(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 736 973**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***G06F 21/00*** (2013.01)
***G06F 17/30*** (2006.01)
***G06F 21/56*** (2013.01)
***G06F 21/62*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.05.2012 PCT/GB2012/051074**

(87) Fecha y número de publicación internacional: **22.11.2012 WO12156720**

(96) Fecha de presentación y número de la solicitud europea: **15.05.2012 E 12722809 (6)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2019 EP 2710780**

(54) Título: **Sistema de control de acceso a la red y método**

(30) Prioridad:

**16.05.2011 GB 201108068**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**09.01.2020**

(73) Titular/es:

**WISCOL LIMITED (100.0%)**
**727-729 High Road**
**London N12 0BP, GB**

(72) Inventor/es:

**KAUFMANN, GRANT DAVID**

(74) Agente/Representante:

**SÁEZ MAESO, Ana**

## DESCRIPCIÓN

Sistema de control de acceso a la red y método

Campo de la invención

La presente invención se refiere a la comunicación de red y la seguridad de acceso. Se refiere particularmente a la prevención del acceso a material y datos no deseados.

La técnica anterior

Los problemas con el material no deseado y malicioso en Internet y en las redes de comunicaciones en general no son nuevos. Se sabe que los correos electrónicos y el tráfico web llevan a los Spam (comunicaciones no deseadas que ofrecen productos, servicios o posibilidades sociales dudosos) como quizás el problema de nivel más bajo. Las comunicaciones de suplantación de identidad (phishing), donde un ladrón busca datos bancarios que proporcionan de manera involuntaria los que responden el mensaje, tampoco son las cosas más maliciosas que ocurren. Los archivos adjuntos de correo electrónico y los elementos de contenido de sitios de Internet pueden llevar la instalación automática del llamado "programa maligno", que puede abarcar desde los "programas espía", que realizan un seguimiento de la actividad del ordenador e informa a un remitente cuestiones como datos bancarios y pulsaciones de teclas de contraseñas, hasta virus que incapacitan totalmente el ordenador que pueden deshabilitar la protección antiviral y dañar y destruir programas y archivos. Tal vez aún peor, el programa maligno introducido de manera maliciosa puede "automatizar" un ordenador receptor para hacer la ocupación de un ordenador maestro remoto y enviar, en nombre del ordenador maestro, correos electrónicos spam y otros ataques automáticos a direcciones de correo electrónico encontradas en las libretas de direcciones de correo electrónico del ordenador víctima. La presente invención busca lograr que un ordenador se encuentre más protegido de recibir un programa maligno.

Las precauciones del procesador en funciones abundan contra los programas malignos. Existen numerosas aplicaciones disponibles que se instalan en un ordenador para ofrecer antivirales, programas antiespía e instalaciones de cortafuegos. Aunque tales precauciones son generalmente efectivas, la efectividad no siempre se mantiene. Por ejemplo, uno solo tiene que ejecutar una aplicación de programa antiespía para descubrir que pueden existir numerosas infecciones sin un impedimento aparente del funcionamiento del ordenador. Cuando se abre algún programa maligno las precauciones antiprograma maligno existentes se desactivan automáticamente, lo que se convierte en una burla al intento de salvaguardar el procesador que ahora se encuentra infectado. La presente invención busca mejorar la protección contra programas malignos y prevenir o hacer menos probable la infección inicial con programas malignos.

Ciertos sitios web conllevan un riesgo para cualquier visitante. El programa maligno se descarga sin el conocimiento o consentimiento del operador por parte de empresas criminales y estatales. Dicha descarga también es una característica de los llamados ataques cibernéticos. La presente invención pretende hacer menos probable una visita a un sitio web riesgoso.

Las precauciones pueden quedar obsoletas rápidamente. Una infección a un procesador puede ocurrir a las horas de su primera aparición en el mundo, y antes de que la mayoría de los procesadores hayan tenido la oportunidad de actualizar sus precauciones. La presente invención trata de hacer posible que las precauciones actualizadas se encuentren disponibles y se apliquen automáticamente en el lapso de tiempo más breve posible.

Las soluciones de la técnica anterior se han sugerido en los documentos de patente.

La solicitud de patente de Estados Unidos US2006048218 (A1) describe un sistema y método para que un usuario final cambie la operación de un mecanismo de filtro de flujo de datos, como un cortafuegos, que opera para controlar los flujos de datos entre una pluralidad de dispositivos informáticos protegidos y uno o más dispositivos informáticos no protegidos. Con el sistema y método un administrador de una subred de dispositivos informáticos puede establecer el alcance de reglas/políticas de un dispositivo informático cliente que un usuario del dispositivo informático cliente puede cambiar, con respecto a un mecanismo de filtro de flujo de datos. El usuario del dispositivo informático cliente o el propio dispositivo informático cliente puede iniciar sesión en el mecanismo de filtro de flujo de datos y modificar la operación del mecanismo de filtro de flujo de datos dentro de los límites que se establecen por el administrador. La presente invención busca limitar las opciones del cliente.

La solicitud de patente internacional WO2008109866 (A2) describe métodos, dispositivos, sistemas y productos de programas informáticos para controlar el acceso a servicios, contenido, aplicaciones y similares en un dispositivo de comunicación inalámbrica. En un aspecto, se proporciona un control de acceso de todo el dispositivo de comunicación inalámbrica, de manera que pueda existir un control de acceso unificado en el dispositivo; lo que proporciona control de acceso a más de uno de, y en algunos casos a todos, los servicios y/o aplicaciones a las cuales se puede acceder en el dispositivo. Adicionalmente, los aspectos proporcionan la limitación o prohibición del acceso en función de numerosos factores de control de acceso, como el tipo de contenido, el tipo de servicio, la ubicación del dispositivo, el tiempo o cualquier otra característica ambiental del dispositivo. Los métodos, dispositivos, sistemas y productos de programas informáticos para el control de acceso al contenido pueden ejecutarse en el dispositivo de comunicación inalámbrica o

pueden ejecutarse dentro de la red inalámbrica. La presente invención busca simplificar el control y la velocidad de acceso al evitar la necesidad de evaluación de contenido.

Resumen de la invención

De acuerdo con un primer aspecto, la presente invención proporciona un sistema para controlar el contenido de la red a la que accede un cliente, el sistema que comprende un administrador que establece reglas y políticas de acceso que el cliente debe seguir, caracterizadas porque:
el cliente 10, se opera para realizar solicitudes de acceso a la red a un recurso en una red 12;
el cliente 10, se opera para acceder a un servidor de acceso a la red 14 en la red 12 para configurar un perfil de acceso a la red;
el cliente 10, se opera para acceder al menos a un sitio de red confiable 16 en la red para configurar al menos un perfil del sitio confiable;
el cliente 10, se opera para pasar la solicitud de acceso a la red al servidor de acceso a la red 14;
el servidor de acceso a la red 14 que comprende un motor de combinación 20 operable que, al recibo de la solicitud de acceso a la red, combina el perfil de acceso a la red con al menos un perfil del sitio confiable para formar un perfil combinado;
y
el servidor de acceso a la red 14 que también comprende un motor de filtrado operable que prueba la solicitud de acceso a la red y permite el acceso al recurso solo si no se viola el perfil combinado.

De acuerdo con un segundo aspecto la presente invención proporciona un método para controlar el acceso al contenido del recurso de red 18 por parte de un cliente, el sistema que comprende un administrador que establece reglas y políticas de acceso a seguir por el cliente, caracterizadas por:
una etapa de acceder a un controlador de acceso a la red 14 en la red 12 y establecer un perfil de acceso a la red;
una etapa de acceder al menos a un sitio confiable 16 en la red 12 y establecer al menos un perfil del sitio confiable
una etapa para emitir una solicitud de acceso a la red al controlador de acceso a la red 14;
una etapa de combinar, por parte del controlador de acceso a la red 14, el perfil de acceso a la red y al menos un perfil del sitio confiable 16; y
una etapa de permitir, por parte del controlador de acceso a la red 14, la solicitud de acceso a los recursos de red siempre y cuando no se viole el perfil combinado.

La invención proporciona, además, que al menos un perfil del sitio confiable sea actualizable en al menos un sitio confiable; y que al menos un perfil del sitio confiable sea transferible de al menos un sitio confiable al servidor de acceso a la red en respuesta a la recepción de una solicitud de acceso a la red.

La invención proporciona, además, que la solicitud de acceso a la red pueda incluir datos del cliente para permitir la identificación del cliente por parte del servidor de acceso a la red.

La invención proporciona, además, que el servidor de acceso a la red pueda pasar los datos del cliente a al menos un sitio confiable, que al menos un sitio confiable pueda emplear los datos del cliente para recuperar el perfil del sitio confiable asociado, y que al menos un sitio confiable pueda pasar el perfil del sitio confiable asociado al servidor de acceso a la red.

La invención también proporciona que al menos un perfil del sitio confiable pueda incluir al menos uno de: la identidad de las direcciones de red; puertos IP; contenido; hora del día en que se permite acceder; y la identidad de las direcciones de red; puertos IP; contenido; y hora del día en que se prohíbe acceder.

Breve descripción de los dibujos

La invención se describe y explica adicionalmente, a manera de ejemplo, mediante la siguiente descripción, que se debe leer junto con los dibujos adjuntos, en los que
La Figura 1 muestra un diagrama esquemático que ilustra una primera fase de operación de un sistema de elementos a través del cual se implementa la invención.
La Figura 2 muestra una segunda fase de operación del sistema de elementos a través del cual se implementa la invención.
La Figura 3 muestra un diagrama de bloques esquemático de elementos ilustrativos de una posible implementación del servidor de acceso a la red de las Figuras 1 y 2.
La Figura 4 muestra un diagrama de flujo ilustrativo que ilustra una de las muchas maneras posibles en las que el cliente puede configurar la opción del servidor cliente antes de usar el servidor de acceso a la red para comunicarse con la red.
La Figura 5 es un diagrama de flujo ilustrativo que ilustra una forma posible en la que un cliente 10 puede seleccionar opciones de cliente confiables que se proporcionan por el sitio confiable 16.
y
La Figura 6 es un diagrama de flujo que ilustra una posible forma en la que un cliente puede acceder al servidor de acceso a la red y al sitio confiable.

Descripción detallada de la invención

Primero se centra la atención en la Figura 1, un diagrama esquemático que ilustra una primera fase de operación de un sistema de elementos a través del cual se implementa la invención, y en la Figura 2, que muestra una segunda fase de operación.

Un procesador cliente 10, como un ordenador personal (PC), se habilita para operar en la red y puede operar con sitios y servicios que se proporcionan en una red 12 como, por ejemplo, Internet, pero que no se limita a esta. El cliente 10 también puede ser un dispositivo portátil con capacidad de acceso a Internet mediante WiFi® o los sistemas de telefonía móvil.

Dentro de la red 12 hay un servidor de acceso a la red 14. El cliente 10 puede acceder al servidor de acceso a la red mediante el direccionamiento a la dirección IP del servidor de acceso a la red 14.

Dentro de la red 12 también hay un sitio confiable 16 que contiene perfiles seleccionables y configurables para controlar la capacidad de acceso a la red del cliente 10, como se explicará, cuando el cliente emplea el servidor de acceso a la red 14 para acceder a otros sitios convenientes 18.

Se involucran dos fases de operación.

La primera fase es la configuración, donde el cliente 10 accede primero al servidor de acceso a la red 14 para configurar las opciones del servidor cliente, y el cliente 10 también accede al sitio confiable 16 para configurar las opciones del sitio confiable del cliente. Como se ilustra en la Figura 1, el sitio confiable 16 y el servidor de acceso a la red 14 se pueden comunicar entre sí para indicar al servidor de acceso a la red 14 a cuál sitio confiable 16 se va a acceder y viceversa.

La segunda fase es la operación, como se ilustra en la Figura 2, donde el cliente 10 accede al servidor de acceso a la red 14 para acceder a los sitios deseados 18 a través del servidor de acceso a la red 14 mediante el uso de la combinación de las opciones del servidor cliente y las opciones del sitio confiable del cliente. Durante la segunda fase de operación el sitio confiable 16 y el servidor de acceso a la red 14 se comunican para transmitir la opción del sitio confiable del cliente al servidor de acceso a la red 14 para su uso.

A continuación, se centra la atención en la Figura 3, un diagrama de bloques esquemático de elementos ilustrativos de una posible implementación del servidor de acceso a la red 14 de las Figuras 1 y 2.

El servidor de acceso a la red 14 comprende un motor de combinación 20 y un motor de filtrado. El servidor de acceso a la red 14 comprende además medios de comunicación digital 24 que pueden incluir, pero que no se restringen a, un módem operable para enviar y recibir datos y solicitudes a través de la red 12 para acceder al cliente 10, al sitio confiable 16 y a cualquier otro sitio en la red 12 con el que el cliente 10 pueda desear entrar en contacto. Aunque la Figura 3 muestra solo un medio de comunicación 24, se debe entender que se pueden emplear dos o más medios de comunicación 24 para proporcionar la función del servidor de acceso a la red, y que antes y de aquí en adelante se describe y reivindica. Los medios de comunicación también pueden incluir una conexión de red.

El servidor de acceso a la red comprende, además, al menos dos memorias, una memoria de cliente 26 y una memoria del sitio confiable 28. La memoria de cliente 26 almacena la identificación del cliente junto con las opciones del servidor cliente, las cuales se configuran por el cliente 10. La memoria del sitio confiable almacena los detalles del sitio confiable, incluida la identidad del sitio confiable 16 y los detalles de configuración del sitio confiable, que se ampliarán más adelante.

A continuación, se centra la atención en la Figura 4 que muestra un diagrama de flujo ilustrativo que ilustra una de las muchas maneras posibles en las que el cliente 10 puede configurar la opción del servidor cliente antes de usar el servidor de acceso a la red 14 para comunicarse con la red 12.

Desde el inicio 30, una primera operación 32 hace que el cliente 10 acceda a la interfaz de configuración del servidor de acceso a la red (NAS) 14 y verifique su identidad mediante, por ejemplo, la dirección IP del cliente 10 o cualquier etiqueta de identidad automática de la máquina, como un número de MAC, que pueda encontrarse disponible, los identificadores automáticos que pueden usarse de manera individual o colectiva. También puede pedirse al cliente 10 que proporcione una contraseña y otra información personal. Si la primera operación descubre que el cliente 10 es desconocido para el servidor de acceso a la red 14 puede solicitarse al cliente que configure una cuenta y que proporcione la información de contraseña individual adecuada. Por supuesto, si el cliente 10 rechaza la configuración de una cuenta, la primera operación 32 puede proceder directamente a la salida 34, y de esta manera permite al cliente 10 volver a intentarlo si el rechazo se debió a una falta de información.

Si la primera operación 32 es exitosa, entonces una segunda operación 36 selecciona la opción antiprograma maligno deseada por el cliente 10. El uso de una opción anti-programa maligno residente en el servidor de acceso a la red 14, le da la ventaja al cliente 10 de que la opción antiprograma maligno esté siempre actualizada y solo se deriva de una fuente confiable. El usuario del cliente 10 selecciona cuál de uno o más programas residentes antiprograma maligno el usuario desea emplear. El programa maligno puede abarcar desde programas espía, virus, programas de automatización y

cookies molestas, por nombrar solo algunos. El usuario del cliente 10 también puede elegir anular la opción de programa maligno y no emplear ninguna opción de programa maligno en el servidor de acceso a la red 14, sino en su lugar usar las opciones anti-programa maligno instaladas en el propio cliente 10.

Luego, una tercera operación 38 selecciona cualquier opción de comunicaciones que el usuario del cliente 10 elija evitar. Por ejemplo, la comunicación WiFi puede estar sujeta a escucha informática, al igual que las redes telefónicas. Como ejemplo, el usuario del cliente 10 puede elegir estar limitado a la comunicación por cable. Ciertos protocolos pueden contener contenido malicioso, por ejemplo, ciertos tipos de imágenes. El usuario del cliente 10 puede elegir evitar determinados tipos de archivos y protocolos.

Al completar la tercera operación 38 una cuarta operación 40 hace luego que el usuario del cliente 10 seleccione cualquier opción personal, como, por ejemplo, cualquier dirección de correo electrónico con la que el usuario no quiera conmutar, cualquier sitio web que el usuario desee evitar, cualquier tipo de correo electrónico que el usuario no desee recibir, y así sucesivamente. Las opciones personales pueden ser muchas y variadas.

Cuando se completa la cuarta operación 40, se completa la configuración de opción del servidor cliente. El proceso acaba por la salida 34. Las opciones del servidor cliente se almacenan en la memoria del cliente 26 listas para que se usen cuando el cliente 10 intente acceder a la red. Las opciones del servidor cliente pueden actualizarse en cualquier momento. La actualización puede elegirse por el usuario del cliente 10. Una opción es tener una configuración y actualización de cuenta solo bajo control del administrador, para que un cliente, típicamente en una organización, pueda configurarse de modo que los usuarios individuales no puedan cambiar la configuración y pueda lograrse una uniformidad de configuración en toda la organización.

A continuación, se centra la atención en la Figura 5, un diagrama de flujo ilustrativo que ilustra una posible forma en la que un cliente 10 puede seleccionar las opciones de cliente confiable que se proporcionan por el sitio confiable 16.

Desde el inicio 42, una quinta operación 44 hace que el cliente 10 acceda a la página de configuración del sitio confiable 16. Al igual que con la configuración de la opción del servidor cliente, como se describió anteriormente, se le puede requerir al cliente 10 que verifique su identidad, por ejemplo, la dirección IP del cliente 10 o cualquier etiqueta de identidad de la máquina automática, como un número MAC, que pueda encontrarse disponible, los identificadores automáticos que pueden usarse de manera individual o colectiva. También puede pedirse al cliente 10 que proporcione una contraseña y otra información personal. Si la quinta operación 44 encuentra que el cliente 10 es desconocida para el sitio confiable 16, se le puede requerir al cliente 10 que configure una cuenta y proporcione información de contraseña individual adecuada. Por supuesto, si el cliente 10 rechaza la configuración de una cuenta, la quinta operación puede proceder directamente a la salida 45, de esta manera se le permite al cliente 10 volver a intentarlo si el rechazo se debió a una falta de información. El acceso al sitio confiable puede encontrarse restringido a un conjunto de organizaciones confiables que pueden requerirse para verificar su identidad.

Entonces, una sexta operación tiene el sitio confiable 16 que muestra las opciones disponibles del sitio confiable.

Estas pueden ser, por ejemplo, sitios que, a la vista de una organización particular, son aceptables para el acceso de los clientes y pueden incluir muchas opciones en dependencia de la función de la máquina del cliente 10 en particular. Por ejemplo, si el cliente 10 va a usarse para una operación de almacén, solo se permitirán los sitios de la red 12 aptos para ver desde una operación de almacén. Otras opciones pueden, pero no se limitan a, incluir sitios adecuados de contabilidad, sitios apropiados de ingeniería, etc.

Las opciones de sitios confiables también pueden incluir, pero no se limitan a, la exclusión de sitios riesgosos donde se ha encontrado programas malignos u otros problemas.

Las opciones de sitios confiables también pueden incluir, pero no se limitan a, la exclusión de los sitios de ocio cuyo acceso puede proporcionar actividades sociales, de juegos o de entretenimiento en detrimento del uso relacionado con el empleo.

Las opciones de sitios confiables también pueden incluir la exclusión del acceso a sitios que son considerados inadecuados desde el punto de vista moral, político o religioso. Esta exclusión es apta para regular la actividad en Internet de jóvenes y alumnos.

Las opciones de sitios confiables pueden incluir una llamada "Lista blanca" de todos los sitios a los que se permite el acceso. Alternativamente, las opciones de sitios confiables pueden incluir una lista de sitios a los que no se permite el acceso. Como segunda alternativa las opciones de sitios confiables pueden incluir una combinación de sitios a los que se permite el acceso junto con sitios a los que se deniega el acceso. Esta última característica tiene la ventaja técnica de impedir el acceso al hacer un clic en un enlace desde un sitio permitido a un sitio no permitido.

A la sexta operación 46 le sigue una séptima operación 48, donde el cliente 10 selecciona entre las opciones de sitios confiables que se muestran en la quinta operación 46. El cliente 10 puede seleccionar solo una opción del sitio confiable o puede seleccionar dos o más opciones de sitio seleccionadas que pueden aplicarse juntas.

Luego, una octava operación 50 almacena la opción u opciones del sitio confiable seleccionadas para una selección y aplicación posterior mediante la identificación del cliente 10 en particular y el acceso a la opción u opciones almacenadas. El proceso luego sale por medio de la salida 45.

Las opciones de sitios confiables pueden actualizarse en cualquier momento. La actualización puede elegirse por el usuario del cliente 10. Una opción es tener una configuración y actualización de cuenta solo bajo control del administrador, para que un cliente, típicamente en una organización, pueda configurarse de modo que los usuarios individuales no puedan cambiar la configuración y pueda lograrse una uniformidad de configuración en toda la organización.

El contenido particular de una opción del sitio confiable también puede actualizarse mediante una organización proveedora. Al iniciar sesión en el servidor de acceso a la red 14, como se explicará más adelante, esto proporciona la ventaja técnica de proporcionar siempre la versión más actualizada de la opción u opciones del sitio confiable para el cliente 10 que selecciona.

A continuación, se centra la atención en la Figura 6, un diagrama de flujo que ilustra una posible forma en que un cliente 10 puede acceder al servidor de acceso a la red 14. La Figura 6 muestra en parte la actividad del cliente 10, en parte la actividad del servidor de acceso a la red 14 y en parte la actividad del sitio confiable 16.

Desde el inicio 52, si una primera prueba 54 detecta que el cliente 10 busca acceso a un sitio web o servicio de Internet deseado, en este ejemplo por medio del uso de un navegador, y el cliente está equipado para utilizar la presente invención, una novena operación 56 sustituye la dirección web del servidor de acceso a la red 14 en el lugar de la dirección deseada y retiene y transmite la dirección deseada y los detalles de identificación del cliente a una décima operación 58 que contacta con el controlador de acceso a la red y transmite los detalles del cliente y la dirección web deseada al servidor de acceso a la red 14. La sustitución de la dirección web del servidor de acceso a la red 14 también puede lograrse mediante cualquier medio que permita que el servidor de acceso a la red actúe como el paso a través del cual se controla y se establece el contacto con la red.

Si una segunda prueba 60 en el servidor de acceso a la red (NAS) 14 detecta que no se reconocen los detalles del cliente que se reciben de la décima operación 58 en el cliente 10, el control se reintegra a la primera prueba 54 para esperar nuevas solicitudes de acceso a la red. Si una segunda prueba 60 en el servidor de acceso a la red (NAS) 14 detecta que se reconocen los detalles del cliente que se reciben de la décima operación 58 en el cliente 10, una undécima operación 62 pasa los detalles del cliente al sitio confiable 16 donde una tercera prueba 64 verifica si se reconocen los detalles del cliente.

Si los datos del cliente no se reconocen por la tercera prueba 64 en el sitio confiable 16, el control se reintegra a la primera prueba 54 para esperar nuevamente una solicitud de acceso a la red del cliente 10. Si los detalles del cliente se reconocen por la tercera prueba 64 en el sitio confiable 16, el control pasa a una duodécima operación 66 que usa los detalles del cliente para identificar la opción del sitio confiable correspondiente y para reintegrar los datos de la opción a una decimotercera operación 68 en el servidor de acceso a la red 14.

No siempre es necesario reintegrar los datos de las opciones del sitio confiable identificados a la decimotercera operación 68. Si las opciones del sitio confiable no han cambiado desde el último acceso puede usarse el contenido que se almacenó de la memoria del sitio confiable 28, lo que acelera el acceso.

La decimotercera operación 68 actúa como un motor de combinación para combinar las restricciones de la memoria del cliente 26 y el contenido de la memoria del sitio confiable 28 para imponer las restricciones combinadas sobre el tráfico hacia y desde el cliente 10.

Una decimocuarta operación 70 en el servidor de acceso a la red 14 verifica la dirección web deseada contra las restricciones combinadas. Si una cuarta prueba 72 detecta que no se permite ningún aspecto de la dirección web deseada el control pasa a la primera prueba 54 nuevamente para esperar una solicitud de acceso del cliente 10. Si la cuarta prueba 72 detecta que se permite la dirección web deseada, una decimoquinta operación 74 en el servidor de acceso a la red 14 accede a la dirección deseada desde la red 12 e inspecciona los datos entregados.

Si una quinta prueba 76 en el servidor de acceso a la red 14 encuentra que algún aspecto de los datos entregados desde el sitio web deseado no es aceptable, de acuerdo con las restricciones combinadas, el control pasa nuevamente a la primera prueba 54 para esperar una solicitud de acceso a la red 12 del cliente 10. Si la quinta prueba 76 en el servidor de acceso a la red 14 encuentra que es aceptable, de acuerdo con las restricciones combinadas, una decimosexta operación 78 envía los datos de la dirección web deseada al cliente 10 y el cliente 10 también es libre de enviar, a través del servidor de acceso a la red 14, cualquier dato o correo que tenga que enviar. Luego, el control se reintegra a la primera prueba 54 para esperar una solicitud de acceso a la red del cliente 10.

Las operaciones de la decimocuarta 70 a la decimosexta 78 y las pruebas cuarta 72 y quinta 72 juntas, en su combinación, actúan como un motor de filtrado.

La invención se ha descrito anteriormente con referencia a la combinación de restricciones de solo dos fuentes. Debe entenderse que la invención incluye la combinación de restricciones de tres o más fuentes separadas.

La invención se ha descrito a manera de ejemplos. Los expertos en la técnica sabrán que hay muchas opciones diferentes de orden de ejecución de una actividad, organización de soporte físico y transferencia de datos e información que pueden emplearse sin apartarse de la invención, como se reivindica de aquí en adelante.

La invención se esclarece y define, además, mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema para controlar el contenido de la red al que puede acceder un cliente, el sistema que comprende:
el cliente (10) que se opera para realizar una solicitud de acceso de red a un recurso en una red 12);
el cliente (10) que se opera para acceder a un servidor de acceso a la red (14) en la red (12) para configurar un perfil de acceso a la red mediante la selección entre las opciones de acceso a la red disponibles, las opciones de acceso a la red disponibles que incluyen al menos uno de:
opciones antiprograma maligno;
opciones de comunicaciones a evitar;
tipos de archivos y protocolos a evitar;
direcciones de correo electrónico a evitar;
sitios web a evitar; y
tipo de correo electrónico que no se va a recibir;
el cliente (10) que se opera para acceder al menos a un sitio de red confiable (16) en la red para configurar al menos un perfil del sitio confiable, que se almacena en el sitio de red confiable, mediante la selección entre las opciones del sitio confiable disponibles, las opciones del sitio confiable disponibles que incluyen al menos uno de:
la identidad de los identificadores de recursos de red a los que se permite acceder;
puertos IP a los que se permite acceder; tipo de contenido al que se permite acceder;
hora del día a la que se permite acceder;
la identidad de los identificadores de recursos de red a los que se prohíbe acceder;
puertos IP a los que se prohíbe acceder; tipo de contenido al que se prohíbe acceder; y
hora del día a la que se prohíbe acceder,
el sitio de red confiable (16) y el servidor de acceso a la red (14) que se comunican entre sí;
el cliente (10) que se opera para pasar la solicitud de acceso a la red al servidor de acceso a la red (14);
el servidor de acceso a la red (14) que comprende un motor de combinación (20) operable que, al recibo de la solicitud de acceso a la red, combina el perfil de acceso a la red con al menos un perfil del sitio confiable para formar un perfil combinado;
el servidor de acceso a la red (14) que comprende, además, un motor de filtrado operable para probar la solicitud de acceso a la red y para permitir el acceso al recurso a través de la autorización del servidor de acceso a la red solo si no se viola el perfil combinado
y
el servidor de acceso a la red 14 que comprende, además, una memoria del cliente (26), en donde el perfil de acceso a la red se almacena en la memoria del cliente (26).

2. El sistema, de acuerdo con la reivindicación 1, se caracteriza, además, por las opciones del servidor cliente que incluyen opciones antiprograma maligno en el servidor de acceso a la red (14) que desee el cliente (10), o que elige anular la opción de programa maligno y no emplear ninguna opción de programa maligno en el servidor de acceso a la red (14), sino en su lugar usa las opciones antiprograma maligno instaladas dentro del propio cliente (10).

3. El sistema, de acuerdo con cualquiera de las reivindicaciones anteriores, que se caracteriza, además, por;
el perfil del sitio confiable que puede actualizarse en el sitio confiable (16); y
al menos un perfil del sitio confiable que se puede transferir desde al menos un sitio confiable (16) al servidor de acceso a la red (14) en respuesta a la recepción de una solicitud de acceso a la red.

4. El sistema, de acuerdo con cualquiera de las reivindicaciones anteriores, en donde la solicitud de acceso a la red incluye datos del cliente (10) que permiten la identificación del cliente (10) por el servidor de acceso a la red (14).

5. El sistema, de acuerdo con la reivindicación 4, que se caracteriza, además, porque el servidor de acceso a la red (14) se opera para pasar los datos del cliente (10) a al menos un sitio confiable (16), al menos un sitio confiable (20) que se opera para emplear los datos del cliente (10) para recuperar el perfil del sitio confiable asociado, y al menos un sitio confiable (16) que se opera para pasar el perfil del sitio confiable asociado al servidor de acceso a la red (14).

6. Un método para controlar el acceso al contenido de recursos de red (18) por un cliente (10) que comprende:
una etapa de acceder, por parte del cliente (10), a un servidor de acceso a la red (14) en la red (12) y establecer, por el cliente (10), un perfil de acceso a la red que se almacena en una memoria del cliente que se incluye en el servidor de acceso a la red (14) mediante la selección de las opciones de acceso a la red disponibles, las opciones de acceso a la red disponibles que incluyen al menos una de:
opciones antiprograma maligno;
opciones de comunicación a evitar;
tipos de archivos y protocolos a evitar;
direcciones de correo electrónico a evitar;
sitios web a evitar; y
tipo de correo electrónico que no se va a recibir;

una etapa de acceder, por parte del cliente (10), a al menos un sitio de red confiable (16) en la red (12), el sitio de red confiable (16) y el servidor de acceso a la red (14) que se comunican entre sí, y establecer, por parte del cliente (10), al menos un perfil del sitio confiable que se almacena en el sitio de red confiable (16), mediante la selección entre las opciones del sitio confiable disponibles, las opciones del sitio confiable disponibles que incluyen al menos una de:
la identidad de los identificadores de recursos de red a los que se permite acceder;
puertos IP a los que se permite acceder; tipo de contenido al que se permite acceder;
hora del día a la que se permite acceder;
la identidad de los identificadores de recursos de red a los que se prohíbe acceder;
puertos IP a los que se prohíbe acceder; tipo de contenido al que se prohíbe acceder; y
hora del día a la que se prohíbe acceder;
una etapa de emitir, por parte del cliente (10), una solicitud de acceso a la red al servidor de acceso a la red (14);
una etapa de combinar, por parte del servidor de acceso a la red (14), el perfil de acceso a la red y al menos un perfil del sitio confiable (16); y
una etapa de permitir, por parte del servidor de acceso a la red (14), la solicitud de acceso a los recursos de red siempre y cuando no se viole el perfil combinado.

7. El método, de acuerdo con la reivindicación 6, que se caracteriza, además, por comprender:
una etapa de actualizar al menos un perfil del sitio confiable (16); y
una etapa de transferir al menos un perfil del sitio confiable (16) desde al menos un sitio de red confiable (16) al servidor de acceso a la red (14) en respuesta a la recepción de una solicitud de acceso a la red.

8. El método, de acuerdo con cualquiera de las reivindicaciones 6 y 7, que se caracteriza, además, por comprender una etapa de incluir datos del cliente (10) en la solicitud de acceso a la red, y una etapa de identificar, en el servidor de acceso a la red (14), el cliente en particular de los datos del cliente.

9. El método, de acuerdo con la reivindicación 8, que se caracteriza, además, por incluir
una etapa de pasar, por parte del servidor de acceso a la red (14), los datos del cliente (10) a al menos un sitio de red confiable (16);
una etapa de emplear, por parte de al menos un sitio de red confiable (16), los datos del cliente (10) para recuperar el perfil del sitio confiable asociado;
y
una etapa de pasar, por parte de al menos un sitio de red confiable (16), el perfil del sitio confiable asociado al servidor de acceso a la red (14).

10. El método, de acuerdo con cualquiera de las reivindicaciones de la 6 a la 9, en donde el perfil del sitio confiable incluye al menos uno de: la identidad de los identificadores de recursos de red a los que se permite acceder; la identidad de los puertos IP a los que se permite acceder; el tipo de contenido al que se permite acceder; la hora del día a la que se permite acceder; la identidad de los identificadores de recursos de red a los que se prohíbe acceder; los puertos IP a los que se prohíbe acceder; el tipo de contenido al que se prohíbe acceder; y la hora del día a la que se prohíbe acceder.

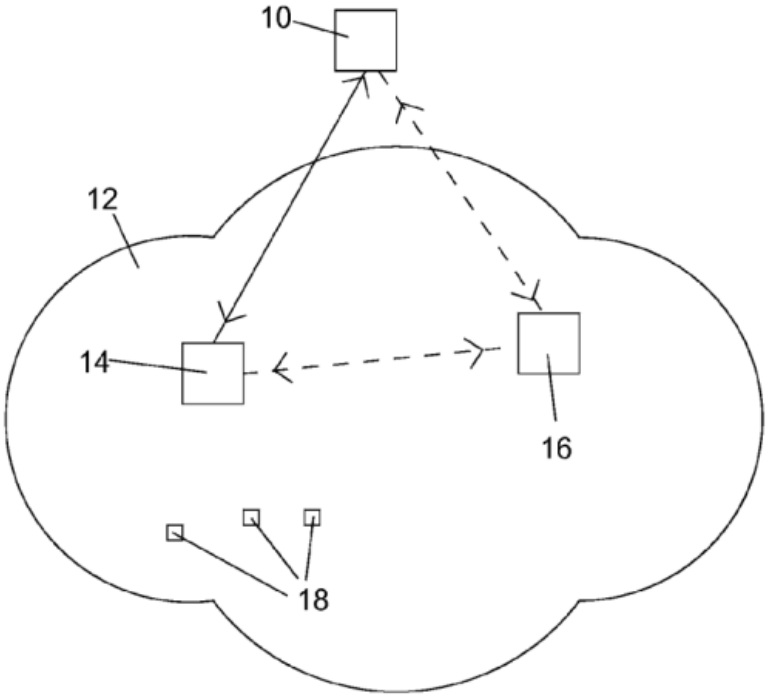


Figura 1

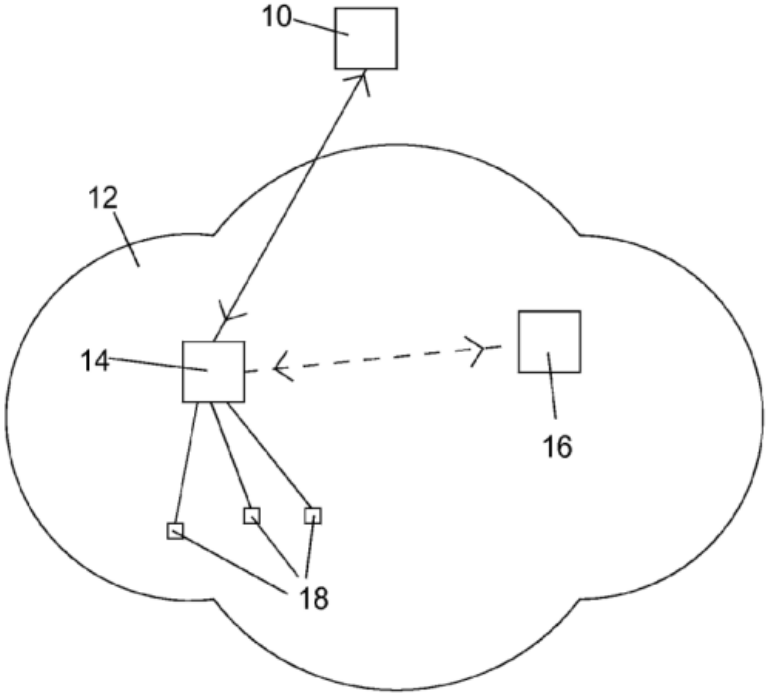


Figura 2

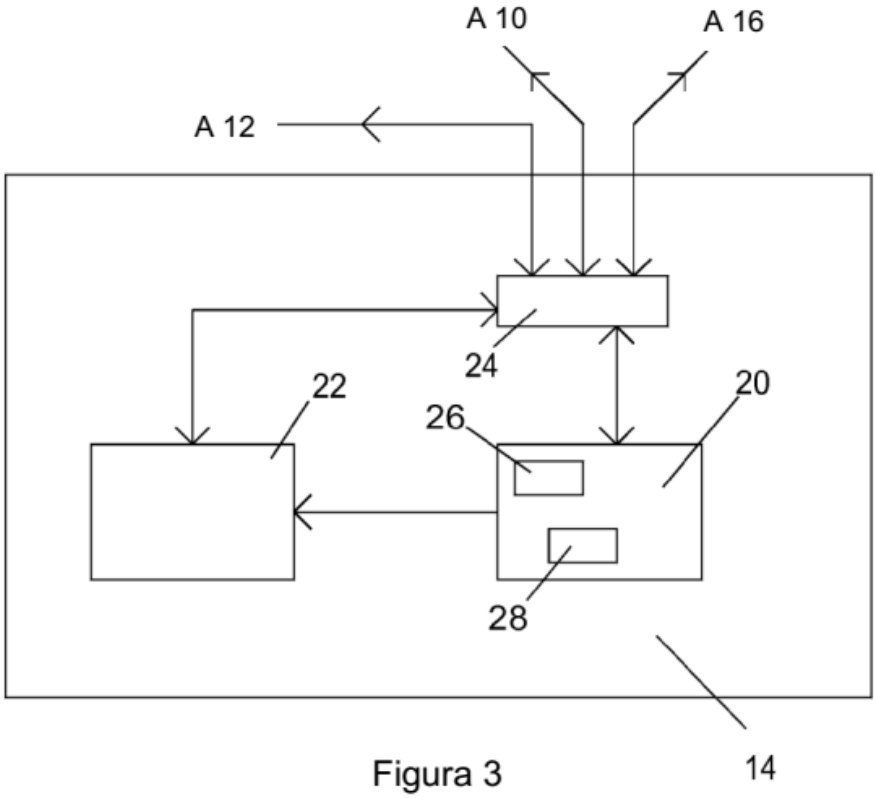


Figura 3

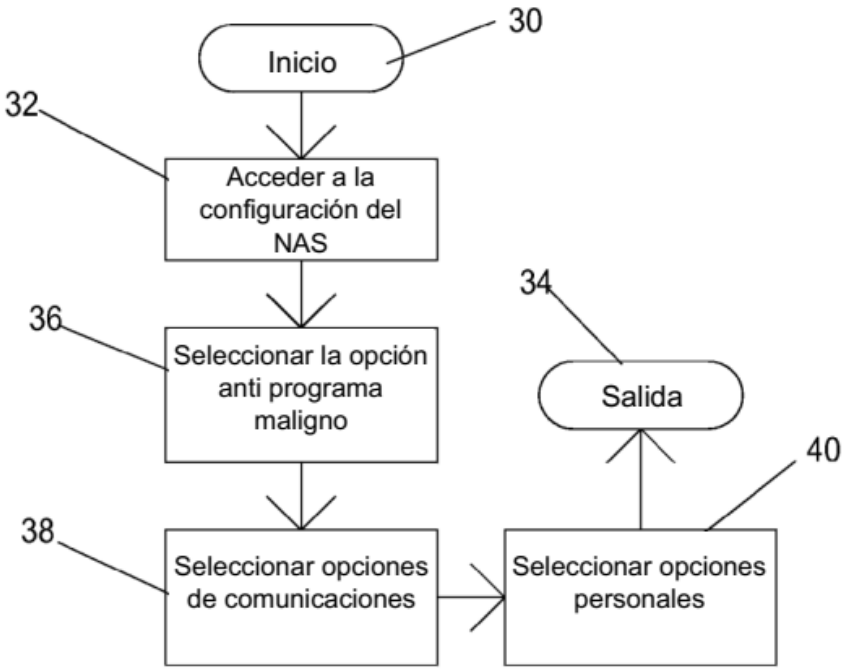


Figura 4

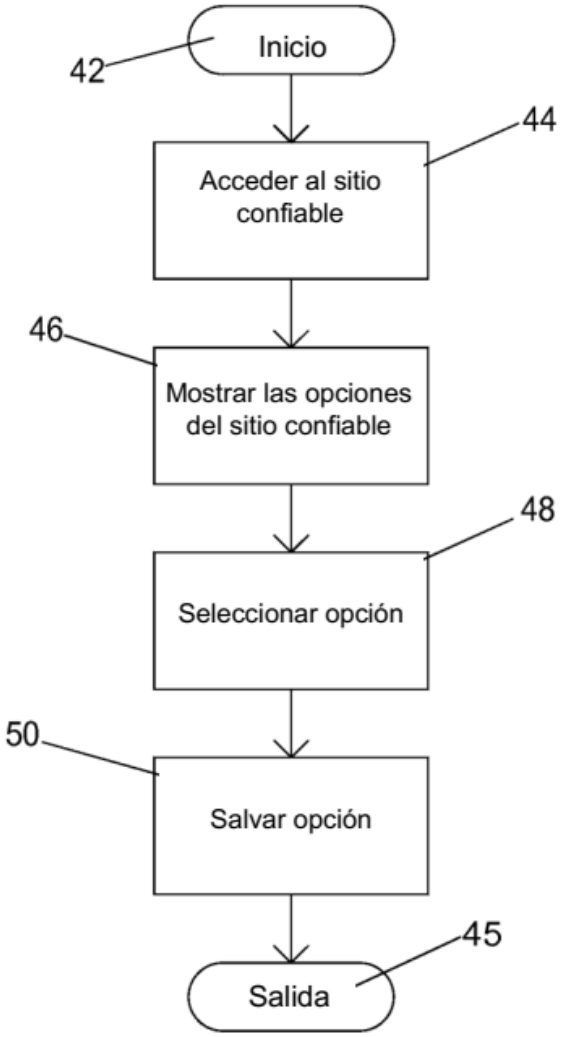
Inicio
42
44
Acceder al sitio confiable
46
Mostrar las opciones del sitio confiable
48
Seleccionar opción
50
Salvar opción
45
Salida

Figura 5

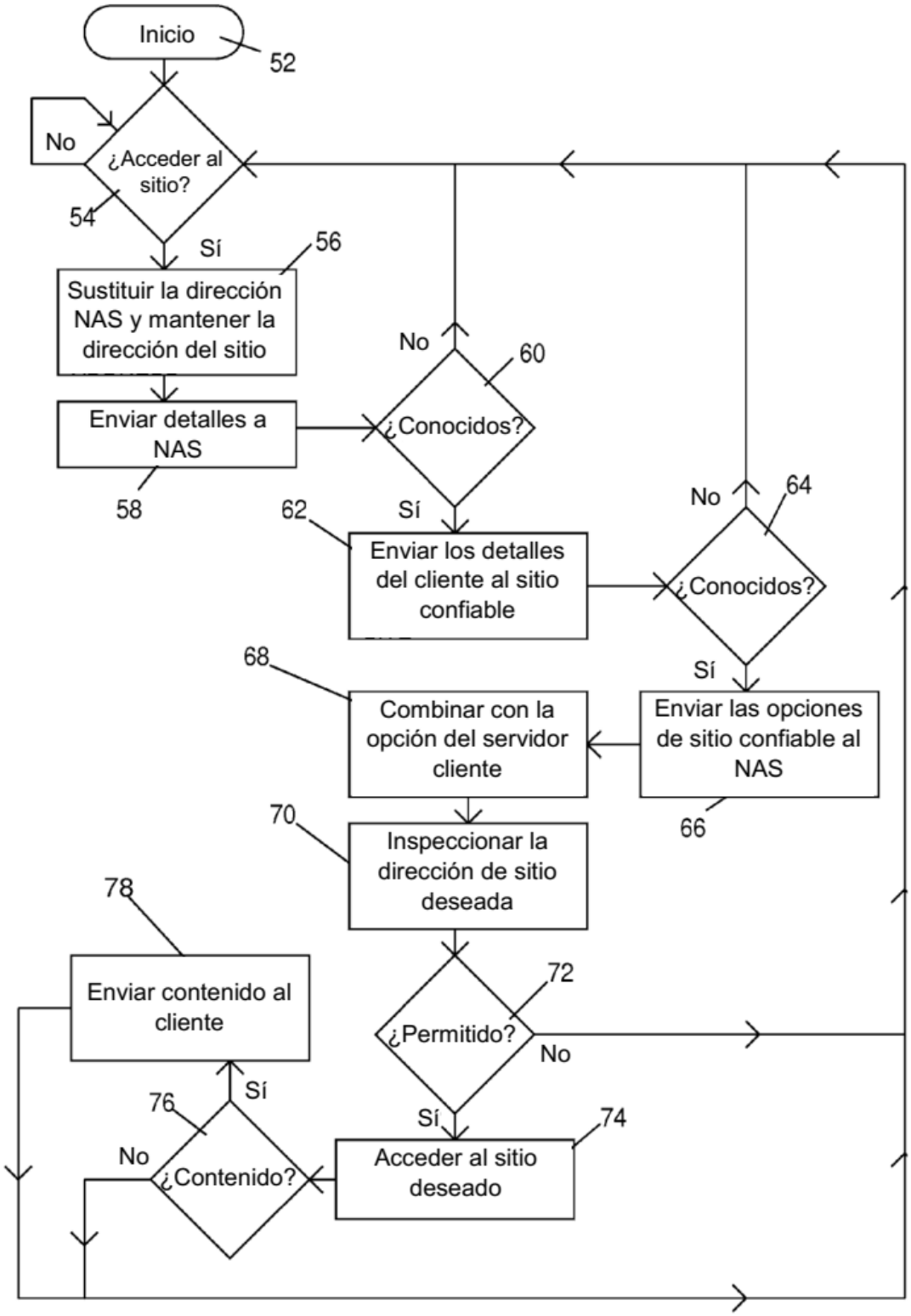
Inicio
52
No
¿Acceder al sitio?
54
Sí
56
Sustituir la dirección NAS y mantener la dirección del sitio
Enviar detalles a NAS
58
No
60
¿Conocidos?
Sí
62
Enviar los detalles del cliente al sitio confiable
No
64
¿Conocidos?
Sí
Enviar las opciones de sitio confiable al NAS
66
68
Combinar con la opción del servidor cliente
70
Inspeccionar la dirección de sitio deseada
72
¿Permitido?
No
Sí
74
Acceder al sitio deseado
76
No
¿Contenido?
Sí
78
Enviar contenido al cliente

Figura 6