(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 364 658**

(51) Int. Cl.:
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00984329 .3**
(96) Fecha de presentación : **14.12.2000**
(97) Número de publicación de la solicitud: **1254432**
(97) Fecha de publicación de la solicitud: **06.11.2002**

(54) Título: **Pasarela segura que tiene identificación de usuario y autentificación por contraseña.**

(30) Prioridad: **14.12.1999 US 170686 P**
23.12.1999 US 471901

(45) Fecha de publicación de la mención BOPI:
08.09.2011

(45) Fecha de la publicación del folleto de la patente:
08.09.2011

(73) Titular/es: **VERIZON PATENT AND LICENSING Inc.**
One Verizon Way
Basking Ridge, New Jersey 07920, US

(72) Inventor/es: **Grantges, David, R., Jr.**

(74) Agente: **Miltenyi Null, Peter**

DESCRIPCION

Pasarela segura que tiene identificación de usuario y autentificación por contraseña.

CAMPO DE LA TÉCNICA

La presente invención se refiere en general a sistemas y redes de comunicaciones, y, más concretamente, a una pasarela segura para facilitar el acceso desde un equipo cliente a través de una red pública no segura a uno de una pluralidad de servidores de destino en una red privada segura.

ANTECEDENTES DE LA INVENCIÓN

Son conocidas redes de computadoras que en general incluyen una gran variedad de dispositivos de computación, tales como equipos clientes y servidores, interconectados mediante varios medios de conexión. En particular, es normal para una institución, tal como una empresa, proporcionar este tipo de red. Dicha red puede incluir una multiplicidad de servidores que ejecutan un número correspondiente de programas de aplicación ("aplicaciones"). Los empleados de la empresa pueden usar una o más de estas aplicaciones para llevar a cabo el negocio de la empresa. Una red como ésta puede estar caracterizada como una red segura, privada, puesto que es accesible bajo condiciones de funcionamiento esperado normal sólo por parte de personas debidamente autorizadas.

Cada vez se ha convertido en más popular, y en muchos casos una necesidad del negocio, que los usuarios ("clientes") accedan remotamente a la red privada. Mientras que el acceso remoto en algunos casos se consigue a través de líneas seguras dedicadas, cada vez se realiza más a través de la red global de comunicaciones conocida como Internet. Las redes de computadoras, en particular Internet, pueden ser vulnerables a violaciones de seguridad. En particular, Internet se considera de manera general como no segura, teniendo en cuenta su acceso generalizado y el uso por parte del público en general. Por consiguiente, un problema que se plantea es cómo permitir el acceso de los clientes de forma segura a los recursos disponibles en la red segura privada (por ejemplo, las aplicaciones) a través de una red pública generalmente no segura, tal como Internet.

Un primer enfoque general conocido en el estado de la técnica se basa en emplear varios esquemas de cifrado. Por ejemplo, un protocolo conocido como protocolo de Capa de Conexión Segura (SSL) protege la información transmitida a través de Internet no seguro utilizando cifrado. Otro esquema de autentificación conocido supone el uso de un llamado certificado digital, que también utiliza cifrado. Tal como se utiliza, el certificado digital puede adjuntarse a un mensaje electrónico para verificar al receptor que el emisor es quien dice ser. Un conocido y ampliamente aceptado estándar para certificados digitales es ITU X.509.

Mientras las técnicas descritas anteriormente son efectivas para lo que se pretende llevar a cabo, el facilitar acceso a una red segura privada a través de una red no segura tal como Internet requiere de una combinación completa de muchas funciones de seguridad. Por consiguiente, es conocido en el estado de la técnica facilitar de manera segura el acceso remoto mediante una arquitectura de pasarela (en inglés, *gateway architecture*). Una arquitectura de pasarela conocida incluye un cortafuegos (en inglés, *firewall*), un servidor web, un colector de información (en inglés, *information collector* - IC), un enrutador de mensajes de aplicación (en inglés, *application message router* - AMR), y un controlador de autorizaciones.

El cortafuegos se dispone entre la red segura privada y la red no segura pública. El servidor web y el colector de información están en el lado del cortafuegos de la red pública no segura. El servidor web se comunica con el colector de información utilizando la interfaz de Entrada Común conocida (CGI), la especificación para transferir información entre un servidor web y un programa CGI. El AMR y el controlador de autorizaciones están en el lado del cortafuegos de la red segura privada. El IC y el AMR se comunican a través del cortafuegos mediante un mecanismo de comunicación de interproceso (IPC). En esta arquitectura de pasarela de comunicación conocida, un usuario que desea tener acceso a una aplicación en la red privada primero accede al servidor web utilizando un navegador web convencional. El usuario se autentifica proporcionando un certificado digital.

El servidor web envía los datos del certificado digital al IC de acuerdo con un script CGI. El colector de información, a su vez, envía el certificado digital a través del cortafuegos al AMR vía el mecanismo IPC. El AMR, también vía un mecanismo IPC, consulta al controlador de autorizaciones para autentificar al usuario. La respuesta del controlador de autorizaciones se devuelve al AMR. Si el usuario es autentificado con éxito, se permite el acceso. Sin embargo, existen diferentes deficiencias en este enfoque.

Primero, el colector de información y el enrutador de mensajes de aplicación son aplicaciones de software programadas personalizadas. Por consiguiente, deben ser portadas para cada nueva plataforma utilizada. Esta dependencia de la plataforma supone un incremento de costes (y retardos) cuando se implementa en nuevas plataformas.

Segundo, la pasarela conocida tiene limitaciones de rendimiento. La interfaz CGI es relativamente lenta, como lo es el link IC-a-AMR porque, entre otras cosas, el mecanismo IPC es de un único hilo.

Tercero, ciertos datos (por ejemplo, HTML estático, gráficos, etc.) son más vulnerables a violaciones de seguridad (es decir, a ser pirateados) porque se mantiene en el servidor web, en el lado de Internet (no segura) del cortafuegos de la red privada. Esta situación no es deseable.

Otra pasarela conocida para facilitar el acceso a una red privada a través de una red no segura requiere de un mecanismo de autentificación de certificado digital del lado cliente de dos niveles. Se proporciona un servidor Proxy para cada aplicación en la red privada, el cual se dispone en el lado de Internet del cortafuegos. Uno de los servidores proxy realiza una verificación de primer nivel del certificado digital, y entonces envía los datos del certificado digital a través del cortafuegos, vía HTTPS, para la verificación de segundo nivel por parte de un servidor de autorización. Mientras esta configuración soluciona alguna de las deficiencias descritas anteriormente, el enrutado en este enfoque es relativamente ineficiente para múltiples aplicaciones (es decir, requiere múltiples servidores proxy).

Además, algunas aplicaciones de la red privada no requieren una autentificación fuerte del certificado digital. En estas situaciones para arquitecturas de pasarela conocidas no hay autentificación del usuario fuera del cortafuegos (es decir, las pasarelas descritas anteriormente autentifican, al menos en algún nivel, antes de permitir además el acceso a través del cortafuegos para la autentificación completa).

Por lo tanto, existe una necesidad de proporcionar una pasarela mejorada que minimice o elimine uno o más de las deficiencias según lo dispuesto anteriormente.

WO 99/53391 describe un sistema que facilita el acceso a recursos en una red de confianza. Cuando un usuario pretende acceder a una red de confianza, se envía una solicitud de acceso desde un navegador cliente, a través de Internet y una red DMZ, al hospedaje web (en inglés, *web host*). Posteriormente, el hospedaje web solicita información de autentificación del usuario por parte del usuario y, después de recibir la información de autentificación, solicita la autentificación de la información recibida desde un servidor de autentificación.

SUMARIO

El objeto de la invención es solucionado mediante la materia de las reivindicaciones independientes. Realizaciones preferidas son materia de las reivindicaciones dependientes.

Una ventaja del sistema informático de acuerdo con la presente invención es que autentifica a un usuario de un equipo cliente remoto en el que el uso de certificados digitales no es deseable o simplemente no está disponible. Otra ventaja es que la autentificación, que preferiblemente implica el uso de un identificador de usuario (ID) y una contraseña, se realiza en el lado no seguro de un sistema cortafuegos que separa la red segura privada y la red pública no segura (es decir, Internet). La autentificación debe realizarse con éxito antes de permitir el acceso a la red privada. Además, la arquitectura de un sistema informático de acuerdo con la invención mantiene datos sensibles de autentificación en un servidor de autorización, el cual está en el lado del cortafuegos de la red privada segura, que reduce la probabilidad de una intrusión “pirata” con éxito.

Se proporciona un sistema informático de acuerdo con la presente invención que permite el acceso desde un equipo cliente a través de una red privada no segura. El sistema informático incluye un sistema cortafuegos, un servidor proxy, un servidor de autentificación, un servidor web y una pasarela. El sistema cortafuegos se dispone entre la red pública no segura (es decir, Internet) y la red privada segura. El servidor proxy y el servidor web están en el lado de la red no segura del sistema cortafuegos y la pasarela y el servidor de autorización están en el lado de la red segura privada del sistema cortafuegos.

El servidor de autentificación está configurado para autentificar al usuario del equipo cliente en base a un identificador de usuario (ID) y a una contraseña del usuario del equipo cliente. El servidor web está configurado para enviar el ID del usuario y la contraseña a través del cortafuegos al servidor de autorización. El servidor web está además configurado para generar una cookie de autentificación que tiene una condición válida cuando el servidor de autorización autentifica al usuario del equipo cliente en base a su ID de usuario y su contraseña.

De acuerdo con la presente invención, el servidor proxy está además configurado para enviar un mensaje desde el equipo cliente al servidor de destino, vía la pasarela, cuando la cookie de autentificación es válida.

Otros objetivos, características y ventajas de la presente invención serán puestas de manifiesto para un experto en la materia a partir de la siguiente descripción detallada y de los dibujos adjuntos que muestran características de esta invención a modo de ejemplo, pero no a modo de limitación.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La presente invención será ahora descrita a modo de ejemplo, con referencia a las figuras adjuntas, en las que:

La Figura 1 es una vista de un diagrama de bloques simplificado de un primer sistema informático de acuerdo con la presente invención;

La Figura 2 es un diagrama de bloques simplificado del sistema de la Figura 1, que muestra las comunicaciones en mayor detalle;

La Figura 3 es un diagrama de bloques más detallado de un mensaje que se pasa entre el servidor proxy y la pasarela de la Figura 1;

La Figura 4A es un diagrama de bloques más detallado de cookies creadas por el sistema de la presente invención;

La Figura 4B es un diagrama de bloques más detallado de un mecanismo para enrutar mensajes a una de las múltiples aplicaciones;

La Figura 5 es un diagrama de flujos simplificado que muestra el funcionamiento de un servidor proxy de pasarela de la Figura 1;

La Figura 6 es un diagrama de bloques que muestra las etapas de obtener un certificado digital para usar con el sistema de la Figura 1;

La Figura 7 es un diagrama de bloques simplificado de un segundo sistema informático de acuerdo con la presente invención; y,

La Figura 8 es un diagrama de flujos simplificado que muestra el funcionamiento del segundo sistema de la Figura 7.

DESCRIPCIÓN DETALLADA

A continuación, con referencia a los dibujos en los que se utilizan las mismas referencias numéricas para identificar componentes idénticos en las diferentes vistas, la Figura 1 es un diagrama de bloques simplificado de un sistema informático útil para autentificar a un usuario 18, es decir, un sistema informático 20, en una primera realización de la presente invención. En la primera realización mostrada, la autentificación de un usuario 18 se realiza mediante el uso de certificados digitales, tales como certificados digitales ITU X.509. Debería entenderse que dichos certificados digitales pueden transferirse a otros equipos clientes. Es el usuario 18 el que está siendo autentificado, no el equipo cliente 22.

Normalmente, el sistema informático 20 está configurado para facilitar el acceso a un usuario 18 de un equipo cliente 22 a una de una pluralidad de aplicaciones de software 24_1, 24_2, …, 24_3. El citado acceso se realiza a través de una red no segura 26, tal como Internet, que se utiliza públicamente, a una red segura privada en la que residen las aplicaciones 24_1, 24_2, …, 24_3. Cada aplicación 24_1, 24_2, …, 24_3 incluye un servidor web respectivo (de aquí en adelante “servidor de destino”) 28_1, 28_2, …, 28_3 y un programa de aplicación 30_1, 30_2, …, 30_3. El sistema informático 20 incluye un sistema cortafuegos 32, un servidor proxy 34 con un plug-in 36, una pasarela de aplicación 38 (en inglés, *application gateway*) que comprende un servidor proxy de pasarela 40 con un plug-in 42 y un servidor web de pasarela 44, y un servidor de autorización 46. Como se muestra también en la Figura 1, hay un bloque 48 de Seguridad de Información, una autoridad de certificación 50, una primera conexión segura 52, una segunda conexión segura 54, y una tercera conexión segura 56.

El sistema informático 20 supera muchas de las deficiencias de sistemas de pasarela conocidos, proporcionando una implementación independiente de plataforma vía el uso de componentes de fácil adquisición (COTS) (en inglés, *comercial-of-the-shelf components*), así como rendimiento mejorado mediante el uso de un protocolo seguro de transferencia de hipertexto basado en SSL (HTTPS) para la mensajería segura y rápida a través del cortafuegos. Además, los datos sensibles se mantienen en el lado del cortafuegos 32 de la red privada segura, no en el lado del cortafuegos de la red pública no segura, reduciendo la oportunidad de los piratas de violar la seguridad.

Antes de proceder a realizar una descripción detallada del sistema informático 20, se establecerá una visión general del funcionamiento establecido por la invención, tal como lo vería un usuario 18 de un equipo cliente 22. Inicialmente, el usuario 18 del equipo cliente 22 introduce la URL de destino en una parte del navegador web del equipo cliente 22. Entonces, el navegador web emite una solicitud HTTP a través de la red no segura 26, la cual se enruta al servidor proxy 34. Entonces, se le puede presentar al usuario 18 un mensaje “popup” conforme se va a establecer una conexión a una red segura. El mensaje también puede preguntar al usuario 18 qué certificado digital X.509 desea usar para la autentificación. El certificado digital X.509 del usuario seleccionado es entonces enviado al servidor proxy 34. En este punto, se lleva a cabo una autentificación de primer nivel, fuera del cortafuegos, por parte del servidor proxy 34 (por ejemplo, verifica si el certificado X.509 ha sido emitido por una autoridad de certificación pre-aprobada predeterminada). Si se ha autentificado en este nivel, entonces el servidor proxy 34 envía la información contenida en el certificado digital del cliente, a través del sistema cortafuegos 32, a la pasarela 38, para ser autentificada en un segundo nivel más sustantivo. La autentificación de segundo nivel supone examinar los datos del certificado digital X.509 utilizando los datos almacenados en el servidor de autorización 46. Si el usuario 18 está autorizado a acceder a múltiples aplicaciones, el siguiente ítem después del mensaje “popup” a mostrar al usuario 18 es una “página de opciones”, que presenta las múltiples selecciones. Una vez se ha seleccionado una aplicación particular, el siguiente ítem a mostrar al usuario 18 es una página de bienvenida de la aplicación seleccionada. El acceso remoto autentificado seguro se completa. De acuerdo con la presente invención, el sistema informático 20 proporciona un mecanismo eficiente para

enrutar el usuario remoto 18 del equipo cliente 22 a la aplicación seleccionada que está siendo servida por uno de los servidores de destino.

Con referencia continua a la Figura 1, el equipo cliente 22 puede ser cualquiera de una pluralidad de dispositivos de computación convencionales, tal como, sólo a modo de ejemplo, un computador personal (PC) sobre el que se ejecuta un sistema operativo Microsoft Windows (por ejemplo, Windows 95, Windows NT, Windows 2000), un computador Macintosh (computador Apple) o una estación de trabajo UNIX. Preferiblemente, el equipo cliente 22 está configurado para incluir un navegador web, tal como, por ejemplo, Netscape Communicator Versión 4.7, disponible comercialmente por parte de Netscape Communications Corporation. Parte del navegador web del equipo cliente 22 incluye preferiblemente las capacidades de transmitir, recibir, y verificar certificados digitales, tales como, certificados digitales de autentificación ITU X.509. Además, parte del navegador web preferiblemente incluye la capacidad de establecer una primera conexión segura 52 con el servidor proxy 34 vía, por ejemplo, el protocolo de Capa de Conexión Segura (SSL) a disposición del público, Versión 3.0, disponible en Netscape Communications Corp. Como se muestra en la Figura 1, la primera conexión segura 52 está referenciada como una conexión “HTTPS”, que indica el uso del protocolo SSL. Por supuesto, pueden usarse otros mecanismos para establecer una conexión segura, tal como el protocolo S-HTTP; sin embargo, es necesario que ambos extremos sean compatibles con dicho otro protocolo. La conexión 52 puede basarse en un protocolo de conexión de red TCP/IP.

Existen aplicaciones 24_1, 24_2, …, 24_3, en particular programas 30_1, 30_2, …, 30_3 de las mismas, independientemente del sistema informático 20. Es decir, no son necesarias modificaciones de los programas 30_1, 30_2, …, 30_3 para utilizarlos en el sistema informático 20. Por ejemplo, las aplicaciones 24_1, 24_2, …, 24_3 pueden requerir Servicios de Subscripción facturados en base al acceso de la portadora (en inglés, *Carrier Access Billing, Subscription Services*) (por ejemplo, portadoras de larga distancia) y similares. Preferiblemente, los servidores de destino 28_1, 28_2, …, 28_3 son compatibles con el Protocolo de Transferencia de HiperTexto (HTTP 1.1) ubicuo, el cual se utiliza en las conexiones 58, 60 y 62. Los servidores de destino 28_1, 28_2, …, 28_3 interconectan el sistema informático 20 con los programas respectivos 30_1, 30_2, …, 30_3. En efecto, el usuario remoto 18 proporciona el navegador web, y la aplicación que ha obtenido acceso seguro indica el servidor de destino. El sistema informático 20 proporciona el resto de la conectividad y seguridad necesarias.

El sistema cortafuegos 32 está dispuesto entre la red pública no segura 26 y la red privada segura, en la que residen y ejecutan las aplicaciones 24_1, 24_2, …, 24_3. El sistema cortafuegos 32 puede implementarse en software, hardware, o ambos. El sistema cortafuegos 32 está configurado para examinar todos los mensajes destinados a, o que salen de, la red segura privada, y para bloquear aquellos que no cumplen los criterios de seguridad predeterminados. Un criterio implica la localización del destino en la red privada, para los mensajes entrantes. En este caso, el sistema cortafuegos 32 restringe la comunicación que se origina desde la red 26 no segura, permitiendo sólo el paso de mensajes destinados a la pasarela 38 de aplicaciones en la red privada (por ejemplo, el servidor proxy de pasarela 40). El sistema cortafuegos 32 puede comprender aparatos convencionales conocidos por expertos en la materia. Por ejemplo, el sistema cortafuegos 32 puede comprender aparatos disponibles comercialmente referenciados como cortafuegos CheckPoint One, de Check Point Software Technologies, Inc. Redwood City, California, USA.

El servidor proxy 34 está dispuesto en el lado del sistema cortafuegos 32 de la red pública no segura, en una zona conocida como desmilitarizada (DMZ). Se localiza una DMZ entre la red 26 no segura (por ejemplo, Internet) y la primera línea de defensa de la red privada, por ejemplo, el sistema cortafuegos 32. El servidor proxy DMZ 34 está dispuesto entre el equipo cliente 22 y los servidores reales asociados a las aplicaciones sustantivas, es decir, los servidores de destino 28_1, 28_2, …, 28_3. En general, los servidores proxy pueden caracterizarse para proporcionar tanto funciones de mapeo como de almacenamiento en caché de datos. En el contexto de la presente invención, el servidor proxy DMZ 34 se proporciona principalmente con fines de mapeo.

Además, el servidor 34 proxy DMZ está configurado para establecer una primer conexión 52 segura con el equipo cliente 22, particularmente la parte del navegador web del mismo. La conexión HTTPS 52 proporciona el cifrado de la información que pasa entre el equipo cliente 22 y el servidor 34 proxy DMZ. Debería entenderse que puede utilizarse otros protocolos de conexión segura adecuados, por ejemplo, HTTP seguro (S-HTTP); sin embargo, es necesario que ambos extremos sean compatibles con dicho otro protocolo.

Además, el servidor 34 proxy DMZ está también configurado para realizar un autentificación de primer nivel del usuario del equipo cliente 22. En una realización, el servidor 34 proxy DMZ está programado para examinar el certificado digital X.509 proporcionado por el equipo cliente 22, para determinar si fue expedido por una autoridad de certificación pre-aprobada, predeterminada. En esta realización, el servidor 34 proxy DMZ no compara los datos del certificado digital X.509 con información en el archivo para autentificación. Esto es debido a que la información requerida para gestionar dicha comparación se almacena de manera segura detrás del sistema 32 cortafuegos en el servidor 46 de autorización en la red privada. El servidor 34 proxy DMZ puede comprende hardware y software convencionales conocidos en el estado de la técnica. Por ejemplo, el servidor 34 proxy DMZ puede comprender software de servidor proxy de Netscape, disponible en el mercado en Netscape Communications Corporation.

El plug-in 36 está asociado con el servidor 34 proxy DMZ y está configurado para proporcionar funcionalidades mejoradas. Como se describirá con más detalle más adelante, en una realización preferida, el plug-in 36 está configurado para capturar los detalles particulares del certificado digital X.509, y enviar estos detalles a través del sistema 32 cortafuegos hacia el servidor 40 proxy de pasarela. Mediante esta funcionalidad, el usuario 18 del equipo cliente 22 puede autentificarse de manera segura en el lado del sistema 32 cortafuegos de la red privada.

La pasarela 38 de la aplicación está dispuesta en el lado del sistema 32 cortafuegos de la red privada, entre el servidor 34 proxy DMZ y las aplicaciones 24_1, 24_2, …, 24_3. La pasarela 38 incluye el servidor 40 proxy de pasarela y el servidor 44 web de pasarela. El servidor 40 proxy de pasarela está configurado para establecer una segunda conexión 54 segura a través del sistema 32 cortafuegos, con el servidor 34 proxy DMZ. En una realización, la conexión 54 segura comprende una conexión HTTPS, aunque podrían utilizarse otros protocolos seguros, tal como se describe más arriba; sin embargo, siempre que ambos extremos sean compatibles con dicho otro protocolo. Como respuesta a la solicitud del servidor 34 proxy DMZ para establecer la conexión 54 segura, el servidor 40 proxy de pasarela presenta su certificado digital X.509, y solicita que el servidor 34 proxy DMZ presente su certificado digital X.509 mediante un mensaje de respuesta. Este apretón de manos (en inglés, *handshaking*) es conocido ampliamente en el estado de la técnica, y no será elaborado en cualquier otro detalle. Sin embargo, se describe para enfatizar que el certificado digital X.509 que se presenta al servidor 40 proxy de pasarela pertenece al servidor 34 proxy DMZ, no al usuario 18 del equipo cliente 22. El software disponible en el mercado en el servidor 34 proxy DMZ no tiene capacidades integradas para realizar esta etapa de envío de información de acuerdo con la invención. Por consiguiente, tal como se ha descrito más arriba, el plug-in 36 se proporciona como parte de la solución de este problema. La otra parte de la solución, el plug-in 42 de autorización, está configurado, entre otras cosas, para extraer los datos embebidos en el mensaje del servidor 34 proxy DMZ, que se corresponden con los datos en el certificado del cliente. El plug-in 36 (captura y embebe) y el plug-in 42 (extrae y analiza) trabajan mano a mano para enviar la información del certificado digital del cliente a través del sistema 32 cortafuegos, para su autentificación.

El servidor 40 proxy de pasarela además realiza funciones de mapeo ampliamente conocidas, y, de acuerdo con la presente invención, enruta de manera eficiente mensajes destinados a varias aplicaciones 24_1, 24_2, …, 24_3 al servidor de destino adecuado de los servidores de destino 28_1, 28_2, …, 28_3. El servidor 40 proxy de pasarela puede comprender aparatos convencionales conocidos en el estado de la técnica, tal como, por ejemplo, software de servidor proxy de Netscape, que se ejecuta en hardware convencional.

Además, el servidor 40 proxy de pasarela está configurado para establecer una tercera conexión 56 segura dentro de la pasarela 38 con el servidor 44 web. La conexión 56 puede establecerse tal como se describe más arriba para la conexión 54 segura.

El servidor web 44 está configurado para almacenar varios ficheros HTML y gráficos, que serán servidor al equipo cliente 22. En particular, los ficheros HTML y de gráficos asociados con la administración de la autorización y de la autentificación del sistema informático 20 están residentes en el servidor 38 de pasarela de aplicaciones. Más concretamente, el servidor web 44 está configurado para proporcionar una “página de opciones” al equipo cliente 22 cuando el usuario es autentificado y autorizado para más de una de las aplicaciones 24_1, 24_2, …, 24_3. Será entendido que el uso de la palabra servidor “web” no debería estar limitado necesariamente a uno o más de los significados atribuidos en el estado de la técnica, sino más bien sólo mediante las reivindicaciones adjuntas. Es importante destacar que estos datos están almacenados en el lado del cortafuegos 32 de la red privada segura, lo que reduce la oportunidad para los piratas de violar la seguridad y acceder o destruir estos datos.

Preferiblemente, el servidor de autorización 46 está dispuesto en el lado del sistema cortafuegos 32 de la red privada. Esta disposición minimiza el riesgo de acceso no autorizado a o la destrucción de los datos sensibles mantenidos en el mismo, puesto que un aspirante a pirata tendría que penetrar el cortafuegos para que sucedan dichas actividades. En una realización, el servidor proxy de pasarela 40 y el servidor de autorización 46 se dirigen mensajes entre sí de acuerdo con un llamado protocolo ligero de acceso a directorios (LDAP). Por consiguiente, el servidor de autorización 46 comprende un servidor con capacidad de LDAP. La información mantenida por el servidor de autorización 46 incluye los datos del certificado digital X.509 ofrecido por el usuario 18 del equipo cliente 22, la identificación de las aplicaciones 24_1, 24_2, …, 24_3 a las que se ha autorizado el acceso al usuario 18 mediante un administrador de aplicaciones, y un identificador (ID) de usuario de pasarela.

La Seguridad de Información 48 es una entidad que, en una realización, actualiza el servidor de autorización 46 con datos obtenidos tanto de un administrador (en inglés, *trustee*) como de una autoridad de certificación 50. Este proceso será descrito en mayor detalle en combinación con la Figura 6. Se proporciona en el servidor de autorización 46 una interfaz administrativa (no mostrada), y permite a cualquier individuo clasificado como usuario “admin” ejecutar determinadas funciones. Estas funciones caen dentro de tres categorías principales: (i) administración de usuarios; (ii) administración de aplicaciones; y, (iii) informes. Por ejemplo, los usuarios “admin” pueden añadir o borrar usuarios, proporcionar actualización/mantenimiento de usuarios, proporcionar búsquedas de usuarios, añadir una aplicación, ocuparse del mantenimiento de aplicaciones, proporcionar informes de acceso de inicio de sesión, proporcionar informes de usuarios inactivos y/o caducados, y proporcionar informes de listas de usuarios. Lo anterior se describe sólo a modo de ejemplo. Normalmente, la administración de aplicaciones viene realizada por un grupo de soporte a la

administración de aplicaciones. Sin embargo, los administradores de aplicaciones son usuarios “admin” y pueden acceder así a esta interfaz.

La autoridad de certificación 50 recibe aplicaciones para certificados digitales X.509 de potenciales usuarios que solicitan acceso a aplicaciones en la red privada. La autoridad de certificación 50 expide un certificado digital X.509 cifrado que contiene la clave pública de usuario y una pluralidad de otra información. Se proporcionan los datos del certificado digital X.509 expedido, a un servidor de autorización 46, con fines de autentificación. En una realización, se utiliza una autoridad de certificación de propósito especial para proporcionar certificados digitales para autentificar usuarios 18. En la realización descrita, el servidor proxy DMZ 34 sólo reconoce certificados digitales de esta autoridad de certificación de propósito especial. Sin embargo, debería entenderse que cualquiera de las autoridades de certificación disponibles en el comercio puede ser substituida por la autoridad de certificación de propósito especial y permanecer dentro del espíritu y del ámbito de protección de la invención. En este caso, el servidor proxy DMZ 34 puede ser reconfigurado para aceptar certificados digitales expedidos por otra Autoridad de Certificación de propósito especial. Autoridades de certificación disponibles en el comercio conocidas incluyen GTE CyberTrust and VeriSign.

La Figura 2 muestra la mensajería que se produce entre el equipo cliente 22, el servidor proxy DMZ 34, el servidor proxy de pasarela 40 y el servidor web de pasarela 44. El usuario 18, vía el equipo cliente 22, mediante su navegador web, inicia una solicitud 64 de acceso seguro autentificado con uno de los servidores de destino en la red privada, la cual es recibida por el servidor proxy DMZ 34. Los mensajes 66, 68 y 70 representan el *handshaking* involucrado con el establecimiento de la conexión segura 52. Vale la pena destacar que el usuario 18/equipo cliente 22 sólo conocen el Localizador Uniforme de Recursos (URL) del servidor proxy DMZ, no el del servidor proxy de pasarela ni el de los servidores de destino. El servidor proxy DMZ 34 responde a la solicitud 64 transmitiendo un mensaje de respuesta 66.

El mensaje 66 será utilizado para autentificar la identidad del servidor de proxy DMZ 34 al equipo cliente 22. Por ejemplo, el servidor proxy DMZ 34 puede enviar al equipo cliente 22 su certificado digital. La parte de navegador web del equipo cliente 22 está configurada para analizar dicho certificado, y para autentificar el servidor proxy DMZ 34. El mensaje 66 también contendrá una petición para presentar información suficiente para autentificar el usuario 18 del equipo cliente 22 a ola red privada que contiene las aplicaciones 24_1, 24_2,... 24_3. Respecto a esto, el mensaje 66 puede causar que se presente una lista “pop-up” al usuario 18 del equipo cliente 22, solicitando la selección de un certificado digital X.509 por parte del usuario.

El certificado X.509 seleccionado se transmite en un mensaje 68 de vuelta al servidor proxy DMZ 34. Si el certificado X.509 presentado satisface ciertos requisitos de un primer y mínimo nivel, se pueden continuar dando más transmisiones, designadas en el mensaje 70, requeridas para establecer una conexión segura 52, mostrada en la figura 1. Se cifran más mensajes entre el equipo cliente 22 y el servidor proxy DMZ 34, de acuerdo con una llave de sesión conocida por el equipo cliente 22 y el servidor proxy DMZ 34. En una realización, el servidor proxy DMZ verifica para ver si el certificado digital ha sido expedido por una autoridad de certificados aprobada previamente.

Se empieza un segundo nivel de autenticación con el mensaje 72. Esta autenticación se realiza comparando datos del certificado digital proporcionado por el equipo cliente 22 con unos datos predeterminados acerca del certificado en el servidor de autorización 46. Para asegurar la transferencia del certificado digital a través del cortafuegos 32, el servidor proxy DMZ 34 y el servidor proxy de pasarela 40 establecen una segunda conexión segura 54, mostrada en la figura 1. Se debe enfatizar que el servidor proxy DMZ 34 tan solo conoce la URL del servidor proxy de pasarela de aplicaciones 40, no la URL de los servidores destino. Tan solo la información de mapeo para el servidor proxy de pasarela 40, que se almacena en un fichero de configuración local (detrás del cortafuegos), proporciona las URL/direcciones de los servidores destino.

Un reto, como se describe más arriba, es el de como el usuario del certificado digital del equipo cliente se pasa a través del cortafuegos 32 para la autenticación. Se configura el Plug-in 36 asociado con el servidor proxy DMZ 34 para extraer el certificado digital del mensaje entrante y pasarlo al servidor proxy de pasarela 40 en una cabecera HTTP, como parte de un mensaje HTTPS 72.

El servidor proxy de pasarela 40 pasa a su vez información del certificado digital presentado por el usuario del equipo cliente 22 al servidor de autorización 46, preferentemente de acuerdo con el protocolo LDAP. El servidor de autorización 46 devuelve los datos de autenticación indicativos de si el certificado digital proporcionado autentica de manera correcta al usuario del equipo cliente 22, así como la identificación de las aplicaciones 24_1, 24_2..., 24_3 para las cuales el acceso por parte del usuario 18 ha sido autorizado. Esta información se devuelve, de una manera que se detallará más adelante, al servidor proxy DMZ 34 por parte del servidor proxy de pasarela 40 mediante el mensaje 74. Cuando se autoriza al usuario para múltiples aplicaciones, el navegador del usuario se redirecciona al servidor 44.

El equipo cliente 22 hace una petición, mediante el mensaje 76, de recursos del servidor web de pasarela 44. El servidor web de pasarela 44 da servicio a dichos recursos, una “páginas de opciones”, al equipo cliente 22 en el mensaje 78. Las “páginas de opciones” presentan una lista de aplicaciones autorizadas 24_1, 24_2,... 24_3 para la selección por parte del usuario 18 del equipo cliente 22.

La selección de una de las aplicaciones presentadas en las “páginas de opciones” resulta en el mensaje 80 enviado por el servidor proxy DMZ 34. El mensaje 80 es un comando HTTP (a través de una conexión segura 54, siendo así un HTTPS) que incluye una composición de URL que comprende una URL base y un identificador asociado. El servidor proxy DMZ 34 enruta el mensaje 80, basándose en la composición URL, al servidor proxy de pasarela en un mensaje 82. El identificador es suficiente para el servidor proxy de pasarela 40 para enrutar el mensaje 82 a la aplicación seleccionada 24_1, 24_2,... 24_3.

La figura 3 muestra una representación simplificada del mensaje 72 que incluye los datos del certificado digital del usuario 18 del equipo cliente 22. El mensaje 72 incluye una cabecera HTTPS 84, una pluralidad de cabeceras HTTP 86, y una porción de datos 88. Nótese que el servidor proxy DMZ y el servidor proxy de pasarela 40 envían mensajes utilizando una conexión segura 56, por ejemplo, utilizando el protocolo SSL (i.e. HTTPS). Así, se utiliza una cabecera HTTPS 84, mientras que el payload, es decir, las cabeceras HTTPS 86 y la porción de datos 88, se encriptan. El Plug-in 36 asociado con el servidor proxy DMZ 34 está configurado para capturar el certificado digital X.509 presentado por el usuario 18 vía el equipo cliente 22, y de una o más cabeceras HTTP que, colectivamente, recogen datos contenidos en el certificado digital como un todo para el servidor proxy de pasarela 40. En una realización, el plug-in 36 puede estar implementado utilizando interfaces de programación de aplicaciones estándar (API), por ejemplo, Netscape APIs (NSAPI) cuando se utiliza el software de servidor proxy Netscape para implementar el servidor proxy DMZ 34.

La figura 4 muestra varias cookies creadas por el servidor proxy de pasarela 40: una cookie de autenticación 90, una cookie de lista de aplicaciones 92, una cookie de aplicaciones seleccionadas 94. Se entrega al cliente un mensaje de cookie (por ejemplo, un navegador web) por un servidor. El cliente almacenara en cache la cookie, y almacenará la cookie en un fichero en el equipo cliente 22 si la cookie es una de las llamadas cookies “persistentes”. En una realización, las cookies son no-persistentes y por tanto tan solo están en la memoria cache, y no almacenadas en un fichero en el equipo cliente 22. A parte del mensaje hay una descripción del rango de URLs para el cual la cookie es válida, y un tiempo durante el que la cookie persistirá (otra vez, tan solo las cookies persistentes). Cualquier petición HTTP futura por parte del cliente que caiga en dicho rango incluirá el valor de ése momento de la cookie (por ejemplo State object) al servidor. Dado que HTTP es un protocolo no dependiente del tiempo (i.e., cada comando HTTP se ejecuta por el servidor independientemente, sin ningún conocimiento de los comandos que le precedieron), la cookie es un mecanismo para transmitir información.

Como se ha descrito previamente, el servidor de autorización 46 devuelve datos de autenticación al servidor proxy de pasarela 40 que indican si el certificado digital ha autenticado correctamente al usuario 18 del equipo cliente 22, así como una identificación de aplicaciones 24_1, 24_2,... 24_3 para las cuales se ha autorizado el acceso. En respuesta, el servidor proxy de pasarela 40 construye una cookie de autenticación 90, y una cookie de lista de aplicaciones. La cookie de autenticación 90 puede incluir información tal como información time-stamp que indica el momento de la autenticación correcta. La cookie de lista de aplicaciones 92 puede incluir una identificación de aplicaciones particulares para las que el equipo cliente 22 está autorizado. Si solo una aplicación se ha autorizado, la cookie de aplicaciones seleccionadas 94 se pospone hasta después que el usuario 18 selecciones una de las aplicaciones de la “página de opciones”. La cookie de autenticación 90 y la cookie de lista de aplicaciones 92 se envían con el mensaje 74 al equipo cliente 22 vía el servidor proxy de pasarela 34, con una redirección al servidor web 44.

Las cookies 90 y 92, a su tiempo, se proporcionan (desde el equipo cliente 22) con un mensaje 76 al servidor web de pasarela 44. El servidor web de pasarela 44, a su vez, genera la “página de opciones”, utilizando la información de la cookie de lista de aplicaciones 92. El HTML que define la “página de opciones” se envía en el mensaje 78 al equipo cliente 22.

En relación a la figura 4B, cada aplicación listada disponible para ser seleccionada en la “página de opciones” incluye una respectiva composición URL 96 que comprende una base URL 98 y un identificador 100. Por ejemplo, la base URL 98, como ejemplo, puede ser HTTPS://url-of-dmz-server. El identificador 100 puede ser seleccionado para identificar o describir una aplicación particular de la pluralidad de aplicaciones, pero no hace falta que se haga, técnicamente. Por ejemplo, para una aplicación particular 24_1, 24_2, … 24_3 que comprenda una facturación, el identificador 100, solo como ejemplo, puede ser “/facturación” – una cadena de caracteres simbólica de la aplicación, incluyendo un carácter de barra como prefijo. El identificador 100, como un todo, se incorpora a la base URL preferentemente con un sufijo. La composición URL se envía en el mensaje 80 desde el equipo cliente 22 a través de una red no segura 26 al servidor proxy DMZ 34. El servidor proxy DMZ 34 mapea a su vez la composición URL para enrutar el mensaje entrante 82 al servidor proxy de pasarela 40. Éste mapeo puede ser una simple función de reemplazamiento del nombre del dominio (por ejemplo Reemplazar url-of-dmz-server por url-of-gateway-server, de manera que se termine con HTTPS://url-of-gateway-server/identifier. El plug-in de autorización 42 está configurado para reconocer el identificador (por ejemplo, "/facturación"), para crear en respuesta la cookie de aplicación seleccionada 94.

La figura 5 muestra un diagrama de flujo describiendo la operación del plug-in de autorización asociada con el servidor proxy de pasarela 40.

En la etapa 100, el plug-in de autorización 42 empieza su ejecución.

En la etapa 102, el plug-in de autorización 42 determina si el mensaje entrante contiene una cookie de autenticación 90 válida. La validez requiere que el certificado digital del usuario haya autenticado al usuario del equipo cliente 22 y, que el time-stamp coincida con un criterio de tiempo preestablecido (i.e., no debe ser demasiado viejo). Más concretamente, la presencia de la cookie de autenticación 90 es indicativo de una autenticación correcta. Dada la naturaleza no persistente de la cookie 90, la cookie 90 no viene de un fichero almacenado, sino tan solo como resultado de una autenticación correcta. Entonces, el requisito restante es que el se satisfaga el criterio temporal. En una realización, siendo la cookie 90 más vieja que, preferentemente, 12 horas, se considera inválida. En otra realización, una cookie 90 mayor de 4 horas se considera inválida. La longitud de tiempo puede seleccionarse en base a el máximo esperado para una sesión por parte del usuario 18. Si la respuesta es "NO", entonces el procedimiento continua en la etapa 104.

En la etapa 104, el plug-in de autorización 42 extrae y analiza el certificado digital X.509 del usuario, del mensaje 72, mostrado simplificado en la figura 3. El procedimiento continua con la etapa 106.

En la etapa 106, el plug-in de autorización 42 asociado al servidor proxy de pasarela 40 consulta con el servidor de autorización 46 para la autenticación del usuario 18. El plug-in 42 proporciona las particularidades del certificado digital X.509 en un mensaje al servidor de autorización 46. En la etapa 108, el plug-in de autorización 42 determina las aplicaciones para las que el usuario tiene un acceso autorizado, todo ello a través de mensajes con el servidor de autorización 46. En la etapa 110, el servidor proxy de pasarela 46 obtiene una identificación de usuario de todas las pasarelas (ID) para el usuario. Este ID de usuario de pasarela puede facilitar el acceso a y la utilización de la pluralidad de las aplicaciones 24_1, 24_2,... 24_3. Por ejemplo, el ID de usuario de pasarela puede pasarse a la aplicación, la cual puede utilizarlo para buscar información de perfil de usuario en su base de datos local que describa qué funciones se le permiten realizar al usuario en la aplicación en particular. Una cookie de ID de usuario de pasarela puede establecerse para implementar ésta transmisión de información. Las etapas 106-110 pueden realizarse de forma secuencial, o como una composición de peticiones, o de cualquier otra forma ya conocida en el estado de la técnica.

En la etapa 112, el plug-in de autorización 42 crea la cookie de autenticación 90, y la cookie de lista de aplicaciones 92, como se describe previamente.

En la etapa 114, el plug-in 42, a través del servidor proxy de pasarela, transmite la cookie 90 (cookie de autenticación) y la cookie 92 (cookie de lista de aplicaciones) al equipo cliente 22 a través del servidor proxy DMZ a través del mensaje 74. El mensaje 74 causa también que el navegador web se redireccione al servidor web 44 vía la conexión 56.

En la etapa 116, el procedimiento termina.

Sin embargo, si en la etapa 102, la respuesta es "SI", entonces el usuario/equipo cliente 22 ya se ha autenticado. El procedimiento continua pues en la etapa 118.

En la etapa 118, se realiza un test para determinar si la composición, URL 96 asociada al mensaje entrante incluye el identificador 100. Si "SI", entonces esto significa que el usuario 18 del equipo cliente remoto 22 acaba de seleccionar la aplicación de la "página de opciones". La "página de opciones" es la única localización de origen que podría generar un mensaje aportando el identificado 100. Los subsiguientes mensajes originando del equipo cliente 22 durante la utilización de una aplicación particular no deberían tener el identificador, dado que ninguna de las aplicaciones 24_1, 24_2,... 24_3 ni el navegador se programan normalmente para incluir dicho identificador. Si la respuesta a la etapa de decisión 118 es "SI" entonces el procedimiento continua en la etapa 120.

En la etapa 120, la cookie de aplicación seleccionada 94 se construye, utilizando el identificador 100. La cookie 94 incluye información correspondiente al identificador 100.

En la etapa 122, la cookie de identificación de usuario de pasarela (i.e., una cabecera HTTP) se genera, utilizando información del ID de usuario de pasarela obtenido en la etapa 110.

En la etapa 124, el mensaje entrante se enruta por el servidor proxy de pasarela 40 al destino particular del servidor 28_1, 28_2, ... 28_3 correspondiente a la aplicación seleccionada. El servidor proxy de pasarela 40 incluye una función de mapeado o enrutamiento que responde frente al identificador 100 incluido, configurada para identificar el servidor destino apropiado 28. El identificador 100 puede ser omitido del mensaje que es eventualmente enrutado a través de una de las conexiones 58, 60 y 62, dado que su función (i.e., enrutar) ya se ha satisfecho. Es importante destacar que la cookie de aplicación seleccionada 94 contiene ahora la información relacionada con la aplicación seleccionada. Así, mensajes subsiguientes, que incluyen la cookie 94, pueden ser enrutados para el servidor destino apropiado. El procedimiento continua en la etapa 116, en donde el procedimiento termina.

Sin embargo, si la respuesta en la etapa 118 es "NO", entonces el procedimiento continua en la etapa 126. Si el usuario del equipo cliente 22 ha sido autenticado, y no se ha incluido un identificador reconocible, ello significa que este mensaje es el segundo o subsiguiente mensaje que pasa a través del servidor proxy de pasarela 40 desde el equipo cliente 22 después de la autenticación. Como se ha descrito antes, los programas de aplicaciones varias 30_1, 30_2,... 30_3 no están generalmente programados para incluir ayudas de enrutamiento, ni deben de estarlo. El equipo informático 20

debe de implementar la función de enrutamiento de manera transparente respecto a las diversas aplicaciones. De acuerdo con la presente invención, el sistema informático 20 cumple ésta función de manera transparente y eficiente.

En la etapa 126, la cookie de aplicación seleccionada 94 es capturada, y de la misma se recupera el identificador 100. Por ejemplo, el identificador 100 puede ser "/facturación" para una aplicación relacionada con la facturación.

En la etapa 128, el identificador 100 recuperado se incluye en la URL especificada en el mensaje entrante. En una realización preferida, el identificador 100 se incluye como un sufijo. De acuerdo con esto, el plug-in 42 incluye medios para incluir, antes de enrutar, el identificador 100 a la URL contenida en el mensaje entrante. Sin embargo, otras configuraciones son posibles, tan solo limitadas por las capacidades de los medios de mapeo que se incluyen en el servidor proxy de pasarela 40.

En la etapa 130, la composición URL (incluyendo el identificador 100) se pasa a la función de mapeo del servidor proxy de pasarela . Esta composición reconstruida de URL contiene así la misma información (i.e., el símbolo incluido) en el mismo formato que la composición URL inicial que tenía como origen la selección del usuario de la "página de opciones". Así, no es necesario que se cambie la función de mapeo del servidor proxy 40 o se altere para soportar un segundo o subsiguientes mensajes, como el caso del primer mensaje.

En la etapa 132, el mensaje entrante se enruta al servidor destino correspondiente a la aplicación seleccionada (como se ha mapeado). El procedimiento continúa en la etapa 116, en donde termina.

De acuerdo con este aspecto de la invención, se proporciona un mecanismo eficiente para proporcionar acceso de un equipo cliente en una red no segura hacia un servidor destino seleccionado de entre una pluralidad de servidores de una red privada. El uso de la cookie de selección de aplicaciones 94, en conexión con un plug-in 42 debidamente programado, configurado para incluir el identificador, opera conjuntamente para obtener un enrutamiento eficiente.

La figura 6 muestra un diagrama de información para un usuario para la obtención de un certificado digital X.509 para ser utilizado en la presente invención. Cada aplicación 24_1, 24_2,... 24_3 tiene una fuente segura 134, que controla a quien se le permite acceso a la aplicación. Inicialmente, un usuario 18 direcciona un mensaje 136 a una fuente segura 134, que incluye información referente al usuario. Esta comunicación (por ejemplo, mensaje 136) puede realizarse vía telefónica. La fuente segura 134 proporciona entonces al usuario un ID/contraseña de usuario, con instrucciones para acceder a la autoridad de certificados 50 utilizando el ID/contraseña proporcionada. La fuente segura 134 envía entonces un mensaje 138 a la Seguridad de Información 48 que contiene la información recopilada del usuario 18 incluyendo qué aplicación(es) se peticionan para su acceso remoto.

La seguridad de información 48 puede tener una interfaz directa 140 (por ejemplo, una página web) para el servidor de autorización 46 con la función de, por ejemplo, entrar la información de usuario que ha proporcionado la fuente segura 134.

El usuario 18 a través del equipo cliente 22 de acuerdo con las instrucciones dadas por la fuente segura, entra en la autoridad de certificados 50 utilizando la contraseña y el ID de usuario originales. Después de entrar, el usuario 18 realiza una petición 142 a la autoridad de certificados 50. La petición 142 comprende la petición del certificado, que incluye también información relacionada con el usuario 18 y las aplicaciones deseadas. La autoridad de certificados 50 proporciona entonces al usuario 18, quizás vía el equipo cliente 22, un PIN o similar (por ejemplo, un número de referencia, frase a completar, etc.).

La seguridad de información 48 puede tener otra interfaz directa 44 (por ejemplo, basada en web) para la autoridad de certificación 50. La seguridad de información 48 utiliza la interfaz 144 para monitorizar peticiones que provienen hacia la autoridad de certificación 50. Cuando la Seguridad de información 48 observa la entrada de la petición del usuario 18, compara la información entrada por el usuario 18 en la autoridad de certificación 50 con la información de usuario recibida vía la fuente segura 134. Si se aprueba, la seguridad de información 48 envía un mensaje de respuesta 146 indicando la aprobación hacia la autoridad de certificación 50. La autoridad de certificación notifica entonces (por ejemplo, e-mail) al usuario 18 que la petición ha sido aprobada, y que el certificado digital está disponible. El usuario 18 accede entonces a la autoridad de certificados 50, y entra utilizando el ID de usuario y contraseña originales proporcionados por la fuente segura 134, y el PIN proporcionado por la autoridad de certificación 50. Cuando esta información es aceptada por la autoridad 50, el certificado digital se envía como se muestra en 148 al equipo cliente 22. En una realización, el certificado digital se descarga directamente al equipo cliente 22 del usuario 18 durante el proceso de obtención (i.e., no se envía posteriormente vía email). La seguridad de información 48 es notificada entonces de los datos de certificación por parte de la autoridad de certificación 50. A su vez, la seguridad de información 48 envía los datos de certificación mediante la interfaz 140 al servidor de autorización 46. Es entonces cuando el servidor de autorización 46 se actualiza.

De acuerdo con otro aspecto de la presente invención, se proporciona un procedimiento mejorado para obtener el certificado X.509. En este aspecto de la invención, después de la petición inicial del usuario a la fuente segura 134 (incluyendo la sumisión de información de usuario requerida, identificación de las aplicaciones seleccionadas, etc..), la

fuente segura 134 proporciona datos recopilados por la seguridad de información 48. La fuente 134 proporciona también al usuario del equipo cliente remoto 22 un ID/contraseña y PIN. La seguridad de información 48 actualiza entonces el servidor de autorización 46 directamente. El usuario del equipo cliente remoto 22 contacta entonces con la autoridad de certificación 50, y proporciona el ID/contraseña del usuario y el PIN. La autoridad de certificación 50 extrae la información directamente del servidor de autorización 46 (i.e., hay un enlace seguro entre la autoridad de certificación 50 y el servidor de autorización 46), y publica el certificado digital al usuario del equipo cliente 22 inmediatamente. La autoridad de certificación 50 actualiza entonces el servidor de autorización 46 con los datos de certificación del certificado digital publicado. Éste procedimiento tiene la ventaja de evitar la volver a teclear datos por parte del usuario quien, mediante el procedimiento previamente descrito, entró datos de la fuente segura, y otra vez para la autoridad de certificación. Además, el desarrollo mejorado proporciona una experiencia de "parada única" al usuario 18.

De acuerdo con otro aspecto de la invención, se proporciona una pasarela segura que permite acceso autenticado desde un equipo cliente en una red publica no segura hacia un servidor destino en una red privada sin la utilización de certificados digitales. En aplicaciones en donde no se requieran los certificados digitales, no habría autenticación de "primer nivel" en la parte de red no segura del cortafuegos, como se describe más arriba respecto el sistema informático 20. Aun con todo y eso, sería preferible realizar dicha autenticación, al menos en un nivel preliminar, en el lado no seguro del cortafuegos antes de permitir el paso de mensajes a través del cortafuegos hacia los servidores destino.

La figura 7 muestra un diagrama de bloques simplificado de una segunda realización de acuerdo con la presente invención, en concreto, un sistema informático 200. Si no se indica lo contrario, se utilizan las misma referencias numéricas para identificar componentes idénticos o substancialmente similares en las diversas vistas. El sistema informático 200 implementa una identificación de usuario (ID) y un esquema de contraseña para autentificar al usuario del equipo cliente 22. La figura 7 es similar a la figura 1, excepto que se proporciona un servidor web DMZ 210 en la parte no segura de la red del sistema de cortafuegos 32, en lugar de un servidor web 44 en la parte de la red privada. Aunque no se muestra en la figura 7, el servidor proxy DMZ 34 y el servidor proxy de pasarela 40 incluye los respectivos plug-ins 36 y 42, como se describe más arriba respecto al sistema informático 20.

La figura 8 es un diagrama de flujo que ilustra el sistema y procedimiento inventivos para autentificar un equipo cliente remoto 22. El procedimiento empieza en la etapa 212.

En la etapa 214, el servidor proxy DMZ 34 determina vía un plug-in programado 36 si el mensaje entrante contiene una cookie de autenticación válida 90. Como se describe más arriba, la presencia de la cookie por ella misma 90, en conjunción con un time-stamp que no sea demasiado viejo, puede satisfacer los requisitos para una cookie de autenticación "válida" 90. Una condición válida o "verdadera" indica que el equipo cliente 22 ha sido autenticado correctamente en el pasado reciente. En una realización alternativa, la cookie de autenticación 90 puede estar configurada para proporcionar información adicional tal como información indicadora del estado. La información indicadora de estado puede incluir datos de un operador booleano de autorización (por ejemplo, VERDADERO O FALSO) indicadores de si el usuario es reconocido por el servidor de autorización 46, y datos indicando si el usuario es reconocido por el servidor de autorización 46, pero que la contraseña proporcionada ha expirado. Si la respuesta a la etapa de decisión 214 es “NO”, entonces el procedimiento continua en la etapa 216.

En la etapa 216, el servidor web 210 formatea un mensaje que se envía a través del servidor proxy 34, mediante una conexión segura 52, al equipo cliente 22, que causa un que aparezca un “pop-up” de una pantalla de entrada para el usuario. La identificación de usuario (ID) y la contraseña se obtienen de un usuario 18 de un equipo cliente 22, las cuales se reenvían de vuelta al servidor web 210 vía el servidor proxy DMZ 34.

En la etapa 218, el servidor web 210 formatea el mensaje que incluye el ID de usuario y la contraseña obtenidas del usuario del equipo cliente remoto 22, y envía ese mensaje a través del cortafuegos 32 mediante una conexión segura 56 al servidor de autorización 46. También se incluye en el mensaje una petición para una respuesta indicativa de si el ID de usuario y la contraseña proporcionadas por el usuario son suficiente para autentificar al usuario del equipo cliente remoto 22. El servidor de autorización 46 puede incluir un demonio de autorización, un proceso configurado para realizar una petición de búsqueda en la porción de servidor LDAP de autorización del servidor 46. La respuesta del servidor 46 puede incluir datos de autenticación representativos de si el usuario está autenticado o no, basados en el ID de usuario y la contraseña proporcionadas. La respuesta puede incluir también una identificación de las aplicaciones 24_1, 24_2, ... 24_3, a las cuales se autoriza el acceso. Basado en ello, el servidor web 210 crea una cookie de autenticación 90 (mostrada en la figura 4A).

En la etapa 220, el servidor web 210 determina si el usuario está autenticado. Esta etapa puede involucrar simplemente evaluar la respuesta devuelta por el servidor de autorización 46. Si la respuesta es “NO”, entonces la etapa de decisión 220 continúa en la etapa 222.

En la etapa 222, se muestra al usuario 18 del equipo cliente remoto 22 un mensaje de error de autorización, generado por el servidor web 210. El procedimiento continua con la etapa 224, en donde éste termina.

Si, sin embargo, la respuesta a la etapa de decisión 220 es “SI”, entonces el procedimiento continua en la etapa 226. En la etapa 226, el servidor web 210 determina si el número de aplicaciones autorizadas es mayor que uno. Si la respuesta es “NO”, el procedimiento continua en la etapa 228.

En la etapa 228, el servidor web 210 crea (si es necesario), y configura la cookie de aplicación seleccionada 94. Esto puede involucrar asociar información, tal como un identificador 100, con la cookie 94. A modo ilustrativo, el identificador 100 puede ser una sucesión de caracteres conteniendo un carácter de contra barra como prefijo, tal como “/facturación” para una aplicación relacionada con facturación.

En la etapa 230, el servidor web 210 configura un sufijo de aplicación para un mapeo de proxy. De hecho, el servidor web 210 se configura con los medios para embeber el identificador 100 a la URL base incluida en el mensaje entrante. Dado que no hay una “página de opciones” para la situación en que tan solo una aplicación es autorizada, el servidor web 210 embebe el identificador 100 al mensaje inicial.

En la etapa 232, el servidor web 210 crea una cabecera HTTP (por ejemplo, una “cookie”) que tiene un ID de usuario de pasarela. Esto puede ser útil o requerido por las aplicaciones 24_1, 24_2 que se ejecutan en los servidores 28_1, 28_2. Esta característica ha sido previamente descrita.

En la etapa 234, el servidor web 210 envía un mensaje de redireccionamiento al equipo cliente 22, redireccionando la porción de navegador web del equipo cliente 22 hacia los recursos de petición (por ejemplo, para el mensaje inicial, una “página de bienvenida”) desde el servidor destino 28, correspondiente a la aplicación autorizada. El procedimiento continua entonces en la etapa 224 en donde termina.

Si la respuesta a la etapa de decisión 226, sin embargo, es “SI”, entonces el procedimiento continua en la etapa 236.

En la etapa 236, el servidor web 210 genera una “página de opciones” referente a lo anterior que lista todas las aplicaciones a la que el equipo cliente 22 está autorizado a acceder. Cuando el usuario del equipo cliente remoto 22 ha realizado la selección de una de las aplicaciones, el equipo cliente 22 envía una petición de HTTP encapsulada en un mensaje HTTPS que incluye una composición URL 96 comprendiendo una URL base 98 y un identificador 100. El procedimiento continua en la etapa 238.

En la etapa 238, se realiza el procesamiento del plug-in 42. Este procesamiento es el mismo que el descrito previamente respecto al sistema informático 20, y como se muestra en la figura 5.

En la etapa 240, el mensaje entrante se direcciona al servidor destino 28 correspondiente a la aplicación seleccionada 24. El procedimiento termina en la etapa 224.

Sin embargo, si la respuesta a la etapa de decisión 214 es “SI”, entonces el procedimiento continua en la etapa 242, en donde el mensaje entrante se enruta por el servidor proxy DMZ 34, a través de el servidor proxy de pasarela 40 al servidor destino 28 correspondiente a la aplicación seleccionada.

Una ventaja del sistema informático 200 es que autentica a un equipo cliente remoto ante de permitir acceso a la red privada segura. El sistema informático 200 consigue la autenticación en donde los certificados digitales no son capaces de hacerlo o no es recomendable que lo hagan. Además, la arquitectura del sistema informático mantiene los datos sensibles de autenticación en la parte segura y de red privada del cortafuegos, reduciendo así las posibilidades de una intrusión ‘’pirata’’ con éxito.

Debe de entenderse que la presente descripción es meramente a modo de ejemplo y no de naturaleza limitativa, estando la invención limitada tan solo por las reivindicaciones adjuntas. Pueden realizarse varias modificaciones y cambios por parte de un experto medio en la materia, que caen dentro de los principios de la invención y de su alcance.

REIVINDICACIONES

1. Sistema informático (20, 200) para facilitar el acceso desde un equipo cliente (22), a través de una red pública no segura, a un servidor de destino (28) en una red privada segura, que comprende:

un sistema cortafuegos (32) entre dicha red no segura y dicha red privada segura;

un servidor de autorización (46) en el lado de la citada red privada del citado sistema cortafuegos (32) para autentificar a un usuario (18) de dicho equipo cliente (22) en base a un identificador (ID) de usuario y una contraseña de dicho usuario de dicho equipo cliente (22);

un servidor web (210, 44) en el lado de la citada red no segura de dicho sistema cortafuegos (32), configurado para enviar dicho ID de usuario al citado servidor de autorización y generar una cookie de autentificación cuando dicho servidor de autorización (46) autentifica a dicho usuario del citado equipo cliente (22) en base a dicho ID de usuario y a dicha contraseña;

caracterizado por

un servidor proxy (34) en el lado de la citada red no segura de dicho sistema cortafuegos (32); y

una pasarela (38) en el lado de la citada red privada de dicho sistema cortafuegos (32);

en el que el citado servidor proxy (34) está configurado además para enviar un mensaje desde dicho equipo cliente (22) a dicho servidor de destino (28) a través de la pasarela (38), cuando la citada cookie de autenticación es válida, y

en el que la pasarela (38) incluye un servidor proxy de pasarela (40) configurado para:

recibir desde el equipo cliente (22) una URL que comprende una parte base y un identificador, extraer dicho identificador, y generar una cookie de aplicación seleccionada,

reconocer la cookie de aplicación seleccionada y adjuntar el identificador recuperado de dicha cookie de aplicación seleccionada a mensajes desde el citado equipo cliente, e

identificar, en base al identificador adjunto, el servidor de destino y enrutar el mensaje hacia dicho servidor de destino en base al citado identificador adjunto.

2. El sistema informático (20, 200) de la reivindicación 1, en el que el citado servidor proxy (34) está configurado para establecer conexiones seguras respectivas con dicho equipo cliente (22) y la citada pasarela (38), y dicho servidor web (44, 210) está configurado para establecer una conexión segura respectiva con el citado servidor de autorización (46).

3. El sistema informático (20, 200) de las reivindicaciones 1 ó 2, en el que

la pasarela (38) está dispuesta entre el citado servidor proxy (34) y dicha red privada en el lado de dicha red privada de dicho sistema cortafuegos (32).

4. El sistema informático (20, 200) según una de las reivindicaciones 1 a 3, en el que dicha conexión al citado servidor proxy (34), a través de la que se recibe dicho ID de usuario y contraseña desde dicho equipo cliente (22), se securiza utilizando un protocolo de Capa de Conexión Segura, SSL.

5. El sistema informático (20, 200) según una de las reivindicaciones 1 a 4, en el que dicho servidor de autorización (46) comprende un servidor capaz de implementar un protocolo ligero de acceso a directorios, LDAP.

6. El sistema informático (20, 200) según una de las reivindicaciones 1 a 5, en el que la citada conexión entre dicho servidor web (44, 210) y dicho servidor de autorización (46) está securizada utilizando un protocolo de Capa de Conexión Segura, SSL, y en el que el citado servidor web (44, 210) y dicho servidor de autorización (46) se proporcionan autentificación entre sí utilizando certificados digitales que cumplen con un estándar de la industria.

7. El sistema informático (20, 200) según la reivindicación 6, en el que dicho estándar de la industria comprende un estándar ITU X.509.

8. El sistema informático (20, 200) según una de las reivindicaciones 1 a 7, en el que la citada conexión entre dicho servidor proxy (34) y dicha pasarela (38) está securizada utilizando un protocolo de Capa de Conexión Segura, SSL, y en el que el citado servidor proxy (34) y dicha pasarela (38) se proporcionan autentificación entre sí utilizando certificados digitales que cumplen con un estándar X.509.

9. El sistema informático (20, 200) según una de las reivindicaciones 1 a 8, en el que dicha red privada incluye una pluralidad de servidores de destino sirviendo cada uno de ellos una aplicación correspondiente, comprendiendo dicho servidor proxy un servidor proxy de zona desmilitarizada, DMZ, y comprendiendo el citado servidor web un servidor web DMZ, incluyendo dicha pasarela un servidor proxy de pasarela, estando configurado el citado servidor web DMZ para transmitir a dicho equipo cliente una lista de aplicaciones para cuyo acceso por parte de dicho usuario del citado equipo cliente está autorizado de acuerdo con dicha respuesta por parte de dicho servidor de autorización, siendo la selección por parte de dicho usuario en el citado equipo cliente de una aplicación de dicha lista operativa para enviar a dicho servidor proxy de pasarela, a través de dicho servidor proxy DMZ, un localizador de uniforme de recursos, URL, que comprende una parte base y un identificador adjunto al mismo como un sufijo.

10. Un procedimiento para facilitar el acceso por parte de un equipo cliente (22) en una red pública no segura, a través de un servidor proxy (34), a un servidor de destino (28) que reside en una red privada segura, comprendiendo dicho procedimiento las etapas de:

A. Recibir en el servidor proxy (34) una solicitud de autentificación por parte de un usuario (18) del equipo cliente (22);

B. Establecer una primera conexión segura entre el servidor proxy (34) y el equipo cliente (22);

C. Obtener, en el servidor web, a través del servidor proxy, un identificador (ID) de usuario y una contraseña del usuario (18) del equipo cliente (22);

D. Establecer una segunda conexión segura entre el servidor web (44, 210) y un servidor de autorización (42) para la transmisión del ID de usuario y la contraseña;

E. Obtener datos de autentificación desde el servidor de autorización (42), utilizando el ID de usuario y la contraseña;

F. Generar una cookie de autentificación utilizando los datos de autentificación;

G. Enrutar mensajes desde el equipo cliente (22), a través del servidor proxy (34), a través de una pasarela (38) al servidor de destino cuando la cookie de autentificación es válida,

caracterizado por

recibir en el servidor proxy de pasarela (40) una URL desde el cliente, comprendiendo dicha URL una parte base y un identificador,

extraer dicho identificador y generar una cookie de aplicación seleccionada en la que

el servidor proxy de pasarela (40) está además configurado para

reconocer la cookie de aplicación seleccionada y adjuntar el identificador en la citada cookie de aplicación seleccionada a mensajes desde dicho equipo cliente (22), y

identificar, en base al identificador adjunto, el servidor de destino y enrutar el mensaje a dicho servidor de destino en base a dicho identificador adjunto.

11. El procedimiento según la reivindicación 10, que incluye además las etapas de:

proporcionar un sistema cortafuegos (32) entre la red pública no segura y la red privada segura;

disponer el servidor proxy (34) y el servidor web (44, 210) en el lado de la red no segura del sistema cortafuegos; y

disponer el servidor de autorización (42) y la pasarela (38) en el lado de la red privada del sistema cortafuegos (32).

12. El procedimiento según una de las reivindicaciones 10 ó 11, en el que dicha etapa de enrutado de mensajes incluye la sub-etapa de:

establecer una tercera conexión segura entre el servidor proxy (34) y la pasarela (38).

13. El procedimiento de la reivindicación 12, en el que dichas etapas de establecer una segunda conexión segura y recibir datos de autentificación incluye una comunicación de acuerdo con un protocolo seguro de transferencia de hipertexto, HTTPS.

14. El procedimiento según una de las reivindicaciones 10 a 13, en el que dicha etapa de enrutar mensajes se realiza por cada mensaje destinado al servidor de destino (28).

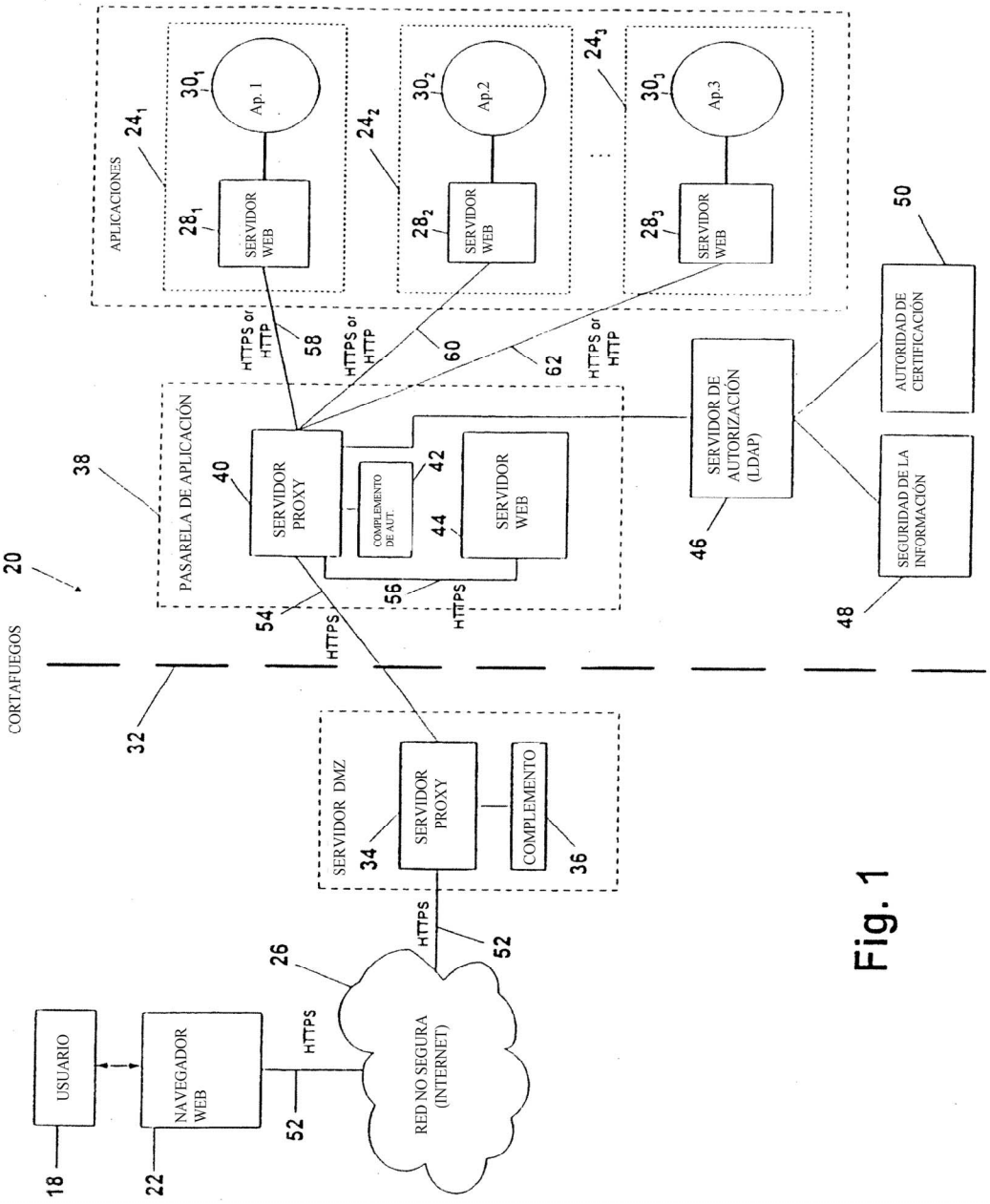
APLICACIONES
Ap. 1
Ap.2
Ap.3
SERVIDOR WEB
HTTPS o HTTP
PASARELA DE APLICACIÓN
SERVIDOR PROXY
COMPLEMENTO DE AUT.
SERVIDOR WEB
SERVIDOR DE AUTORIZACIÓN (LDAP)
AUTORIDAD DE CERTIFICACIÓN
SEGURIDAD DE LA INFORMACIÓN
CORTAFUEGOS
SERVIDOR DMZ
SERVIDOR PROXY
COMPLEMENTO
HTTPS
RED NO SEGURA (INTERNET)
USUARIO
NAVEGADOR WEB
20
18
22
24 1
24 2
24 3
26
28 1
28 2
28 3
30 1
30 2
30 3
32
34
36
38
40
42
44
46
48
50
52
54
56
58
60
62

Fig. 1

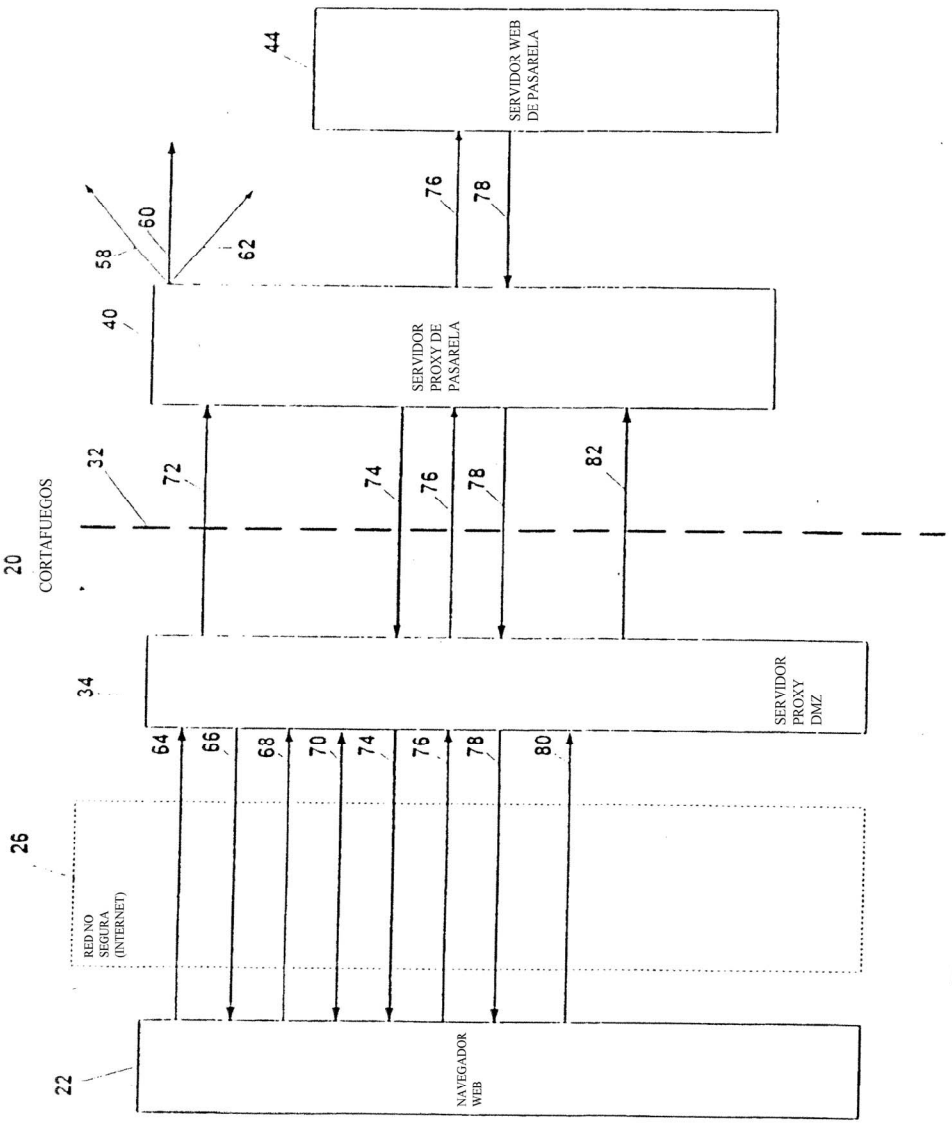
44
SERVIDOR WEB DE PASARELA
76
78
58
60
62
40
SERVIDOR PROXY DE PASARELA
32
72
74
76
78
82
20
CORTAFUEGOS
34
SERVIDOR PROXY DMZ
64
66
68
70
74
76
78
80
26
RED NO SEGURA (INTERNET)
22
NAVEGADOR WEB

Fig. 2

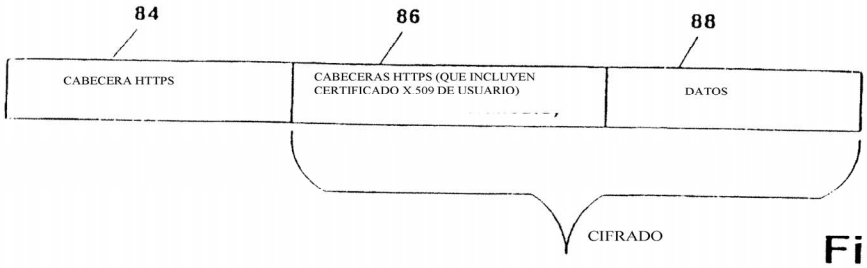

Fig. 3

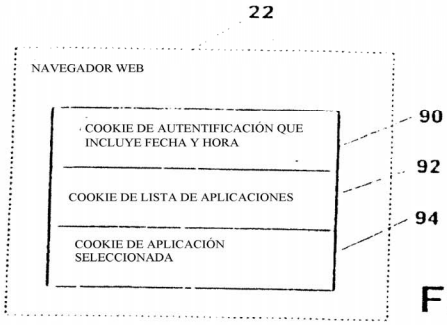

Fig. 4A

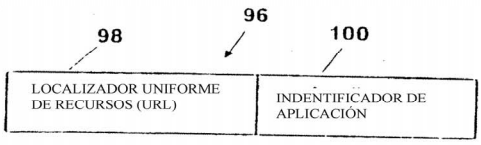

Fig. 4B

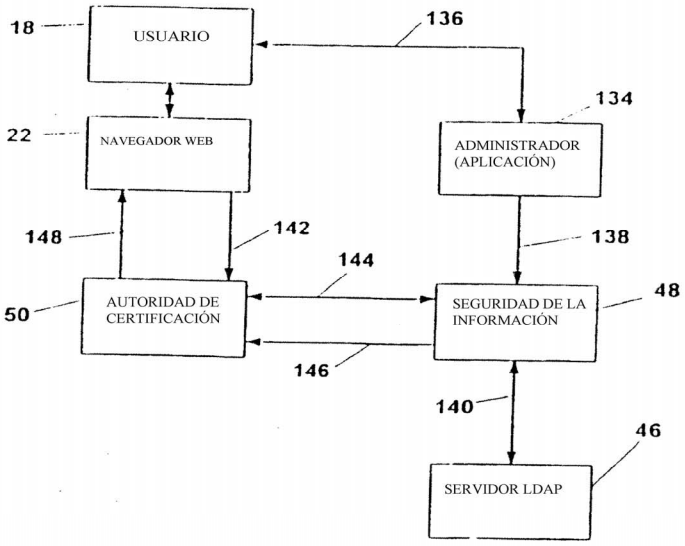

Fig. 6

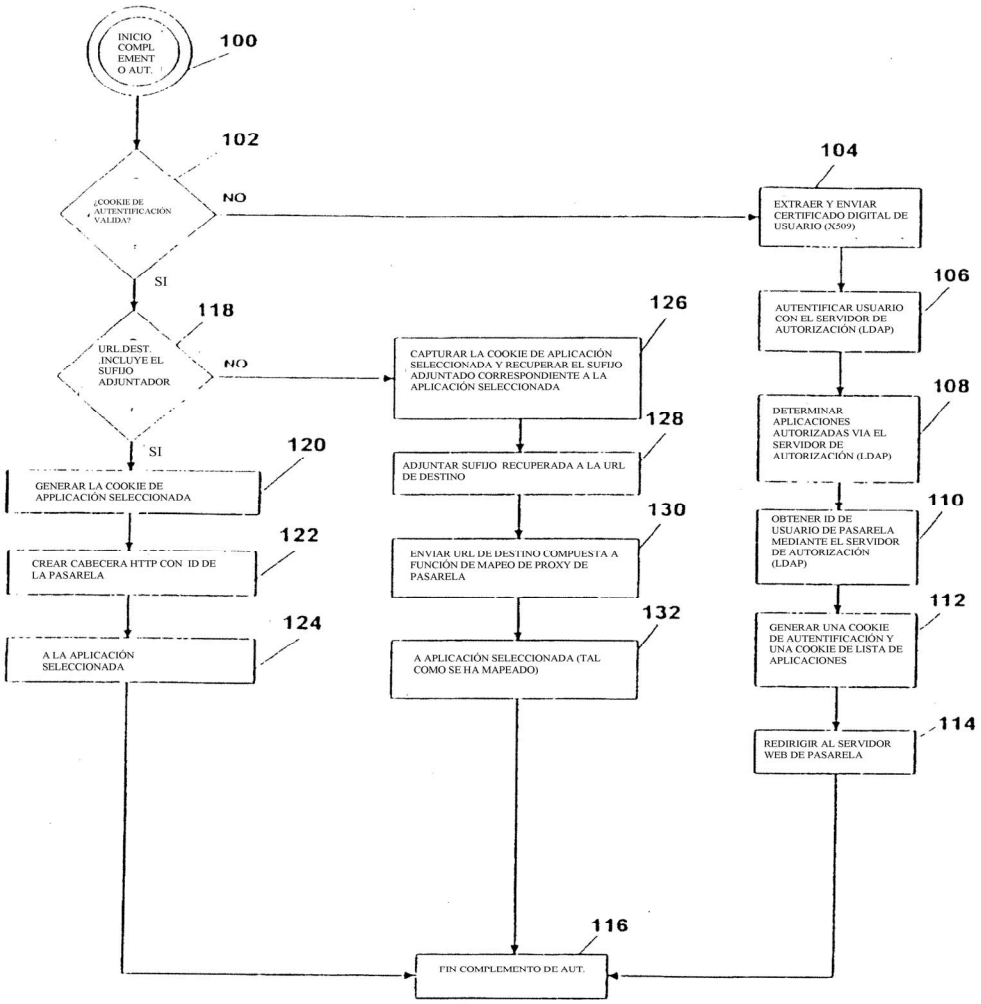
INICIO COMPL EMENT O AUT.
100
102
¿COOKIE DE AUTENTIFICACIÓN VALIDA?
NO
SI
104
EXTRAER Y ENVIAR CERTIFICADO DIGITAL DE USUARIO (X509)
106
AUTENTIFICAR USUARIO CON EL SERVIDOR DE AUTORIZACIÓN (LDAP)
108
DETERMINAR APLICACIONES AUTORIZADAS VIA EL SERVIDOR DE AUTORIZACIÓN (LDAP)
110
OBTENER ID DE USUARIO DE PASARELA MEDIANTE EL SERVIDOR DE AUTORIZACIÓN (LDAP)
112
GENERAR UNA COOKIE DE AUTENTIFICACIÓN Y UNA COOKIE DE LISTA DE APLICACIONES
114
REDIRIGIR AL SERVIDOR WEB DE PASARELA
118
URL.DEST. .INCLUYE EL SUFIJO ADJUNTADOR
NO
SI
126
CAPTURAR LA COOKIE DE APLICACIÓN SELECCIONADA Y RECUPERAR EL SUFIJO ADJUNTADO CORRESPONDIENTE A LA APLICACIÓN SELECCIONADA
128
ADJUNTAR SUFIJO RECUPERADA A LA URL DE DESTINO
130
ENVIAR URL DE DESTINO COMPUESTA A FUNCIÓN DE MAPEO DE PROXY DE PASARELA
132
A APLICACIÓN SELECCIONADA (TAL COMO SE HA MAPEADO)
120
GENERAR LA COOKIE DE APPLICACIÓN SELECCIONADA
122
CREAR CABECERA HTTP CON ID DE LA PASARELA
124
A LA APLICACIÓN SELECCIONADA
116
FIN COMPLEMENTO DE AUT.

Fig. 5

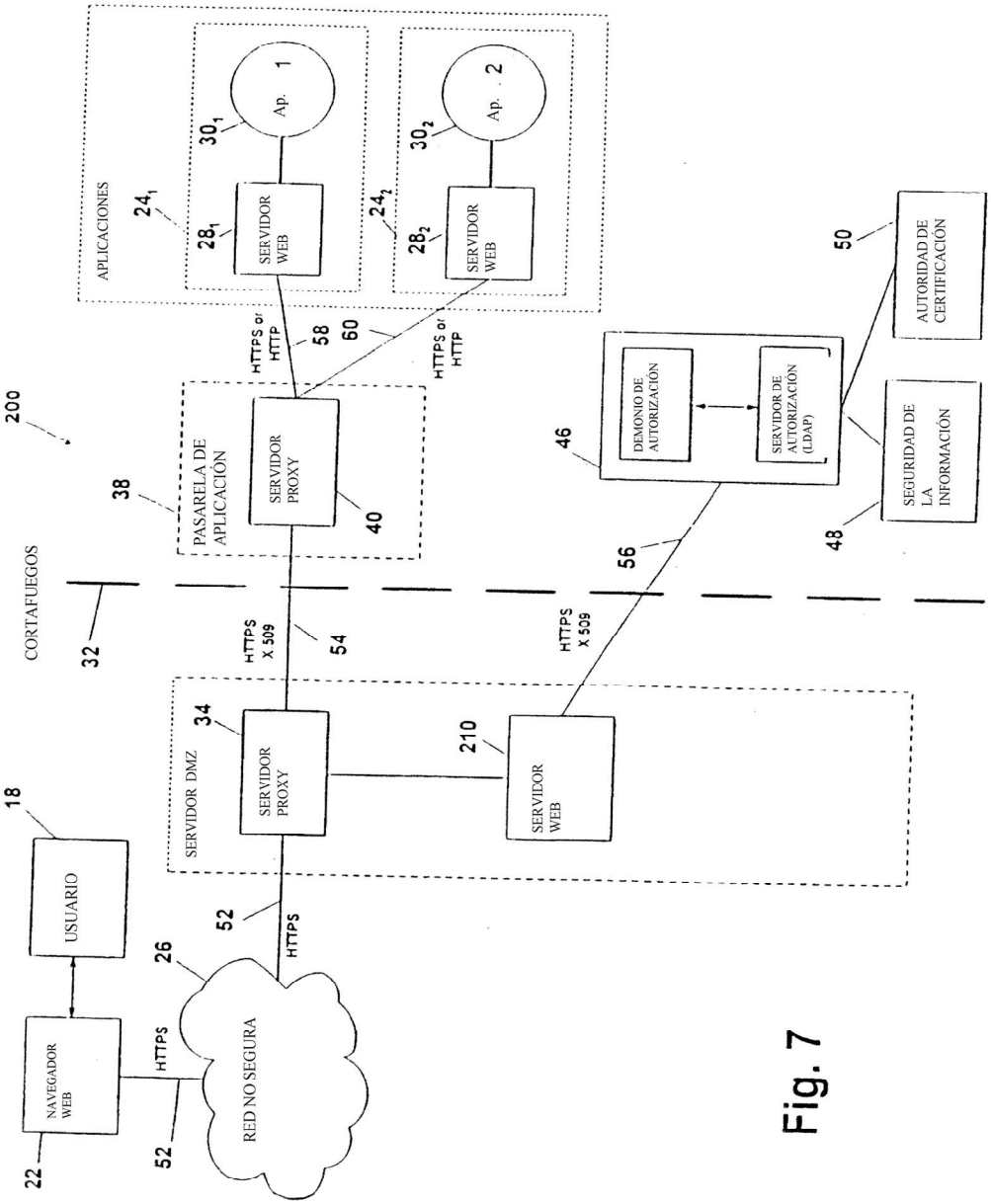
200
APLICACIONES
24 1
24 2
30 1
30 2
Ap. 1
Ap. 2
28 1
28 2
SERVIDOR WEB
SERVIDOR WEB
HTTPS o HTTP
58
60
HTTPS o HTTP
PASARELA DE APLICACIÓN
38
SERVIDOR PROXY
40
46
DEMONIO DE AUTORIZACIÓN
SERVIDOR DE AUTORIZACIÓN (LDAP)
AUTORIDAD DE CERTIFICACIÓN
50
SEGURIDAD DE LA INFORMACIÓN
48
56
CORTAFUEGOS
32
HTTPS X 509
54
HTTPS X 509
SERVIDOR DMZ
34
SERVIDOR PROXY
210
SERVIDOR WEB
18
USUARIO
52
HTTPS
26
RED NO SEGURA
HTTPS
NAVEGADOR WEB
22
52

Fig. 7

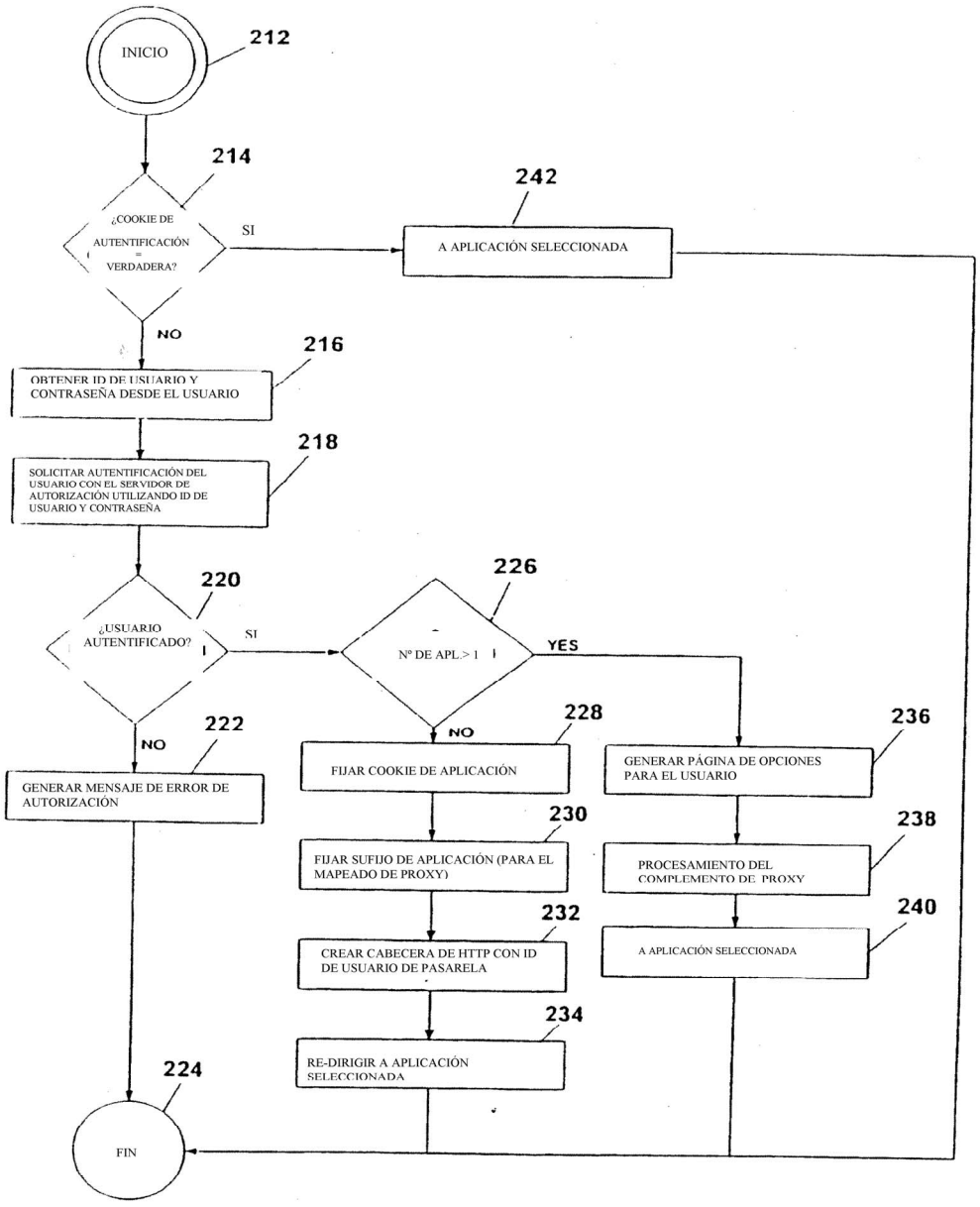
INICIO
212
214
¿COOKIE DE AUTENTIFICACIÓN = VERDADERA?
SI
242
A APLICACIÓN SELECCIONADA
NO
216
OBTENER ID DE USUARIO Y CONTRASEÑA DESDE EL USUARIO
218
SOLICITAR AUTENTIFICACIÓN DEL USUARIO CON EL SERVIDOR DE AUTORIZACIÓN UTILIZANDO ID DE USUARIO Y CONTRASEÑA
220
¿USUARIO AUTENTIFICADO?
SI
226
Nº DE APL. > 1
YES
NO
222
GENERAR MENSAJE DE ERROR DE AUTORIZACIÓN
228
FIJAR COOKIE DE APLICACIÓN
236
GENERAR PÁGINA DE OPCIONES PARA EL USUARIO
230
FIJAR SUFIJO DE APLICACIÓN (PARA EL MAPEADO DE PROXY)
238
PROCESAMIENTO DEL COMPLEMENTO DE PROXY
232
CREAR CABECERA DE HTTP CON ID DE USUARIO DE PASARELA
240
A APLICACIÓN SELECCIONADA
234
RE-DIRIGIR A APLICACIÓN SELECCIONADA
224
FIN

Fig. 8