(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 199**

(51) Int. CI.:

G06F 15/16 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.07.2015 PCT/US2015/040726**

(87) Fecha y número de publicación internacional: **21.01.2016 WO16011239**

(96) Fecha de presentación y número de la solicitud europea: **16.07.2015 E 15822312 (3)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3170091**

(54) Título: **Método y servidor de consulta de información remota**

(30) Prioridad:

17.07.2014 CN 201410342598

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.01.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

LU, KUN

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Método y servidor de consulta de información remota

Campo técnico

La presente divulgación se refiere al campo tecnológico de las comunicaciones, y en particular, a métodos y servidores de consulta de información remota.

Antecedentes

Con el rápido desarrollo de Internet, el número de usuarios de Internet aumenta diariamente. Algunos de estos usuarios de Internet pueden sabotear sistemas de Internet intencionadamente para participar en actividades ilegales, como el robo de datos. Por tanto, surge una cuestión de analizar la seguridad de los usuarios de Internet.

En tecnologías existentes, la información necesaria para el análisis de seguridad de un usuario se obtiene usando un enfoque de consulta remota para determinar si el usuario es un usuario seguro cuando se analiza la seguridad del usuario. Sin embargo, enfoques de consulta remota, como RPC (llamada a procedimiento remoto), SOAP (protocolo simple de acceso a objetos) o REST (transferencia de estado representacional), etc., se basan en TCP (protocolo de control de transmisión)/HTTP (protocolo de transferencia de hipertexto). Cuando el análisis de seguridad de un usuario se realiza basándose en estos protocolos, a menudo se necesita un desarrollo de un módulo de software correspondiente en un lado de cliente para facilitar una construcción de una solicitud de consulta correspondiente. También es necesario un desarrollo de un módulo de software correspondiente para un servidor de contenido al que se dirige la solicitud de consulta con el fin de reconocer esta solicitud de consulta construida. En resumen, al realizar el análisis de seguridad del usuario, las tecnologías existentes necesitan construir y reconocer la solicitud de consulta, resultando de ese modo en un método de reconocimiento complicado.

El documento US7228359 (B1) da a conocer un sistema de distribución de contenido que tiene un servidor DNS que se configura para proporcionar respuestas DNS en respuesta a solicitudes DNS, y un dispositivo que interconecta entre un cliente y el servidor DNS. El dispositivo incluye una interfaz que se comunica con el cliente, y un controlador acoplado a la interfaz. El controlador puede interceptar una primera solicitud DNS en ruta desde el cliente al servidor DNS, y proporcionar una segunda solicitud DNS al servidor DNS a través de la interfaz en respuesta a la intercepción de la primera solicitud DNS. La segunda solicitud DNS incluye de manera selectiva un identificador de cliente que identifica al cliente, y que no incluye el identificador de cliente que identifica al cliente, basándose en una decisión de selección. El controlador puede además transmitir una respuesta DNS desde el servidor DNS al cliente a través de la interfaz. La respuesta DNS incluye un identificador de servidor de contenido que identifica un servidor de contenido.

El documento US8650245 (B1) da a conocer un método implementado por un componente informático para proporcionar vistas adaptativas de datos de reputación asociados a una consulta de sistema de nombres de dominio. Se recibe una consulta de sistema de nombres de dominio. Se identifica una parte de filtro dentro de la consulta. Se consulta un archivo de zona virtual según la parte de filtro de la consulta. Se genera una respuesta a la consulta. La respuesta comprende un análisis de los datos de reputación según la parte de filtro.

El documento de Yong Jin *et al*, “Proposal of an adaptive firewall system in collaboration with extended DNS”, Applications and the internet (SAINT), 2011 IEEE/IPSJ 11º International Symposium On, IEEE, (20110718), doi: 10.1109/SAINT.2011.40, ISBN 978-1-4577-0531-1, páginas 222 - 225, da a conocer que, con la popularidad de los servicios de Internet, la seguridad de red se convierte en un tema crítico en el mundo de Internet. Especialmente, las amenazas de accesos maliciosos hacen que los sistemas de cortafuegos tengan que reducir su rendimiento debido a inspecciones estrictas. Se da a conocer un sistema de cortafuegos adaptativo en colaboración con DNS que introduce la característica de notificación de dirección IP del solicitante de consulta. Con una característica de este tipo, el sistema puede identificar si cada flujo de comunicación puede ser de confianza o no comprobando la dirección IP del solicitante de consulta y el nombre de dominio objetivo de consulta DNS. Basándose entonces en el resultado de la comprobación, el sistema de cortafuegos decide de manera adaptativa la operación específica para una conexión específica.

Sumario

Este sumario se proporciona para introducir una selección de conceptos de forma simplificada que además se describen más adelante en la descripción detallada. Este sumario no se pretende que identifique todas las características clave o características esenciales de la materia objeto reivindicada, ni se pretende que se use por sí solo como ayuda para determinar el alcance de la materia objeto reivindicada. El término “técnicas”, por ejemplo, puede referirse a dispositivo(s), sistema(s), método(s) y/o instrucciones legibles por ordenador según lo permitido por el contexto anterior y a lo largo de la presente divulgación.

Realizaciones de la presente divulgación proporcionan un método y un servidor de consulta de información remota. Al añadir un identificador de tipo correspondiente a un tipo de solicitud de consulta en las solicitudes de consulta

existentes, puede realizarse un reconocimiento más simple y altamente eficiente de la seguridad de usuario.

En un primer aspecto, la presente divulgación proporciona un método implementado por uno o más dispositivos informáticos tal como se define en la reivindicación 1. En un segundo aspecto, la presente divulgación proporciona un servidor tal como se define en la reivindicación 6. En un tercer aspecto, la presente divulgación proporciona uno o más medios legibles por ordenador tal como se define en la reivindicación 11. Se definen características opcionales en las reivindicaciones dependientes.

Se da a conocer un método de consulta de información remota, que incluye recibir mediante un servidor de contenido una solicitud de consulta enviada desde un lado de cliente; obtener, mediante un servidor de contenido, contenido de un campo de tipo de la solicitud de consulta; obtener un tipo de la solicitud de consulta basándose en el contenido del campo de tipo; añadir mediante un servidor de contenido un identificador de tipo correspondiente al tipo y un nombre de dominio de un sistema de nombres de dominio (DNS) autorizado preestablecido en la solicitud de consulta para obtener una solicitud de consulta objetivo; enviar mediante un servidor de contenido la solicitud de consulta objetivo a un DNS local para permitir que el DNS local envíe la solicitud de consulta objetivo al DNS autorizado preestablecido según el nombre de dominio del DNS autorizado preestablecido en la solicitud de consulta objetivo; y recibir un mensaje de respuesta que corresponde al tipo de la solicitud de consulta del DNS autorizado preestablecido, en el que el lado de cliente gestiona con el DNS local y el DNS autorizado preestablecido con antelación con respecto a la información respectiva representada por cada segmento en el mensaje de respuesta. Se da a conocer un aparato que comprende un servidor de contenido, un sistema de nombres de dominio (DNS) local y un DNS autorizado preestablecido, que incluye una unidad de recepción, una unidad de adquisición, una unidad de adición y una unidad de envío. La unidad de recepción recibe una solicitud de consulta desde un lado de cliente y obtiene contenido de un campo de tipo de la solicitud de consulta. La unidad de adquisición adquiere un tipo de la solicitud de consulta basándose en el contenido del campo de tipo. La unidad de adición añade un identificador de tipo correspondiente al tipo adquirido mediante la unidad de adquisición y un nombre de dominio de un DNS autorizado preestablecido en la solicitud de consulta para adquirir una solicitud de consulta objetivo. La unidad de envío envía la solicitud de consulta objetivo adquirida mediante la unidad de adición a un DNS local para permitir que el DNS local envíe la solicitud de consulta objetivo al DNS autorizado preestablecido según el nombre de dominio del DNS autorizado preestablecido en la solicitud de consulta objetivo, y recibe un mensaje de respuesta correspondiente al tipo de la solicitud de consulta desde el DNS autorizado preestablecido. El lado de cliente gestiona con el DNS local y el DNS autorizado preestablecido con antelación con respecto a la información respectiva representada por cada segmento en el mensaje de respuesta.

El método y el servidor de consulta de información remota proporcionados por la presente divulgación obtienen primero una solicitud de consulta enviada desde un lado de cliente, y añaden un identificador de tipo y un nombre de dominio de un DNS autorizado preestablecido a la solicitud de consulta adquirida para enviar al DNS autorizado preestablecido. Finalmente, el método y el servidor, mediante el DNS autorizado preestablecido, devuelven un mensaje de respuesta de esta solicitud de consulta. Por tanto, el método dado a conocer añade un identificador de tipo correspondiente a un tipo de una solicitud de consulta en una solicitud de consulta existente basándose en un protocolo DNS, logrando de ese modo un reconocimiento más simple y altamente eficiente de la seguridad de usuario.

Descripción de los dibujos

La figura 1 es un diagrama esquemático de un método de consulta de información remota por un lado de cliente según tecnologías existentes.

La figura 2 es un diagrama de flujo de un método de consulta de información remota según una primera realización de la presente divulgación.

La figura 3 es un sistema de gestión distribuido según la presente divulgación.

La figura 4 es un diagrama esquemático de un servidor según una segunda realización de la presente divulgación.

La figura 5 es un diagrama estructural del servidor de ejemplo como se describe en la figura 4 en más detalle.

Descripción detallada

Para hacer más comprensibles los objetivos, soluciones técnicas y ventajas de las realizaciones de la presente divulgación, las soluciones técnicas en las realizaciones de la presente divulgación se describen de manera clara y completa en el presente documento con referencia a los dibujos adjuntos en las realizaciones de la presente divulgación. Aparentemente, las realizaciones que van a describirse representan algunas y no todas las realizaciones de la presente divulgación. Todas las demás realizaciones adquiridas por un experto en la técnica basándose en las realizaciones de la presente divulgación sin realizar ningún esfuerzo creativo, pertenecen al alcance de protección de la presente divulgación. Con el fin de facilitar el entendimiento de las realizaciones de la presente divulgación, se explican y se describen realizaciones a modo de ejemplo en más detalle en el presente documento junto con los dibujos. Estas realizaciones, sin embargo, no limitan las implementaciones de la presente divulgación.

Con el fin de facilitar el entendimiento de las realizaciones de la presente divulgación, se explican y se describen realizaciones a modo de ejemplo en más detalle en el presente documento junto con los dibujos. Estas realizaciones, sin embargo, no limitan implementaciones de la presente divulgación.

El método y el servidor de consulta de información remota proporcionados por las realizaciones de la presente divulgación son aplicables a escenarios en los que se realiza un análisis de seguridad para un usuario de comercio electrónico, especialmente escenarios en los que se realiza un análisis de seguridad para usuario de comercio electrónico remoto. En la presente divulgación, se realiza un análisis de seguridad de un usuario de Internet remoto basándose en un protocolo DNS (sistema de nombres de dominio). El protocolo DNS por sí mismo es un protocolo relativamente simple y, por tanto, puede lograrse una consulta de información remota con una alta eficiencia.

La figura 1 es un diagrama esquemático de un método 100 de consulta de información remota por un lado de cliente en las tecnologías existentes, que incluye un lado de cliente 102, un DNS local 104, un DNS autorizado 106, un DNS 108 y un DNS de segundo nivel 110. En la figura 1, el lado de cliente 102 primero envía una solicitud de consulta al DNS local 104. La solicitud de consulta incluye una dirección URL (localizador de recursos uniforme), por ejemplo, “www.alipay.com”. Si la dirección IP (protocolo de Internet) correspondiente a esta dirección URL es 110.75.142.111 y el lado de cliente 102 no envía esta solicitud de consulta por primera vez, el DNS local 104 directamente devuelve “110.75.142.111” y “www.alipay.com” al lado de cliente 102. “110.75.142.111” representa una dirección IP correspondiente a la dirección URL enviada por el lado de cliente 102 y “www.alipay.com” representa un nombre de alias de la dirección URL enviada por el lado de cliente 102. Dado que esta dirección URL no tiene un nombre de alias en este ejemplo, un nombre de alias que se devuelve es el mismo que la dirección URL.

Debe indicarse que la dirección IP es la que se almacena localmente en caché después de que el DNS local 104 adquiera la dirección IP del DNS autorizado 106 en respuesta al lado de cliente 102 que envía la solicitud de consulta al DNS local 104 por primera vez. Esta dirección IP se elimina del DNS local 104 después de que finalice un TTL (tiempo de vida).

Como puede verse a partir del ejemplo anterior, el DNS local 102 y el DNS autorizado 106 en las tecnologías existentes simplemente resuelven la dirección URL enviada por el lado de cliente 102, y devuelven la dirección IP correspondiente al mismo, y no soportan consultas de otra información. Por ejemplo, al analizar una cuestión de seguridad asociada a un usuario, es necesario que se consulte información como una ubicación en la que el usuario está ubicado y si el usuario ya se ha incluido en una lista negra.

La figura 2 es un diagrama de flujo de un método de consulta de información remota según una primera realización de la presente divulgación. Como se muestra en la figura 2, el método incluye:

S210 recibe una solicitud de consulta enviada por un lado de cliente y obtiene contenido de un campo de tipo de la solicitud de consulta.

Un servidor de contenido recibe una solicitud de consulta, por ejemplo, recibe una solicitud para consultar una ubicación de una dirección IP “192.168.22.1”. El servidor de contenido se ubica entre un lado de cliente y un DNS local, y se usa para modificar la solicitud de consulta enviada por el lado de cliente (como añadir un identificador de tipo correspondiente a un tipo de la solicitud de consulta) y enviar la solicitud de consulta modificada al DNS local. La solicitud de consulta incluye contenido de un campo de tipo de la solicitud de consulta. En una realización, el contenido del campo de tipo de la solicitud de consulta puede incluir una consulta de una ubicación a la que pertenece una dirección IP o una consulta sobre si la dirección IP está incluida en una lista negra. En este ejemplo, el contenido del campo de tipo de la solicitud de consulta es una consulta de la ubicación a la que pertenece la dirección IP.

Debe indicarse que el contenido del campo de tipo de la solicitud de consulta puede incluir además una consulta de información de datos que no se cambia de manera frecuente, por ejemplo, una consulta de la calidad del aire, etc., del distrito ZZ de la ciudad YY en la provincia XX.

S220 obtiene un tipo de la solicitud de consulta basándose en el contenido del campo de tipo.

Debe indicarse que puede definirse con antelación un número determinado de tipos de solicitudes de consulta. Por ejemplo, pueden definirse con antelación mil tipos de solicitudes de consulta, que se representan como q_1, q_2, ..., q_{1000} respectivamente. Cuando el contenido de los campos de tipo de solicitudes de consulta son diferentes, los tipos correspondientes a estas solicitudes de consulta son diferentes. Por ejemplo, cuando el contenido del campo de tipo de la solicitud de consulta es una consulta de una ubicación a la que pertenece una dirección IP, un tipo de la solicitud de consulta puede ser q_1, y cuando el contenido del campo de tipo de la solicitud de consulta es una consulta sobre si la dirección IP está incluida en una lista negra, el tipo de la solicitud de consulta puede ser q_2. De manera similar, cuando el contenido del campo de tipo de la solicitud de consulta es una consulta de otra información de datos que no se cambia de manera frecuente, el tipo de la solicitud de consulta puede ser q_i, en el que $3 \leq i \leq 1000$. Por ejemplo, cuando el contenido del campo de tipo de la solicitud de consulta es la calidad del aire del distrito ZZ de la ciudad YY en la provincia XX, el tipo de la solicitud de consulta puede ser q_3.

S230 añade un identificador de tipo correspondiente al tipo y un nombre de dominio de un DNS autorizado preestablecido en la solicitud de consulta para adquirir una solicitud de consulta objetivo.

Debe indicarse en el presente documento que el nombre de dominio del DNS autorizado preestablecido se aplica con antelación. Opcionalmente, el nombre de dominio puede ser un nombre de dominio de segundo nivel, por ejemplo, “alipay.com”. El DNS autorizado preestablecido se usa para resolver una solicitud de consulta que incluye el nombre de dominio, es decir, resolver todas las solicitudes de consulta para “*.alipay.com”. El DNS autorizado preestablecido puede formarse por un módulo que se añade recientemente en el DNS autorizado para resolver solicitudes de consulta que incluyen el nombre de dominio mencionado anteriormente como se muestra en la figura 1. Por tanto, el DNS autorizado preestablecido en la presente divulgación tiene las ventajas de diseño simple y bajo coste de desarrollo.

Cuando la solicitud de consulta incluye una dirección IP del lado de cliente, el bloque de método S230 puede incluir además: disponer todos los segmentos de la dirección IP en orden inverso, y añadir un identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido a la misma secuencialmente para adquirir una solicitud de consulta objetivo.

Por ejemplo, si la dirección IP incluida en la solicitud de consulta es “192.168.22.1”, “1.22.168.192” se obtiene después de disponer todos los segmentos de la dirección IP dispuestos en orden inverso. Si el tipo de la solicitud de consulta obtenida en S220 es q_1 y el nombre de dominio del DNS autorizado preestablecido es “alipay.com”, una solicitud objetivo que se obtiene es “1.22.168.192.q_1.alipay.com” después de que q_1 y el nombre de dominio del DNS autorizado preestablecido se añadan secuencialmente a “1.22.168.192”. Puede entenderse que la solicitud objetivo obtenida es “1.22.168.192.q_2.alipay.com” si el tipo de la solicitud de consulta obtenida en S220 es q_2 después de que q_2 y el nombre de dominio del DNS autorizado preestablecido se añadan secuencialmente a “1.22.168.192”.

Debe indicarse que, cuando la solicitud de consulta no incluye una dirección IP del lado de cliente e incluye otra información de dirección, como una dirección URL, la información de dirección también necesita disponerse en orden inverso. Además, el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido se añaden secuencialmente al mismo para generar una solicitud de consulta objetivo. Por ejemplo, si una solicitud de consulta recibida mediante el servidor de contenido corresponde a una consulta de la calidad del aire del distrito Shangcheng de la ciudad de Hangzhou en la provincia de Zhejiang, una solicitud de consulta objetivo que se genera es “shangcheng.hz.zj.q_3.alipay.com”, donde q_3 es el tipo (una consulta de la calidad del aire) de la solicitud de consulta, zj representa la provincia de Zhejiang, hz representa la ciudad de Hangzhou y shangcheng representa el distrito de Shangcheng.

S240 envía la solicitud de consulta objetivo a un DNS local para permitir que el DNS local envíe la solicitud de consulta objetivo al DNS autorizado preestablecido según el nombre de dominio del DNS autorizado preestablecido en la solicitud de consulta objetivo, y recibe un mensaje de respuesta correspondiente al tipo de la solicitud de consulta devuelta desde el DNS autorizado preestablecido.

Al obtener la solicitud de consulta objetivo, el servidor de contenido envía la solicitud de consulta objetivo a un DNS local. En respuesta a la recepción de la solicitud de consulta objetivo, el DNS local busca el DNS autorizado preestablecido a través de un modo de recurrencia/iteración basándose en “alipay. com” en la solicitud de consulta objetivo. Alternativamente, la información de dirección del DNS autorizado preestablecido puede registrarse directamente en el DNS local. En respuesta a la recepción de la solicitud de consulta que incluye el nombre de dominio del DNS autorizado preestablecido, el DNS local envía la solicitud de consulta directamente al DNS autorizado preestablecido.

Debe indicarse que un modo de recurrencia/iteración de búsqueda de un DNS autorizado preestablecido pertenece a las tecnologías existentes, que no se describe de manera redundante en el presente documento.

Debe indicarse en el presente documento que, cuando el contenido del campo de tipo de la solicitud de consulta en S210 es una consulta de una ubicación a la que pertenece la dirección IP, el mensaje de respuesta incluye información que identifica la ubicación de la dirección IP. Cuando el contenido del campo de tipo de la solicitud de consulta en S210 es una consulta sobre si la dirección IP está incluida en una lista negra, el mensaje de respuesta incluye información que identifica si la dirección IP está incluida en una lista negra. De manera similar, cuando el contenido del campo de tipo de la solicitud de consulta en S210 es una consulta de otra información de datos que no se cambia de manera frecuente, el mensaje de respuesta incluye información de identificación correspondiente a la otra información de datos que no se cambia de manera frecuente.

En el ejemplo anterior, cuando el tipo de la solicitud de consulta es q_1, la información que identifica la ubicación a la que pertenece la dirección IP puede ser un código asociado a un área. Opcionalmente, el mensaje de respuesta puede incluir además otra información como el/los proveedor(es) de servicios, etc. Cuando el mensaje de respuesta incluye otra información, el mensaje de respuesta puede representarse en segmentos, por ejemplo, “10.0.0.25”, donde el último segmento se designa como información que identifica la ubicación a la que pertenece la dirección IP.

Para otro ejemplo, cuando el tipo de solicitud de consulta es q_2, la información que identifica si la dirección IP está incluida en una lista negra puede ser un número de un dígito. Opcionalmente, el mensaje de respuesta puede incluir además otra información, como un número de veces de inicio de sesión y un número de veces de delitos cometidos. Cuando el mensaje de respuesta incluye otra información, el mensaje de respuesta puede representarse en segmentos, por ejemplo, “127.0.0.1”, donde el último segmento se designa como información que identifica que la dirección IP está incluida en una lista negra. Cuando la dirección IP está incluida en una lista negra, el último segmento puede ser 1. Cuando la dirección IP no está incluida en una lista negra, el último segmento puede ser 0.

Después de que el DNS local recibe el mensaje de respuesta devuelto por el DNS autorizado preestablecido, se almacena en caché una relación de correspondencia entre la dirección IP y la información que identifica la ubicación a la que pertenece la dirección IP en el DNS local. De manera alternativa, una relación de correspondencia entre la dirección IP y la información que identifica si la dirección IP está incluida en una lista negra que se almacena en caché en el DNS local.

Por ejemplo, en el ejemplo anterior, cuando la dirección IP incluida en la solicitud de consulta es “192.168.22.1” y el mensaje de respuesta devuelto es “10.0.0.25”, se almacena en caché una relación de correspondencia entre la dirección IP y el mensaje de respuesta devuelto. Antes del final del TTL, el DNS local directamente devuelve el mensaje de respuesta “10.0.0.25” al lado de cliente cuando el DNS local recibe la solicitud de consulta mencionada anteriormente de nuevo y el tipo de la solicitud de consulta es q_1.

En la presente divulgación, debe indicarse que el lado de cliente necesita gestionar con el DNS local y el DNS autorizado preestablecido con antelación con respecto a la información representada por cada segmento en un mensaje de respuesta. Por ejemplo, el lado de cliente puede gestionar con el DNS local y el DNS autorizado preestablecido con antelación para usar el último segmento de un mensaje de respuesta para representar la información que identifica una ubicación a la que pertenece una dirección IP. Después de eso, si desea obtener la ubicación de la dirección IP, el lado de cliente puede resolver directamente la información del último segmento en respuesta a la recepción de un mensaje de respuesta devuelto por el DNS local. En una realización, el lado de cliente puede registrar el contenido representado por la información de identificación recibida en un formato tabular. Se da un ejemplo de contenido tabular registrado por el lado de cliente de la siguiente manera:

24	Pekín
25	Hubei

En el ejemplo anterior, cuando el mensaje de respuesta recibido por el lado de cliente es “10.0.0.25”, por ejemplo, la información del último segmento “25” se resuelve directamente, es decir, una ubicación a la que pertenece una dirección IP “192.168.22.1” se encuentra como “Hubei” consultando la tabla anterior.

Como se describe en las realizaciones mencionadas anteriormente, después de que se adquiere la ubicación a la que pertenece la dirección IP en la solicitud de consulta, un módulo o software de análisis de seguridad puede realizar un análisis de la seguridad del/de los usuario(s) de Internet que usa(n) esta dirección IP. Por ejemplo, si la ubicación adquirida a la que pertenece la dirección IP “192.168.22.1” al principio es “Hubei” y la ubicación a la que pertenece esta dirección IP es “Pekín” después de media hora, esta dirección IP se incluye como una dirección IP insegura porque la ubicación ha cambiado rápidamente en media hora.

El método de consulta de información remota proporcionado por la presente divulgación obtiene primero una solicitud de consulta enviada por un lado de cliente, añade un identificador de tipo y un nombre de dominio de un DNS autorizado preestablecido a la solicitud de consulta obtenida, que se envía al DNS autorizado preestablecido a partir de entonces. Finalmente, el DNS autorizado preestablecido devuelve un mensaje de respuesta para la solicitud de consulta. Por tanto, el método dado a conocer puede implementar una consulta de información remota altamente eficiente bajo un entorno de configuración de software existente del lado de cliente.

Debe indicarse que el método dado a conocer es aplicable no solo al análisis de seguridad de los usuarios de Internet, sino también a un sistema de gestión distribuido. La figura 3 muestra un sistema de gestión distribuido 300 proporcionado por la presente divulgación. Un DNS autorizado 302 puede ser un DNS autorizado proporcionado en la primera realización. Un primer DNS local 304 puede ser responsable de consultar las ubicaciones respectivas a las que pertenecen las direcciones IP. Un segundo DNS local 306 puede ser responsable de consultar una lista negra y una lista blanca de direcciones IP. Un tercer DNS local 308 puede ser responsable de consultar los recursos del sistema. En respuesta a la recepción de una solicitud de consulta objetivo enviada por un lado de cliente, el DNS autorizado 302 en la figura 3 obtiene un tipo de la solicitud de consulta objetivo mediante el análisis de la solicitud de consulta objetivo. Por ejemplo, cuando el contenido de un campo de tipo de la solicitud de consulta es una consulta de una ubicación a la que pertenece una dirección IP, la solicitud de consulta se envía al primer DNS local 304. Por tanto, la carga de trabajo del DNS autorizado 302 puede compartirse, y puede evitarse un problema de consumo de recursos debido a la sincronización de base de datos en las tecnologías existentes.

Correspondiente al método mencionado anteriormente de consulta de información remota, las realizaciones de la presente divulgación proporcionan además un servidor 400. El servidor 400 puede ser el servidor de contenido dado en la primera realización. Como se muestra en la figura 4, el servidor 400 incluye: una unidad de recepción 401, una unidad de adquisición 402, una unidad de adición 403 y una unidad de envío 404.

La unidad de recepción 401 se usa para recibir una solicitud de consulta enviada por el lado de cliente y obtener contenido de un campo de tipo de la solicitud de consulta.

La unidad de adquisición 402 se usa para obtener un tipo de la solicitud de consulta basándose en el contenido del campo de tipo.

La unidad de adición 403 se usa para añadir un identificador de tipo correspondiente al tipo obtenido mediante la unidad de adquisición 402 y un nombre de dominio de un DNS autorizado preestablecido (sistema de nombres de dominio) en la solicitud de consulta para obtener una solicitud de consulta objetivo.

La unidad de envío 404 se usa para enviar la solicitud de consulta objetivo obtenida mediante la unidad de adición 403 a un DNS local para permitir que el DNS local envíe la solicitud de consulta objetivo al DNS autorizado preestablecido según el nombre de dominio del DNS autorizado preestablecido en la solicitud de consulta objetivo, y recibir un mensaje de respuesta correspondiente al tipo de solicitud de consulta del DNS autorizado preestablecido.

Opcionalmente, la solicitud de consulta puede incluir una dirección IP (protocolo de Internet) del lado de cliente.

En una realización, la unidad de adición 403 se usa además para disponer todos los segmentos de la dirección IP en orden inverso y añadir el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido al mismo secuencialmente para obtener la solicitud de consulta objetivo.

Opcionalmente, el contenido del campo de tipo de las solicitudes de consulta puede incluir una consulta de una ubicación a la que pertenece la dirección IP o una consulta sobre si la dirección IP está incluida en una lista negra.

Opcionalmente, el mensaje de respuesta incluye información que identifica la ubicación a la que pertenece la dirección IP o información que identifica si la dirección IP está incluida en la lista negra.

Opcionalmente, el servidor 400 puede incluir además: una unidad de almacenamiento en caché 405 que se usa para almacenar en caché una relación de correspondencia entre la dirección IP y la información que identifica la ubicación a la que pertenece la dirección IP en el DNS local o para almacenar en caché una relación de correspondencia entre la dirección IP y la información que identifica si la dirección IP está incluida en la lista negra en el DNS local.

Opcionalmente, el lado de cliente gestiona con el DNS local y el DNS autorizado preestablecido con antelación sobre la información respectiva representada por cada segmento en el mensaje de respuesta.

El método proporcionado por la primera realización de la presente divulgación se integra en el servidor 400 proporcionado por la segunda realización de la presente divulgación. Por tanto, los detalles de un proceso de operaciones del servidor dado a conocer no se describen repetidamente en el presente documento.

El servidor dado a conocer obtiene primero una solicitud de consulta enviada por un lado de cliente, añade un identificador de tipo y un nombre de dominio de un DNS autorizado preestablecido a la solicitud de consulta obtenida, que se envía al DNS autorizado preestablecido a partir de entonces. Finalmente, el DNS autorizado preestablecido devuelve un mensaje de respuesta para la solicitud de consulta. Por tanto, el método dado a conocer puede implementar una consulta de información remota altamente eficiente bajo un entorno de configuración de software existente del lado de cliente.

Un experto en la técnica debe además entender que objetos y bloques del método de algoritmos de cada ejemplo descritos en las realizaciones dadas a conocer realizaciones de la presente divulgación pueden implementarse en forma de hardware electrónico, software informático, o una combinación de los mismos. Con el fin de describir claramente la intercambiabilidad de hardware y software, la descripción anterior ha descrito generalmente la composición y los bloques de método de cada realización en términos de funcionalidades. Si estas funcionalidades se realizan mediante hardware o software depende de las aplicaciones específicas y de las condiciones de restricción de diseño de las soluciones técnicas. Un experto en la técnica puede usar diferentes métodos para implementar las funciones descritas para cada aplicación particular. Sin embargo, tal implementación no debe considerarse que esté fuera del alcance de la presente divulgación.

Los bloques de método del método o el algoritmo descrito en las realizaciones dadas a conocer en el presente documento pueden implementarse mediante hardware, módulo(s) de software ejecutado(s) por procesador(es) o una combinación de los mismos. El/los módulo(s) de software pueden desplegarse en una memoria de acceso aleatorio (RAM), una memoria interna, una memoria de solo lectura (ROM), una ROM programable eléctricamente, una ROM

programable borrable eléctricamente, un registro, un disco duro, un disco extraíble, un CD-ROM o cualquier otro medio de almacenamiento bien conocido en la técnica.

Por ejemplo, la figura 5 muestra un servidor o aparato de ejemplo 500, como se describe en la figura 4, con más detalle. En una realización, el aparato 500 puede incluir uno o más procesadores 502, una interfaz de entrada/salida 504, una interfaz de red 506 y una memoria 508.

La memoria 508 puede incluir una forma de medio legible por ordenador como memoria volátil, memoria de acceso aleatorio (RAM) y/o una memoria no volátil, por ejemplo, memoria de solo lectura (ROM) o memoria RAM flash, etc. La memoria 508 es un ejemplo de un medio legible por ordenador.

El medio legible por ordenador puede incluir un tipo permanente o no permanente, un medio extraíble o no extraíble, que puede lograr el almacenamiento de información usando cualquier método o tecnología. La información puede incluir un comando legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Ejemplos de medios de almacenamiento por ordenador incluyen, pero no se limitan a, memoria de cambio de fase (PRAM), memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica (DRAM), otros tipos de memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria programable de solo lectura borrable electrónicamente (EEPROM), memoria flash rápida u otra tecnología de almacenamiento interno, memoria de solo lectura en disco compacto (CD-ROM), disco versátil digital (DVD) u otro almacenamiento óptico, cinta magnética de casete, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio de no transmisión, que puede usarse para almacenar información a la que pueda accederse mediante un dispositivo informático. Tal como se define en el presente documento, los medios legibles por ordenador no incluyen medios transitorios, como señales de datos moduladas y ondas portadoras.

En una realización, la memoria 508 puede incluir unidades de programa 510 y datos de programa 512. Las unidades de programa 510 pueden incluir uno o más módulos como se describe en las anteriores realizaciones. Por ejemplo, las unidades de programa 510 pueden incluir una o más de una unidad de recepción 401, una unidad de adquisición 402, una unidad de adición 403, una unidad de envío 404 y una unidad de almacenamiento en caché 405. Detalles de estas unidades se han descrito en las realizaciones anteriores, por lo que no se han descrito repetidamente en el presente documento.

REIVINDICACIONES

1. Método implementado por uno o más dispositivos informáticos, el método que comprende:

recibir (S210) mediante un servidor de contenido (400) una solicitud de consulta enviada por un lado de cliente (102) y obtener contenido de un campo de tipo de la solicitud de consulta;

obtener (S220) mediante el servidor de contenido (400) un tipo de la solicitud de consulta basándose al menos en parte en el contenido del campo de tipo, en el que si el contenido de los campos de tipo de solicitudes de consulta son diferentes los tipos correspondientes a esas solicitudes de consulta son diferentes;

añadir (S230) mediante el servidor de contenido (400) un identificador de tipo correspondiente al tipo y un nombre de dominio de un sistema de nombres de dominio autorizado preestablecido, DNS, (302) en la solicitud de consulta para obtener una solicitud de consulta objetivo; y

enviar (S240) mediante el servidor de contenido (400) la solicitud de consulta objetivo a un DNS local (104) para permitir que el DNS local (104) envíe la solicitud de consulta objetivo al DNS autorizado preestablecido (106) según el nombre de dominio del DNS autorizado preestablecido (106) en la solicitud de consulta objetivo y recibir un mensaje de respuesta que incluye información correspondiente al tipo de solicitud de consulta del DNS autorizado preestablecido (106),

en el que el lado de cliente (102) gestiona con el DNS local (104) y el DNS autorizado preestablecido (302) con antelación con respecto a la información respectiva representada por cada segmento en el mensaje de respuesta.

2. Método según la reivindicación 1, en el que la solicitud de consulta comprende una dirección de protocolo de Internet, IP, del lado de cliente (102).

3. Método según la reivindicación 2, en el que añadir (230) el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido (302) en la solicitud de consulta para obtener la solicitud de consulta objetivo comprende:

disponer una pluralidad de segmentos de la dirección IP en orden inverso; y

añadir secuencialmente el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido (302) a la pluralidad de segmentos de la dirección IP que están en el orden inverso para obtener la solicitud de consulta objetivo.

4. Método según la reivindicación 2 o la reivindicación 3, en el que el contenido del campo de tipo de la solicitud de consulta comprende una o más de una consulta de una ubicación a la que pertenece la dirección IP y una consulta sobre si la dirección IP está incluida en una lista negra.

5. Aparato que comprende un servidor de contenido (500), un sistema de nombres de dominio (DNS) local (104) y un DNS autorizado preestablecido (302),

el servidor (500) comprende:

uno o más procesadores (502);

memoria (508);

una unidad de recepción (401) almacenada en la memoria (508) y ejecutable por los uno o más procesadores (502) para recibir una solicitud de consulta enviada por un lado de cliente (102) y para obtener contenido de un campo de tipo de la solicitud de consulta;

una unidad de adquisición (402) almacenada en la memoria (508) y ejecutable por los uno o más procesadores (502) para obtener un tipo de la solicitud de consulta basándose en el contenido del campo de tipo, en el que si el contenido de los campos de tipo de solicitudes de consulta son diferentes los tipos correspondientes a esas solicitudes de consulta son diferentes;

una unidad de adición (403) almacenada en la memoria (508) y ejecutable por los uno o más procesadores (502) para añadir un identificador de tipo correspondiente al tipo obtenido mediante la unidad de adquisición (402) y un nombre de dominio del DNS autorizado preestablecido, (106) en la solicitud de consulta para obtener una solicitud de consulta objetivo; y

una unidad de envío (404) almacenada en la memoria (508) y ejecutable por los uno o más procesadores

(502) para enviar la solicitud de consulta objetivo obtenida mediante la unidad de adición (403) al DNS local (104) para permitir que el DNS local (104) envíe la solicitud de consulta objetivo al DNS autorizado preestablecido (302) según el nombre de dominio del DNS autorizado preestablecido (302) en la solicitud de consulta objetivo y para recibir un mensaje de respuesta que incluye información correspondiente al tipo de la solicitud de consulta del DNS autorizado preestablecido (106),

en el que el DNS local (104) y el DNS autorizado preestablecido (302) están configurados para gestionar con el lado de cliente (102) con antelación con respecto a la información respectiva representada por cada segmento en el mensaje de respuesta.

6. Servidor según la reivindicación 5, en el que la solicitud de consulta incluye una dirección de protocolo de Internet, IP, del lado de cliente (102).

7. Servidor según la reivindicación 6, en el que la unidad de adición (403) está configurada además para disponer una pluralidad de segmentos de la dirección IP en orden inverso y para añadir secuencialmente el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido (302) a la pluralidad de segmentos de la dirección IP que están en el orden inverso para obtener la solicitud de consulta objetivo.

8. Servidor según la reivindicación 6 o la reivindicación 7, en el que el contenido del campo de tipo de la solicitud de consulta comprende una o más de: una consulta de una ubicación a la que pertenece la dirección IP y una consulta sobre si la dirección IP está incluida en una lista negra.

9. Uno o más medios legibles por ordenador que almacenan instrucciones ejecutables que, cuando se ejecutan por uno o más procesadores (502), provocan que los uno o más procesadores (502) realicen acciones que comprenden:

recibir (S210) mediante un servidor de contenido (400) una solicitud de consulta enviada por un lado de cliente (102) y obtener contenido de un campo de tipo de la solicitud de consulta;

obtener (S220) mediante el servidor de contenido (400) un tipo de la solicitud de consulta basándose al menos en parte en el contenido del campo de tipo, en el que si el contenido de los campos de tipo de solicitudes de consulta son diferentes los tipos correspondientes a esas solicitudes de consulta son diferentes;

añadir (S230) mediante el servidor de contenido (400) un identificador de tipo correspondiente al tipo y un nombre de dominio de un sistema de nombres de dominio autorizado preestablecido (DNS) en la solicitud de consulta para obtener una solicitud de consulta objetivo; y

enviar (S240) mediante el servidor de contenido (400) la solicitud de consulta objetivo a un DNS local (302),

enviar mediante el DNS local (104) la solicitud de consulta objetivo al DNS autorizado preestablecido (302) según el nombre de dominio del DNS autorizado preestablecido (106) en la solicitud de consulta objetivo, y

recibir mediante el servidor de contenido (400) un mensaje de respuesta que incluye información correspondiente al tipo de solicitud de consulta del DNS autorizado preestablecido (106),

en el que el lado de cliente (102) gestiona con el DNS local (104) y el DNS autorizado preestablecido (302) con antelación con respecto a la información respectiva representada por cada segmento en el mensaje de respuesta.

10. Uno o más medios legibles por ordenador según la reivindicación 9, en los que la solicitud de consulta incluye una dirección de protocolo de Internet, IP, del lado de cliente (102).

11. Uno o más medios legibles por ordenador según la reivindicación 10, en el que añadir (S230) el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido (106) en la solicitud de consulta para obtener la solicitud de consulta objetivo comprende:

disponer una pluralidad de segmentos de la dirección IP en orden inverso; y

añadir secuencialmente el identificador de tipo correspondiente al tipo y el nombre de dominio del DNS autorizado preestablecido (106) a la pluralidad de segmentos de la dirección IP que están en el orden inverso para obtener la solicitud de consulta objetivo.

12. Uno o más medios legibles por ordenador según la reivindicación 10 o la reivindicación 11, en el que el contenido del campo de tipo de la solicitud de consulta comprende una o más de una consulta de una ubicación a la que pertenece la dirección IP y una consulta sobre si la dirección IP está incluida en una lista

negra.

13. Uno o más medios legibles por ordenador según la reivindicación 12, en el que el mensaje de respuesta comprende una o más de información que identifica la ubicación a la que pertenece la dirección IP e información que identifica si la dirección IP está incluida en la lista negra.

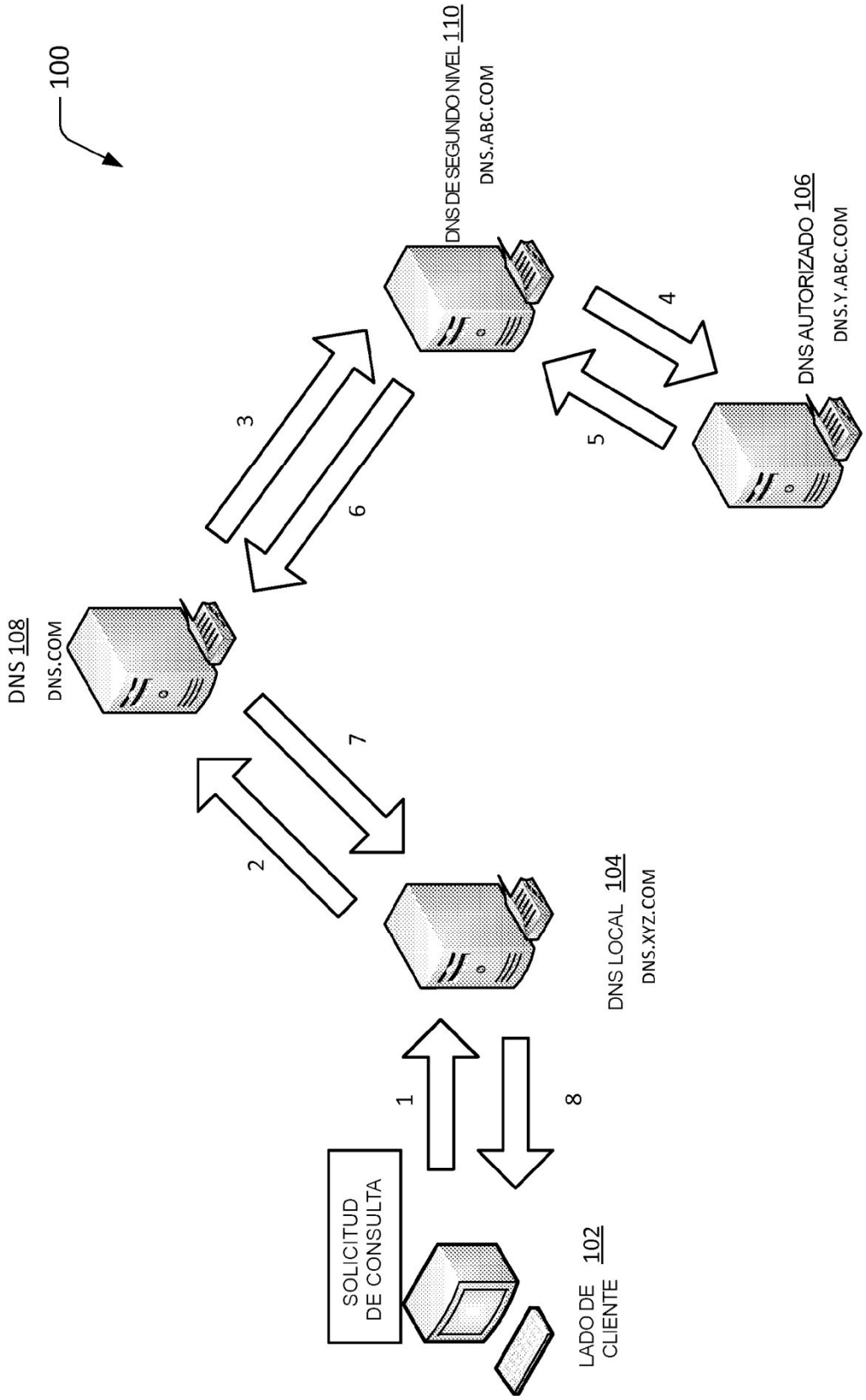

FIG. 1 (TÉCNICA ANTERIOR)

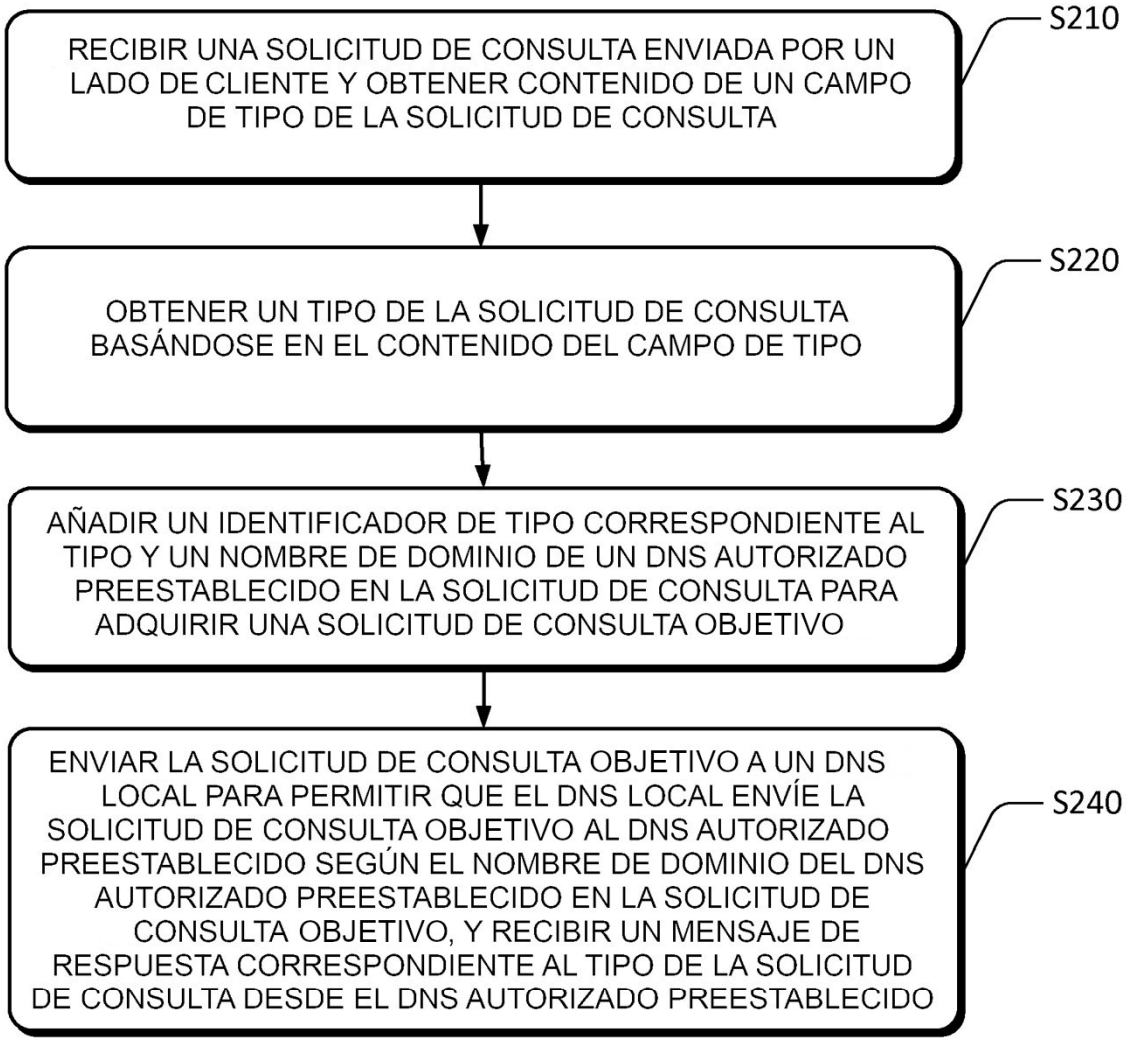
RECIBIR UNA SOLICITUD DE CONSULTA ENVIADA POR UN LADO DE CLIENTE Y OBTENER CONTENIDO DE UN CAMPO DE TIPO DE LA SOLICITUD DE CONSULTA
S210
OBTENER UN TIPO DE LA SOLICITUD DE CONSULTA BASÁNDOSE EN EL CONTENIDO DEL CAMPO DE TIPO
S220
AÑADIR UN IDENTIFICADOR DE TIPO CORRESPONDIENTE AL TIPO Y UN NOMBRE DE DOMINIO DE UN DNS AUTORIZADO PREESTABLECIDO EN LA SOLICITUD DE CONSULTA PARA ADQUIRIR UNA SOLICITUD DE CONSULTA OBJETIVO
S230
ENVIAR LA SOLICITUD DE CONSULTA OBJETIVO A UN DNS LOCAL PARA PERMITIR QUE EL DNS LOCAL ENVÍE LA SOLICITUD DE CONSULTA OBJETIVO AL DNS AUTORIZADO PREESTABLECIDO SEGÚN EL NOMBRE DE DOMINIO DEL DNS AUTORIZADO PREESTABLECIDO EN LA SOLICITUD DE CONSULTA OBJETIVO, Y RECIBIR UN MENSAJE DE RESPUESTA CORRESPONDIENTE AL TIPO DE LA SOLICITUD DE CONSULTA DESDE EL DNS AUTORIZADO PREESTABLECIDO
S240

FIG. 2

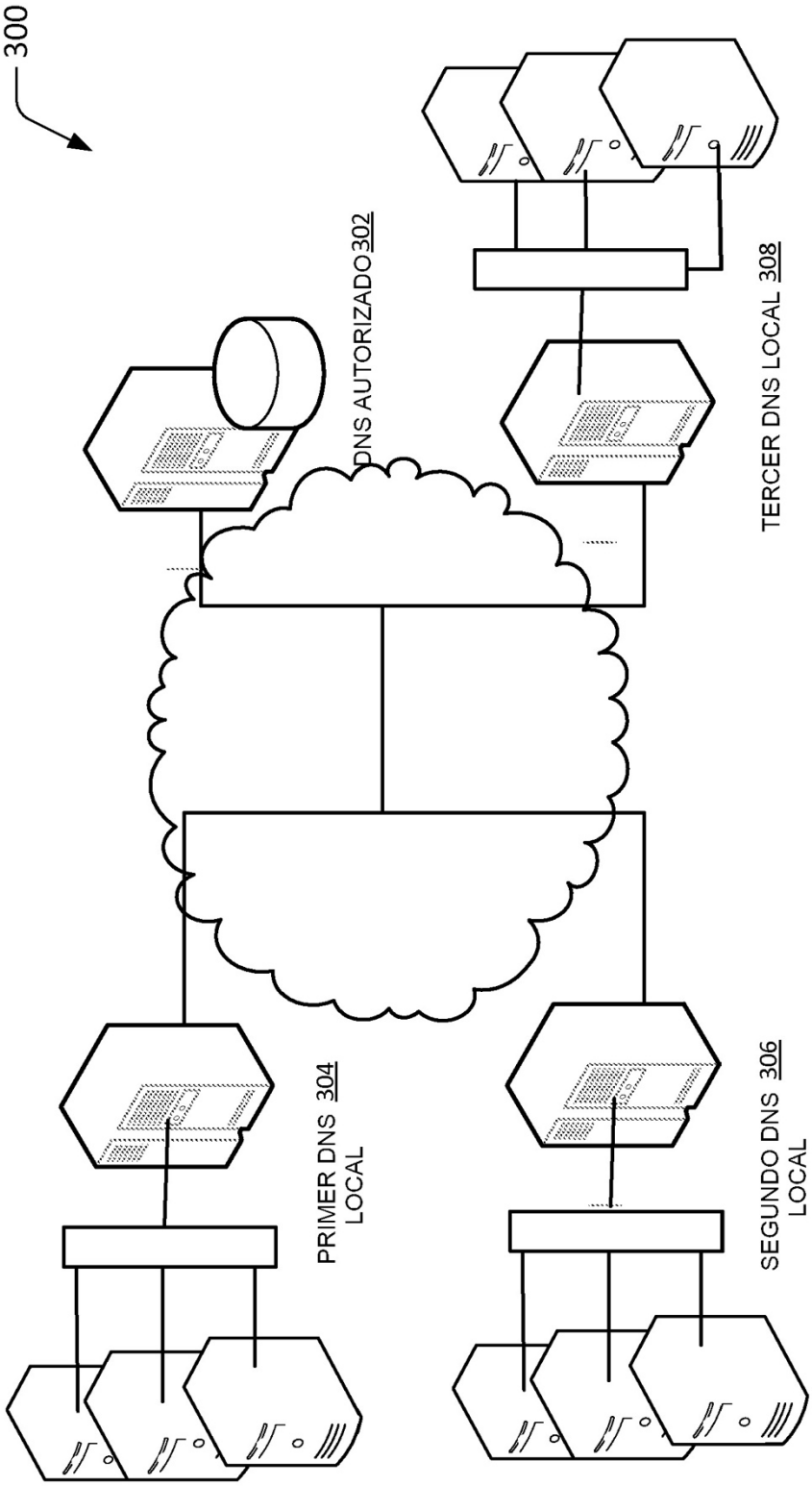
300
DNS AUTORIZADO 302
TERCER DNS LOCAL 308
PRIMER DNS LOCAL 304
SEGUNDO DNS LOCAL 306

FIG. 3

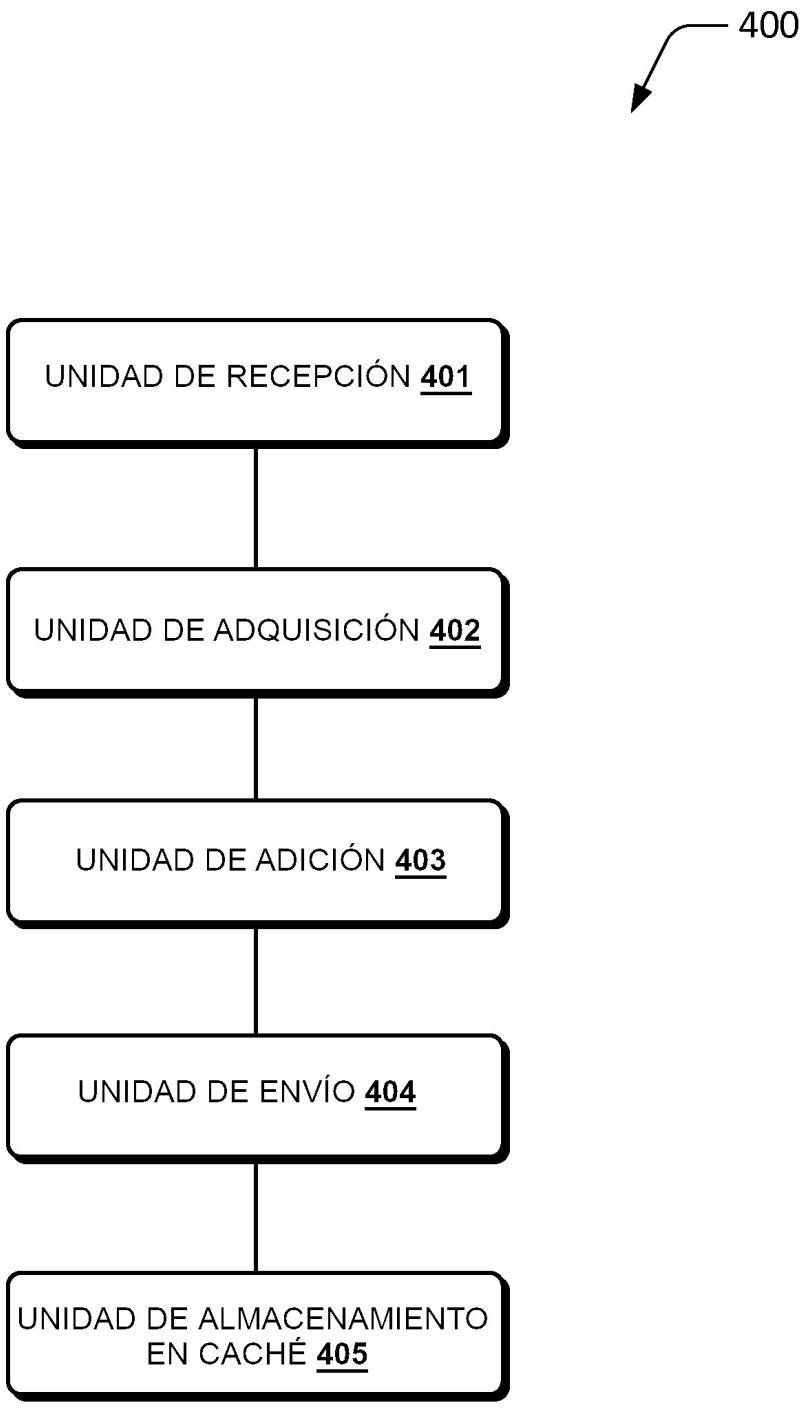
400
UNIDAD DE RECEPCIÓN 401
UNIDAD DE ADQUISICIÓN 402
UNIDAD DE ADICIÓN 403
UNIDAD DE ENVÍO 404
UNIDAD DE ALMACENAMIENTO EN CACHÉ 405

FIG. 4

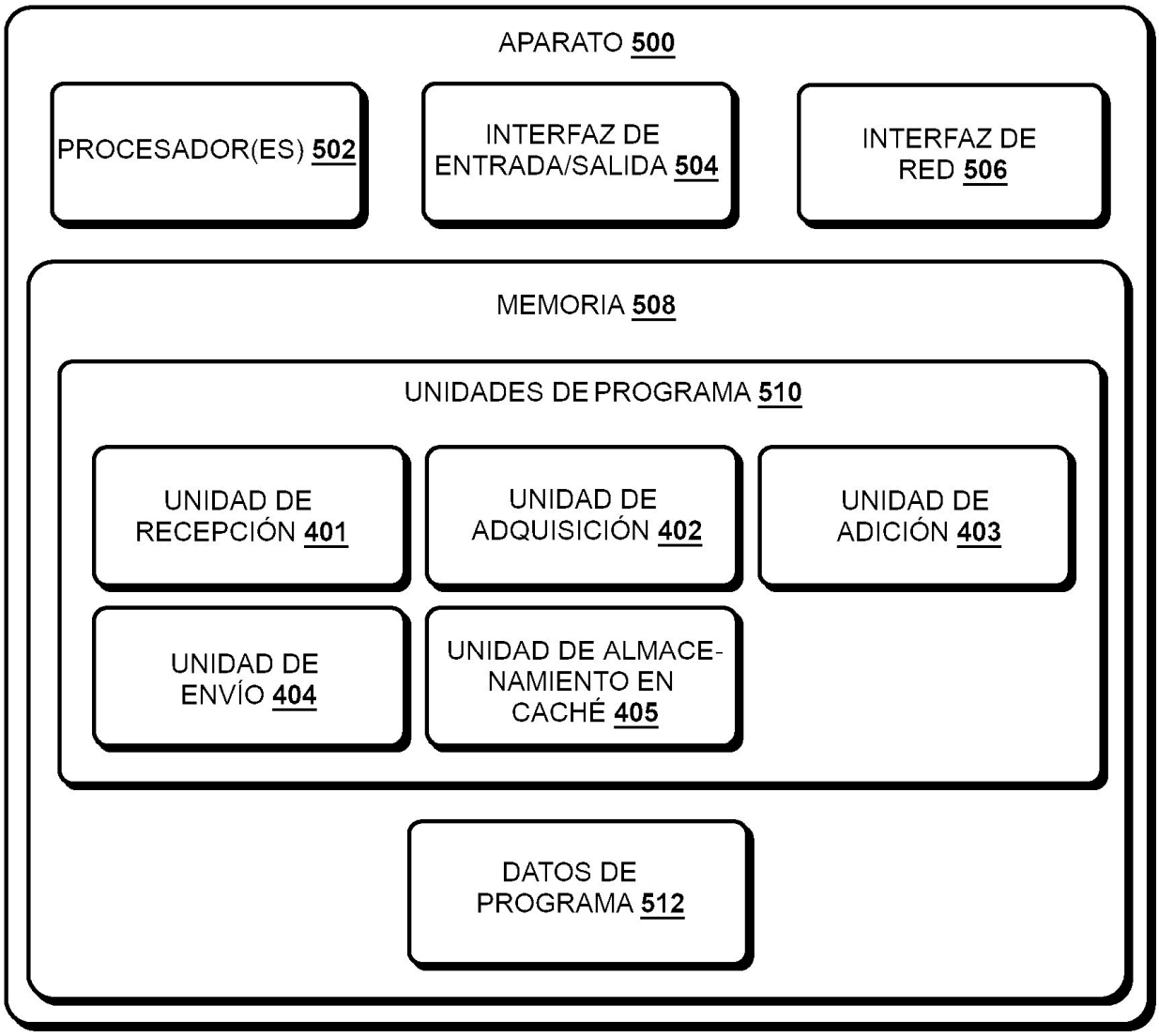
APARATO 500
PROCESADOR(ES) 502
INTERFAZ DE ENTRADA/SALIDA 504
INTERFAZ DE RED 506
MEMORIA 508
UNIDADES DE PROGRAMA 510
UNIDAD DE RECEPCIÓN 401
UNIDAD DE ADQUISICIÓN 402
UNIDAD DE ADICIÓN 403
UNIDAD DE ENVÍO 404
UNIDAD DE ALMACE-NAMIENTO EN CACHÉ 405
DATOS DE PROGRAMA 512

FIG. 5