(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 409 629**

(51) Int. CI.:

H04L 9/00 (2006.01)
G06F 3/00 (2006.01)
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.08.2000 E 00961372 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2013 EP 1216533**

(54) Título: **Control de acceso multi-dominio**

(30) Prioridad:

23.08.1999 US 150392 P
23.03.2000 US 535080

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.06.2013

(73) Titular/es:

ENTRUST, INC. (100.0%)
4975 Preston Park Boulevard, Suite 400
Plano, TX 75093, US

(72) Inventor/es:

SAMPSON, LAWRENCE;
BELMONTE, EMILIO;
FANTI, MARCO y
MEDINA, RAUL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Control de acceso multi-dominio.

SOLICITUD RELACIONADA

Esta solicitud de patente reivindica prioridad de la Solicitud de Patente Provisional de EE.UU. Nº 60/150.392, presentada el 23 de octubre de 1999, titulada Soporte Multi-Dominio en un Sistema de Acceso de Aplicaciones Web, que se incorpora por este medio por referencia en su totalidad.

CAMPO DE LA INVENCIÓN

La presente invención se refiere a la gestión de acceso a recursos accesibles sobre una red.

ANTECEDENTES DE LA INVENCIÓN

Las redes informáticas han llegado a ser ubicuas en la empresa, la industria, y la educación. Las redes tienen uno o más recursos, tales como programas de aplicaciones que proporcionan diversas funciones informáticas, que están disponibles para todos los usuarios. El desarrollo de la red globalmente accesible, de paquetes conmutados conocida como Internet ha permitido que los recursos de red lleguen a estar disponibles en todo el mundo. El desarrollo del protocolo de hipertexto ("HTTP") que implementa la Telaraña Mundial (la "web") permite redes que sirven como plataforma para el comercio electrónico global. En particular, a través de la web una empresa intercambia fácilmente información con sus clientes, suministradores y socios en todo el mundo. Debido a que alguna información intercambiada es valiosa y sensible, el acceso a ella se debería limitar a usuarios seleccionados. De esta manera, hay una necesidad de proporcionar información de acceso selectivo disponible sobre la web.

Un planteamiento para solventar el problema anteriormente mencionado es proteger un conjunto de recursos accesibles sobre la red con un mecanismo de control de acceso. Un mecanismo de control de acceso es una combinación de soporte lógico y componentes físicos configurados para gestionar el acceso a un conjunto de recursos conectados a una red. A menudo, el mecanismo de control de acceso es un programa informático comercial, que se adquiere como un programa informático disponible comercialmente de suministradores de mecanismos de control de acceso. Un recurso es una fuente de información, identificada por un identificador, tal como un localizador de recursos uniforme ("URL") o una dirección del protocolo de Internet ("IP"). Un recurso protegido por un sistema de control de acceso puede ser un archivo estático ("página") que contiene un código conforme al Lenguaje de Marcado de Hipertexto ("HTML") o una página generada dinámicamente creada por programas en base a la Interfaz de Pasarela Común ("CGI"). Ejemplos de recursos incluyen una página web, un sitio web completo, una base de datos habilitada para web, y una mini aplicación.

La FIGURA 1 es un diagrama de bloques que representa una arquitectura de red ejemplar 100 que incluye un sistema protegido por un mecanismo de control de acceso 101. La arquitectura de red ejemplar 100 incluye un navegador 110 acoplado por un enlace de comunicación a una red 102. El bloque mostrado para el navegador 110 representa un terminal, un ordenador de estación de trabajo, o un equivalente que ejecuta un programa de navegador estándar o un equivalente, tal como Netscape, Navigator, Internet Explorer, o NCSA Mosaic. La red 102 es una red de comunicación de información compatible, preferiblemente Internet. En realizaciones alternativas, el navegador 100 es un proceso cliente o una estación de trabajo cliente de cualquier tipo conveniente, y la red 102 es una red de comunicación de datos que puede transferir información entre el cliente y un servidor que también está acoplado a la red.

El término servidor se usa aquí para referirse a uno o más elementos de soporte lógico o componentes físicos informáticos que están dedicados a proporcionar las funciones requeridas ("servicios") en nombre de clientes que transmiten las peticiones. Un servidor puede ser un módulo de soporte lógico que se puede invocar por y ejecutar por un proceso cliente, un proceso separado que recibe peticiones de otros procesos cliente que ejecutan el mismo sistema informático, o un conjunto de procesos que se ejecutan en un conjunto de ordenadores, donde los procesos responden a las peticiones mediante clientes que se ejecutan en otros ordenadores.

El sistema de control de acceso 190 está acoplado a la red 102 y suministra servicios usados para gestionar acceso a servidores protegidos 150, incluyendo autentificación de usuarios y servicios de verificación, de una manera que se describirá más tarde en mayor detalle. Los servidores protegidos 150 también están acoplados a la red 102 y suministran uno o más recursos.

Antes de que un usuario pueda acceder a un recurso de los servidores protegidos 150, el usuario debe primero registrarse en el sistema de control de acceso 190, suministrando información al sistema de control de acceso 190 usada para autentificar al usuario. Los usuarios pueden registrarse o bien con un certificado digital transmitido al sistema de control de acceso 190 o bien abriendo una página de registro suministrada por el sistema de control de acceso 190 con el navegador 110 e introduciendo un nombre y una contraseña. Una vez que el usuario es autentificado, se asocia una sesión autentificada con el usuario, y el usuario puede acceder entonces a uno o más recursos en los servidores protegidos durante la vida de la sesión autentificada.

Para este propósito, el sistema de control de acceso 190 transmite uno o más datos de identificación, por ejemplo, chivatos, al navegador 110 que se usan, al menos en parte, por un servidor protegido para verificar que el usuario ha sido autentificado. Los chivatos son piezas de información que un servidor puede crear y transmitir a un navegador, para hacer al navegador almacenar el chivato y retransmitirlo en peticiones posteriores a los servidores. Un chivato se puede asociar con un nombre de dominio usado para identificar la dirección IP de un servidor. Un nombre de dominio es un identificador que identifica un conjunto o una o más direcciones IP. Ejemplos de nombres de dominio son 'enCommerce.com' o 'uspto.gov'. Un navegador transmite un chivato en conjunto con una petición al servidor para acceder a un recurso, transmitiendo los chivatos como parte de la petición. Los chivatos transmitidos están asociados con el nombre de dominio del servidor.

Se puede usar un nombre de dominio en una dirección que identifica un recurso, tal como un URL. Por ejemplo, se puede usar un dominio para identificar recursos "sample1File.htm" y "sample2File.htm", usando el URL "www.demoDomain/sample2File.htm", donde 'demoDomain' es el nombre de dominio. El nombre de dominio corresponde a la dirección IP de un servidor que puede suministrar un recurso.

Un dominio es un conjunto de recursos que puede ser identificado por el nombre de dominio. De esta manera, 'sample1File.htm' 'sample2File.htm' son recursos que pertenecen al mismo dominio. El proceso de acceder a un recurso a través de una petición que identifica el recurso usando un nombre de dominio se conoce como acceder al dominio.

Cuando un servidor protegido recibe una petición para acceso desde un cliente que ha sido autentificado, el servidor protegido recibe unos "chivatos de control de acceso" para el dominio del servidor. Los chivatos de control de acceso pueden contener información usada para verificar que un usuario ha sido autentificado, y pueden contener datos que especifican los privilegios del usuario. Un privilegio es un derecho para acceder a un recurso particular. Los chivatos de control de acceso típicamente están cifrados para propósitos de seguridad.

Una desventaja principal para un sistema de control de acceso convencional es que solamente controla el acceso a un conjunto de servidores y recursos que pertenecen a un dominio. La razón subyacente para esta limitación es la siguiente. Cuando un sistema de control de acceso convencional suministra unos chivatos de control de acceso a un usuario que acaba de ser autentificado, los chivatos transmitidos se asocian con el dominio del sistema de control de acceso. Cuando el navegador requiere acceso a otro recurso en otro dominio, los chivatos de control de acceso no se transmiten debido a que están asociados con otro dominio. De esta manera, cada nombre de dominio usado para desplegar un conjunto de servidores o recursos requiere su propia implementación y el mantenimiento de un sistema de control de acceso, añadiendo el coste de asegurar recursos accesibles sobre una red. Además, para cada nombre de dominio un usuario debe registrarse. De esta manera, el usuario se puede sobrecargar por procedimientos de registro repetitivos, o el número de nombres de dominio que se pueden usar son limitados por los esfuerzos para evitar sobrecargar al usuario.

En base a lo anteriormente mencionado, es claramente deseable proporcionar un sistema de control de acceso que se pueda usar para gestionar el acceso a un conjunto de recursos desplegados bajo múltiples nombres de dominio, en particular, requiere que un usuario se registre sólo una vez para acceder al conjunto de recursos.

SUMARIO DE LA INVENCIÓN

La GB-A-2326802 describe un método para controlar el acceso a un recurso protegido por un sistema de control de acceso que usa la información de control de acceso transmitida en conjunto con las peticiones para acceder al recurso para determinar si se puede permitir el acceso, el método que comprende generar un ID de sesión y almacenar el ID en una base de datos. Después de una verificación inicial, las verificaciones posteriores se realizan por el servidor contactando con un controlador para verificar la validez del ID de la sesión.

Se describe un mecanismo que usa un sistema de control de acceso único para gestionar el acceso por los usuarios a los recursos que pertenecen a múltiples dominios. En una realización, se asocia un servidor con cada dominio en un conjunto de dominios. El acceso a los recursos en los dominios está gobernado por un sistema de control de acceso. Un primer servidor para un primer dominio transmite un testigo de datos a un cliente que busca acceso a un recurso en un segundo dominio. El cliente transmite el testigo de datos a un segundo servidor en el otro dominio. El segundo servidor usa el testigo de datos para verificar que el usuario está autorizado para acceder a los recursos protegidos por el sistema de control de acceso. Una vez se determina que el usuario está autorizado para acceder a los recursos, los "chivatos" de control de acceso se transmiten al cliente.

Según otra realización de la presente invención, cuando el cliente requiere acceso a un recurso en el segundo dominio, y la petición no incluye chivatos de control de acceso para el segundo dominio, los datos se transmiten al navegador haciéndolo generar otra petición al primer servidor. El primer servidor asegura que el usuario se ha autentificado antes de transmitir el testigo de datos al navegador. Además, el primer servidor puede hacer copias de los chivatos de control de acceso para el usuario a ser almacenados para transmisión posterior al segundo servidor.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención se ilustra a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos anexos y en los cuales números de referencia iguales se refieren a elementos similares y en los cuales:

La FIGURA 1 es un diagrama de bloques que representa una red ejemplar, unos recursos acoplados a la red, y un sistema de control de acceso usado para gestionar el acceso a los recursos;
La FIGURA 2 es un diagrama de bloques que representa una red ejemplar, unos recursos acoplados a la red, y un sistema de control de acceso usado para gestionar el acceso a los recursos en múltiples dominios;
La FIGURA 3A es un diagrama de flujo que representa un proceso usado para gestionar el acceso a recursos en múltiples dominios;
La FIGURA 3B es un diagrama de flujo que representa un proceso usado para gestionar el acceso a recursos en múltiples dominios;
La FIGURA 4A es un diagrama de flujo que representa un proceso usado para gestionar el acceso a recursos en múltiples dominios;
La FIGURA 4B es un diagrama de flujo que representa un proceso usado para gestionar el acceso a recursos en múltiples dominios; y
La FIGURA 5 es un diagrama de bloques de un sistema informático que se puede usar para implementar una realización.

DESCRIPCIÓN DETALLADA DE LA REALIZACIÓN PREFERIDA

Se describe un método y aparato para un sistema de control de acceso multi-dominio. En la siguiente descripción, para los propósitos de explicación, se establecen en adelante numerosos detalles específicos para proporcionar una comprensión minuciosa de la presente invención. Será evidente, no obstante, para un experto en la técnica que la presente invención se puede poner en práctica sin estos detalles específicos. En otros ejemplos, se muestran unas estructuras y dispositivos bien conocidos en forma de diagrama de bloques para evitar oscurecer innecesariamente la presente invención.

La FIGURA 2 es un diagrama de bloques que representa la arquitectura de red ejemplar 200, una arquitectura que incorpora un sistema de control de acceso multi-dominio. Un sistema de control de acceso multi-dominio permite a un usuario acceder a múltiples dominios pero solamente requiere al usuario registrarse una vez para conseguir el acceso. Los dominios protegidos por un sistema de control de acceso multi-dominio se conocen en la presente memoria como dominios de confianza con respecto al sistema de control de acceso multi-dominio.

La arquitectura de red ejemplar 200 incluye los navegadores 210, cada uno de los cuales está acoplado por un enlace de comunicación a una red 202. Los bloques mostrados para los navegadores 210 pueden representar un terminal, ordenador de estación de trabajo, o un equivalente que ejecuta un programa de navegador Web estándar o un equivalente, tal como Netscape Communicator o, Internet Explorer. Los usuarios 212 interactúan con los navegadores 210 para acceder a los recursos a través de la red 202. La red 102 es una red comunicación de información compatible, preferiblemente Internet. En realizaciones alternativas, un navegador 210 es un proceso cliente o estación de trabajo cliente de cualquier tipo conveniente, y la red 202 es una red de comunicación de datos que puede transferir información entre el cliente y un servidor que también está acoplado a la red.

Los navegadores 210 transmiten peticiones para recursos (“petición de recursos”) a los servidores protegidos 205, que transmiten el recurso requerido siempre que el usuario que inicia la petición a través de un navegador 210 se haya autentificado mediante un sistema de control de acceso 220. Las peticiones se pueden ajustar, y responder, de una manera que se ajuste a HTTP. Los servidores protegidos 205, que incluyen los servidores protegidos 240, 260, 280, pueden ser servidores Web. En la determinación de quién ha sido autentificado, los servidores protegidos 205 y los recursos puestos a disposición por los recursos protegidos 205 pueden usar uno o más servicios del sistema de control de acceso 220.

Cada uno de los recursos protegidos 205 se puede direccionar mediante un nombre de dominio. De esta manera, cada uno de los recursos protegidos 205 y los recursos a los que se puede acceder a través de los servidores pertenecen a un dominio. El Servidor Protegido 240 y los recursos 248 y 249 pertenecen al Dominio Primario 241, el Servidor Protegido 260 y los recursos 268 y 269 pertenecen al Agente de Dominio Secundario 262, y el Servidor Protegido 280 y los recursos 288 y 289 pertenecen al Dominio Secundario 282. Los dominios representados en la FIGURA 2 están etiquetados dominio y secundario por razones que se explicarán en mayor detalle.

Para determinar si un usuario está autorizado para acceder al recurso, un servidor protegido 205 usa chivatos de control de acceso, que transmiten información derivada de ellos al sistema de control de acceso 220. Los chivatos de control de acceso pueden contener datos cifrados que especifican la información usada para verificar que el usuario es auténtico. El servidor protegido 205 puede derivar información a partir de los chivatos, y entonces transmitir una petición al sistema de control de acceso 120 para verificar si el usuario está autorizado, pasando la información derivada a partir de los chivatos, así como el recurso requerido. A continuación, el sistema de control de acceso 120 responde transmitiendo de vuelta un mensaje que especifica si el usuario está o no autorizado para acceder al recurso o cualquier otro recurso.

COMPONENTES PARA PROPORCIONAR ACCESO MULTI-DOMINIO

Para proporcionar acceso multi-dominio, se crea y almacena una información de control de acceso. Cuando un usuario se autentifica primero, un navegador recibe un conjunto de chivatos de control de acceso asociados con un dominio particular desde el que se transmiten los chivatos. Posteriormente, el usuario puede requerir acceso a otro dominio protegido mediante el sistema de control de acceso 220. Por lo tanto, cuando el navegador transmite la petición a un servidor web que pertenece al otro dominio, no se transmiten los chivatos de control de acceso para el usuario. Un mecanismo verifica si un usuario se ha autentificado sin tener que recibir chivatos de control de acceso o hacer al usuario registrarse de nuevo.

Tal mecanismo se proporciona mediante los siguientes componentes del sistema de control de acceso 220: el Agente de Dominio Primario 242, los Agentes de Dominio Secundario 262 y 282, y el Servidor de Testigo Multi-Dominio 208. Estos elementos pueden ser servidores que cooperan uno con otro para proporcionar un sistema de control de acceso multi-dominio, que usa una variedad de técnicas que se describirán más tarde en mayor detalle.

Aunque cada técnica es diferente, hay aspectos de las funciones desempeñadas en cada una por un componente que siguen siendo los mismos. Además, diferentes componentes, o unos pocos componentes, que llevan a cabo las mismas funciones, son equivalentes y se pueden usar. Por lo tanto es útil describir la función que cada componente desempeña proporcionando una visión general de un proceso multi-dominio, como sigue.

Generalmente, en una realización, cuando un navegador transmite una petición a un servidor protegido en nombre de un usuario para acceder a un recurso en un dominio, y el navegador no transmite ningún chivato de control de acceso para el dominio, el navegador se conecta al agente de dominio secundario que pertenece al dominio. El agente de dominio secundario hace al navegador conectarse con el Agente de Dominio Primario 242. Si el usuario se ha autentificado, entonces el Agente de Dominio Primario 242 transmite al Servidor de Testigo Multi-Dominio 208 una petición para un “Testigo Multi-Dominio.” Un Testigo Multi-Dominio es un elemento de datos cifrado usado para verificar que el usuario se ha autentificado mediante el Sistema de Control de Acceso 220, y se explicará en mayor detalle. El Servidor de Testigo Multi-Dominio 208 genera un Testigo Multi-Dominio y lo suministra al Agente de Dominio Primario 242.

El Agente de Dominio Primario 242 transmite el Testigo Multi-Dominio al navegador, y hace al navegador conectarse al Agente de Dominio Secundario. Cuando el navegador conecta con el Agente de Dominio Secundario, el navegador transmite un Testigo Multi-Dominio al Agente de Dominio Secundario. El Agente de Dominio Secundario entonces transmite al Servidor de Testigo Multi-Dominio 208 una petición para verificar que el Testigo Multi-Dominio representa a un usuario que se ha autentificado por el sistema de control de acceso 220. Tras recibir desde el Servidor de Testigo Multi-Dominio 208 un mensaje que confirma que el usuario se ha autentificado, el Agente de Dominio Secundario transmite al navegador los chivatos de control de acceso que están asociados con el dominio del Agente de Dominio Secundario.

El Servidor de Testigo Multi-Dominio 208 incluye diversas funciones API para soportar el control multi-dominio. Éstas incluyen funciones para crear un Testigo Multi-Dominio, verificar un Testigo Multi-Dominio, almacenar y obtener datos para los chivatos de control de acceso asociados con un dominio particular, y añadir un dominio de confianza. Una lista de dominios de confianza se mantiene por el Servidor de Testigo Multi-Dominio 208.

El Servidor de Testigo Multi-Dominio 208 verifica que un Testigo Multi-Dominio fue expedido desde el Servidor de Testigo Multi-Dominio 208 a través del uso de tecnología de cifrado. Debido a que los Testigos Multi-Dominio se expiden solamente para usuarios autentificados, se puede suponer que un navegador que presenta un Testigo Multi-Dominio ha sido autentificado.

En una realización preferida, el tamaño del un Servidor de Testigo Multi-Dominio 208 se hace lo bastante pequeño de manera que pueda ser transportado como parte de la cadena de URL en una petición HTTP. La cadena de URL son datos transmitidos como parte de una petición de recursos, y se transmite con independencia del dominio al cual se requiere acceso. La cadena de URL contiene datos que especifican el URL, y puede contener otros datos, tales como parámetros en forma de parejas de nombre-valor. La cantidad de datos que se puede incluir en una cadena de URL es limitada. Debido a que la cadena de URL se transmite siempre en una petición de recursos, cuando se incluye un Testigo Multi-Dominio en una cadena de URL, se transmitirá. Si el Testigo Multi-Dominio fuera incluido en un chivato, solamente se transportaría en una petición de acceso al dominio asociado con el chivato.

En una realización, los servidores protegidos 205 y el sistema de control de acceso 220 se almacenan en y ejecutan por un servidor u ordenador físico. En realizaciones alternativas, uno o más de estos componentes están distribuidos en ordenadores separados; este planteamiento puede mejorar la seguridad y el rendimiento. Por ejemplo, cada uno de los servidores protegidos 205 se puede instalar en o ejecutar por ordenadores separados. El Agente de Dominio Primario 242 y los Agentes de Dominio Secundarios 262 y 282 se pueden instalar en el mismo ordenador como servidores protegidos 240, 260, 280 respectivamente. Cada uno de los servidores protegidos 205 y el Agente de Dominio Secundario y otros diversos componentes del controlador de Acceso 220 se pueden situar en una extranet para acceso por usuarios externos. El Servidor de Testigo Multi-Dominio 208 se puede acoplar a una Intranet segura que está protegida usando un cortafuegos.

Para que un Agente de Dominio Secundario realice su función, debe estar accesible a los usuarios para quienes no se puede proporcionar los chivatos de control de acceso autentificados. Por consiguiente, los Agentes de Dominio Secundarios 262 y 282 no están protegidos por el sistema de control de acceso 120. Por otra parte, el Agente de Dominio Primario 242 está inherentemente protegido. Debido a que está protegido, cualquier navegador que intente acceder al Agente de Dominio Primario 242 debe transmitir unos chivatos de control de acceso que muestren que el usuario es auténtico. Si el navegador no presenta tales chivatos de control de acceso, se pueden obtener realizando procedimientos de registro.

El Agente de Dominio Primario 242, los Agentes de Dominio Secundarios 262 y 282, y el Servidor de Testigo Multi-Dominio 208 se pueden implementar usando una variedad de tecnologías de soporte lógico. Por ejemplo, el Agente de Dominio Primario 242, los Agentes de Dominio Secundarios 262 y 282 se pueden escribir como secuencias de comandos CGI, API de Servidor Netscape, complementos API de Servidor de Internet. El Servidor de Testigo Multi-Dominio 208 se puede escribir usando soporte lógico usado para generar módulos y objetos compatibles con CORBA.

CONTROL DE ACCESO MULTI-DOMINIO

La FIGURA 3A, la FIGURA 3B, la FIGURA 4A, y la FIGURA 4B son diagramas de flujo que representan, en parte, una realización de un proceso para implementar un sistema de control de acceso multi-dominio. Los pasos se ilustran usando la arquitectura de red ejemplar en la FIGURA 2. En la ilustración, los clientes comunican usando el protocolo HTTP. No obstante, se puede usar cualquier versión de HTTP, o cualquier otro protocolo de comunicación adecuado.

Con referencia a la FIGURA 3A, en el paso 310, el navegador 210-1 transmite una petición de recursos al servidor protegido 260 para el recurso 268, un recurso protegido. Un recurso protegido es un recurso al que solamente se puede acceder por usuarios autentificados por el sistema de control de acceso 220. En la transmisión de la petición de recursos, el navegador 210-1 no transmitió ningún chivato de control de acceso para el dominio del recurso 268, es decir, el dominio secundario 261, que en la presente memoria se conoce como el dominio requerido.

En el paso 314, el servidor protegido 260 determina si los chivatos de control de acceso para el dominio requerido se transmitieron o no al servidor protegido 260 como parte de la petición de recursos transmitida en el paso 310. Si los chivatos de control de acceso fueron recibidos, entonces los pasos mostrados en la FIGURA 3A finalizan. Cuando los pasos en las FIGURA 3A – 4B se describen como que finalizan, alternativamente, puede ocurrir otro procesamiento. Este procesamiento puede incluir, por ejemplo, operaciones para verificar que los chivatos de control de acceso representan un usuario auténtico y proporcionar acceso al recurso requerido, u operaciones para denegar acceso al recurso requerido. El procesamiento adicional que ocurre puede depender de dónde finalizan los pasos en el proceso representado en las FIGURA 3 – FIGURA 4B.

Si por otra parte, en el paso 314, el servidor protegido 260 determina que los chivatos de control de acceso para el dominio requerido no se han transmitido, entonces la ejecución pasa al paso 318.

En el paso 318, el servidor protegido 260 redirige el navegador 210-1 a un Agente de Dominio Secundario, por ejemplo, el Agente de Dominio Secundario 262. El término redirigir se refiere a transmitir una redirección a un navegador, que son datos que hacen al navegador generar otra petición de acceso a otro recurso especificado en la redirección. La redirección puede especificar parámetros y valores de parámetros para pasar junto con una petición dirigida al otro recurso. Por ejemplo, la redirección se puede consumar transmitiendo una página con una etiqueta de redirección HTML. La etiqueta incluye datos que especifican el URL del Agente de Dominio Secundario 262. La etiqueta también puede incluir valores de parámetros en forma de, por ejemplo parejas de valor de nombre que se pasan con la petición dirigida.

En el paso 322, el Agente de Dominio Secundario 262 recibe la petición dirigida desde el navegador 210-1. En respuesta, en el paso 324, el Agente de Dominio Secundario redirige el navegador 210-1 al Agente de Dominio Primario 242. La redirección especifica los valores del parámetro para pasar como parte de la petición dirigida al Agente de Dominio Primario 242. En una realización preferida, estos parámetros se conocen en la presente memoria como ORIGINATING_SDA, y pueden incluir lo siguiente.

1. El recurso requerido originalmente.
2. El dominio requerido, es decir, el dominio del recurso requerido originalmente.
3. El Agente de Dominio Secundario.

Los parámetros pueden comprender identificar información, por ejemplo, los URL o las direcciones IP.

Con referencia a la FIGURA 3B, en el paso 328, el Agente de Dominio Primario 242 recibe la petición dirigida iniciada en el paso 324.

En el paso 330, el Agente de Dominio Primario 242 determina si los chivatos de control de acceso para su dominio se han transmitido con la petición dirigida recibida en el paso 328. Si no, entonces el control pasa al paso 332, donde se determina si el usuario es auténtico. El paso puede incluir diversos procesos para autentificar usuarios, incluyendo autentificación de usuario/contraseña, o uso de certificados digitales. Si el usuario no es auténtico, entonces la ejecución de los pasos finaliza. De otro modo, el control fluye al paso 336, donde los chivatos de control de acceso para el dominio del Agente de Dominio Primario 242, el dominio 241, se transmiten al navegador 210-1. En el paso 338, el navegador se redirige al Agente de Dominio Primario 242. En el paso 328, el Agente de Dominio Primario 242 recibe la petición dirigida, que incluye los chivatos de control de acceso. En el paso 330, el Agente de Dominio Primario 242 determina que los chivatos de control de acceso para su dominio se han transmitido como parte de la petición dirigida.

Con referencia a la FIGURA 4A, en el paso 410, el Agente de Dominio Primario 242 determina si el dominio requerido, según se especifica en ORIGINATING_SMDA, es o no un dominio de confianza. Para realizar esta determinación, el Agente de Dominio Primario 242 puede invocar una función API del Servidor de Testigo Multi-Dominio 208. Si el Agente de Dominio Primario 242 determina que el dominio requerido no es un dominio de confianza, entonces la ejecución de los pasos finaliza. De otro modo, la ejecución de los pasos pasa al paso 414.

En el paso 414, el Agente de Dominio Primario 242 transmite copias de los chivatos de control de acceso recibidos en el paso 328 al Servidor de Testigo Multi-Dominio 208.

En el paso 418, el Servidor de Testigo Multi-Dominio 208 recibe los chivatos y los almacena en memoria caché. Se pueden almacenar aquí durante periodo de tiempo configurable.

En el paso 422, el Servidor de Testigo Multi-Dominio 208 genera un Testigo Multi-Dominio y lo transmite al Agente de Dominio Primario 242. El Testigo Multi-Dominio puede tener una variedad de elementos de datos. Por ejemplo, puede incluir (1) datos que identifican la copia de los chivatos almacenados en el Servidor de Testigo Multi-Dominio 208 según el paso 418 (“ID del Conjunto de Chivatos”), (2) el URL original del recurso requerido originalmente, y (3) un valor de generación de claves en base a los dos elementos previos. Un Testigo Multi-Dominio no está limitado a contener cualquier conjunto particular de elementos de datos y otra información equivalente se puede usar.

En el paso 424, el Agente de Dominio Primario 242 redirige el navegador 210-1 al Agente de Dominio Secundario 262, transmitiendo el Testigo Multi-Dominio.

Con referencia a la FIGURA 4B, en el paso 428, el Agente de Dominio Secundario 262 recibe la petición dirigida, incluyendo el Testigo Multi-Dominio.

En el paso 432, para verificar el Testigo Multi-Dominio, el Agente de Dominio Secundario 262 transmite el Testigo Multi-Dominio al Servidor de Testigo Multi-Dominio 208.

En el paso 436, el Servidor de Testigo Multi-Dominio 208 determinar si es auténtico o no el Testigo Multi-Dominio, es decir, si se ha expedido por un Servidor de Testigo Multi-Dominio 208 para un usuario auténtico. El proceso de hacer esta determinación implica descifrar el testigo. Si el Testigo Multi-Dominio no es auténtico, entonces la ejecución de los pasos finaliza. De otro modo, el control fluye al paso 440.

En el paso 440, los chivatos de control de acceso almacenados previamente, que se identifican por Cookie_Set_Id, se transmiten al Agente de Dominio Secundario. Ya no es necesario almacenar en memoria caché los chivatos de control de acceso. En el paso 444, el Agente de Dominio Secundario 262 redirige el navegador 210-1 al recurso requerido originalmente, transmitiendo los chivatos de control de acceso al navegador 210-1.

En el paso 448, el navegador 210-1 transmite la petición dirigida, solicitando el recurso requerido originalmente. Como resultado del navegador que recibe los chivatos de control de acceso transmitidos a él por el agente de dominio secundario 262 en el paso 444, la petición de redirección transmitida por el navegador 210-1 incluye los chivatos de control de acceso. Consecuentemente, el navegador 210-1 puede acceder al recurso requerido originalmente, suponiendo que los chivatos de control de acceso especifican suficientes privilegios.

CONTROL DE ACCESO MULTI-DOMINIO ALTERNATIVO

En el paso 414, el Agente de Dominio Primario 242 transmite copias de los chivatos de control de acceso recibidos en el paso 328 al Servidor de Testigo Multi-Dominio 208, que hace al Servidor de Testigo Multi-Dominio 208 almacenar los chivatos de control de acceso en memoria caché hasta que se requieren más tarde por un Agente de Dominio Secundario. Más que transportar los chivatos de control de acceso al Agente de Dominio Secundario de esta manera, se pueden transportar a través del Testigo Multi-Dominio. Por supuesto el Testigo Multi-Dominio está limitado en tamaño, y no es capaz de mantener la cantidad de datos que se pueden almacenar en el chivato y que se pueden necesitar para privilegios de control de acceso.

Después de que el navegador 210-1 recibe los chivatos de control de acceso a través de un Agente de Dominio Secundario 260, el navegador 210-1 puede requerir un recurso en otro dominio de confianza. Si el navegador no

está almacenando los chivatos de control de acceso para este dominio, entonces no se transmitirán chivatos de control de acceso con la petición para acceder al recurso en el otro dominio de confianza. Consecuentemente, los pasos mostrados en las FIGURA 3A y las FIGURA 4B se vuelven a ejecutar, y estos pasos pueden llegar a ser un ciclo que se repite cada vez que se accede a otro dominio de confianza.

La repetición de los pasos mostrados en las FIGURA 3A – 4B se puede evitar modificando el proceso representado como sigue. En el paso 444, más que redirigir el navegador al recurso requerido originalmente, el Agente de Dominio Secundario redirige el navegador a otro Agente de Dominio Secundario, transmitiendo el Testigo Multi-Dominio con la petición de redirección. Después de verificar el Testigo Multi-Dominio, el otro Agente de Dominio Secundario redirige el navegador aún a otro Agente de Dominio Secundario en otro dominio de confianza, transmitiendo los chivatos de control de acceso al navegador y el Testigo Multi-Dominio al navegador. Este proceso se repite hasta que el navegador recibe los chivatos de control de acceso para todos los dominios de confianza, en cuyo punto el navegador se redirige al recurso requerido originalmente.

Para propósitos de eficiencia y manejo de fallos, puede ser deseable ejecutar réplicas de Servidores de Testigo Multi-Dominio. Los chivatos de control de acceso se podrían replicar en cada réplica de Servidor de Testigo Multi-Dominio. De esta manera, cuando un Servidor de Testigo Multi-Dominio recibe una petición para almacenar los chivatos de control de acceso, los almacena y comunica a las otras réplicas del Servidor de Testigo Multi-Dominio. Consecuentemente, para propósitos de recuperación de los chivatos de control de acceso, un Agente de Dominio secundario puede requerir una copia de un conjunto de chivatos de control de acceso desde cualquier réplica.

Para evitar replicar los chivatos de control de acceso en todas las réplicas de un Servidor de Testigo Multi-Dominio, se almacenaría solamente un conjunto de chivatos de control de acceso para un usuario en una réplica. Específicamente, en respuesta a una petición de almacenar copias de chivatos de control de acceso, una réplica de Servidor de Testigo Multi-Dominio genera un Testigo Multi-Dominio que incluye un Id de Réplica que identifica el Servidor de Testigo Multi-Dominio. Un Agente de Dominio Secundario requiere chivatos de control de acceso del Servidor de Testigo Multi-Dominio identificados por un Testigo Multi-Dominio.

Si una réplica falla, un Agente de Dominio Secundario redirige los navegadores que presentan un Testigo Multi-Dominio que identifica el Servidor de Testigo Multi-Dominio 208 fallado al Agente de Dominio Primario 242. Esta redirección puede conducir eventualmente a generar y almacenar otro conjunto de chivatos de control de acceso en una réplica de Servidor de Testigo Multi-Dominio en funcionamiento, y la generación de otro Testigo Multi-Dominio que identifica el Servidor de Testigo Multi-Dominio en funcionamiento.

VISIÓN GENERAL DE LOS COMPONENTES FÍSICOS

La FIGURA 5 es un diagrama de bloques que ilustra un sistema informático 500 sobre el cual se puede implementar una realización de la invención. El sistema informático 500 incluye un canal principal 502 u otro mecanismo de comunicación para comunicar información, y un procesador 504 acoplado con el canal principal 502 para el procesamiento de la información. El sistema informático 500 también incluye una memoria principal 506, tal como una memoria de acceso aleatorio (RAM) u otro dispositivo de almacenamiento dinámico, acoplado al canal principal 502 para almacenar la información y las instrucciones a ser ejecutadas por el procesador 504. La memoria principal 506 también se puede usar para almacenar variables temporales u otra información intermedia durante la ejecución de instrucciones a ser ejecutadas por el procesador 504. El sistema informático 500 además incluye una memoria sólo de lectura (ROM) 508 u otro dispositivo de almacenamiento estático acoplado al canal principal 502 para almacenar información estática e instrucciones para el procesador 504. Un dispositivo de almacenamiento 510, tal como un disco magnético o disco óptico, se proporciona y acopla al canal principal 502 para almacenar la información y las instrucciones.

El sistema informático 500 se puede acoplar a través del canal principal 502 a un visualizador 512, tal como un tubo de rayos catódicos (CRT), para visualizar información para un usuario del ordenador. Un dispositivo de entrada 514, que incluye teclas alfanuméricas y otras, está acoplado al canal principal 502 para comunicar la información y las selecciones de comandos al procesador 504. Otro tipo de dispositivo de entrada de usuario es el control de cursor 516, tal como un ratón, bola de apuntamiento, o teclas de dirección de cursor para comunicar la información de dirección y las selecciones de comando al procesador 504 y para controlar el movimiento del cursor sobre el visualizador 512. Este dispositivo de entrada típicamente tiene dos grados de libertad en dos ejes, un primer eje (por ejemplo, x) y un segundo eje (por ejemplo, y), que permite al dispositivo especificar las posiciones en un plano.

La invención está relacionada con el uso del sistema informático 500 para implementar las técnicas descritas en la presente memoria. Según una realización de la invención, esas técnicas se implementan por el sistema informático 500 en respuesta al procesador 504 que ejecuta una o más secuencias de una o más instrucciones contenidas en la memoria principal 506. Tales instrucciones se pueden leer en la memoria principal 506 desde otro medio legible por ordenador, tal como el dispositivo de almacenamiento 510. La ejecución de las secuencias de instrucciones contenidas en la memoria principal 506 hace al procesador 504 realizar los pasos del proceso descritos en la presente memoria. En realizaciones alternativas, se puede usar una circuitos cableados en lugar de o en combinación con instrucciones de soporte lógico para implementar la invención. De esta manera, las realizaciones

de la invención no están limitadas a cualquier combinación específica de circuitos de componentes físicos y soporte lógico.

El término “medio legible por ordenador” como se usa en la presente memoria se refiere a cualquier medio que participa en proporcionar instrucciones al procesador 504 para la ejecución. Tal medio puede tomar muchas formas, incluyendo pero no limitadas a, medios no volátiles, medios volátiles, y medios de transmisión. Los medios no volátiles incluyen, por ejemplo, discos ópticos o magnéticos, tales como el dispositivo de almacenamiento 510. Los medios volátiles incluyen una memoria dinámica, tal como la memoria principal 506. Los medios de transmisión incluyen cables coaxiales, hilos de cobre y fibras ópticas, incluyendo los hilos que comprenden el canal principal 502. Los medios de transmisión también pueden tomar la forma de ondas acústicas o luminosas, tales como aquéllas generadas durante las comunicaciones de datos de ondas de radio e infrarrojos.

Las formas comunes de medios legibles por ordenador incluyen, por ejemplo, un disquete, un disco flexible, un disco duro, cinta magnética, o cualquier otro medio magnético, un CD-ROM, cualquier otro medio óptico, tarjetas perforadas, cinta de papel, y cualquier otro medio físico con patrones de agujeros, una RAM, una PROM, y EPROM, una FLASH-EPROM, cualquier otro circuito integrado o cartucho de memoria, una onda portadora como se describe en lo sucesivo, o cualquier otro medio desde el cual puede leer un ordenador.

Se pueden implicar diversas formas de medios legibles por ordenador en transportar una o más secuencias de una o más instrucciones al procesador 504 para la ejecución. Por ejemplo, las instrucciones se pueden llevar a cabo inicialmente en un disco magnético de un ordenador remoto. El ordenador remoto puede cargar las instrucciones en su memoria dinámica y enviar las instrucciones sobre una línea de teléfono usando un módem. Un módem local para el sistema informático 500 puede recibir los datos en la línea de teléfono y usar el transmisor de infrarrojos para convertir los datos a una señal de infrarrojos. Un detector de infrarrojos puede recibir los datos transportados en la señal de infrarrojos y los circuitos adecuados pueden situar los datos en el canal principal 502. El canal principal 502 transporta los datos a la memoria principal 506, desde la que el procesador 504 recupera y ejecuta las instrucciones. Las instrucciones recibidas por la memoria principal 506 se puede almacenar de manera opcional en el dispositivo de almacenamiento 510 o bien antes o bien después de la ejecución por el procesador 504.

El sistema informático 500 también incluye una interfaz de comunicación 518 acoplada al canal principal 502. La interfaz de comunicación 518 proporciona una comunicación de datos de dos vías que se acopla a un enlace de red 520 que está conectado a una red local 522. Por ejemplo, la interfaz de comunicación 518 puede ser una tarjeta de red digital de servicios integrados (ISDN) o un módem para proporcionar una conexión de comunicación de datos a un tipo correspondiente de línea de teléfono. Según otro ejemplo, la interfaz de comunicación 518 puede ser una tarjeta de red de área local (LAN) para proporcionar conexión de comunicación de datos a una LAN compatible. También se pueden implementar enlaces inalámbricos. En cualquier implementación tal, la interfaz de comunicación 518 envía y recibe señales eléctricas, electromagnéticas u ópticas que transportan secuencias de datos digitales que representan diversos tipos de información.

El enlace de red 520 típicamente proporciona comunicación de datos a través de una o más redes a otros dispositivos de datos. Por ejemplo, el enlace de red 520 puede proporcionar una conexión a través de la red local 522 a un ordenador principal 524 o al equipo de datos operado por un Proveedor de Servicios de Internet (ISP) 526. El ISP 526 a su vez proporciona servicios de comunicación de datos a través de la red de comunicación de datos por paquetes en todo el mundo ahora comúnmente conocida como “Internet” 528. La red local 522 e Internet 528 ambas usan señales eléctricas, electromagnéticas u ópticas que transportan secuencias de datos digitales. Las señales a través de las diversas redes y las señales en el enlace de red 520 y a través de la interfaz de comunicación 518, que transporta los datos digitales a y desde el sistema informático 500, son formas ejemplares de ondas portadoras que transportan la información.

El sistema informático 500 puede enviar mensajes y recibir datos, incluyendo un código de programa, a través de la(s) red(es), el enlace de red 520 y la interfaz de comunicación 518. En el ejemplo de Internet, un servidor 530 podría transmitir un código requerido para un programa de aplicaciones a través de Internet 528, el ISP 526, la red local 522 y la interfaz de comunicación 518. De acuerdo con la invención, una aplicación descargada tal implementa las técnicas descritas en la presente memoria.

El código recibido se puede ejecutar por el procesador 504 según se recibe, y/o almacenar en el dispositivo de almacenamiento 510, u otro almacenamiento no volátil para ejecución posterior. De esta manera, el sistema informático 500 puede obtener un código de aplicación en forma de una onda portadora.

En la especificación anteriormente mencionada, la invención se ha descrito con referencia a realizaciones específicas de la misma.

REIVINDICACIONES

1. Un método para controlar el acceso por un cliente (210-1) a un recurso (268) protegido por un sistema de control de acceso (220) que usa chivatos de control de acceso, transmitidos en conjunto con peticiones de acceso al recurso, para determinar si se puede permitir el acceso, en donde dichos chivatos de control de acceso se transmiten solamente entre dicho cliente y uno o más servidores que pertenecen a un primer dominio, el método que comprende los pasos de:

un primer servidor (260) que pertenece a dicho primer dominio que recibe un elemento de datos particular desde dicho cliente (210-1);
en donde dicho elemento de datos particular:

fue transmitido a dicho cliente desde un segundo servidor (242) que no pertenece a dicho primer dominio, e
indica que un usuario se ha autentificado por dicho sistema de control de acceso;

dicho primer servidor (260) que determina que dicho usuario se ha autentificado por dicho sistema de control de acceso (220) en base a dicho elemento de datos particular; y
en respuesta a dicho primer servidor (260) determinar que dicho usuario puede acceder a dicho recurso, dicho primer servidor (260) que transmite a dicho cliente un chivato de control de acceso generado por dicho sistema de control de acceso (220).

2. El método de la reivindicación 1, que además incluye los pasos de:

recibir una primera petición desde dicho cliente (210-1) para acceder a dicho recurso (268);
determinar que dicho cliente no transmitió un chivato de control de acceso particular en conjunto con dicha primera petición que se puede usar para determinar si dicho cliente puede acceder a dicho recurso (268); y
en respuesta a determinar que dicho cliente no transmitió un chivato de control de acceso particular en conjunto con dicha primera petición, dicho primer servidor (260) hacer a dicho cliente transmitir una segunda petición a dicho segundo servidor (242) para determinar los derechos de acceso de dicho cliente.

3. El método de la reivindicación 2, en donde dicho elemento de datos particular fue transmitido a dicho cliente (210-1) desde dicho segundo servidor (242) en respuesta a dicho segundo servidor que determina que dicho usuario se ha autentificado, en donde dicho segundo servidor que determina que dicho usuario se ha autentificado incluye dicho servidor que realiza al menos uno de:

hacer a dicho usuario registrarse a dicho sistema de control de acceso para ser autentificado por dicho sistema de control de acceso (220), y
examinar uno o más chivatos que están asociados con un nombre de dominio asociado con dicho segundo servidor pero no dicho primer servidor.

4. El método de cualquier reivindicación precedente, que además incluye los pasos de:

hacer que dicho cliente transmita dicho elemento de datos particular a uno o más de otros servidores, en donde cada uno de los otros servidores de dicho uno o más de otros servidores transmite otros elementos de datos que se transmiten solamente entre dicho cliente y otro dominio de uno o más servidores al que pertenece dicho cada uno de otro servidor; y
dicho cada uno de otro servidor de dicho uno o más de otros servidores que transmiten otra información de control de acceso generada por dicho sistema de control de acceso en otro elemento de datos o dichos otros elementos de datos respectivos.

5. El método de cualquier reivindicación precedente, el método que además incluye los pasos de:

dicho segundo servidor (242) hacer que un segundo chivato de control de acceso que refleja dicho chivato de control de acceso sea almacenado en un mecanismo de almacenamiento que se puede acceder por dicho primer servidor (260); y
dicho primer servidor que recupera dicho chivato de control de acceso para generar dicho chivato de control de acceso;
en donde preferiblemente dicho mecanismo de almacenamiento es un servidor particular (208) dedicado a generar chivatos de control de acceso que cada uno indica que un usuario particular se ha autentificado por dicho sistema de control de acceso, el método que además incluye el paso de dicho servidor particular generar dicho elemento de datos particular en respuesta a una petición transmitida por dicho segundo servidor a dicho servidor particular.

6. El método de cualquier reivindicación precedente, que además incluye los pasos de:

dicho segundo servidor (242) que transmite una petición para dicho elemento de datos particular a un servidor particular (208) dedicado a generar chivatos de control de acceso que cada uno indica que un usuario particular ha sido autentificado por dicho sistema de control de acceso; y
dicho servidor particular generar dicho elemento de datos particular y transmitir dicho elemento de datos particular a dicho segundo servidor; en donde el paso de que dicho primer servidor determine que dicho usuario se ha autentificado por dicho sistema de control de acceso preferiblemente incluye que dicho primer servidor transmita una petición a dicho servidor particular para verificar que dicho elemento de datos particular está asociado con un usuario que se ha autentificado.

7. Un medio legible por ordenador que transporta una o más secuencias de una o más instrucciones para controlar el acceso por un cliente (210-1) a un recurso (268) protegido por un sistema de control de acceso (220) que usa chivatos de control de acceso, transmitidos en conjunto con las peticiones para acceder al recurso, para determinar si se puede permitir el acceso, en donde dichos chivatos de control de acceso solamente se transmiten entre dicho cliente (210-1) y uno o más servidores que pertenecen a un primer dominio, la una o más secuencias de una o más instrucciones que incluyen instrucciones que cuando se ejecutan por uno o más procesadores, hacen al uno o más procesadores realizar los pasos de:

un primer servidor (260) que pertenece a dicho primer dominio recibir un elemento de datos particular de dicho cliente (210-1);
en donde dicho elemento de datos particular:

fue transmitido a dicho cliente desde un segundo servidor (242) que no pertenece a dicho primer dominio, e
indica que un usuario se ha autentificado por dicho sistema de control de acceso;

dicho primer servidor (260) que determina que dicho usuario se ha autentificado por dicho sistema de control de acceso (220) en base a dicho elemento de datos particular; y
en respuesta a dicho primer servidor (260) determinar que dicho usuario puede acceder a dicho recurso, dicho primer servidor (260) que transmite a dicho cliente (210-1) un chivato de control de acceso generado por dicho sistema de control de acceso (220).

8. El medio legible por ordenador de la reivindicación 7, que además incluye los pasos de:

recibir una primera petición desde dicho cliente (210-1) para acceder a dicho recurso (268);
determinar que dicho cliente no transmitió un chivato de control de acceso particular en conjunto con dicha primera petición que se puede usar para determinar si dicho cliente puede acceder a dicho recurso (268); y
en respuesta a determinar que dicho cliente no transmitió dicho chivato de control de acceso particular en conjunto con dicha primera petición, dicho primer servidor (260) hacer a dicho cliente transmitir una segunda petición a dicho segundo servidor (242) para determinar los derechos de acceso de dicho cliente.

9. El medio legible por ordenador de la reivindicación 8, en donde dicho elemento de datos particular fue transmitido a dicho cliente (210-1) desde dicho segundo servidor (242) en respuesta a dicho segundo servidor que determina que dicho usuario se ha autentificado.

10. El medio legible por ordenador de las reivindicaciones 8 o 9, en donde dicho segundo servidor (242) que determina que dicho usuario (210-1) se ha autentificado incluye dicho servidor que realiza al menos uno de:

hacer a dicho usuario registrarse a dicho sistema de control de acceso (220) a ser autentificado por dicho sistema de control de acceso, y
examinar uno o más chivatos que están asociados con un nombre de dominio asociado con dicho segundo servidor pero no con dicho primer servidor.

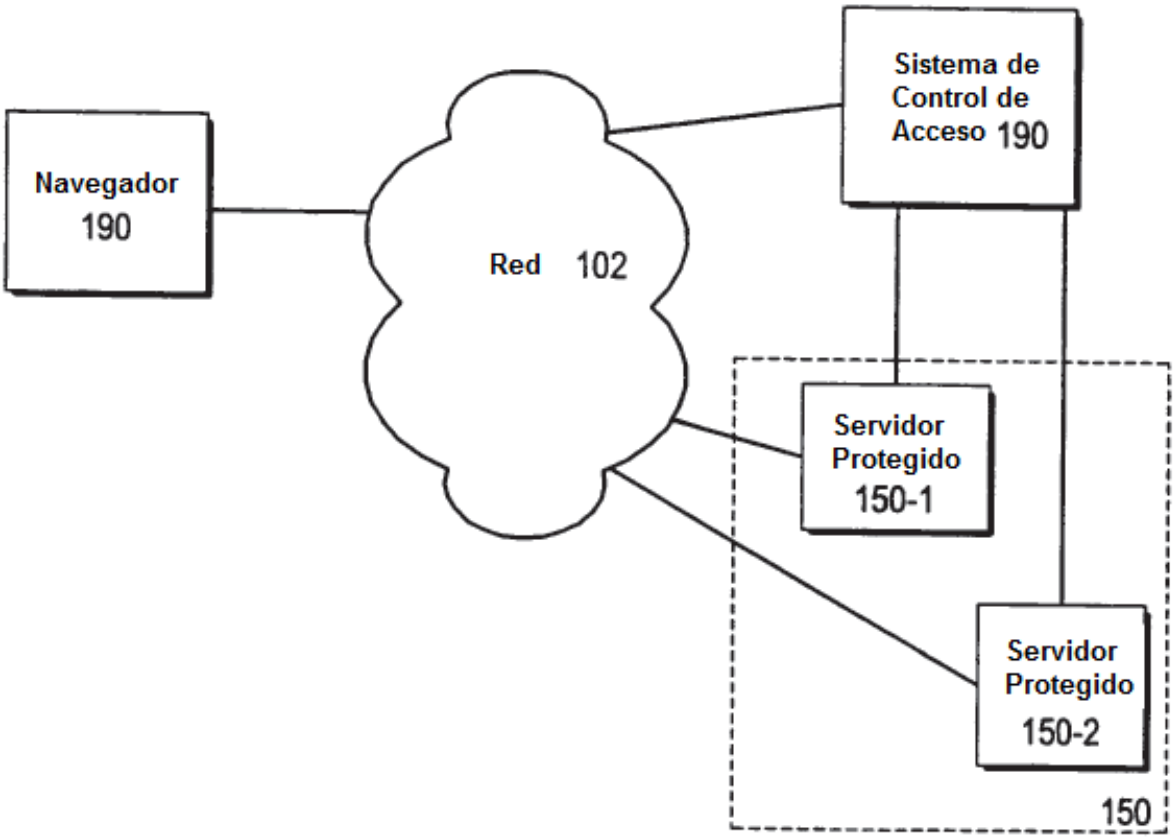
Navegador
190
Red 102
Sistema de
Control de
Acceso 190
Servidor
Protegido
150-1
Servidor
Protegido
150-2
150

Fig. 1

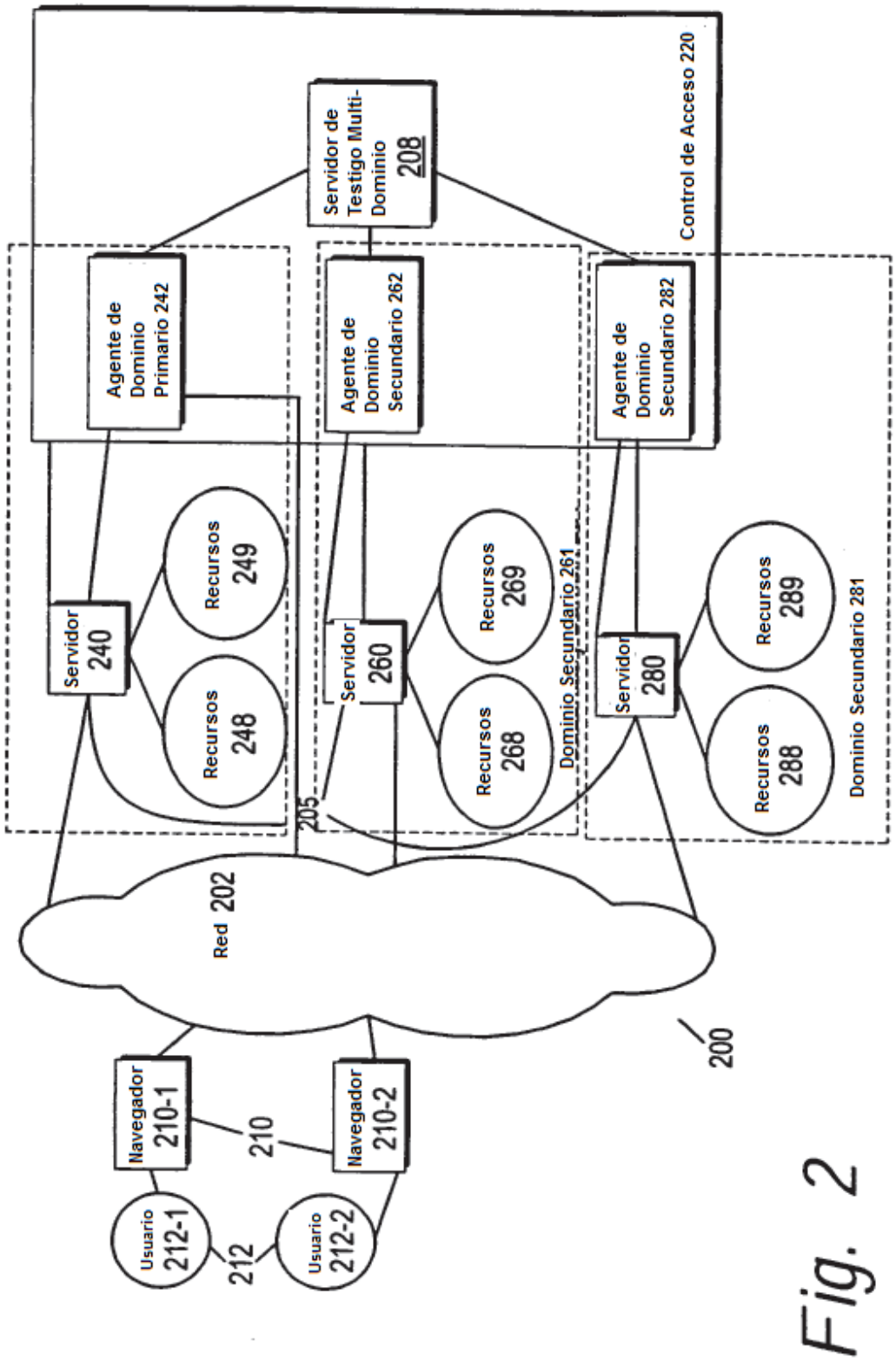
Control de Acceso 220
Servidor de Testigo Multi-Dominio 208
Agente de Dominio Primario 242
Agente de Dominio Secundario 262
Agente de Dominio Secundario 282
Servidor 240
Recursos 249
Recursos 248
Servidor 260
Recursos 269
Recursos 268
Dominio Secundario 261
Servidor 280
Recursos 289
Recursos 288
Dominio Secundario 281
205
Red 202
200
Navegador 210-1
210
Navegador 210-2
Usuario 212-1
212
Usuario 212-2

Fig. 2

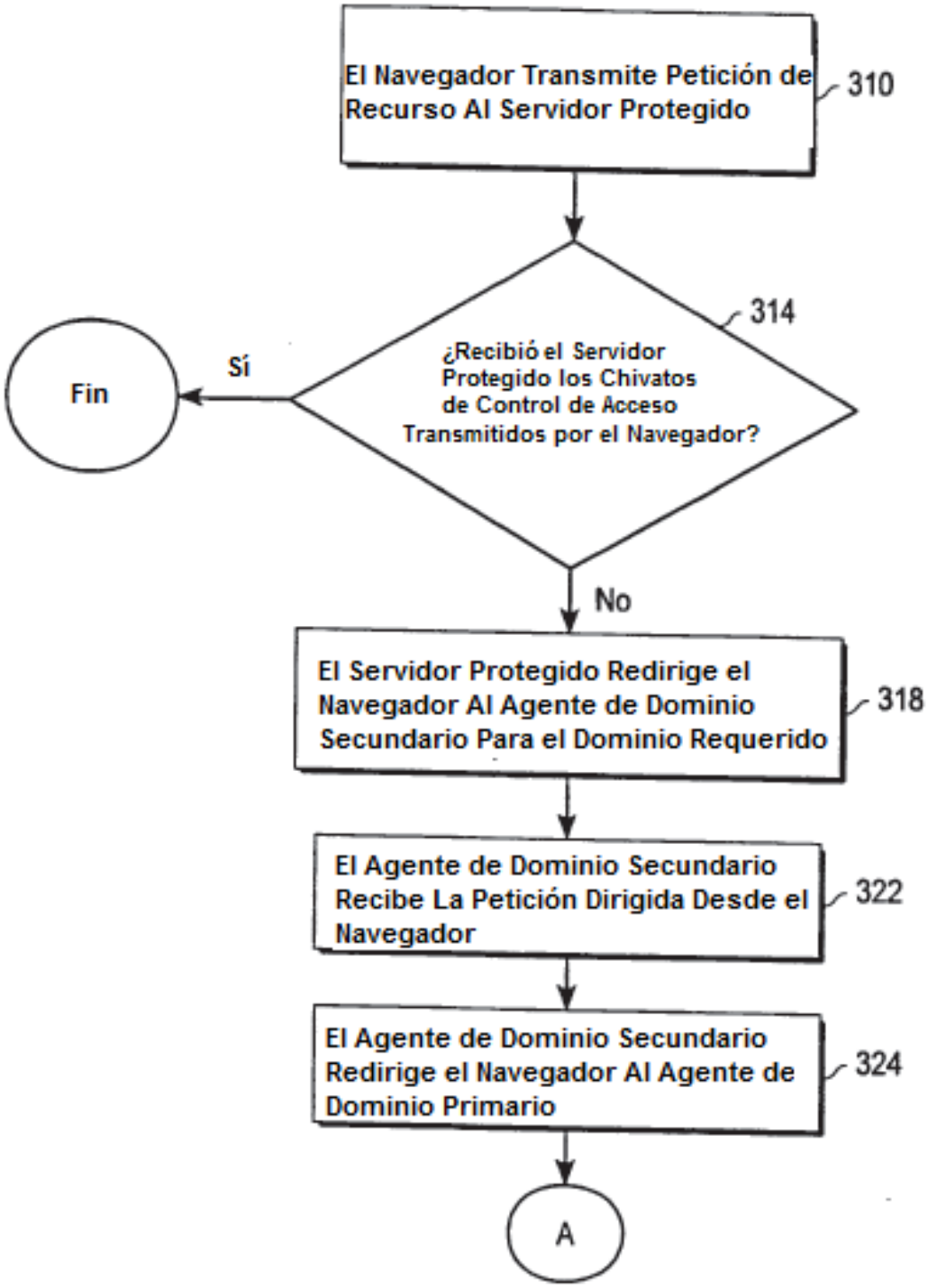
El Navegador Transmite Petición de Recurso Al Servidor Protegido
310
314
¿Recibió el Servidor Protegido los Chivatos de Control de Acceso Transmitidos por el Navegador?
Sí
Fin
No
El Servidor Protegido Redirige el Navegador Al Agente de Dominio Secundario Para el Dominio Requerido
318
El Agente de Dominio Secundario Recibe La Petición Dirigida Desde el Navegador
322
El Agente de Dominio Secundario Redirige el Navegador Al Agente de Dominio Primario
324
A

Fig. 3A

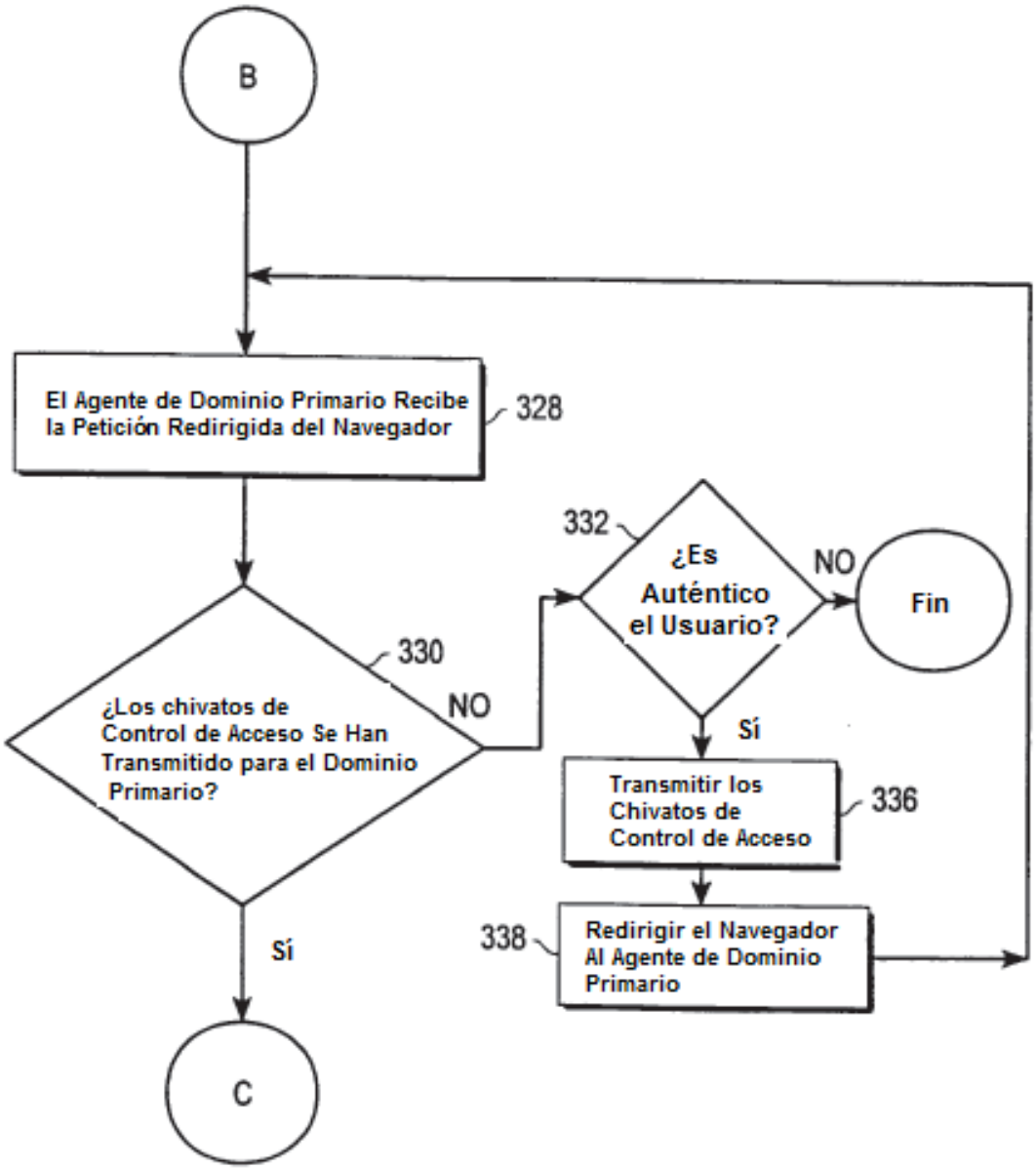
B
El Agente de Dominio Primario Recibe la Petición Redirigida del Navegador
328
332
¿Es Auténtico el Usuario?
NO
Fin
330
¿Los chivatos de Control de Acceso Se Han Transmitido para el Dominio Primario?
NO
Sí
Transmitir los Chivatos de Control de Acceso
336
338
Redirigir el Navegador Al Agente de Dominio Primario
Sí
C

Fig. 3B

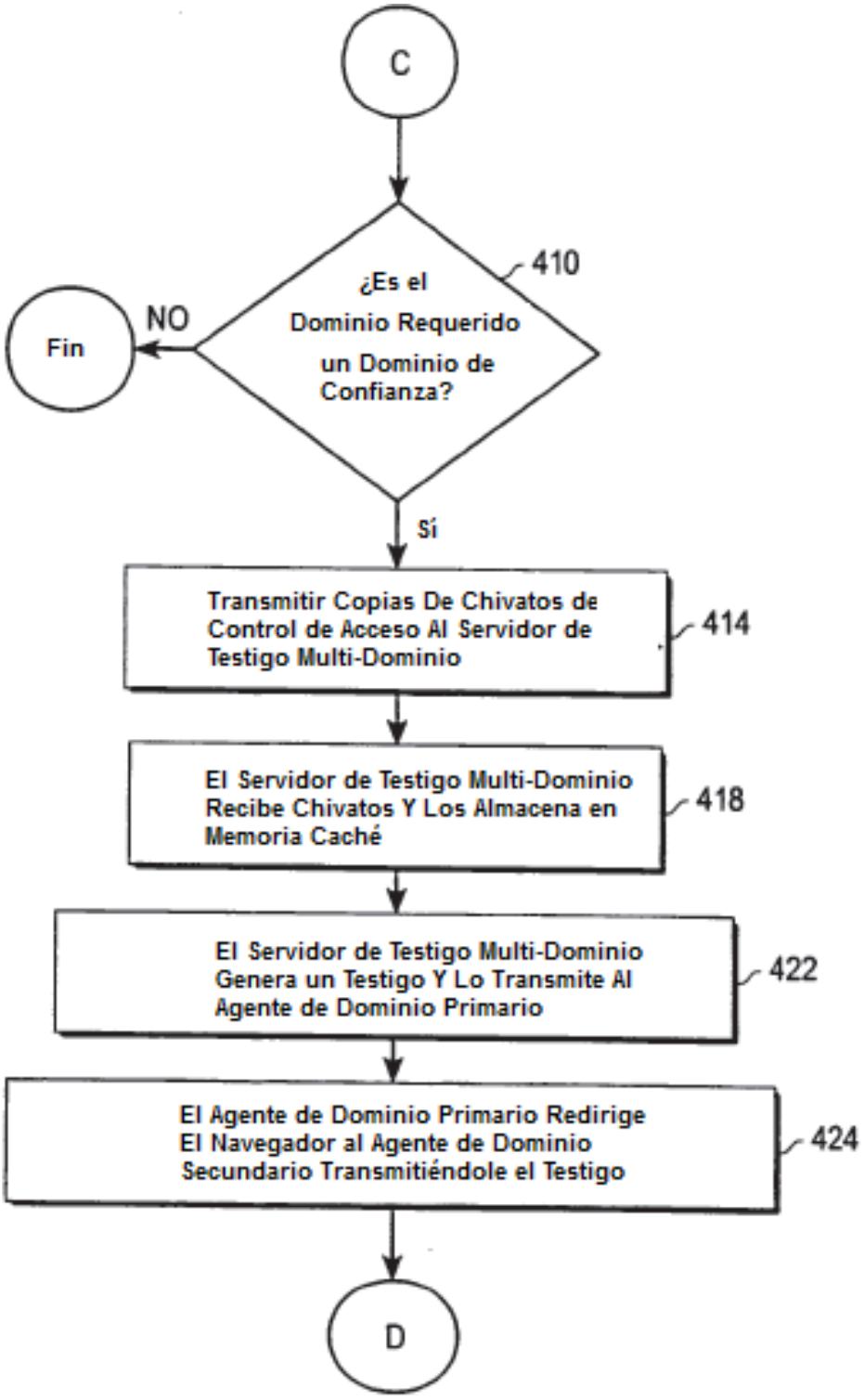
C
410
¿Es el Dominio Requerido un Dominio de Confianza?
NO
Fin
Sí
Transmitir Copias De Chivatos de Control de Acceso Al Servidor de Testigo Multi-Dominio
414
El Servidor de Testigo Multi-Dominio Recibe Chivatos Y Los Almacena en Memoria Caché
418
El Servidor de Testigo Multi-Dominio Genera un Testigo Y Lo Transmite Al Agente de Dominio Primario
422
El Agente de Dominio Primario Redirige El Navegador al Agente de Dominio Secundario Transmitiéndole el Testigo
424
D

Fig. 4A

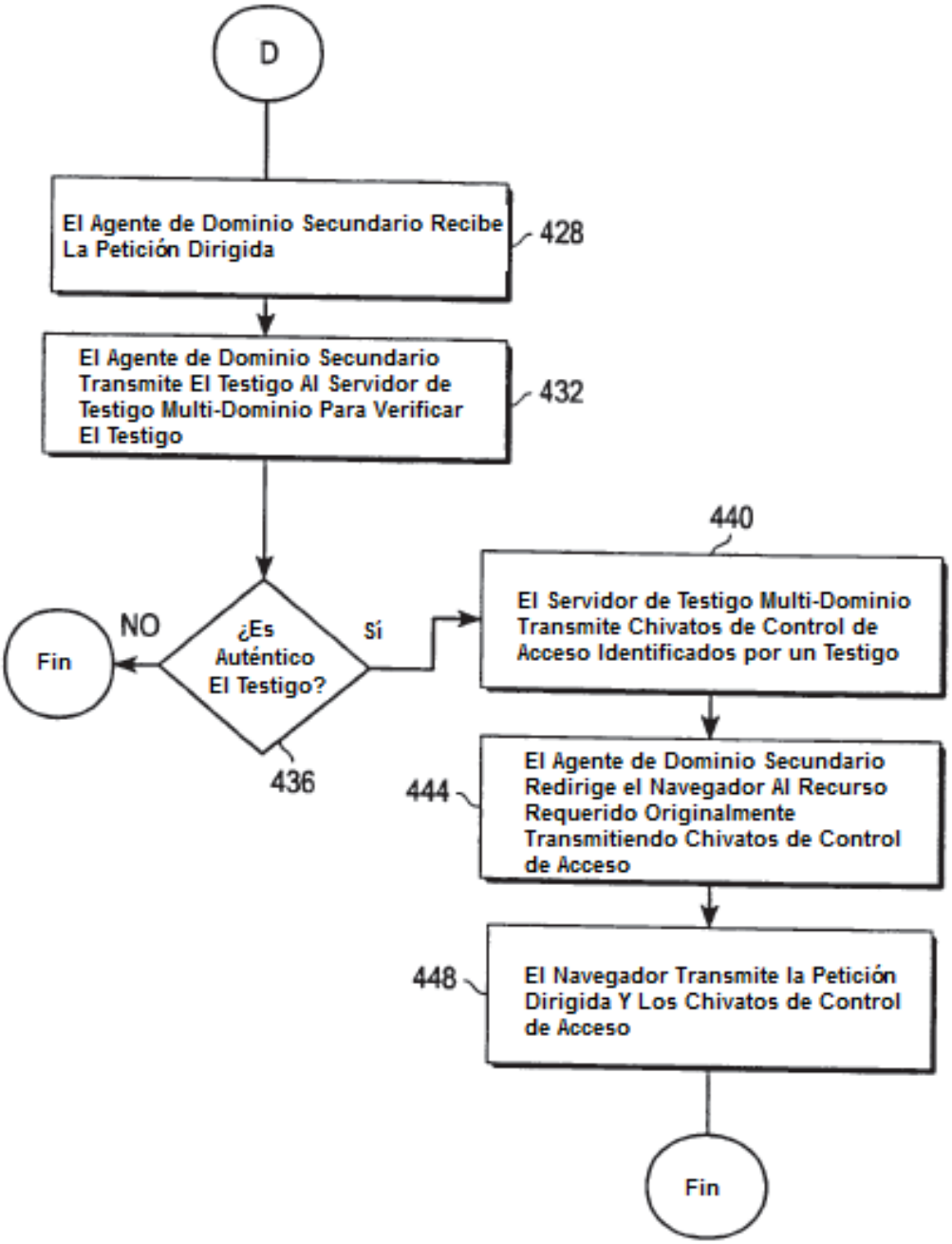
D
El Agente de Dominio Secundario Recibe La Petición Dirigida
428
El Agente de Dominio Secundario Transmite El Testigo Al Servidor de Testigo Multi-Dominio Para Verificar El Testigo
432
¿Es Auténtico El Testigo?
NO
Fin
Sí
436
440
El Servidor de Testigo Multi-Dominio Transmite Chivatos de Control de Acceso Identificados por un Testigo
444
El Agente de Dominio Secundario Redirige el Navegador Al Recurso Requerido Originalmente Transmitiendo Chivatos de Control de Acceso
448
El Navegador Transmite la Petición Dirigida Y Los Chivatos de Control de Acceso
Fin

Fig. 4B

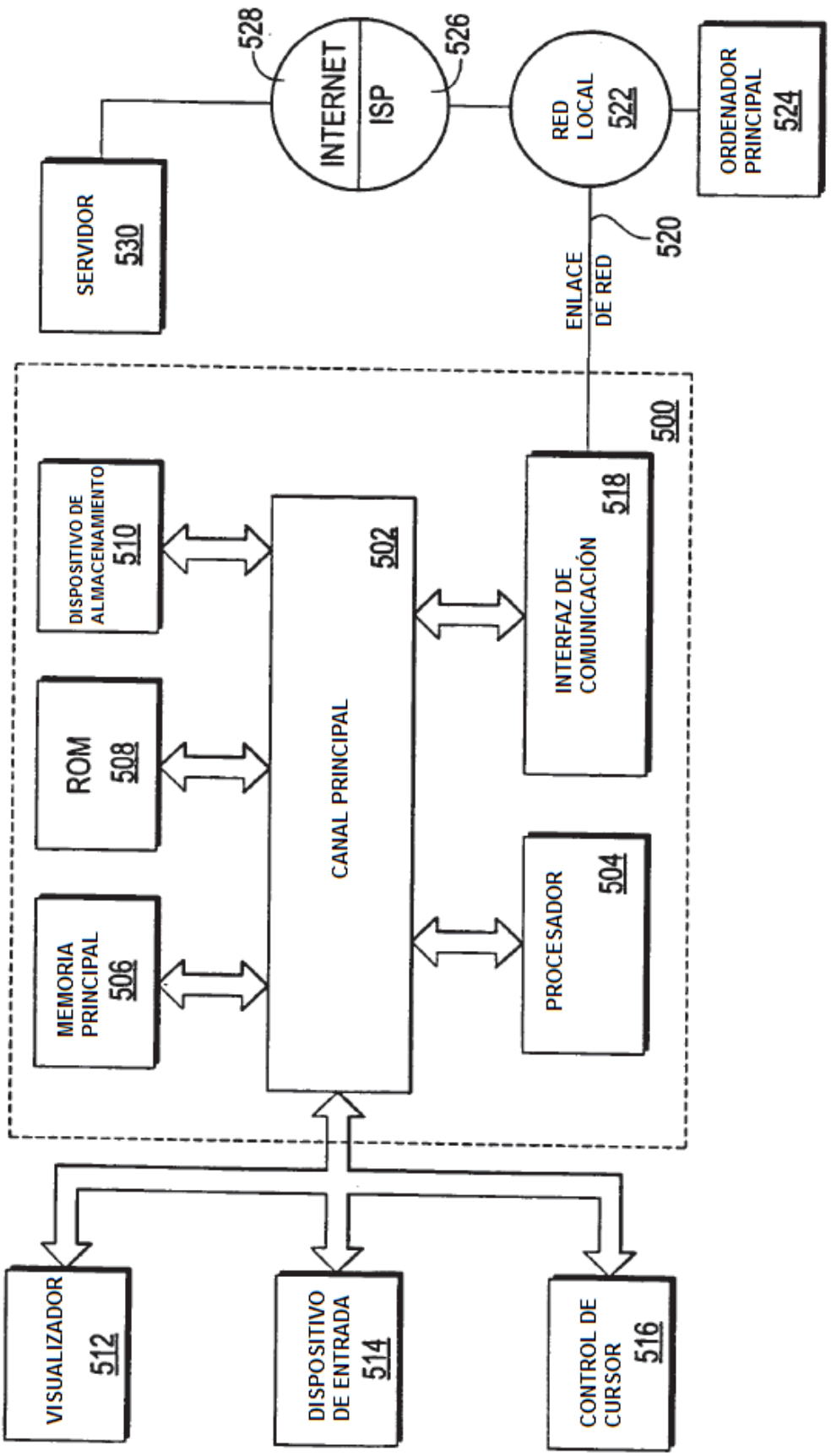
528
INTERNET
ISP
526
RED LOCAL 522
ORDENADOR PRINCIPAL 524
SERVIDOR 530
520
ENLACE DE RED
500
DISPOSITIVO DE ALMACENAMIENTO 510
ROM 508
MEMORIA PRINCIPAL 506
CANAL PRINCIPAL 502
INTERFAZ DE COMUNICACIÓN 518
PROCESADOR 504
VISUALIZADOR 512
DISPOSITIVO DE ENTRADA 514
CONTROL DE CURSOR 516

Fig. 5