresar atributos de un archivo de disco; contenido de un archivo de disco (límite de tamaño modificable); una lista de servicios instalados en la máquina remota (incluye el estado actual); detalles de un servicio o proceso en particular; una lista de los procesos en ejecución o aplicaciones disponibles en la máquina de destino; una lista de variables de entorno del usuario actual; información general de la máquina y del sistema operativo (versión, paquete de servicio construido); e información del programa de cliente general (VPNConnect).

Acciones para llevar a cabo por el cliente pueden incluir, pero no se limitan a, mostrar un mensaje al usuario y opcionalmente, si el usuario lo solicita, abrir una URL web. Si la URL no es http, https, o ftp, el cliente puede mostrar una advertencia adicional que puede no ser seguro abrir este URL. Típicamente, la URL está pensada como una manera de señalar al usuario a una página web que describe con más detalles las condiciones que deben ser satisfechas por el ordenador cliente antes de que se le permita acceder a la red; y ejecutar una actualización de definiciones antivirus.

La aplicación de cliente VPN procesa la solicitud(es), y después de los datos se procesan y se recogen, los datos se transmiten al servidor en la etapa 312. Las etapas 306-312 se repiten, indicadas por la caja de trazos 320, hasta que se recibe el testigo o perfil. En la etapa 314, el testigo o el perfil se pasan al cliente VPN y el cliente inicia sesión en el servidor en la etapa 316.

La figura 4 es un diagrama de flujo que ilustra una realización preferida que ilustra el funcionamiento del sistema para el procesamiento de servidor de inicio de sesión. Como se muestra en la figura 4, en la etapa 402, el servidor está configurado para el acceso VPN. En una realización, el servidor está configurado con grupos de usuarios definidos o perfiles que tienen diferentes niveles de acceso. Estos niveles de acceso pueden incluir, pero no están limitados a, acceso completo, acceso intermedio, acceso menor y sin acceso, que puede definirse además como el nivel de acceso predeterminado. La configuración de cada nivel de acceso o grupo puede alterarse en cualquier momento en el servidor, y de esta manera, la política de seguridad de la empresa puede adaptarse a las nuevas amenazas que puedan surgir. Los perfiles pueden incluir, pero no están limitados a, el nivel de acceso de grupo, nivel de acceso a los recursos, el acceso de puerta de enlace basado en el perfil, la dirección IP para el servidor VPN, la edad del perfil o testigo, y las restricciones de acceso específicos. La figura 5 muestra una captura de pantalla ejemplar de selección de acceso de nivel de usuario en una realización de la presente invención.

Cada servidor 102 también está configurado con uno o más archivos de control de seguridad (controles de seguridad) que definen las pruebas a realizar para un nivel de acceso particular y restricciones de nivel de acceso que se pueden aplicar si cualquier prueba de seguridad fallara. Como se reconocerá, no es necesario que una prueba de fallo para dar lugar a una denegación de acceso, más bien, la política de seguridad en su lugar simplemente puede restringir el acceso al siguiente nivel inferior, es decir, de acceso intermedio a nivel de acceso

bajo. A modo de ejemplo solamente, los archivos de control también pueden contener cualquiera de los siguientes: lista de archivos resultantes en la negación; lista del registro de entradas, claves o valores resultantes en la negación; archivos requeridos para el acceso a un determinado nivel; entradas del registro, claves o valores requeridos para el acceso a un nivel determinado; versiones de productos necesarios para el acceso a un nivel determinado; servicio de estado requerido para el acceso a un nivel determinado; y los mensajes de la pantalla en el ordenador remoto.

Además, los archivos de control podrán requerir que el sistema operativo tenga parches actualizados o parches de seguridad instalados. Cuando los programas, procesos, entradas de registro, etc. desconocidos o no definidos, se encuentran en el ordenador remoto, la política de seguridad se puede configurar para negar o restringir el acceso a la red interna y al mismo tiempo transmitir un mensaje al usuario indicando la misma. Ciertas aplicaciones de terceros, entradas de registro, claves de registro, o valores del registro en el ordenador remoto se pueden definir para hacer que el servidor niegue o restrinja el acceso a la red interna. La figura 6 muestra la lista de dicha información o estado de configuración ejemplar prohibida que puede usarse en algunas realizaciones de la presente invención para negar o restringir el acceso a la red interna.

Como será reconocido, puede existir cualquier número de perfiles en, o ser accesible para, el servidor. Cada perfil puede requerir un diferente nivel de cumplimiento de la seguridad antes de que el servidor distribuya el perfil al ordenador remoto. Por ejemplo, un perfil que solo permita el pleno acceso a las aplicaciones puede tener unos requisitos de seguridad más estrictos que un perfil que solo permita el acceso completo a los servidores de correo electrónico. Cualquier combinación de nivel de acceso de grupo y de recursos corporativos puede ser implementada para proporcionar la política de seguridad más adaptable a la red corporativa. Por ejemplo, los recursos tales como impresoras, servidores de correo electrónico, aplicaciones, servidores proxy, etc., se pueden definir con las restricciones de política de seguridad en cada uno de los grupos de usuarios deseados.

En una realización alternativa, la solicitud de testigo se transmite a un servidor de perfil independiente que existe independientemente (física o lógicamente) del servidor de puerta de enlace VPN. El servidor de perfiles contiene preferentemente el perfil y la información de seguridad del recurso relacionado por cada ubicación de puerta de enlace VPN, es decir, un perfil para cada nivel de acceso para cada puerta de enlace VPN. Los perfiles pueden contener información sobre la forma en que el cliente VPN debe conectarse a los servidores VPN. Esta información puede incluir direcciones IP o nombres DNS de los servidores VPN adecuados para la ubicación y el nombre del grupo en esos servidores correspondientes al nivel de acceso del perfil y la contraseña correspondiente. Los testigos se pasan desde el servidor de perfiles en el ordenador remoto, y estas testigos se utilizan para la conexión con el servidor de puerta de enlace VPN. De esta manera, los recursos del servidor VPN no se utilizan para la asignación de perfil y otras tareas relacionadas con la seguridad.

En la etapa 404, el servidor 102 recibe un testigo o solicitud de acceso desde un ordenador remoto. El servidor 102 analiza la solicitud de testigo y realiza pruebas en los datos en base a los archivos de control de seguridad en la etapa 406. Las pruebas correspondientes a los requisitos de seguridad de la red interna y verifican que el ordenador remoto no se vea comprometido. Por ejemplo, las pruebas pueden verificar las claves o las entradas del registro, el directorio de disco y atributos, los atributos de aplicaciones, los atributos de archivo, los servicios instalados, los procesos en ejecución, las variables ambientales de usuario, la máquina remota y la información del sistema operativo, la información del cliente VPN, la información del programa anti-virus, o información de definición de virus del ordenador remoto. Como se mencionó anteriormente, estas pruebas pueden ser modificadas o nuevas pruebas agregadas en cualquier momento para hacer frente a la nueva amenaza de seguridad, o para proporcionar perfiles o niveles de acceso diferentes. Por otra parte, cualquier combinación de estas pruebas se puede implementar para proporcionar el nivel de seguridad deseado.

Si los datos recibidos cumplen con la política de seguridad del perfil solicitado o asignado, el servidor transmite un testigo al cliente en la etapa 412. Si los datos no se cumplen, el servidor puede determinar la información adicional necesaria para determinar el cumplimiento en la etapa 408. Como se reconocerá, poca o ninguna información puede estar presente con la solicitud de testigo inicial. En esta situación, el servidor puede determinar que todas las pruebas deben realizarse y, en consecuencia, el servidor solicita los datos correspondientes desde el ordenador remoto. La solicitud de datos adicionales se transmite al ordenador remoto en la etapa 410.

El servidor recibe el seguimiento de la información, y el proceso continúa a través de las etapas 404 hasta 410 para un número predeterminado de iteraciones, o hasta que se reciben los datos de prueba conforme. El cuadro de líneas discontinuas etiquetado 420, en la figura 4, ilustra el proceso iterativo de la recepción de datos en el servidor, la evaluación de los datos, el procesamiento de los datos para las nuevas solicitudes de información, y la transmisión de la petición de datos.

En una realización, el servidor retiene el estado de la negociación con el ordenador remoto. De esta manera, cada solicitud es tratada como un conjunto independiente de datos. Si los datos de prueba son incompletos, toda la lista de datos requerida se envía de vuelta al cliente. En otra realización, sólo los datos de las pruebas adicionales necesarias se solicitan desde el ordenador remoto. En una realización preferida, puede ser necesario para el ordenador remoto extender la solicitud dos o tres veces antes de que la solicitud contenga toda la información requerida por el servidor.

En otra realización, el servidor no puede saber qué información se necesitará desde un ordenador remoto en particular hasta después de que haya recibido la petición de señal inicial desde el ordenador remoto. El servidor analiza la solicitud de testigo y se identifican las pruebas de seguridad que se deben realizar con el fin de otorgar un perfil determinado al cliente. El servidor transmite las solicitudes de datos identificados en el ordenador remoto y recibe los datos correspondientes a las pruebas requeridas desde el ordenador remoto. El servidor analiza los datos, y determina si los datos son suficientes para otorgar el perfil. Con respecto a este seguimiento de datos, el servidor determina si se requiere información adicional. Por ejemplo, el servidor no puede saber solicitar la ruta de un archivo hasta que recibe una entrada de registro o disco que indica que existe un archivo, o, el servidor no puede saber verificar la integridad del archivo .dll o la integridad macro hasta que reciba proceso relacionado o datos de aplicación.

El servidor evalúa la solicitud de seguimiento para determinar si se deben ejecutar las pruebas adicionales. Si es así, el servidor transmite solicitudes de datos adicionales repitiendo las etapas anteriores 420. Después de que se han realizado todas las evaluaciones de adaptación, el servidor podrá conceder un perfil particular. Sin embargo, si se han realizado todas las pruebas definidas y el servidor determina que la seguridad todavía puede verse comprometida, se podrá conceder un menor nivel de acceso a nivel de perfil más bajo, o ningún acceso. Por ejemplo, una corporación puede no tener parámetros de prueba para un proceso en particular, por lo que el servidor no puede evaluar el proceso y, en consecuencia, el servidor restringe el acceso a los recursos corporativos. La figura 7 es una captura de pantalla ejemplar de un ciclo de comunicación cliente-servidor en una realización de la presente invención que ilustra los intercambios repetidos de información entre el ordenador remoto y el servidor antes del establecimiento de una conexión entre el ordenador remoto y el servidor.

Habiendo descrito así al menos formas de realización ilustrativas de la invención, varias modificaciones y mejoras se les ocurrirán fácilmente a los expertos en la técnica y se pretende que estén dentro del ámbito de la invención. En consecuencia, la descripción anterior es a modo de ejemplo solamente y no se pretende como una limitación. La invención sólo está limitada tal como se define en las siguientes reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para un servidor (102) para permitir a un ordenador remoto (105) el acceso a una red interna que comprende:

recibir (404) una petición de acceso desde el ordenador remoto;

solicitar y recibir información del ordenador remoto que representa un estado de configuración del ordenador remoto, estando la información solicitada basada al menos en la solicitud de acceso recibida desde el ordenador remoto;

determinar (406) el cumplimiento del ordenador remoto con una política de seguridad basada al menos en la información recibida desde el ordenador remoto;

solicitar (410) y recibir información adicional desde el ordenador remoto si el ordenador remoto no está en conformidad con la política de seguridad, estando la solicitud de información adicional basada al menos en la información recibida y en la política de seguridad; y

permitir (412) el acceso del ordenador remoto a la red interna si el ordenador remoto está en conformidad con la política de seguridad.

2. El procedimiento de la reivindicación 1, que comprende además denegar el acceso a la red interna si la información adicional recibida incluye un estado de configuración prohibido.

3. El procedimiento de la reivindicación 1, en el que la etapa de permitir incluye además transmitir un testigo al ordenador remoto.

4. El procedimiento de la reivindicación 3, en el que el testigo expira después de un período predeterminado.

5. El procedimiento de la reivindicación 3, en el que la petición de acceso incluye un nivel de acceso solicitado, siendo el nivel de acceso solicitado seleccionado a partir de una pluralidad de niveles de acceso mantenidos por la red interna, autorizando cada uno de la pluralidad de niveles de acceso el acceso a un recurso de red.

6. El procedimiento de la reivindicación 5, en el que el testigo recibido incluye un nivel de acceso concedido.

7. El procedimiento de la reivindicación 6, en el que el nivel de acceso concedido no es el nivel de acceso solicitado cuando, en base a los datos recibidos, el ordenador remoto no cumple con una política de seguridad asociada con el nivel de acceso solicitado, pero cumple con una política de seguridad asociada con el nivel de acceso concedido.

8. El procedimiento de la reivindicación 3, en el que el servidor (102) tiene una pluralidad de niveles de acceso, comprendiendo cada nivel un perfil de usuario correspondiente a un nivel de acceso, y en el que la etapa de determinación comprende la evaluación de la petición de acceso para el cumplimiento con al menos uno de la pluralidad de niveles de acceso.

9. El procedimiento de la reivindicación 8, que comprende además una etapa de evaluación de la información adicional recibida para el cumplimiento con al menos uno de la pluralidad de niveles de acceso.

10. El procedimiento de la reivindicación 9, que comprende además repetir las etapas de solicitar y recibir información adicional y evaluar la información adicional recibida hasta que la respuesta recibida cumpla con al menos uno de la pluralidad de niveles de acceso.

11. El procedimiento de la reivindicación 10, que comprende además la actualización de los niveles de acceso cuando se disponga de nuevos datos, garantizando así el cumplimiento de la seguridad sin actualizar los datos en ordenadores remotos.

12. El procedimiento de la reivindicación 10, en el que la etapa de evaluación de la información adicional recibida comprende verificar que la información adicional recibida cumple con al menos uno de la pluralidad de niveles de acceso, y el uso de la información adicional recibida para determinar al menos otra solicitud de datos de seguridad a transmitir si la información adicional recibida no cumple con al menos uno de la pluralidad de niveles de acceso

13. El procedimiento de la reivindicación 10, en el que los niveles de acceso comprenden acceso completo, acceso intermedio, acceso de bajo nivel, y no acceso, a los recursos del servidor.

14. El procedimiento de la reivindicación 10, en el que la etapa de evaluación de la información adicional recibida comprende además negar el acceso al ordenador servidor si la información adicional recibida incluye un estado de configuración prohibido.

15. El procedimiento de la reivindicación 1, en el que la etapa de solicitar y recibir información comprende transmitir al ordenador remoto un programa para su ejecución por el ordenador remoto, siendo la información solicitada

generada por el programa en el ordenador remoto.

16. El procedimiento de la reivindicación 15, en el que el programa es ejecutado automáticamente por el ordenador remoto.

17. Un procedimiento para un ordenador remoto (170) para acceder a una red interna asegurada (170) que comprende:

(a) transmitir (304) una solicitud de acceso a un servidor de puerta de enlace (160) en comunicación con la red interna;

(b) recibir (306) una solicitud de datos desde el servidor de puerta de enlace que solicita información que representa un estado de configuración del ordenador remoto, estando la información solicitada basada al menos en la solicitud de acceso;

(c) transmitir (312) la información solicitada al servidor de puerta de enlace;

(d) recibir (306) una solicitud de datos desde el servidor de puerta de enlace solicitando información adicional si el ordenador remoto no está en conformidad con la política de seguridad, estando la solicitud de información adicional basada al menos en la información recibida y en la política de seguridad;

(e) transmitir (312) la información adicional solicitada al servidor de puerta de enlace;

(f) repetir las etapas (d) - (e) hasta que se reciba un testigo (308) desde el servidor de puerta de enlace; y

(g) transmitir (316) el testigo recibido para acceder a la red interna.

18. El procedimiento de la reivindicación 17, en el que la petición de acceso incluye un nivel de acceso solicitado, siendo el nivel de acceso solicitado seleccionado de una pluralidad de niveles de acceso mantenidos por la red interna, autorizando cada uno de la pluralidad de niveles de acceso el acceso a un recurso de red.

19. El procedimiento de la reivindicación 18, en el que el testigo recibido incluye un nivel de acceso concedido.

20. El procedimiento de la reivindicación 19, en el que el nivel de acceso concedido no es el nivel de acceso solicitado cuando, en base a los datos transmitidos, el ordenador remoto no cumple con una política de seguridad asociada con el nivel de acceso solicitado, pero cumple con una política de seguridad asociada con el nivel de acceso concedido.

21. El procedimiento de la reivindicación 17, en el que la etapa de recibir (306) una solicitud de datos comprende además: la recepción de un programa desde el servidor de puerta de enlace; y ejecutar el programa.

22. El procedimiento de la reivindicación 17, en el que el testigo recibido expira después de un período predeterminado.

23. Un medio legible por ordenador que comprende instrucciones para controlar un ordenador para llevar a cabo un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 22.

24. Un aparato configurado para llevar a cabo un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 22.

25. Una red segura que comprende:

una red de comunicación interna; y
un ordenador de puerta de enlace conectado a la red de comunicación interna y una red de comunicación externa, estando el ordenador de puerta de enlace configurado para llevar a cabo un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 16.

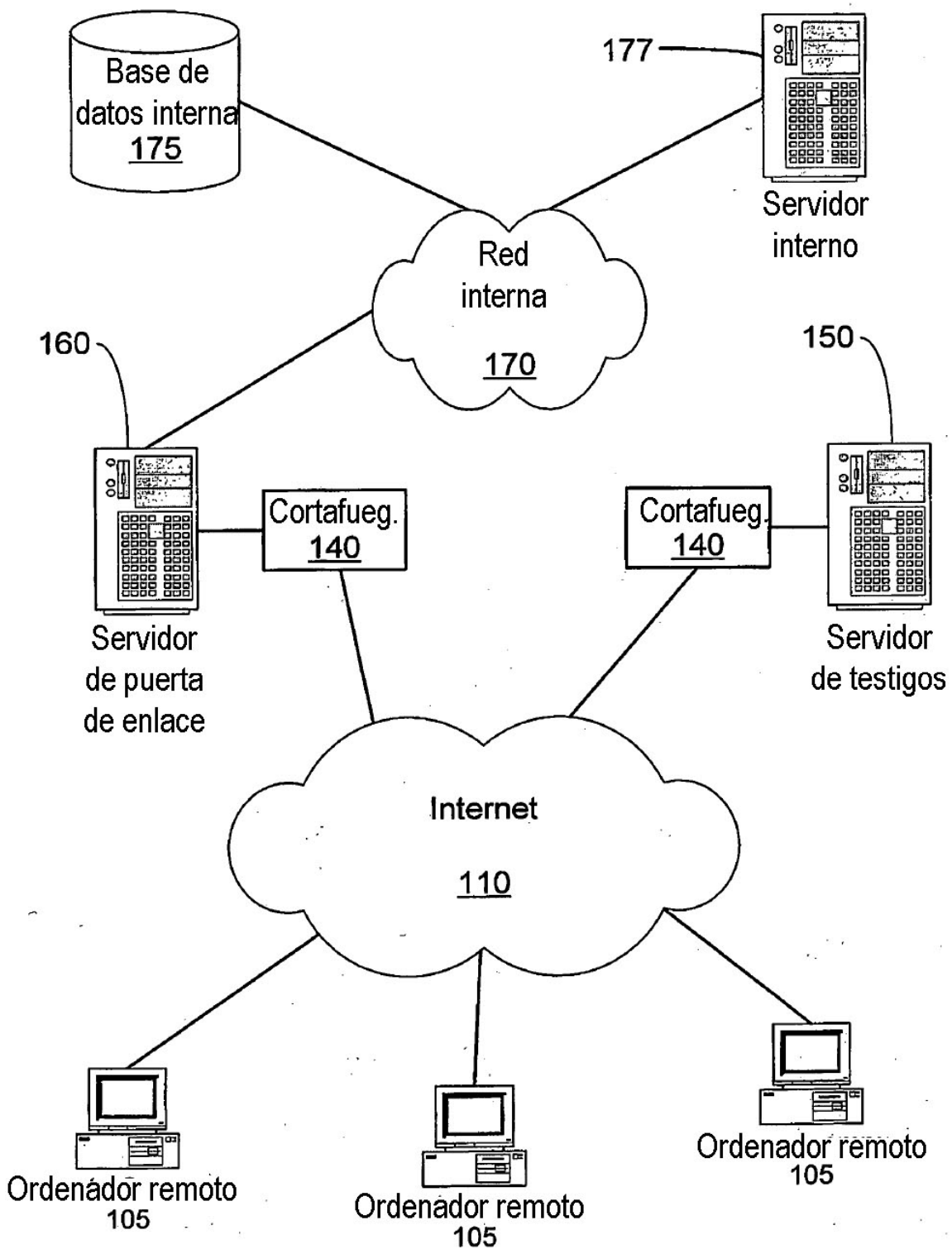
Base de datos interna 175
177
Servidor interno
Red interna 170
160
150
Cortafueg. 140
Cortafueg. 140
Servidor de puerta de enlace
Servidor de testigos
Internet 110
Ordenador remoto 105
Ordenador remoto 105
Ordenador remoto 105

Fig. 1

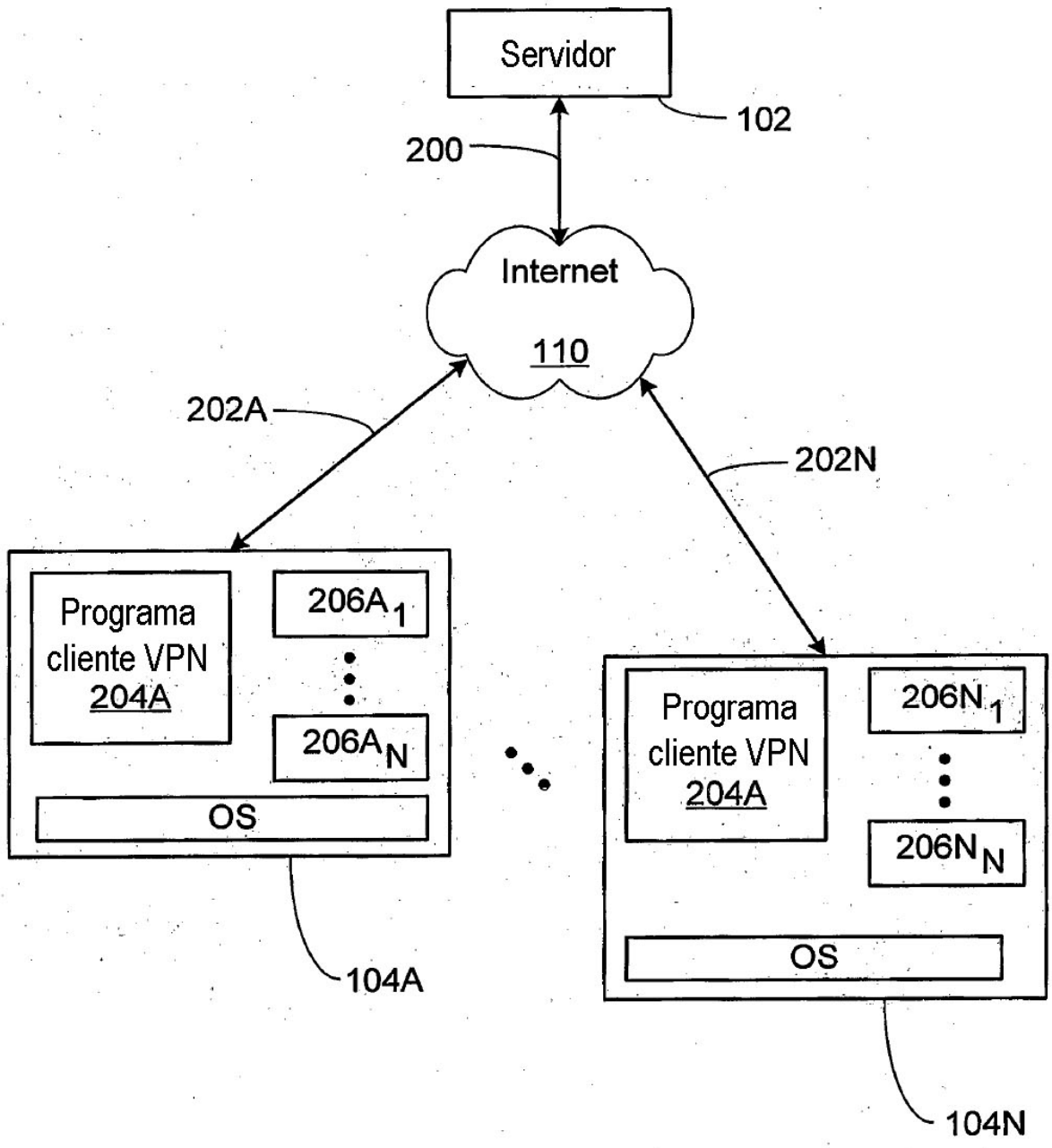
Servidor
102
200
Internet
110
202A
202N
Programa cliente VPN 204A
206A 1
206A N
OS
104A
Programa cliente VPN 204A
206N 1
206N N
OS
104N

Fig. 2

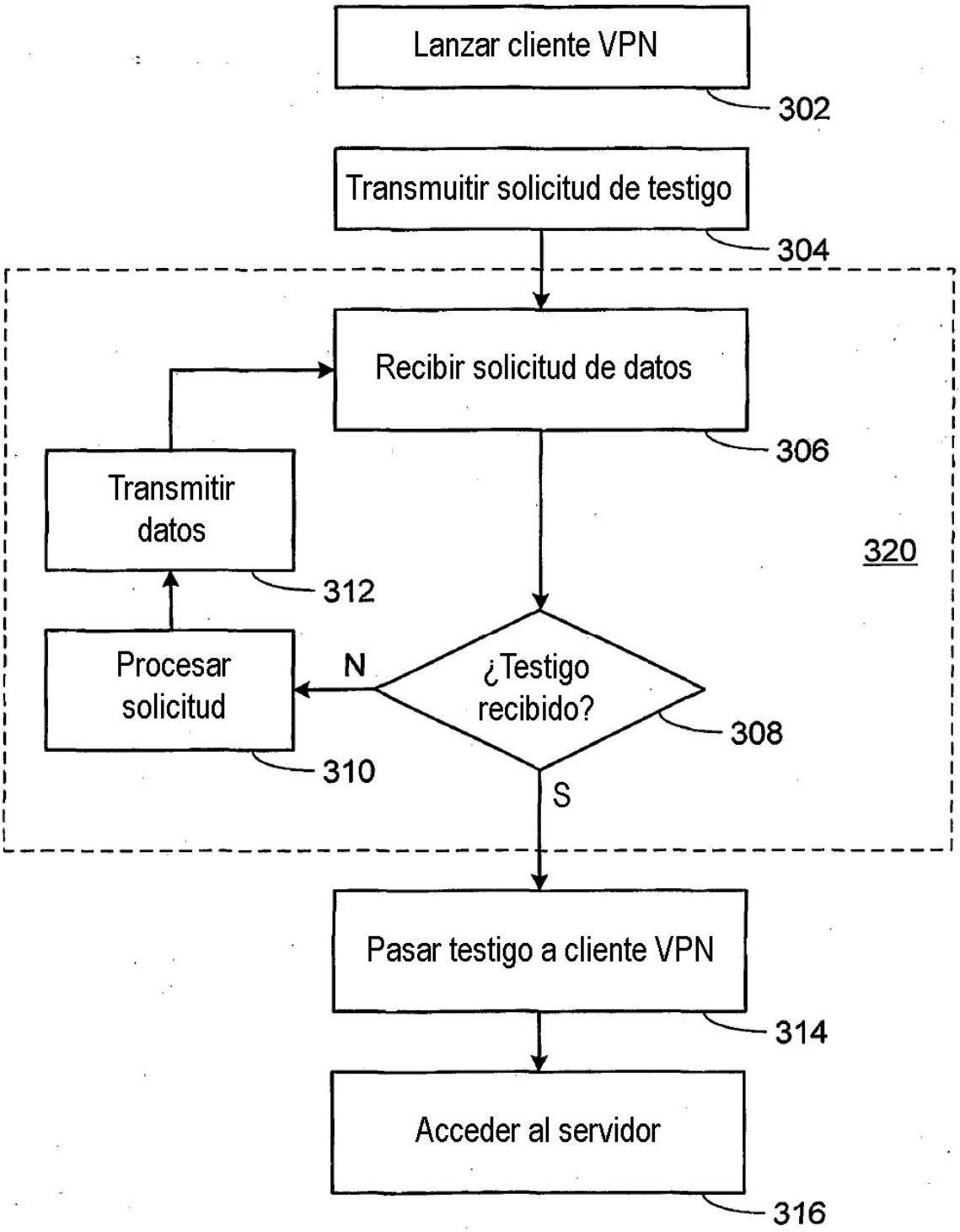
Lanzar cliente VPN
302
Transmuitir solicitud de testigo
304
Recibir solicitud de datos
306
Transmitir datos
312
320
Procesar solicitud
310
N
¿Testigo recibido?
308
S
Pasar testigo a cliente VPN
314
Acceder al servidor
316

Fig. 3

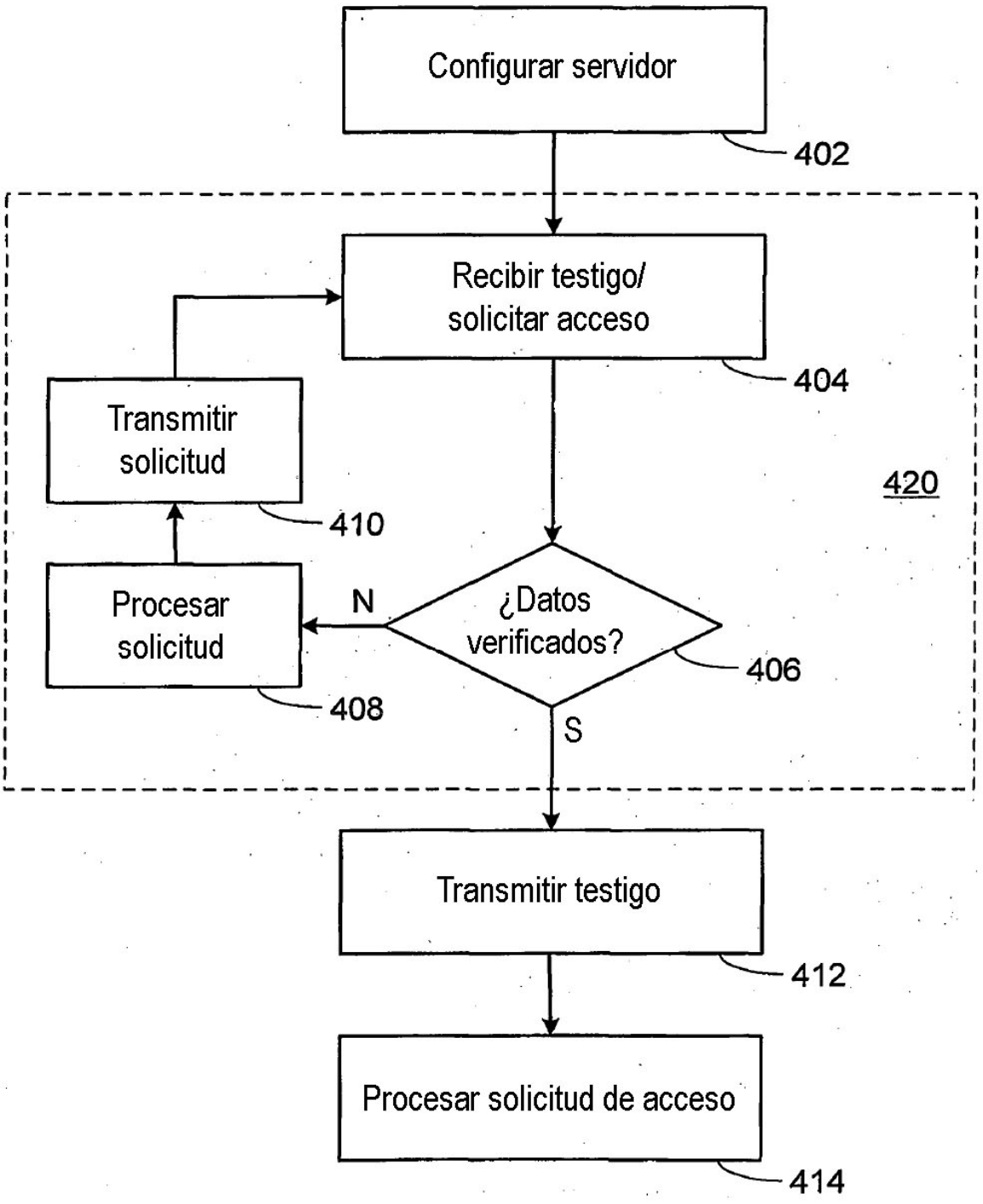
Configurar servidor
402
Recibir testigo/
solicitar acceso
404
Transmitir
solicitud
410
420
Procesar
solicitud
408
N
¿Datos
verificados?
406
S
Transmitir testigo
412
Procesar solicitud de acceso
414

Fig. 4

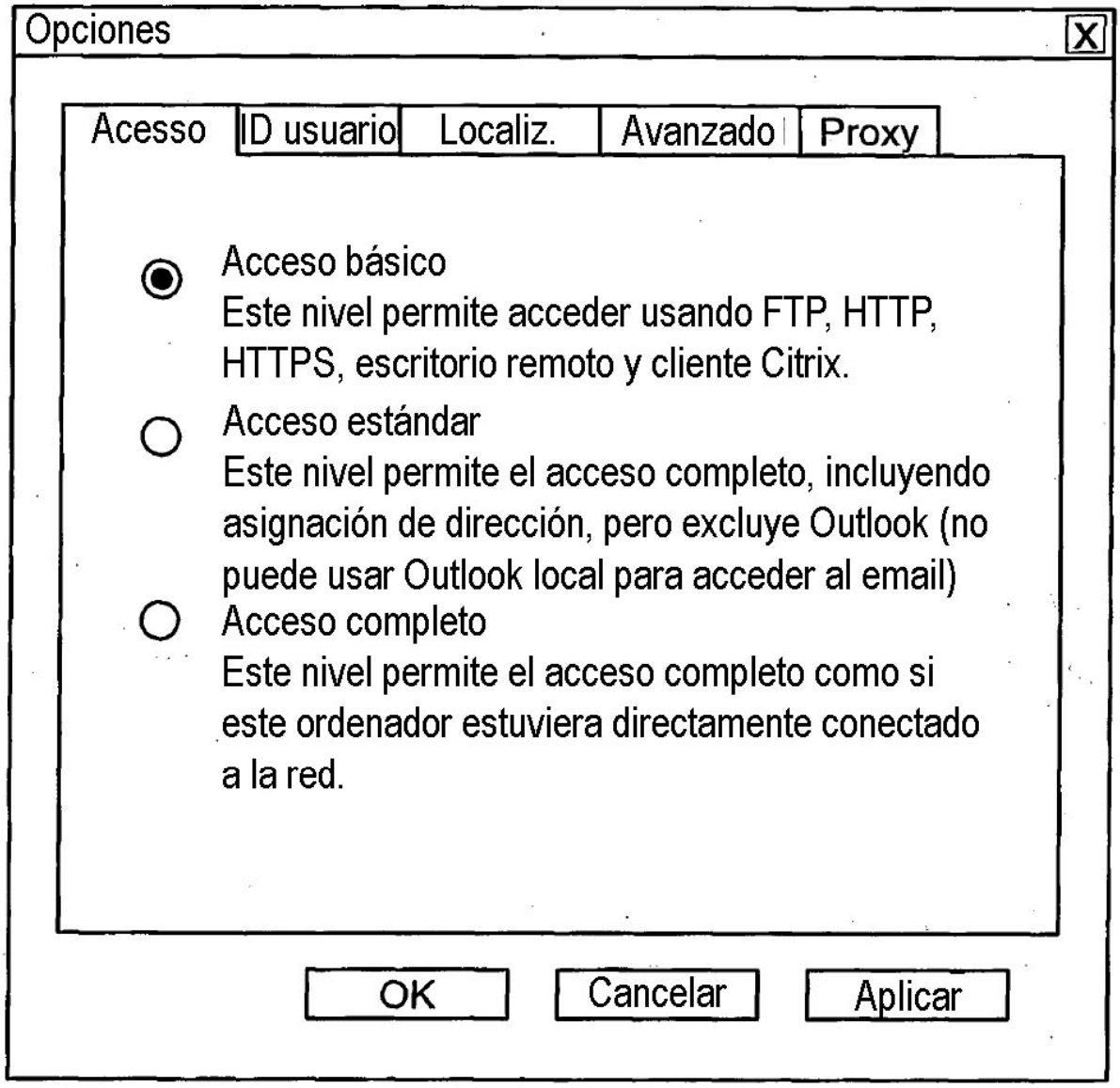
Opciones
X
Acesso
ID usuario
Localiz.
Avanzado
Proxy
Acceso básico
Este nivel permite acceder usando FTP, HTTP, HTTPS, escritorio remoto y cliente Citrix.
Acceso estándar
Este nivel permite el acceso completo, incluyendo asignación de dirección, pero excluye Outlook (no puede usar Outlook local para acceder al email)
Acceso completo
Este nivel permite el acceso completo como si este ordenador estuviera directamente conectado a la red.
OK
Cancelar
Aplicar

Fig. 5

[Claves de registro]

- HKLM\SOFTWARE\Classes\BonziBDY.Document=shell
- HKLM\SOFTWARE\Classes\daffile=shell
- HKLM\SOFTWARE\Classes\AIM=shell
- HKLM\SOFTWARE=Gator.com
- HKLM\SOFTWARE=Brilliant Digital Entertainment
- HKLM\SOFTWARE=Kazaa
- HKLM\SOFTWARE=CommonName
- HKLM\SOFTWARE=Cydoor
- HKLM\SOFTWARE=BearShare
- HKLM\SOFTWARE=WhenU
- HKLM\SOFTWARE=NeoModus
- HKLM\SOFTWARE=rdxr
- HKLM\SOFTWARE=Distributed Computing Technologies, Inc.
- HKLM\SOFTWARE=Qtrax
- HKLM\SOFTWARE=iMesh
- HKLM\SOFTWARE=GoToMyPC

[Valores o datos del registro]

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Audiogalaxy Satellite=UninstallString
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run=XupiterStartup
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run=SQUpdatesChecker
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{E499428A-E04F-4683-8A21-42A5E6D1C651}=UninstallString
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Trillian=UninstallString;
- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\ AllowMultipleTSSessions=0

[Archivos prohibidos]

- %ProgramFiles%\Gator.com*.*=
- %ProgramFiles%\PrecisionTime*.*=

Fig. 6

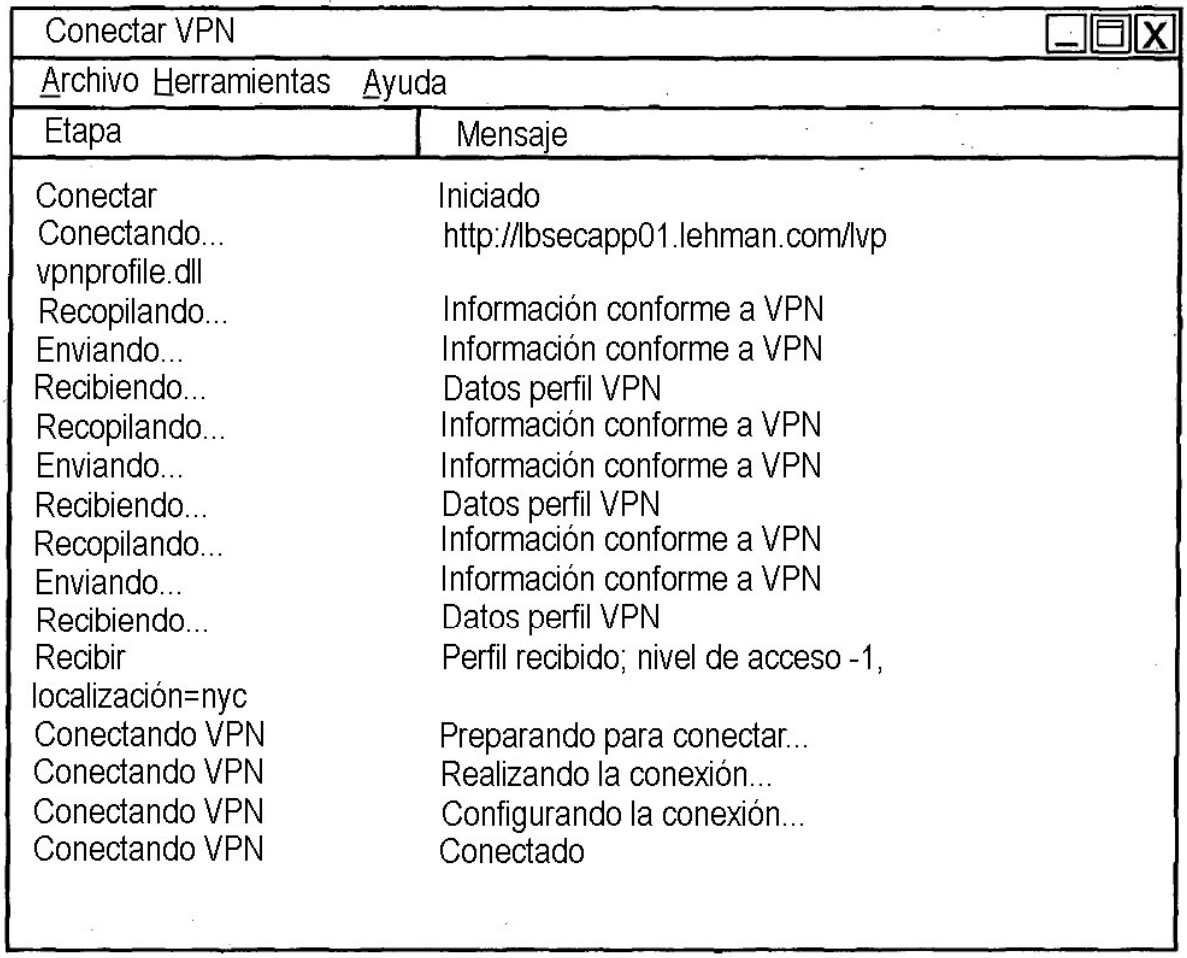
Conectar VPN
Archivo Herramientas Ayuda
Etapa
Mensaje
Conectar
Iniciado
Conectando...
http://lbsecapp01.lehman.com/lvp
vpnprofile.dll
Recopilando...
Información conforme a VPN
Enviando...
Información conforme a VPN
Recibiendo...
Datos perfil VPN
Recopilando...
Información conforme a VPN
Enviando...
Información conforme a VPN
Recibiendo...
Datos perfil VPN
Recopilando...
Información conforme a VPN
Enviando...
Información conforme a VPN
Recibiendo...
Datos perfil VPN
Recibir
Perfil recibido; nivel de acceso -1,
localización=nyc
Conectando VPN
Preparando para conectar...
Conectando VPN
Realizando la conexión...
Conectando VPN
Configurando la conexión...
Conectando VPN
Conectado

Fig. 7