(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 292**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.05.2016 E 16382216 (6)**

(97) Fecha y número de publicación de la concesión europea: **27.02.2019 EP 3247084**

(54) Título: **Servidor y método para proporcionar un acceso seguro a servicios basados en la red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2019

(73) Titular/es:

NOLVE DEVELOPMENTS S.L. (100.0%)
Margarita Salas, 34
28918 Leganés (Madrid), ES

(72) Inventor/es:

LARGO DEL AMO, MARIANO y
JURADO MARTÍNEZ, VICTOR

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Servidor y método para proporcionar un acceso seguro a servicios basados en la red

Campo técnico

La presente invención se refiere a un servidor para proporcionar un acceso seguro a una página web de un servicio basado en la red, y un método para proporcionar acceso seguro a una página web.

Estado de la técnica

El número de dispositivos con conectividad a Internet ha aumentado drásticamente en la última década, y se espera que el número va a seguir creciendo en el futuro puesto que el acceso a Internet no sólo se limita a conexiones de línea terrestre, por lo que dispositivos distintos de ordenadores personales (PC) pueden tener acceso a Internet también. En este sentido, los sistemas de comunicaciones móviles han tenido un enorme impacto en la conectividad a Internet: virtualmente cualquier dispositivo inalámbrico que incluya una antena para comunicaciones móviles puede conectarse ahora a Internet.

Internet también ha evolucionado en lo que respecta al contenido accesible en la red. Ahora, los servicios basados en Internet pueden incluso sustituir el software tradicional, ya que varias aplicaciones en línea ofrecen capacidades similares y están disponibles dentro de un explorador web convencional. En este sentido, muchas aplicaciones y sitios web ofrecen servicios o proporcionan características avanzadas cuando se introducen datos personales. Estos servicios son, por ejemplo, la compra de artículos como ropa, libros, música, entre otros, la realización de transacciones bancarias, escritura y lectura de correo electrónico o documentos, etc.

Así, un usuario puede beneficiarse de muchos de estos servicios, pero siempre hay preocupaciones en cuanto a la seguridad: aplicaciones y técnicas maliciosas que tienen el único propósito de robar, modificar y/o borrar datos, dan lugar a fenómenos como la suplantación de identidad, falsificación, secuestro del navegador, etc., para el beneficio personal de un atacante.

Aunque hay muchos tipos de ataques maliciosos, una de las formas más comunes de infectarse es navegar por páginas web en Internet. Aunque existen programas de software tales como cortafuegos, antivirus, kits anti-software maligno, etc., para prevenir la infección del dispositivo de usuario, dichas aplicaciones no son capaces de detectar, detener y eliminar muchas de las infecciones. Por lo tanto, incluso con estas aplicaciones, el usuario sigue siendo propenso a infectarse.

Una de las mayores amenazas a las que un usuario está expuesto cuando se infecta su ordenador o navegador web, es que sus datos personales pueden robarse. Esto puede ocurrir en dispositivos infectados con software maligno que sirve versiones falsas del sitio web por el que se está navegando, es decir, falsificación de sitio web, engañando al usuario para introducir su información de inicio de sesión que se envía a continuación al atacante. Gracias a esta información, el atacante puede entonces tener acceso a las cuentas personales en el sitio web original, por ejemplo, un proveedor de correo electrónico, un servicio bancario, un comercio electrónico, etc. Un ataque de este tipo también puede consistir en el robo de información sensible diferente como datos de tarjeta de crédito o el número de la seguridad social.

Otra amenaza es el software maligno que manipula la información introducida en los formularios, de forma transparente para el usuario (él/ella no aprecia ningún cambio visible de los datos) dando como resultado, por ejemplo, que se envíe diferente contenido de correo electrónico, dinero transferido a un número de cuenta bancaria diferente, etc.

Ha habido algunos intentos en la técnica anterior para resolver algunas de estas situaciones mediante el uso de un servidor que supuestamente envía versiones limpias de sitios web para que, en principio, el usuario pueda navegar por sitios web con un menor riesgo de que se infecte.

La publicación de la solicitud de patente de Estados Unidos 2014/0283071 A1 se refiere a un sistema y un método para aislar el software maligno de una aplicación con el uso de una aplicación física remota separada del cliente. Un módulo de codificación de aislamiento crea versiones seguras re-codificadas del contenido de la aplicación remota, por ejemplo, un sitio web visitado con un navegador web, por lo que el cliente descarga una versión sin software maligno del sitio web. La aplicación remota puede basarse en VM (es decir, máquina virtual), por lo tanto pueden ser necesarios muchos recursos para servir a una sola aplicación remota y/o a un único cliente. El documento 2014/0283071 A1 no dice nada sobre cómo prevenir ataques maliciosos cuando el software maligno ya está presente en la máquina cliente o navegador web, en ese caso, los datos podrían aún manipularse y/o robarse.

La publicación de solicitud de patente internacional n.º WO 2013/079113 A1 se refiere a un sistema cliente-servidor seguro de navegación y un método de uso del mismo. Un servidor transmite un archivo ejecutable que se ejecuta en un dispositivo cliente en respuesta a una solicitud hecha por el cliente para navegar por Internet. El archivo

ejecutable establece una comunicación entre el cliente y el servidor. El servidor, a su vez, crea una instancia de un contenedor, que luego crea una instancia de navegación que comprende un navegador remoto que descarga una página web, la representa, y la envía al cliente en la forma de imagen. Las instancias de contenedores -de un sistema de virtualización basado en contenedores- por lo tanto, se pueden crear después de que el archivo ejecutable se descarga y ejecuta en cliente después de que el cliente haya realizado la solicitud correspondiente. Un gestor de monitorización, monitoriza cada uno de estas instancias, y detecta si es necesario aplicar medidas de seguridad adicionales, o mover algunas instancias a otros servidores con el fin de minimizar el riesgo de que un atacante pueda obtener acceso al servidor.

El uso de técnicas de virtualización para lograr el aislamiento entre instancias, limita la cantidad de sesiones concurrentes o instancias a las que un servidor puede hacer frente, ya que se usan una cantidad significativa de recursos para ejecutar toda la máquina virtual o contenedor.

Además, el uso de archivos adicionales que se deben ejecutar en el dispositivo del cliente restringe el alcance de la navegación segura a los dispositivos en los que dichos archivos pueden ejecutarse. Este enfoque conlleva otros problemas tales como que el usuario deberá tener permiso o privilegios para su ejecución, y que cualquier antivirus y/o cortafuegos que estén instalados en el dispositivo del cliente no considere los archivos como una amenaza, y los marque como no maliciosos. Dado que las interacciones del usuario como las pulsaciones de teclado y los desplazamientos de ratón se transmiten a un servidor, el archivo puede marcarse como una aplicación de registro de teclas maliciosa.

Además, la empresa que presta un servicio que puede asegurarse y que es accesible en línea a través de un navegador web puede ser considerada responsable de la ejecución del software en el dispositivo del cliente con o sin su consentimiento. El software puede traspasarse proporcionando con ello una puerta trasera a través de la cual el usuario puede ser atacado; por lo que un intento de proporcionar un acceso seguro a un servicio en Internet expone al cliente a otros ataques maliciosos.

Otro aspecto importante para cualquier usuario es que no tener una implementación completamente transparente de un sistema de navegación segura es perjudicial en términos de experiencia de usuario y/o el nivel de confianza del sitio web navegado puede no ser legítimo.

Descripción de la invención

El servidor y método para proporcionar un acceso seguro a los servicios basados en la red que se dan a conocer en la presente invención tienen la intención de resolver los problemas y deficiencias de sistemas de navegación segura y métodos de la técnica anterior.

Un primer aspecto de la invención se refiere a un servidor intermediario para proporcionar acceso seguro a una página web de un servicio basado en la red a un terminal de cliente a petición de un servidor web y un terminal de cliente, el terminal de cliente incluye un navegador web, comprendiendo el servidor intermediario:

- un sistema operativo configurado para ejecutar una instancia de un motor de navegación web;
- el motor de navegación web está configurado para generar una imagen de la página web representada en la instancia del motor de navegación web, y para transmitir una página web de acceso al navegador web del terminal de cliente; y
- la página web de acceso está configurada para recuperar la imagen desde el motor de navegación web, y para mostrarla en el navegador web.

El servidor intermediario proporciona ventajosamente una conexión segura y fiable, e interacción con un servicio de Internet basado en la red que puede implicar el intercambio de información sensible, por ejemplo, pero sin limitación, un sitio web bancario, un comercio electrónico, un servicio de correo electrónico, otras páginas web particulares que soliciten credenciales del usuario, etc.

Cuando un sitio web solicita las credenciales de usuario, por ejemplo en forma de un inicio de sesión con nombre de usuario y contraseña o similares, el usuario puede estar expuesto a los riesgos de aplicaciones de registro de pulsaciones, conocidos como registradores de teclas (key-logger). Un registrador de teclas puede registrar cualquier entrada de un usuario y enviarla remotamente a la persona o pirata que instaló la aplicación. Esto es particularmente crítico cuando el usuario introduce sus credenciales en un formulario de inicio de sesión, ya que el pirata puede potencialmente utilizar esta información para obtener acceso privilegiado y/o hacerse pasar por el verdadero usuario. Aunque la criticidad de la información depende del sitio web que el cliente esté navegando, el servidor intermediario puede usarse para navegar por cualquier página web de una manera segura.

Por otra parte, el servidor intermediario también puede proporcionar un acceso seguro a los sitios web que hayan sido comprometidos o infectados de alguna manera. Un usuario o cliente navegando por un sitio web comprometido utilizando el servidor intermediario puede aún recuperar el contenido sin riesgo de que el equipo de usuario -por ejemplo PC, ordenador portátil, teléfono móvil, teléfono inteligente, tableta, TV inteligente, consola de videojuegos, y

en general cualquier dispositivo electrónico que comprenda una aplicación de navegador web- se infecte con un virus, software maligno o similares.

El sistema operativo comprende un motor de navegación web, que es una aplicación configurada para representar contenido en lenguaje de marcado -por ejemplo HTML, XHTML, etc.-, leguaje de hoja de estilo -por ejemplo XSL, CSS, etc.-, y contenido adicional de una página web que es visible para el usuario -por ejemplo imágenes, vídeos, animaciones, etc.-, de manera que se pueden mostrar a un usuario. Los motores de navegación web realizan principalmente las funciones de representación del contenido web, por lo que son también conocidos como motores de representación. Un motor de navegación web es uno de los muchos componentes que comprende un navegador web.

Cuando el servidor intermediario tiene que proporcionar un acceso seguro a una página web, el sistema operativo ejecuta una instancia del motor de navegación web. Esta instancia, carga el URL, es decir, localizador de recursos uniforme, a acceder, descarga o recupera los archivos de ese URL que, en general son, al menos: un primer archivo con contenido en lenguaje de marcado; archivos de hojas de estilo, si los hubiera, que el primer archivo solicita a través del código HTML o XHTML, por ejemplo; archivos de guiones, si los hubiera, que realizan funciones particulares dentro de la página web; y contenido multimedia, tal como imágenes, vídeos, animaciones, o similares, si los hubiera. Navegar por sitios web escritos en lenguajes tales como PHP, ASP, CGI o similares, en concreto, lenguajes de guiones del lado del servidor, también es posible con el servidor intermediario, ya que el código que se ejecuta en el servidor web está aún en ejecución, y el contenido resultante que ha de mostrarse al usuario -en lenguaje de marcado- se representa a continuación por el servidor intermediario.

La instancia del motor de navegación web representa la página web utilizando el archivo con lenguaje de marcado e incluye el contenido de cualquiera de los archivos adicionales que se tengan que mostrar, incluyendo archivos adicionales con lenguaje de marcado que puedan cargarse por el primer archivo. La página web representada va a transmitirse a una máquina de cliente en formato de imagen, de modo que el dispositivo de usuario sólo representa la imagen en sí misma en lugar de los archivos que se recuperan del sitio web. En particular, cuando el usuario navega a una página web a través del servidor intermediario, el motor de navegación web transmite una página web de acceso al navegador web en la máquina de cliente, y el navegador web carga dicha página de acceso.

Con la página web de acceso, el usuario puede navegar por una versión segura de una página web que se proporciona por el servidor intermediario, es decir, navegar por la página web representando únicamente imágenes creadas en el servidor intermediario. Así que la página web de acceso está configurada para obtener una imagen de la página web solicitada que se representa en la instancia del motor de navegación web y se muestra en el navegador web, es decir, para representar dicha imagen.

La página web de acceso también está configurada para enviar las interacciones del usuario con la página web de acceso -que muestra la página web solicitada- a la instancia del motor de navegación web en el servidor intermediario. La instancia, a su vez, reproduce las interacciones ya que dicha instancia comprende la página web representada; mediante la replicación de estas interacciones, la página web se navega dentro de la instancia y, adicionalmente, puede representarse de nuevo para que el cliente pueda ver el resultado de sus interacciones.

En otras palabras, cuando el cliente hace clic en un hiperenlace, es decir, enlace, en las flechas de la barra de desplazamiento, o rellena un formulario, los eventos de ratón y teclado se registran por la página web de acceso y se envían a la instancia en el servidor intermediario. Todas estas interacciones se reproducen a continuación dentro de la instancia, por lo que las acciones en realidad se llevan a cabo en el servidor intermediario, y la instancia genera imágenes de la página web después de cada una de estas interacciones independientemente de si la instancia representa una nueva página web o interactúa con la página web ya representada. La página web de acceso sondea el servidor intermediario, y recupera cualquier nueva imagen de la instancia de manera que se puede mostrar en el navegador web del cliente cuando se representa la imagen. Por lo tanto, el usuario puede interactuar, de hecho, con la página web, aunque lo que se muestra al usuario es sólo una imagen en lugar del código original o contenido de la página web que, en última instancia, permite la interacción del usuario.

El usuario, mientras navega por versiones seguras de las páginas web proporcionadas por el servidor intermediario, puede evitar la infección por el software maligno que está presente en las páginas web visitadas: sitios web infectados con código malicioso que, una vez que se descargan en la máquina cliente a través del navegador web, infectan ordenador si un antivirus, cortafuegos, o un software anti-software maligno no lo detiene a tiempo. Estas aplicaciones no solo son a menudo ineficaces contra muchos programas maliciosos, sino también es responsabilidad del usuario instalar y mantener estas aplicaciones actualizadas, así que tener conocimientos informáticos es una necesidad desde el punto de vista del usuario. La mayoría de las veces, el usuario medio no sabe mucho acerca de informática por lo que es poco probable que el usuario vaya a llevar a cabo cualquiera de estas tareas. Además, esto puede ser imposible en escenarios en los que los ordenadores se mantienen por un administrador de red, por ejemplo, en un entorno empresarial donde los PC se administran por un responsable o departamento informático. Del mismo modo, un usuario puede estar expuesto a estos ataques en dispositivos con sistemas operativos para los que no haya soluciones de antivirus fiables. Así que el servidor intermediario es el equipo que descarga cualquier contenido malicioso incluido en la página web solicitada; el servidor intermediario

está provisto de aplicaciones y mecanismos que deniegan posibles infecciones que puedan afectar a su correcto funcionamiento.

A pesar de que el servidor intermediario inmuniza al usuario contra estos ataques maliciosos, la máquina cliente puede ya estar infectada en el momento que utiliza el servidor intermediario para navegar por Internet. Esto significa que el software maligno que reside en el terminal del cliente puede tener acceso a la información y contenidos que el usuario está recuperando a través de Internet, y enviarlos a un pirata para su beneficio personal.

El software maligno también puede manipular la información descargada de manera que el cliente vea o acceda a un contenido falso o fraudulento -por ejemplo, la versión falsa de una página web, además de publicidad, etc.-, o puede manipular la información introducida por el cliente -por ejemplo, número de cuenta bancaria de transferencia, el contenido o la dirección de destinatario de un correo electrónico, etc.-. En ambos casos, el servidor intermediario puede disminuir el efecto dañino del software maligno.

En lo que respecta al primer caso, es decir, cuando el software maligno intenta manipular la información descargada, a medida que el navegador web del cliente descarga la página web de acceso y una versión en formato imagen sin software maligno de una página web navegada en lugar de sus archivos de código y cualquier otro archivo - que, virtualmente, puede ser de cualquier tipo-, el software maligno en el navegador web no puede reconocer ninguna información porque sólo se descarga el código de la página web de acceso. Por lo tanto, el software maligno programado para modificar la página web descargada, así como para incluir o reemplazar contenido como los anuncios, por ejemplo, no puede colocar el contenido ya que no detecta el código de marcado que está configurado para reconocer y modificar. Así que el contenido malicioso puede añadirse en una ubicación que no se corresponde, por ejemplo por encima o por debajo de la imagen producida por el servidor intermediario, si llega a añadirse en su totalidad. En algunos casos, la información fraudulenta, que está fuera de lugar, no engaña a los usuarios a hacer clic en ella o a rellenar información sensible. Por otra parte, los usuarios pueden sospechar que la página web ha sido comprometida (independientemente de si ocurrió en el servidor web o en su propio dispositivo).

En el segundo caso, es decir, cuando el usuario se está rellenado formularios, ningún formulario HTML está presente en el navegador web del cliente, así que el software maligno programado para reconocer tipos de formularios y la información introducida en ellos, no es capaz de entender la información, ya que todo lo que se captura son pulsaciones del teclado y movimientos del ratón y/o eventos. Es en el servidor intermediario –dentro de la instancia- donde el formulario HTML se rellena con la información del usuario y no en la máquina cliente. El software maligno puede intentar identificar el tipo de información que el usuario está insertando mediante el análisis de las imágenes representadas, sin embargo los algoritmos de OCR (Reconocimiento Óptico de Caracteres) hacen un uso intensivo de la CPU y no son del todo fiables, por lo que es más complejo para los piratas obtener cualquier información de valor de una máquina infectada.

Del mismo modo, esto no permite que el software maligno cambie de forma trasparente la información en el formulario, por ejemplo, no puede detectar cuándo se está presionando el botón de envío para manipular el mismo, por ejemplo, escribir un número de cuenta bancaria diferente. El software maligno puede interceptar las pulsaciones del teclado, por ejemplo, y reemplazarlas por sus propios caracteres, pero no puede detectar qué parte del formulario está seleccionada actualmente, si hay alguna seleccionada, por lo que debe adivinar qué tipo de información se está escribiendo, reemplazarla, y esperar que el usuario no se dé cuenta de que la información que aparece en el formulario no es la misma que él/ella está escribiendo.

En contraste con tecnologías anteriores, el servidor intermediario no se basa en técnicas de virtualización. El servidor intermediario proporciona un acceso seguro a los servicios de Internet basados en la red por medio de motores de navegación web en lugar de virtualización por medio de máquinas virtuales, también conocidas como VM, o virtualización a nivel de sistema operativo, también conocido como contenedores.

Las máquinas virtuales y contenedores emulan un sistema informático y un sistema operativo completos, respectivamente. Esto significa que un sistema operativo completo debe replicarse para proporcionar una máquina virtual, o parte de un sistema operativo debe replicarse para proporcionar un contenedor. En ambos casos, muchos archivos deben copiarse y ejecutarse con el fin de ejecutar un navegador web para proporcionar un acceso seguro a las páginas web. Por lo tanto, son necesarias gran cantidad de espacio en disco y gran capacidad de procesamiento: los archivos se deben almacenar en algún lugar en el medio de almacenamiento de datos del servidor, y ejecutarse para replicar el sistema operativo o para proporcionar un contenedor, que luego pueda ejecutar un navegador web. Esto implica una enorme carga computacional que tiene un fuerte impacto en el procesador y la memoria del servidor, así que la mayor parte de los recursos del servidor están reservados para la ejecución de la máquina virtual o el contendor, y una pequeña parte de los recursos se utilizan por los navegadores web que, en realidad, proporcionan un acceso seguro a páginas web, no al sistema de virtualización.

Por otra parte, la creación o el inicio de una máquina virtual o contenedor requiere de tiempo, incluso cuando la mayoría de los recursos del sistema están libres, por lo que la capacidad de respuesta del servidor intermediario es lenta si no se crean máquinas virtuales o contenedores antes de que la solicitud llegue al servidor, en cuyo caso la potencia de procesamiento del sistema se gasta de manera inútil, mientras que el consumo de potencia se

incrementa a medida que la potencia demandada por la fuente de alimentación aumenta.

Por el contrario, la creación de una nueva instancia de un motor de navegación web -que, además, no es un navegador web completo, por lo que requiere menos asignación de memoria y capacidades de procesamiento- puede tardar pocos segundos o incluso menos de un segundo, por lo que la capacidad de respuesta es casi instantánea y lo suficientemente rápida para llevarse a cabo tan pronto como se recibe la solicitud de acceso seguro por el servidor intermediario. Por lo tanto, un servidor intermediario como se describe en la presente invención puede dar servicio a más usuarios o peticiones concurrentes que los servidores utilizando máquinas virtuales o contenedores con una misma máquina, ya que exige menos potencia de procesamiento y memoria. También, el consumo de potencia mientras da servicio a un número determinado de usuarios o solicitudes es inferior a la potencia consumida por los servidores que ejecutan las VM o contenedores.

Además de los reducidos requisitos de carga y almacenamiento de datos computacionales involucrados en la creación de instancias de motores de navegación web en comparación con máquinas virtuales o sistemas operativos virtuales, un servidor intermediario que ejecuta dichos motores de navegación web puede proporcionar protección contra ataques maliciosos que son eficaces y puede ser incluso superior a la proporcionada por los contenedores o las VM. Particularmente, diferentes contenedores o VM pueden aislar las infecciones entre sí, es decir, cuando un contenedor o máquina virtual está infectado con software maligno, la infección podría no propagarse a otros contenedores o máquinas virtuales, ya que pueden ejecutarse de manera independiente. Sin embargo, los contenedores o máquinas virtuales no pueden prevenir una infección: un proceso malicioso puede descargarse en el navegador web del contenedor o de la VM y ejecutarse a sí mismo, convirtiéndose así en un proceso activo que se ejecuta en la memoria del sistema. Y puesto que el aislamiento entre los contenedores o máquinas virtuales no es completo, en el momento que se borra el contenedor o VM después de que haya terminado una sesión de usuario, el proceso que se ejecuta en la memoria puede ya haber afectado a otras instancias que usan los adaptadores de red o las API -es decir, interfaz de programación de aplicaciones-, por ejemplo.

El servidor intermediario ejecuta motores de navegación web que están configurados para acceder sólo a directorios de acceso temporales que se crean en la inicialización de los motores, y otros directorios particulares determinados por el administrador, para el correcto funcionamiento del servidor intermediario, si lo hubiera. Esto significa que los motores de navegación web no pueden acceder a las carpetas o directorios del sistema operativo que no sean estos directorios temporales y/o directorios particulares especificados, y el sistema operativo también se configura para denegar cualquier operación con archivos no pertenecientes a los directorios temporales, por lo que se bloquea cualquier intento de crear un archivo fuera de las carpetas temporales.

Además, el sistema operativo también está configurado para gestionar qué procesos pueden lanzarse y estar en ejecución y los que no, es decir, el sistema operativo tiene una lista blanca de los procesos y se niega la ejecución de cualquier proceso que no esté presente en esa lista. Con este fin, el núcleo se modifica de manera que sea capaz de efectuar dicho proceso de filtrado, proporcionando de ese modo al sistema operativo la capacidad de gestionar si un proceso se puede lanzar y ejecutar o si debe bloquearse. Entonces, en el caso de que el software maligno se descargue en una instancia del motor de navegación web, se almacene en un directorio temporal e intente ejecutarse, el sistema operativo no le permite hacerlo. El sistema operativo entonces puede registrar también una advertencia que indica un intento de ejecución de una aplicación no permitida junto con la URL de la página web que origina la amenaza.

El uso de un motor de navegación web también es ventajoso para evitar el software maligno particular destinado a atacar a un navegador web, es decir, un navegador web en toda regla, que comprende un motor de navegación web. Muchos virus pueden infectar a ciertas partes de un navegador web como, por ejemplo, sistemas para la sincronización de datos personales a través de los navegadores web de plataformas cruzadas, módulos de extensión, complementos, etc. A pesar de que sólo se utiliza y ejecuta el motor de navegación web, el motor de navegación web también puede estar configurado para implementar capacidades como las incluidas en complementos, disminuyendo así el riesgo de infección.

Con el servidor intermediario, los dispositivos con capacidades de procesamiento o memoria limitadas también pueden navegar por páginas web que requieren un uso intensivo de la CPU o que incluyen contenido no descifrable por estos dispositivos como, por ejemplo, animaciones, aplicaciones, etc., accionadas por Flash, OpenGL, o los vídeos codificados con códecs que no están instalados en los dispositivos. En este caso, es el servidor intermediario el dispositivo que debe ser capaz de decodificar y reproducir el contenido, y luego producir las imágenes que serán obtenidas por la página web de acceso.

Otro aspecto importante es que la experiencia de usuario al navegar por Internet a través del servidor intermediario debe ser buena: las páginas web deben tener una respuesta aceptable en términos de tiempo que se tarda en reaccionar a las interacciones del cliente y/o el tiempo que tarda en cargar la página web; el aspecto y la sensación deben ser exactamente los mismos que si el cliente estuviera navegando por la página web original; las sesiones de usuario con o sin las cookies deben mantenerse mientras se mueve de una página web a otra, ya sea haciendo clic en los enlaces o escribiendo un URL diferente en la barra de direcciones, etc.

En este sentido, la instancia del motor de navegación web representa la página web como se mostraría al usuario, y luego se recupera y se muestra mediante la página web de acceso en el navegador web del cliente de la misma manera, por lo tanto el cliente no ve un navegador web dentro de un navegador web, haciendo que sea transparente para él/ella.

La capacidad de respuesta de la página web de acceso depende en gran medida del ancho de banda de cada uno de los clientes y del servidor intermediario: las conexiones lentas tardarán más tiempo en interactuar con la página web y en recuperar nuevas imágenes producidas por el servidor intermediario o los archivos desde el servidor web que aloja la página web. El retardo que el servidor intermediario puede introducir puede ser tan bajo como unos milisegundos puesto que el tiempo transcurrido durante la creación de una nueva instancia del motor de navegación web puede estar en el orden de decenas o cientos de milisegundos.

La instancia del motor de representación puede estar configurada para mantener las sesiones de usuario activas hasta que el usuario deja de usar la instancia, es decir, dejar de navegar una página web a través del servidor intermediario. Esto significa que las sesiones que no utilizan cookies pueden mantenerse durante toda la instancia; lo mismo ocurre para las sesiones que utilizan cookies, ya que los archivos correspondientes a las cookies se pueden almacenar en el directorio temporal y también utilizarse.

En las realizaciones preferidas de la invención, la página web de acceso comprende un código JavaScript o HTML configurado para cargar un código JavaScript obtenible desde el servidor intermediario.

El código JavaScript de la página web de acceso, que se ejecuta en el navegador web del cliente, establece comunicación con la correspondiente instancia del servidor intermediario para que el usuario pueda navegar con seguridad una página web en particular. Así que el código JavaScript está configurado para descargar las imágenes representadas de la instancia a través de una red -por ejemplo Internet-, para capturar las pulsaciones del teclado e interacciones del ratón del usuario mientras él/ella navega en la página web de acceso y transmitir esta entrada del usuario al servidor intermediario. El registro de la entrada del usuario se limita a la pestaña en la que se visualiza la página web de acceso, si el navegador web del cliente se proporciona con navegación web con pestañas, o a la ventana en la que se muestra la página web de acceso cuando el navegador web no soporta pestañas. El código JavaScript no registra las pulsaciones del teclado ni los movimientos del ratón mientras la pestaña o ventana no está activa o tiene el foco, es decir, cuando la página web de acceso es visible para el usuario en la pantalla pero el usuario ha hecho clic en una aplicación diferente al navegador web, por lo que el sistema operativo ha declarado otra aplicación como activa. Esto no significa que el navegador web no esté ejecutándose porque, de hecho, cualquier cambio que se produce en la página web solicitada puede mostrarse al usuario en la página web de acceso -si se recuperan las imágenes producidas en el servidor intermediario-, significa que otra aplicación está registrando la entrada del usuario para realizar cualquier tarea para la que la aplicación esté configurada a ejecutar.

El uso de JavaScript también es ventajoso, porque se ejecuta confinado dentro del navegador web. Por lo tanto, el código JavaScript no necesita que el usuario tenga privilegios de administrador en el sistema operativo o similar, siempre que el usuario pueda ejecutar el navegador web, el código JavaScript también se ejecutará. Esto, a su vez, hace que el código JavaScript sólo pueda acceder a aquellas partes del sistema operativo a las que el navegador web tiene acceso, mientras que una aplicación que se ejecute fuera del entorno del navegador web podría tener acceso al registro del sistema operativo, directorios del sistema, las bibliotecas de enlace dinámico y similares, dependiendo de los permisos que se concedan durante su ejecución.

Asimismo, la mayoría de los navegadores web son capaces de ejecutar código JavaScript: el uso del servidor intermediario y la página web de acceso es prácticamente transparente para el sistema operativo que el equipo de cliente esté utilizando. En otras palabras, no es necesaria una aplicación o implementación diferente para cada sistema operativo. Como la página de acceso web no necesita utilizar plataformas de software como Java o similar, el cliente no está expuesto a ninguna vulnerabilidad o problema que estas plataformas puedan presentar.

Las tareas realizadas por el código JavaScript que se han descrito anteriormente pueden programarse en uno o más códigos de JavaScript, es decir, diferentes guiones pueden implementar las diferentes funcionalidades. El código JavaScript puede estar incluido en la página web de acceso, o también puede estar incluido dentro de la página web de acceso un código que solicite la recuperación de uno o más códigos de JavaScript; en este último caso, cuando la página web de acceso se analiza por el navegador web del cliente, el navegador web descarga y ejecuta el código o los códigos JavaScript. En cualquier caso, las variaciones en las implementaciones no tienen ningún impacto en el comportamiento o rendimiento del código JavaScript y están dentro del alcance de la invención.

En algunas implementaciones, el motor de navegación web está configurado adicionalmente para sanear las pulsaciones de teclado detectables por la página web de acceso.

En algunas implementaciones de la invención, el sistema operativo está configurado adicionalmente para ejecutar una nueva instancia del motor de navegación web para cada solicitud de suministro de un acceso seguro a una página web de un servicio basado en la red.

Como cada instancia del motor de navegación web puede tener acceso a su propia carpeta temporal específica, las instancias también están aisladas unas de otras. Por otra parte, la forma particular en que el servidor intermediario puede proporcionar un acceso seguro a las páginas web proporciona una capa adicional de seguridad a los usuarios, ya que cada petición puede asignarse a una nueva instancia diferente. El motor del navegador web puede estar configurado de manera que un mismo usuario navegando por dos páginas web diferentes utilice dos instancias independientes, o utilice una misma instancia para navegar por las dos páginas web diferentes; el primer esquema de configuración es conveniente para conseguir un alto aislamiento, mientras que el segundo esquema de configuración puede ser ventajoso desde el punto de vista de la usabilidad ya que las sesiones, cookies y/o cualquier medio de autentificación común a ambas páginas web se pueden compartir, por ejemplo, entre varias aplicaciones accedidas en una intranet. Por el contrario, los servidores que proporcionan dicho acceso utilizando las VM o contenedores, y con el fin de maximizar la eficiencia de los recursos empleados en la creación de dichas VM o contenedores, un mismo usuario navegando por dos páginas web diferentes con el mismo servidor puede hacerlo con dos navegadores web, pero dentro de la misma máquina virtual o contenedor. Así, a pesar de que diferentes contenedores o VM se pueden aislar entre sí, si un contenedor o VM se infectara, todos sus procesos se ven afectados, incluyendo los dos o más navegadores web en uso.

En algunas implementaciones de la invención, el motor de navegación web está configurado además para detectar el cambio de partes de la página web en la instancia, y para producir imágenes de las partes cambiantes. En algunas de estas implementaciones, la página web de acceso está configurada, además, para recuperar las imágenes de las partes cambiantes desde el motor de navegación web, y para sustituir las partes de la imagen visualizada en el navegador web con las imágenes de las partes cambiantes.

El motor de navegación web puede detectar las partes de la página web representada que cambian con el tiempo, por ejemplo, imágenes animadas, videos, u otro contenido dinámico como partes de la página web en AJAX, es decir, JavaScript asíncrono. El motor de navegación web puede producir imágenes para cada una de estas partes, por lo que el tamaño de la imagen puede estar limitado a las dimensiones del contenido dinámico.

Estas imágenes pueden recuperarse por la página web de acceso junto con la posición en la que se encuentran en la página web, y se reemplazan las partes de la imagen representada con las imágenes de las partes cambiantes, con el consiguiente ahorro de ancho de banda que supone el envío de una imagen que comprende la totalidad de la página web con la parte cambiante, y también la mejora de la capacidad de respuesta de la página web de acceso.

En algunas de estas implementaciones, el motor de navegación web está configurado además para detectar el tipo de contenido al que pertenecen las partes cambiantes, y/o las características visuales de las partes cambiantes. En estas implementaciones, el motor de navegación web está configurado, además, para seleccionar una compresión de la imagen particular y/o el formato de archivo de imagen para la producción de las imágenes de las partes cambiantes.

A medida que la instancia del motor de navegación web está representando el contenido de la página web descargada en el lenguaje de marcado, el motor de navegación web puede identificar la etiqueta HTML correspondiente a una porción cambiante, es decir, puede identificar si la parte que ha cambiado es una imagen, un vídeo, texto, etc. También puede inspeccionar de forma dinámica, con un algoritmo, los píxeles de la parte cambiante y detectar la paleta de color, histograma, nitidez, etc. Con esta información, el motor de navegación web puede decidir aplicar una mayor o menor compresión o no comprimir la imagen producida; del mismo modo, puede decidir utilizar un formato de archivo de imagen u otro, teniendo en cuenta la compresión característica y parámetros de calidad de cada formato. Así, el motor de navegación web puede estimar la importancia de reproducir, con mayor o menor calidad, una parte cambiante basándose en sus características o en el tipo de contenido de la parte cambiante, con el fin de mejorar la capacidad de respuesta y ahorrar ancho de banda. En un caso a modo de ejemplo de una parte cambiante, que sólo incluye texto negro sobre fondo blanco, el motor de navegación web puede producir una imagen de pequeño tamaño usando un formato de imagen GIF con una paleta 10 colores, que puede ser suficiente para reproducir el texto nítidamente.

En realizaciones preferidas de la invención, el motor de navegación web está configurado para comunicarse con el navegador web utilizando el protocolo HTTPS.

Toda la información que se va a transferir entre el motor de navegación web en el servidor intermediario, y el navegador web en el terminal de usuario, puede utilizar un protocolo HTTPS con el fin de, al menos, cifrar la interacción del usuario en la página web de acceso y las imágenes producidas en el servidor intermediario.

En realizaciones preferidas, el motor de navegación web está configurado, además, para crear al menos un directorio temporal en el sistema operativo para cada una de las instancias y cualquiera nueva del motor de navegación web y para permitir el acceso de cada instancia y cualquiera nueva a su respectivo al menos un directorio temporal en el sistema operativo.

El servidor intermediario asigna a cada solicitud de acceso seguro a páginas web una nueva instancia del motor de navegación web. Cada instancia puede borrarse una vez que el usuario deje de navegar por la página web de

acceso o su sesión expira después de un cierto periodo de inactividad. El motor de navegación web crea una carpeta temporal para cada una de estas instancias, por lo que cada instancia es independiente y está aislada de las demás, y puede eliminar una carpeta temporal y todo su contenido cuando se elimina la instancia asociada.

En realizaciones preferidas, el servicio basado en la red está disponible en Internet, es decir, las páginas web que proporcionan el servicio basado en la red están alojadas en servidores web con conectividad a Internet.

En algunas implementaciones, el motor de navegación web además está configurado para descargar un archivo en una instancia de un servidor diferente del servidor intermediario, y para explorar el archivo en busca de virus y/o software maligno. En algunas de estas realizaciones, el motor de navegación web está configurado adicionalmente para servir el archivo en el terminal de cliente cuando no se ha detectado ningún virus y/o software maligno. En algunas otras realizaciones, el motor de navegación web está configurado adicionalmente para proporcionar una versión sin virus y/o software maligno del archivo cuando se ha detectado un virus y/o software maligno, y servir la versión sin virus y/o software maligno del fichero al terminal de cliente. En estas realizaciones, la página web de acceso está configurada para descargar el archivo servido por el motor de navegación web.

En algunas realizaciones, el motor de navegación web además está configurado para recibir un archivo desde el terminal del cliente, y para escanear el archivo en busca de virus y/o software maligno. En algunas de estas realizaciones, el motor de navegación web está configurado para servir el archivo a un servidor diferente del servidor intermediario cuando no se ha detectado ningún virus y/o software maligno. En algunas otras implementaciones, el motor de navegación web está configurado adicionalmente para proporcionar una versión sin virus y/o software maligno del archivo cuando se ha detectado un virus y/o software maligno, y para servir la versión sin virus y/o software maligno a un servidor diferente del servidor intermediario.

Entonces, cuando el usuario pretende descargar o cargar un archivo, el servidor intermediario primero obtiene el archivo y lo escanea para buscar contenido malicioso, y puede que paralice la descarga en la máquina del cliente o la carga en un servidor si el archivo está infectado, o limpie el contenido malicioso del archivo y lo sirva sin virus y/o software maligno.

Además, el servidor intermediario también puede detectar si la página web de acceso es objeto de manipulaciones, es decir, en algunas realizaciones el motor de navegación web, está configurado adicionalmente para comprobar la integridad de la página web de acceso. De esta manera, el servidor intermediario puede saber si el navegador web en la máquina de cliente está infectado.

Un fragmento o la totalidad del código de página web de acceso se transmite al servidor intermediario donde se aplica una función de troceo a dicho código. El valor de troceo resultante se compara con el valor de troceo que se calculó cuando la página web de acceso se transmitió a la máquina de cliente. Además, la página web de acceso puede estar configurada adicionalmente para calcular el valor de troceo de la secuencia de pulsaciones de teclado y para transmitir el valor de troceo al servidor intermediario, que a su vez calcula el valor de troceo de la secuencia de pulsaciones de teclado recibida y lo compara con el valor de troceo recibido. Si el software maligno ha manipulado los datos introducidos por el usuario, el servidor intermediario recibiría una secuencia alterada de pulsaciones de teclado, por lo tanto el valor de troceo en última instancia sería diferente al valor de troceo calculado en la máquina del cliente, que de hecho corresponde a la secuencia original de las pulsaciones de teclado.

Por otra parte, en algunas realizaciones, el motor de navegación web está configurado adicionalmente para ofuscar el código en la página web de acceso, de manera que sea más complejo y engorroso de comprender y manipular, sin embargo, la página web de acceso mantiene su funcionalidad intacta. En cualquier caso, una página web de acceso manipulada no afectaría a la correcta operación del servidor intermediario ya que la página web de acceso no incluye ninguna operación que pueda atacar el servidor.

Otro aspecto de la invención se refiere a un método para proporcionar un acceso seguro a una página web de un servicio basado en la red para un terminal de cliente que comprende un navegador web, comprendiendo el método:

- recibir una solicitud para proporcionar, al terminal de cliente, el acceso seguro a la página web;
- ejecutar una instancia de un motor de navegación web;
- producir una imagen de la página web tras la representación en la instancia del motor de navegación web; y
- transmitir una página web de acceso al navegador web, estando configurada la página web de acceso para recuperar una imagen desde el motor de navegación web, y para mostrar la imagen en el navegador web.

Una instancia de motor de navegación web se ejecuta con el fin de recuperar los archivos de una página web solicitada. Los archivos se representan en la instancia, y se produce una imagen representada de la página web.

Mediante la transmisión de una página web de acceso a un terminal de cliente, particularmente al navegador web que solicitó la página web que se va a navegar, el navegador web puede tener acceso a una versión segura del servicio basado en la red. La página web de acceso está configurada para descargar la imagen en la instancia producida por el motor de navegación web, y para mostrarla al usuario mediante el navegador web.

La transmisión de una página web de acceso que puede analizarse y representarse en un navegador web limita el acceso del posible software maligno a aquellas partes del dispositivo de cliente y su sistema operativo que son accesibles por el navegador web. Además, la posibilidad de navegar por una versión segura de una página web con el método descrito en este documento se determina por el navegador web en el terminal de cliente: si el navegador web puede analizar y representar dicha página web de acceso, la navegación segura es posible.

Podría ser inviable si, por ejemplo, dicha navegación segura se proporcionase por medio de un archivo ejecutable en lugar de una página web de acceso. En primer lugar, el archivo tendría que ser compatible con el sistema operativo; en segundo lugar, el cliente tendría que tener suficientes privilegios en el sistema para ejecutar o instalar el archivo o aplicación; y, por último, durante la ejecución del proceso, estaría en la memoria del sistema, por lo que podría ser potencialmente vulnerable al software maligno dirigido para atacar este proceso, que puede ser de interés tanto para el cliente como para el servidor que proporciona el archivo al cliente, ya que, en un intento de proporcionar una manera de navegación segura por sitios web, habría expuesto la máquina de cliente a una posible nueva forma de ser violada.

Ventajas similares a las descritas para el primer aspecto de la invención también pueden ser aplicables a este aspecto de la invención.

En realizaciones preferidas de la invención, la solicitud de proporcionar un acceso seguro es una petición de un servidor web. En algunas otras realizaciones preferidas de la invención, la solicitud de proporcionar un acceso seguro es una petición del terminal del cliente.

Un servidor web que aloja un determinado servicio basado en la red puede beneficiarse de que los usuarios naveguen el servicio de una manera segura, ya que el servidor web puede solicitar el acceso seguro para un usuario que está intentando navegar una de sus páginas web alojadas. En particular, el software maligno que reside en el equipo cliente puede manipular la información introducida por el cliente en un formulario, lo que afecta negativamente al servidor web o servicio, que debe evitar a toda costa cualquier operación fraudulenta. Por ejemplo, el número de cuenta bancaria usado en una transferencia realizada desde un sitio web de un banco puede ser sustituido por otro número de cuenta bancaria. Por lo tanto, con el fin de evitar las transacciones bancarias fraudulentas, el servidor web puede solicitar el suministro de acceso seguro a su servicio para que el cliente pueda navegar de forma segura las páginas web en las que se va a introducir información sensible.

Por otro lado, el usuario también puede solicitar dicho acceso seguro para que él/ella no tenga que preocuparse por la posible presencia de software maligno que pueda infectar el dispositivo del usuario en los sitios web visitados.

En realizaciones preferidas de la invención, la página web de acceso comprende código JavaScript o HTML configurado para cargar código JavaScript recuperable desde el servidor.

En algunas realizaciones, el método comprende adicionalmente:

- recibir pulsaciones de teclado e interacciones de ratón detectables por la página web de acceso;
- sanear las pulsaciones de teclado; e
- introducir las pulsaciones de teclado saneadas y las interacciones del ratón en la instancia del motor de navegación web.

La página web de acceso podrá registrar toda la entrada del usuario en forma de pulsaciones de teclado e interacciones de ratón que se produzcan en dicha página web de acceso. Dicha entrada de usuario puede utilizarse a continuación para interactuar con la página web. Además, en algunas implementaciones, las pulsaciones de teclado de la entrada de usuario pueden sanearse por lo que los servicios basados en la red que quieran ser visitados de forma segura son menos propensos a vulnerarse. Es decir, caracteres particulares y/o secuencias o cadenas de texto pueden suprimirse o sustituirse por otros caracteres, por lo que las técnicas tales como inyección de SQL, que consisten en sentencias SQL adaptadas para aprovechar las vulnerabilidades de la base de datos, se vuelven menos eficaces.

En algunas realizaciones de la invención, el método incluye:

- detectar partes cambiantes de la página web en la instancia del motor de navegación web; y
- producir imágenes de las partes cambiantes.

Además, la página web de acceso está configurada adicionalmente para recuperar las imágenes de las partes cambiantes desde el motor de navegación web, y para sustituir partes de la imagen mostrada en el navegador web con las imágenes de las partes cambiantes.

En realizaciones preferidas, el método comprende adicionalmente ejecutar en el servidor una nueva instancia del motor de navegación web por cada solicitud recibida en el servidor, para proporcionar un acceso seguro a una página web de un servicio basado en la red.

En realizaciones preferidas de la invención, la instancia y cada nueva instancia del motor de navegación web se crean tras la recepción de una solicitud para proporcionar un acceso seguro a una página web de un servicio basado en la red.

En realizaciones preferidas, el servicio basado en la red está disponible en Internet, es decir, las páginas web que proporcionan el servicio basado en la red están alojadas en servidores web con conectividad a Internet.

En algunas implementaciones, el método comprende además:

- descargar un archivo desde un servidor o recibir un archivo desde el terminal de cliente; y
- escanear el archivo en busca de virus y/o software maligno.

En algunas de estas realizaciones, el método comprende adicionalmente, en el caso de que en la exploración del archivo no haya detectado ningún virus o software maligno, servir el archivo descargado al terminal del cliente o el archivo cargado al servidor. En algunas otras realizaciones, el método comprende adicionalmente, en el caso de que el escaneo del archivo haya detectado un virus o software maligno, proporcionar una versión del archivo sin virus o software maligno al terminal de cliente o servidor.

Cuando la página web de acceso transmite -al servidor intermediario- una pulsación de teclado y/o interacción de ratón del usuario que se corresponde con la descarga de un archivo, el servidor intermediario en primer lugar descarga el archivo, comprueba si está sin virus y/o software maligno, y sirve el archivo descargado en el servidor intermediario al terminal de cliente. Dicho archivo, que puede considerarse como un archivo descargable, puede ser cualquiera de, por ejemplo, audio -por ejemplo mp3, wav, ogg, wma, etc.-, imagen -por ejemplo jpg, bmp, gif, png, etc.-, vídeo -por ejemplo mp4, avi, mkv, flv, etc.-, documento -por ejemplo doc, docx, pdf, rtf, txt, etc.-, comprimido -por ejemplo, zip, 7z, RAR, etc.-, y virtualmente cualquier otro formato de archivo, incluyendo archivos ejecutables. Con este fin, la página web de acceso está configurada para descargar el archivo que se sirve por el servidor intermediario.

Cuando el servidor intermediario detecta contenido malicioso en el archivo, el servidor puede intentar eliminar -con soluciones software de antivirus y anti-software maligno - dicho contenido de manera que se proporcione una versión limpia del archivo, que luego se sirve al terminal de cliente. Cuando se comprime el archivo descargable e incluye varios archivos, todos los archivos comprimidos pueden analizarse y limpiarse antes de servir el archivo descargable.

En cualquier caso, el motor de navegación web puede estar configurado para permitir o prohibir la carga/descarga de archivos, y/o permitir solamente la carga/descarga de archivos con formatos de fichero particulares.

Del mismo modo, el usuario puede cargar o enviar archivos en algunos servicios basados en la red, por ejemplo, cuando se adjuntan archivos a un correo electrónico, o se almacenan fotos en un servicio en la nube. Cuando se navega este servicio basado en la red a través del servidor intermediario, el servidor intermediario también puede escanear los archivos con el fin de evitar que el servidor web del servicio basado en la red se infecte con virus, software maligno, y similares.

El método descrito en este documento también podrá comprobar si el navegador web del usuario está infectado. En este sentido, en algunas implementaciones de la invención, el método comprende adicionalmente:

- calcular un primer valor de troceo de un fragmento o la totalidad del código de la página web de acceso antes de transmitir la página web de acceso al navegador web;
- recibir el fragmento o la totalidad del código de la página web de acceso desde el navegador web;
- calcular un segundo valor de troceo del código recibido de la página web de acceso; y
- comparar el primer valor de troceo con el segundo valor de troceo.

En algunas realizaciones, la página web de acceso está configurada además para calcular un primer valor de troceo de una secuencia de pulsaciones de teclado, y el método comprende adicionalmente:

- calcular un segundo valor de troceo de una secuencia de pulsaciones de teclado recibida desde el terminal de cliente detectable por la página web de acceso; y
- comparar el primer valor de troceo con los segundos valores de troceo.

En algunas realizaciones, el método además comprende la ofuscación del código de la página web de acceso antes de transmitir la página web de acceso al navegador web.

Otro aspecto de la invención se refiere a un programa informático que comprende medios de código de programa informático adaptados para realizar las tareas de un método de acuerdo con el segundo aspecto de la invención cuando dicho programa se ejecuta en un ordenador, un procesador de señal digital, un campo de matrices de puertas programables, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador, o

cualquier otra forma de hardware programable.

Un cuarto aspecto de la invención se refiere a una memoria legible por ordenador o medio que almacena instrucciones de programa o código para ejecutar un método de acuerdo con el segundo aspecto de la invención.

Breve descripción de los dibujos

Para completar la descripción y con el fin de proporcionar una mejor comprensión de la invención, se proporciona un conjunto de dibujos. Dichos dibujos forman parte integral de la descripción e ilustran una realización de la invención, que no debe interpretarse como una restricción del alcance de la invención, pero sólo como un ejemplo de cómo la invención puede llevarse a cabo. Los dibujos comprenden las siguientes figuras:

La Figura 1 es una representación esquemática de las posibles conexiones entre el equipo de usuario y servidores web mediante un servidor intermediario de acuerdo con la invención.
La Figura 2 es otra representación esquemática de las posibles conexiones entre el equipo de usuario y los servidores web utilizando un servidor intermediario de acuerdo con la invención.
La Figura 3 es un servidor intermediario de acuerdo con una realización de la invención.
La Figura 4 es una página web de acceso de acuerdo con una realización de la invención.
Las Figuras 5A-5B son diagramas que muestran la comunicación entre el equipo de usuario y el servidor intermediario de acuerdo con las implementaciones de la invención.

Descripción de una forma para llevar a cabo la invención

La figura 1 muestra esquemáticamente las posibles formas de navegar por las páginas web de los servicios basados en la red a través de Internet 100, dependiendo de la configuración de cada servidor web 120-122.

Un servidor intermediario 101, para proporcionar un acceso seguro a las páginas web está conectado a Internet 100. Un primer usuario puede navegar por las páginas web de cualquiera de los servidores web 120-122 con un teléfono celular 110 que incluye un navegador web, y un segundo usuario puede hacerlo de manera similar con un ordenador personal PC 111.

Un primer servidor web 120 está configurado para permitir conexiones directas de los equipos cliente con el servidor web 120, por lo que la máquina cliente puede estar expuesta a cualquier software maligno presente en el servidor web 120. Aunque no se ilustra con las flechas, el usuario puede solicitar al servidor intermediario 101 el acceso seguro a cualquier servidor web, incluyendo el servidor web 120. Por lo tanto, en este caso, las solicitudes de acceso seguro se originarían por el terminal de usuario en lugar del servidor web 120.

Un segundo servidor web 121 está configurado para solicitar el acceso seguro a todas las páginas web que alberga cuando un navegador web de un cliente, como los que hay en el teléfono celular 110 o en el PC 111, intenta conectarse a cualquier página web alojada en el servidor web 121. El servidor intermediario 101 ejecuta una instancia de un motor de navegación web, recupera los archivos de la página web en particular, representa y produce una imagen de la página web para que la máquina cliente pueda navegar una versión segura de la página web. Un servidor web de ejemplo 121 puede ser un servicio basado sólo en la nube, en el que la pantalla de presentación es básicamente un formulario de inicio de sesión para iniciar sesión en el servicio.

Por último, un tercer servidor web 122 está configurado para proporcionar navegación de forma segura por páginas web específicas, es decir, a través del servidor intermediario 101, mientras que otras páginas web pueden visitarse directamente. Esto se puede corresponder, por ejemplo, con el servidor web de un sitio web de un banco en el que una primera parte de la página web es de carácter informativo, es decir, que se dedica a los servicios de publicidad ofrecidos por el banco, mientras que una segunda parte es una red para los clientes, donde es posible realizar transacciones bancarias; la primera parte se puede mostrar directamente al usuario porque no se va a introducir o mostrar información sensible, y la segunda parte sólo se puede acceder a través del servidor intermediario 101. En este sentido, el servidor web puede estar configurado para solicitar el uso del servidor intermediario 101 para acceder a páginas web específicas.

La figura 2 muestra una representación de los diferentes terminales de usuario que pueden usarse para visitar las páginas web de servidores web 220-221 y que se conectan al servidor intermediario 201 a través de diferentes redes. El servidor intermediario 201 está dentro de la misma red de área local 230 que el servidor web 220, y pertenece a una empresa.

Un empleado de la empresa quiere leer su correo electrónico desde una aplicación de correo web en el servidor web 220, sin embargo el empleado está en casa y está usando su ordenador personal 210 conectado a Internet 200. El navegador web en el PC 210 recupera una página web de acceso desde el servidor intermediario 201, a través de Internet 200, lo que le permite navegar al servicio de correo web desde el servidor web 220 de una manera segura.

Un segundo empleado en la oficina tiene la intención de revisar su correo a través de la aplicación de correo web,

por lo que su PC 240 establece una conexión con el servidor intermediario 201 a través de la red de área local 230 de la oficina. Aunque el PC 240 está gestionado por un administrador de servicios informáticos y está, en principio, sin virus y software maligno, puede haber sido infectado de todos modos, así que acceder a su cuenta de correo electrónico por medio del servidor intermediario 201 protege de que sus mensajes de correo electrónico se manipulen y almacenen en forma de texto.

Del mismo modo, un tercer empleado necesita navegar por una página web en un servidor web remoto 221. El empleado no es consciente de que el servidor web 221 está infectado y que cualquier software maligno que se descargue en su PC 241 de la oficina se puede propagar a través de la red de área local 230, infectando de esta manera a otros ordenadores dentro de la misma red de área local 230. El PC 241 se ha configurado para navegar por páginas web de cualquier servidor web, incluyendo el servidor web 221, a través del servidor intermediario 201. Así, el navegador web en el PC 230 descarga una página web de acceso desde el servidor intermediario 201 a través de LAN 230, y el servidor intermediario 201 descarga la página web original del servidor web 221 a través de Internet 200. El servidor intermediario 201 produce imágenes de las páginas web representadas que luego pueden recuperarse por la página web de acceso en el PC 230.

La Figura 3 es una representación, en forma de diagrama de bloques, de un servidor intermediario 301 de acuerdo con una realización de la invención.

El servidor intermediario 301 tiene conectividad a Internet e incluye un sistema operativo 302 configurado para ejecutar una o más instancias 304-305 de un motor de navegación web que puede representar páginas web de servicios basados en la red que pueden recuperarse, por ejemplo a través de Internet, con el fin de servir versiones seguras de páginas web a terminales de cliente. El sistema operativo 302 incluye un gestor de navegación segura 303 que es un software que se ejecuta como un servicio en el sistema operativo 302. El gestor 303 actúa como un servidor web y, por lo tanto, escucha un puerto asociado a las peticiones HTTP (normalmente en los puertos 80 y 443, pero puede estar configurado para otros números de puerto) para las peticiones entrantes. A la llegada de una solicitud, el administrador de la navegación segura 303 puede iniciar (es decir, lanzar) una nueva instancia del motor de navegación web 304-305 que se ejecuta por el sistema operativo 302, transmitir una página web de acceso para la navegación segura al terminal del cliente asociado con la instancia, gestionar las comunicaciones entre el terminal del cliente (por ejemplo, transmitir imágenes de las páginas web representadas, recibir la entrada del usuario, transmitir y recibir archivos que se descargan o cargan, etc.) y su instancia, ajustar la compresión, la calidad, y/o el formato del archivo de imagen de las imágenes producidas, etc. El gestor de navegación segura 302 también puede ajustar la forma en que el servidor intermediario sirve las actualizaciones al terminal del cliente basándose en la información recopilada durante la sesión de usuario, es decir, el gestor 302 pueden evaluar la latencia y/o ancho de banda en las comunicaciones con el terminal del cliente y modificar parámetros como la calidad de las imágenes, la tasa de actualización, etc., que pueden mejorar la experiencia del usuario. Por lo tanto, el administrador de navegación segura 303 puede gestionar y controlar todas las instancias existentes 304-305 del motor de navegación web e iniciar otras nuevas.

Cada instancia 304-305 está aislada de las otras de manera que cualquier ataque malicioso que afecte a una instancia particular está confinado en esa instancia. Con este fin, el sistema operativo 302 incluye un gestor de filtrado de procesos 306 en el núcleo, que controla el proceso que se ejecuta en el sistema operativo 302, y también monitoriza cualquier proceso que se intente lanzar. El gestor de filtrado de procesos 306 detecta la ejecución de cualquier nueva aplicación y comprueba si tiene permiso para hacerlo, es decir, comprueba si está en la lista blanca y lo permite o bloquea. En algunos casos, una aplicación puede estar en la lista blanca cuando se cumplen ciertas condiciones, por ejemplo, la ejecución está condicionada a si la instrucción de lanzar el proceso se originó en un proceso diferente del motor de navegación web, o si el directorio donde se almacena el archivo ejecutable es o no es una carpeta temporal. Además, el gestor de la navegación segura 302 está configurado para crear un directorio temporal al inicio de cada instancia 304-305 del motor de navegación web con el fin de aislar aún más las instancias: cada instancia sólo podrá acceder a su directorio temporal respectivo y, en algunos casos, otros directorios particulares. Una instancia puede, por ejemplo, almacenar archivos descargados desde los servidores web, archivos de caché, o archivos transmitidos desde la máquina cliente al servidor intermediario 301.

Algunas instancias 304 pueden estar especializadas a la navegación de una página web a la vez para mejorar el aislamiento entre sesiones o usuarios concurrentes, mientras que algunas otras instancias 305 pueden navegar por varias páginas web a la vez (en una misma sesión por un mismo usuario) con el fin de compartir contenidos tales como cookies o información de la sesión.

La figura 4 muestra una página web de acceso 401 de acuerdo con una realización de la invención.

La página web de acceso 401 se genera por un servidor intermediario, como el representado en la figura 3, y se transmite a un terminal de usuario de modo que, una vez que se carga en el navegador web del usuario, el usuario puede tener acceso a versiones seguras de páginas web.

En particular, la página web de acceso 401 incluye un código JavaScript 402 que está configurado para realizar las siguientes tareas: comunicarse con el servidor intermediario 403; recuperar las imágenes que el servidor

intermediario pudiera haber generado y mostrarlas en el navegador web del usuario 404; y registrar cualquier pulsación de teclado y/o interacciones/eventos del ratón del usuario 405 y la transmisión de esta entrada del usuario al servidor intermediario.

En lo que respecta a la comunicación con el servidor intermediario 403, la página web de acceso 401 puede establecer una nueva comunicación o volver a utilizar una ya establecida con el servidor intermediario, por ejemplo, la establecida durante la transmisión de datos inicial, para solicitar el acceso seguro a una página web o para descargar la página web de acceso o establecer una nueva. Dicha comunicación puede no ser un enlace de conexión físico dedicado o similar, puede, por ejemplo, basarse en datagramas, y en algunas realizaciones también puede utilizar el protocolo HTTPS que cifra los datos intercambiados.

Entre las imágenes que la página web de acceso 401 puede recuperar 404 del servidor intermediario, las imágenes correspondientes a las partes cambiantes de la página web representada en la instancia del servidor intermediario también pueden descargarse en el navegador web del cliente. Con este fin, el código JavaScript 402 puede estar configurado para reemplazar partes de una imagen ya mostrada en el navegador web del cliente con imágenes de partes cambiantes: el usuario será capaz de ver la página web como se muestra actualmente en el servidor intermediario sin la necesidad de descargar una imagen completa de la página web representada, mejorando así el uso del ancho de banda y la capacidad de respuesta de la página web de acceso 401.

En algunas implementaciones, el código JavaScript 402 no está incrustado en la página web de acceso 401, sino que se recupera desde un sitio separado del servidor intermediario y se ejecuta por la página web de acceso 401.

La Figura 5A es un diagrama que muestra la evolución de las conexiones entre el navegador web 501 de una máquina cliente, un servidor intermediario 502 que comprende un motor de navegación web y un servidor web 503. En particular, el navegador web 501 puede comunicarse con el servidor intermediario 502 a través de una primera red 505, y el servidor intermediario 502 puede comunicarse con el servidor web 503 a través de una segunda red 506.

El cliente carga una URL en la barra de direcciones del navegador web 501 que pertenece al servidor web 503, por lo que primero intenta conectarse 511 al servidor web usando el protocolo HTTP o HTTPS. El servidor web 503 está configurado para utilizar el servidor intermediario 502 para asegurar el acceso al servidor web, de modo que transmite una petición 512 al servidor intermediario 502 y redirige la conexión de usuario. El servidor intermediario 502, a su vez, transmite una página web de acceso 513 al navegador web del cliente 501 y crea 514 una instancia 504 del motor de navegación web. La instancia 504 establece una conexión 515 con el servidor web 503 y descarga 516 los archivos de la página web. A continuación, la instancia 504 representa los archivos y produce una imagen de la página web 517 que se recupera 518 por la página web de acceso cargada en el navegador web 501 del cliente.

De un modo similar, la Figura 5B muestra otro diagrama en el que el usuario carga un URL en el navegador web que corresponde a una página web navegada a través del servidor intermediario 502, es decir, el URL identifica la página web que se va a visitar a través del servidor intermediario 502. Por lo tanto, la máquina cliente está solicitando el acceso seguro a la página web. El navegador web 501 se conecta directamente 521 con el servidor intermediario 502 que envía una página web de acceso 522 al cliente e inicia 523 una nueva instancia 504 del motor de navegación web. La instancia 523 se conecta a continuación 524 al servidor web 503 con el fin de descargar 525 los archivos de la página web. Finalmente, la imagen de la página web representada se genera 526, y dicha imagen se obtiene 527 a través de la página web de acceso, por lo que el cliente puede navegar de forma segura la página web solicitada.

En este texto, el término "comprende" y sus derivaciones (tales como "que comprende", etc.) no deben entenderse en un sentido excluyente, es decir, estos términos no deben interpretarse como excluyentes de la posibilidad de que lo que se describe y define pueda incluir más elementos, etapas, etc.

La invención, obviamente, no se limita a las realizaciones específicas que se describen en el presente documento, sino que también incluye cualquier variación que pueda considerarse por cualquier experto en la materia (por ejemplo, en cuanto a la elección de materiales, dimensiones, componentes, configuración, etc.), dentro del alcance general de la invención tal como se define en las reivindicaciones.

REIVINDICACIONES

1. Un servidor intermediario (101, 201, 301, 502) para proporcionar un acceso seguro a una página web de un servicio basado en la red para un terminal de cliente (110, 111, 210, 240, 241) a petición de uno de un servidor web (120-122, 220, 221, 503) y un terminal de cliente (110, 111, 210, 240, 241) que comprende un navegador web (501), comprendiendo el servidor intermediario (101, 201, 301, 502):

un sistema operativo (302) configurado para ejecutar una instancia (304, 305, 504) de un motor de navegación web (303);
el motor de navegación web (303) está configurado para producir una imagen de la página web representada en la instancia (304, 305, 504) del motor de navegación web (303), y para transmitir una página web de acceso (401) al navegador web (501) del terminal de cliente (110, 111, 210, 240, 241); y
la página web de acceso (401) está configurada para obtener (404) la imagen del motor de navegación web (303), y para mostrar (404) la imagen en el navegador web (501).

2. El servidor intermediario (101, 201, 301, 502) de la reivindicación 1, en el que la página web de acceso (401) comprende código JavaScript (402) o código HTML configurado para cargar código JavaScript (402) recuperable desde el servidor intermediario (101, 201, 301, 502).

3. El servidor intermediario (101, 201, 301, 502) de cualquiera de las reivindicaciones anteriores, en el que el sistema operativo (302) está configurado además para ejecutar una nueva instancia (304, 305, 504) del motor de navegación web (303) por cada solicitud para proporcionar un acceso seguro a una página web de un servicio basado en la red.

4. El servidor intermediario (101, 201, 301, 502) de cualquiera de las reivindicaciones anteriores, en el que el motor de navegación web (303) está configurado además para detectar partes cambiantes de la página web en la instancia (304-305), y para producir imágenes de las partes cambiantes.

5. El servidor intermediario (101, 201, 301, 502) de la reivindicación 4, en el que la página web de acceso (401), además, está configurada para recuperar (404) las imágenes de las partes cambiantes del motor de navegación web (303) y para sustituir partes de la imagen mostrada en el navegador web (501) con las imágenes de las partes cambiantes.

6. El servidor intermediario (101, 201, 301, 502) de cualquiera de las reivindicaciones anteriores, en el que:

el motor de navegación web (303) está configurado para comunicarse con el navegador web (501) usando el protocolo HTTPS.

7. El servidor intermediario (101, 201, 301, 502) de cualquiera de las reivindicaciones anteriores, en el que:

el motor de navegación web (303) está además configurado para crear al menos un directorio temporal en el sistema operativo (302) para cada una de las instancias (304, 305, 504) y cualquier nueva instancia (304, 305, 504) del motor de navegación web (303), y para permitir el acceso a la instancia (304, 305) y cualquier nueva instancia (304, 305) a su respectivo al menos un directorio temporal del sistema operativo (302).

8. Un método para proporcionar un acceso seguro a una página web de un servicio basado en la red a un terminal de cliente (110, 111, 210, 240, 241) que comprende un navegador web (501), comprendiendo el método:

recibir (512, 521) una solicitud para proporcionar, al terminal de cliente (110, 111, 210, 240, 241), acceso seguro a la página web; y
caracterizado por

ejecutar (514, 523) una instancia (304, 305, 504) de un motor de navegación web (303);
producir (517, 526) una imagen de la página web mediante representación en la instancia (304, 305, 504) del motor de navegación web (303); y
transmitir (513, 522) una página web de acceso (401) al navegador web (501), estando la página web de acceso (401) configurada para recuperar (404) una imagen del motor de navegación web (303), y para mostrar (404) la imagen en el navegador web (501).

9. El método de la reivindicación 8, en el que la solicitud (512) para proporcionar un acceso seguro es una solicitud desde un servidor web (120-122, 220, 221, 503).

10. El método de la reivindicación 8, en el que la solicitud (521) para proporcionar un acceso seguro es una petición del terminal de cliente (110, 111, 210, 240, 241).

11. El método de cualquiera de las reivindicaciones 8-10, en el que la página web de acceso (401) comprende

código JavaScript (402) o código HTML configurado para cargar código JavaScript (402) recuperable de un servidor.

12. El método de cualquiera de las reivindicaciones 8-11, que comprende adicionalmente:

recibir pulsaciones de teclado e interacciones detectables de ratón (405) por la página web de acceso (401); sanear las pulsaciones de teclado; e
introducir las pulsaciones de teclado saneadas y las interacciones con el ratón en la instancia (304, 305, 504) del motor de navegación web (303).

13. El método de cualquiera de las reivindicaciones 8-12, en donde el método además comprende:

detectar partes cambiantes de la página web en la instancia (304, 305, 504) del motor de navegación web (303); y
producir imágenes de las partes cambiantes; y
en donde la página web de acceso (401) está configurada, además, para recuperar (404) las imágenes de las partes cambiantes del motor de navegación web (303), y para sustituir las partes de las imágenes mostradas en el navegador web (501) con las imágenes de las partes cambiantes.

14. Un programa informático que comprende un medio de código de programa informático adaptado para realizar las etapas del método de acuerdo con cualquiera de las reivindicaciones 8-13 cuando dicho programa se ejecuta en un ordenador, un procesador de señal digital, un campo de matrices de puertas programables, un circuito integrado específico de la aplicación, un micro-procesador, un microcontrolador, o cualquier otra forma de hardware programable.

15. Una memoria o un medio legible por un ordenador que almacena instrucciones de programa o código para realizar el método de acuerdo con cualquiera de las reivindicaciones 8-13.

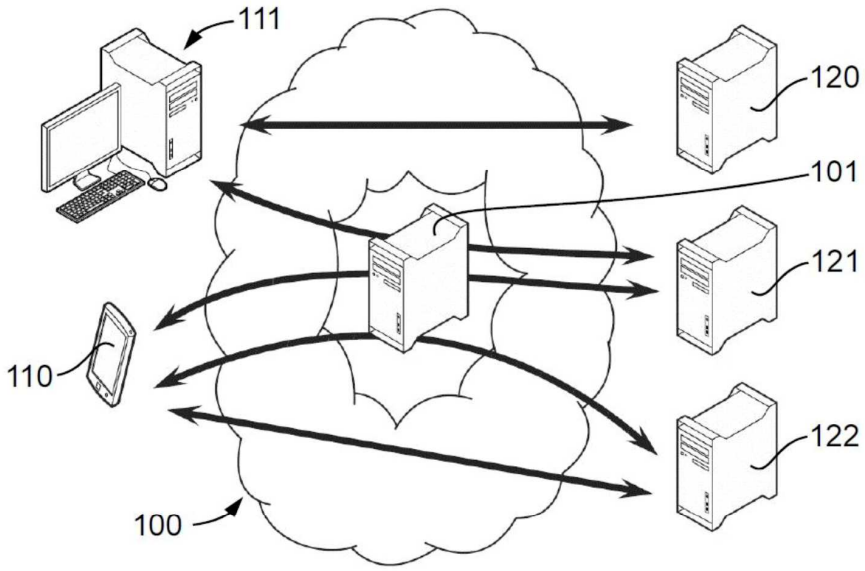

FIG. 1

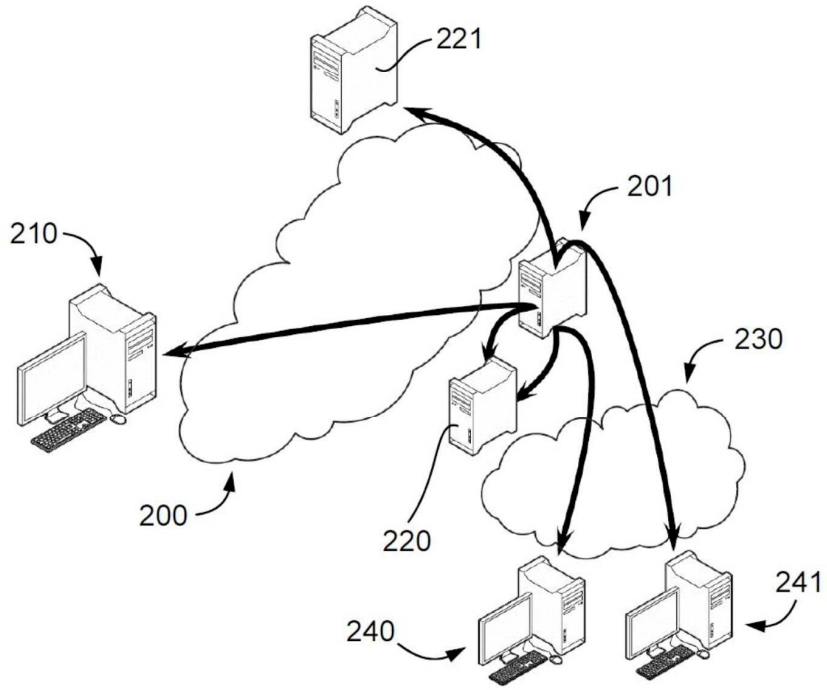

FIG. 2

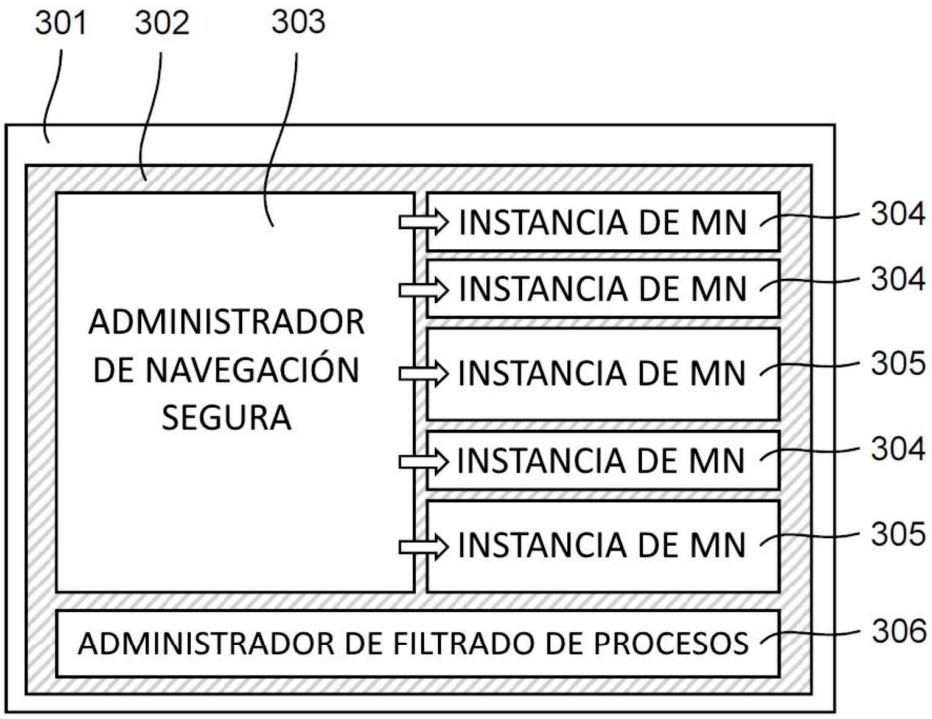
301
302
303
ADMINISTRADOR DE NAVEGACIÓN SEGURA
INSTANCIA DE MN
INSTANCIA DE MN
INSTANCIA DE MN
INSTANCIA DE MN
INSTANCIA DE MN
304
304
305
304
305
ADMINISTRADOR DE FILTRADO DE PROCESOS
306

FIG. 3

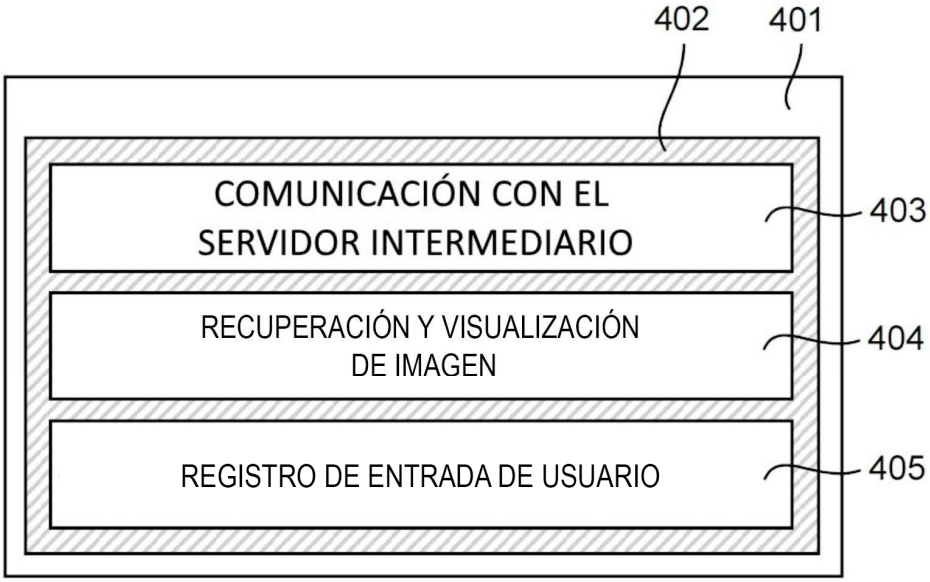
402
401
COMUNICACIÓN CON EL SERVIDOR INTERMEDIARIO
403
RECUPERACIÓN Y VISUALIZACIÓN DE IMAGEN
404
REGISTRO DE ENTRADA DE USUARIO
405

FIG. 4

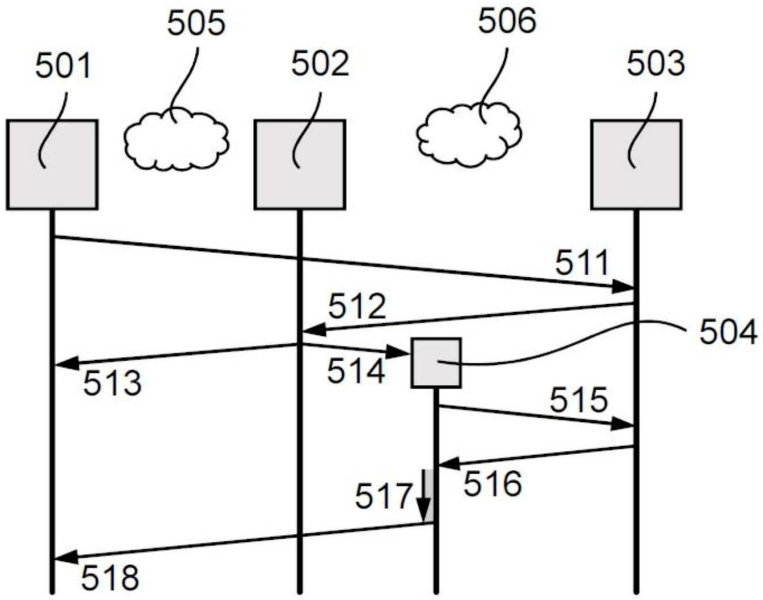
505
506
501
502
503
511
512
504
513
514
515
517
516
518

FIG. 5A

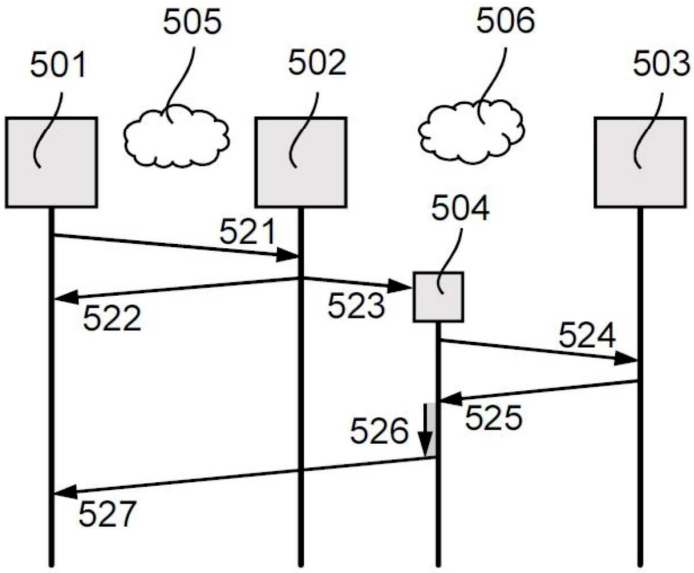
505
506
501
502
503
504
521
522
523
524
526
525
527

FIG. 5B