(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 844 975**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.02.2017 PCT/US2017/016550**

(87) Fecha y número de publicación internacional: **31.08.2017 WO17146891**

(96) Fecha de presentación y número de la solicitud europea: **03.02.2017 E 17706056 (3)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2020 EP 3420696**

(54) Título: **Aparato y procedimiento para conectarse de forma segura a un servidor remoto**

(30) Prioridad:

24.02.2016 US 201615052736

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.07.2021

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

FROELICHER, JEFFREE;
SURYANARAYANA, LALITHA B.S. y
MANDYAM, GIRIDHAR

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Aparato y procedimiento para conectarse de forma segura a un servidor remoto

REFERENCIA CRUZADA A SOLICITUD RELACIONADA

[0001] Esta solicitud reivindica la prioridad y el beneficio de la solicitud no provisional n.º 15/052.736 presentada en la Oficina de Patentes y Marcas de los Estados Unidos el miércoles, 24 de febrero de 2016.

ANTECEDENTES

Campo

[0002] La presente invención se refiere, en general, a la seguridad de Internet y, más en particular, a la conexión segura a un servidor remoto en base a la resolución de nombres de dominio.

Antecedentes

[0003] La mayoría de los navegadores web indican http o https para las conexiones web en base a la URL a la que está conectado el dispositivo. Un usuario puede determinar si la conexión de la capa de aplicación es segura en base a ver "https://" en la URL y un icono que indica que se está usando https. Cuando se usan otros protocolos de seguridad, tales como IPsec de un extremo a otro, para comunicarse con un servidor, el navegador no realiza dicha indicación. También es difícil obligar a los servidores a hacer cumplir las políticas de seguridad con respecto a cómo se protegen y procesan los datos y la información confidencial de un usuario. Además, una red privada virtual (VPN) típicamente requiere que el usuario inicie primero el software del cliente antes de su uso.

[0004] Por lo tanto, existe la necesidad de una técnica mejorada para conectarse de forma segura a un servidor remoto en la capa IP.

[0005] El documento US 2002/0093915 A1 divulga un procedimiento para establecer una conexión VPN entre dos dispositivos.

BREVE EXPLICACIÓN

[0006] Un aspecto de la presente invención puede residir en un procedimiento para conectarse de forma segura a un servidor remoto, que comprende: recibir, por parte de un cliente, una solicitud para conectarse a un servidor remoto asociado con un nombre de dominio; determinar, por parte del cliente al resolver el nombre de dominio, si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio; realizar, por parte del cliente, un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; y conectarse, por parte del cliente, al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado

[0007] En aspectos más detallados de la invención, el cliente puede determinar que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado en base a un dominio de nivel superior del nombre de dominio. De forma alternativa, el cliente puede determinar que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado en base a la validación del nombre de dominio usando comunicaciones con un servidor del Sistema de Nombres de Dominio (DNS). Las comunicaciones con el servidor DNS pueden usar un protocolo DNS seguro. El cliente puede recibir, del servidor DNS, un registro de servicio DNS para el nombre de dominio validado que incluye al menos un parámetro que indica que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado.

[0008] En otros aspectos más detallados de la invención, el cliente puede determinar que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado en base a que el cliente determina que el nombre de dominio está en una lista de nombres de dominio de confianza que soportan el al menos un protocolo de seguridad de capa IP predeterminado. Además, el nombre de dominio puede resolverse en una dirección IP.

[0009] Otro aspecto de la invención puede residir en un aparato para conectarse de forma segura a un servidor remoto, que comprende: un medio para recibir una solicitud para conectarse a un servidor remoto asociado con un nombre de dominio; un medio para determinar si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio; un medio para realizar un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; y un medio para conectarse al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado.

[0010] Otro aspecto de la invención puede residir en un aparato, que comprende: un procesador configurado para: recibir una solicitud para conectarse a un servidor remoto asociado con un nombre de dominio; determinar si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio; realizar un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; y conectarse al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado.

[0011] Otro aspecto de la invención puede residir en un medio legible por ordenador, que comprende: un código para hacer que un ordenador reciba una solicitud para conectarse a un servidor remoto asociado con un nombre de dominio; un código para hacer que el ordenador determine si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio; un código para hacer que el ordenador realice un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; un código para hacer que el ordenador se conecte al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado.

[0012] La invención se define por las reivindicaciones adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0013]

La FIG. 1 es un diagrama de bloques de un ejemplo de sistema de comunicación inalámbrica.

La FIG. 2 es un diagrama de flujo de un procedimiento para conectarse de forma segura a un servidor remoto, de acuerdo con la presente invención.

La FIG. 3 es un diagrama de bloques de un modo de realización de un sistema que permite que un cliente se conecte de forma segura a un servidor remoto.

La FIG. 4 es un diagrama de bloques de un ordenador que incluye un procesador y una memoria.

La FIG. 5 es un diagrama de bloques de un procedimiento para conectarse de forma segura a un servidor remoto.

La FIG. 6 es un diagrama de bloques de otro procedimiento para conectarse de forma segura a un servidor remoto.

La FIG. 7 es un diagrama de bloques de otro procedimiento para conectarse de forma segura a un servidor remoto.

DESCRIPCIÓN DETALLADA

[0014] El término "ejemplar" se usa en el presente documento en el sentido de "que sirve de ejemplo, caso o ilustración". No se ha de interpretar necesariamente que cualquier modo de realización descrito en el presente documento como "ejemplar" sea preferente o ventajoso con respecto a otros modos de realización.

[0015] Con referencia a las FIG. 2 y 3, un aspecto de la presente invención puede residir en un procedimiento 200 para conectarse de forma segura a un servidor remoto. En el procedimiento, un cliente 310 recibe una solicitud para conectarse a un servidor remoto 320 asociado con un nombre de dominio (etapa 210). El cliente, al resolver el nombre de dominio, determina si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado (etapa 220). El cliente realiza un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado (etapa 230). El cliente se conecta al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado (etapa 240).

[0016] En aspectos más detallados de la invención, el cliente 310 puede determinar que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado en base a un dominio de nivel superior del nombre de dominio. Por ejemplo, determinados dominios de nivel superior pueden estar asociados con soportar un protocolo de seguridad de capa IP predeterminado, tal como IPsec. Soportar de dominios de nivel superior puede incluir .sec, .secure, .msec, .ipsec, .scom y similares. Una solicitud que incluya el nombre de dominio www-punto-ejemplo-punto-sec indicaría que el servidor remoto asociado con el nombre de dominio es compatible con el protocolo de seguridad de capa IP predeterminado, tal como IPsec.

[0017] De forma alternativa, el cliente 310 puede determinar que el servidor remoto 320 soporta el al menos un protocolo de seguridad de capa IP predeterminado en base a la validación del nombre de dominio usando comunicaciones con un servidor 330 del Sistema de Nombres de Dominio (DNS). Las comunicaciones con el servidor DNS pueden usar un protocolo DNS seguro, tal como DNSsec. El cliente puede recibir, del servidor DNS, un registro

de servicio DNS para el nombre de dominio validado que incluye al menos un parámetro que indica que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado.

[0018] En otros aspectos más detallados de la invención, el cliente 310 puede determinar que el servidor remoto 320 soporta el al menos un protocolo de seguridad de capa IP predeterminado en base a que el cliente determina que el nombre de dominio está en una lista de nombres de dominio de confianza que soportan el al menos un protocolo de seguridad de capa IP predeterminado. Además, el nombre de dominio puede resolverse en una dirección IP.

[0019] Con más referencia a la FIG. 4, el cliente 310 (por ejemplo, la estación remota 102 (FIG. 1)) puede comprender un ordenador 400 que incluye un procesador 410, un medio de almacenamiento 420 tal como una memoria y/o una unidad de disco, una pantalla 430 y una entrada tal como como un teclado 440 y una red inalámbrica/conexión a Internet 450. El procesador puede incluir un entorno seguro tal como un módulo de plataforma de confianza (TPM).

[0020] Otro aspecto de la invención puede residir en un aparato 310 para conectarse de forma segura a un servidor remoto, que comprende: un medio (por ejemplo, procesador 410) para recibir una solicitud para conectarse a un servidor remoto 320 asociado con un nombre de dominio; un medio (por ejemplo, procesador 410) para determinar si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado cuando se resuelve el nombre de dominio; un medio (por ejemplo, procesador 410) para realizar un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; y un medio (por ejemplo, procesador 410) para conectarse al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado.

[0021] Otro aspecto de la invención puede residir en un aparato 310, que comprende: un procesador 410 configurado para: recibir una solicitud para conectarse a un servidor remoto 320 asociado con un nombre de dominio; determinar si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio; realizar un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; y conectarse al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado.

[0022] Otro aspecto de la invención puede residir en un medio legible por ordenador 420, que comprende: un código para hacer que un ordenador 400 reciba una solicitud para conectarse a un servidor remoto 320 asociado con un nombre de dominio; un código para hacer que el ordenador determine si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio; un código para hacer que el ordenador realice un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP predeterminado; un código para hacer que el ordenador se conecte al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP predeterminado.

[0023] El cliente 310 puede tener una capa de aplicación, una capa de Internet/IP y una capa física/de enlace. En el modelo OSI, la capa 7 se puede asociar con la capa de aplicación, la capa 3 se puede asociar con la capa de Internet/IP y las capas 1 y 2 se pueden asociar con la capa física/de enlace. El servidor remoto 320 y/o el servidor DNS 330 también pueden tener una capa de aplicación, una capa de Internet/IP y una capa física/de enlace.

[0024] Las técnicas de la presente invención pueden activar/iniciar protocolos de capa IP seguros tales como IPsec y hacer cumplir determinadas políticas de seguridad, en base a, por ejemplo, la resolución de nombres de dominio. Las técnicas pueden aprovechar el Protocolo de Internet versión 6 (IPv6) con IPsec nativo usando encabezados IPv6 integrados y encabezados adicionales según sea necesario. Las técnicas pueden usar el modo de transporte IPsec para la comunicación de punto extremo a punto extremo (no el típico VPN IPsec). El modo de transporte IPsec puede incluir un encabezado de autenticación (AH) para garantizar la integridad total del paquete y la autenticidad del origen (ICV) e identificar los parámetros de seguridad (SPI) y evitar la reproducción (SQN). La carga útil de seguridad encapsulada (ESP) se puede usar para garantizar la confidencialidad de los datos. Se puede usar al menos el cifrado AES-256 y se puede usar el Intercambio de Claves de Internet (IKEv2) para negociar claves y parámetros. DNSsec puede proporcionar certificados X.509 iniciales. Los clientes pueden tener certificados X.509 con claves seguras. Se puede realizar un intercambio de claves Diffie-Hellman para generar al menos un secreto compartido, tal como claves de sesión, y la Asociación de Seguridad IPsec puede usar los secretos compartidos.

[0025] El modo de transporte IPsec puede implementarse usando Descriptores de Política de Seguridad (SPD) particulares que establecen algunas Asociaciones de Seguridad (SA) predefinidas para servidores previamente conectados. Las SA de IPsec son nativas del sistema operativo y las configura IKE a través de servicios o aplicaciones del sistema operativo tales como StrongSWAN, LibreSWAN, OpenSWAN, IPsec-Tools y similares. IPv6 puede incluir IPsec nativo.

[0026] En un ejemplo mostrado con referencia a la FIG. 5, el cliente 310, a través de una aplicación o navegador

web, puede iniciar una conexión a un dominio de nivel superior (TLD) específico tal como '.sec' para el sitio web www-punto-url-punto-sec que el resolutor del cliente tomaría como indicación de que pueden ser necesarias Asociaciones de Seguridad IPsec (etapa 510). Todos los Nombres de Dominio Totalmente Cualificados asignados bajo dichos TLD estarían certificados para cumplir con determinados requisitos de seguridad y privacidad establecidos por el propietario del TLD. El FQDN está validado y resuelto. El cliente puede requerir la verificación de DNSsec para el TLD usando el servidor DNS 330 (etapa 520 y 530). El cliente verifica la ruta y descarga y valida el certificado X.509 desde el servidor remoto 320 y cualquier Autoridad Certificadora (CA) raíz para ese TLD. El sistema de resolución de DNS del cliente puede validar que se hayan cumplido y verificado las condiciones para establecer IPsec (etapa 540). Por tanto, el cliente puede utilizar el TLD validado para determinar el "tráfico interesante" e iniciar una conexión IPsec al servidor remoto 320 asociado con el nombre de dominio url.sec (etapa 550). Cabe señalar que determinar si el servidor remoto soporta al menos un protocolo de seguridad de capa IP predeterminado al resolver el nombre de dominio puede comprender la etapa de solicitud 520, la etapa de recepción 530 y la etapa de validación 540. El cliente puede establecer la conexión IPsec iniciando IKE o IKEv2 con el servidor remoto. Se puede usar un protocolo de enlace IKEv2 para generar uno o más secretos compartidos para establecer una conexión segura de extremo a extremo entre el cliente y el servidor remoto. Ambas partes, al usar el TLD, aceptan al menos una configuración y un protocolo predeterminados de IPsec/ISAKMP, lo que simplifica el proceso de configuración. Debido a que la certificación TLD hace cumplir determinadas políticas (es decir, a través de la Certificación de una Autoridad de Certificación), un usuario sabe que el cliente está conectado de forma segura y los datos transferidos serán manejados por el servidor remoto de acuerdo con las políticas necesarias para la certificación. Se podría aplicar una técnica similar al subdominio (sec.dominio.com) si el certificado firmado incluye la misma CA raíz.

[0027] En otro ejemplo mostrado con referencia a la FIG. 6, el cliente 310 puede iniciar una conexión a un servidor remoto 320 de confianza desde un navegador o aplicación usando una URL típica (etapa 610). La resolución de DNS con el servidor DNS 330 puede contener la dirección IP (IPv6), la verificación de DNSsec, un certificado DANE X.509 y un registro de servicio DNS (registro de servicio SRV) que indica que el servidor remoto admite un determinado protocolo de seguridad tal como IKE e IPsec (etapas 620 y 630). El sistema de resolución de DNS del cliente puede validar que se hayan cumplido y verificado las condiciones para establecer IPsec (etapa 640). Tanto el cliente como el servidor remoto, al usar el registro de servicio, aceptan algunas configuraciones y protocolos IKE/IPsec predefinidos, lo que simplifica el proceso de configuración. Debido a que el registro de servicio y la CA raíz imponen determinadas políticas, el cliente está conectado de forma segura y los datos del usuario serán manejados por el servidor remoto de acuerdo con las políticas necesarias para la certificación (etapa 650). El cliente puede establecer la conexión IPsec iniciando IKE o IKEv2 con el servidor remoto.

[0028] En otro ejemplo mostrado con referencia a la FIG. 7, el cliente 310 puede iniciar una conexión en base a la URL de un servidor 320 de confianza (etapa 710). La URL (es decir, FQDN) se valida y se resuelve en una dirección IP. Una lista de FQDN admitidos está preconfigurada para indicar qué servidores remotos aceptan algunas configuraciones y protocolos IKE/IPsec predefinidos, lo que simplifica el proceso de configuración. Una solicitud y respuesta de DNS verifica que la dirección IP coincida con el valor almacenado previamente (etapas 720 y 730). El FQDN coincide con un FQDN soportado en la lista. El cliente puede validar que se hayan cumplido y verificado las condiciones para establecer IPsec (etapa 740). Debido a que estas listas de FQDN predefinidas y la validación de la CA raíz requieren/hacen cumplir determinadas políticas, el cliente está conectado de forma segura y los datos del usuario serán manejados por el servidor de acuerdo con las políticas necesarias para la certificación (etapa 750). El cliente puede establecer la conexión IPsec iniciando IKE o IKEv2 con el servidor remoto.

[0029] A diferencia de la seguridad de conexión de la capa de aplicación, tal como SSL o TLS cuando un navegador web usa https, el protocolo de seguridad de capa IP puede proporcionar protección de seguridad de la capa IP. Además, a diferencia de una red privada virtual (VPN) de capa de aplicación, el protocolo de seguridad de capa IP puede activarse automáticamente para un servidor remoto 320 sin requerir la intervención o iniciación del usuario. En su lugar, el protocolo de seguridad de capa IP puede activarse en respuesta a la determinación, por parte del cliente 310 al resolver el nombre de dominio, de que el servidor remoto 320 soporta el protocolo de seguridad de capa IP.

[0030] Con referencia a la FIG. 1, una estación remota inalámbrica (RS) 102 (por ejemplo, una estación móvil MS) puede comunicarse con una o más estaciones base (BS) 104 de un sistema de comunicación inalámbrica 100. El sistema de comunicación inalámbrica 100 puede incluir además uno o más controladores de estación base (BSC) 106, y una red central 108. La red central puede estar conectada a Internet 110 y a una Red telefónica pública conmutada (PSTN) 112 a través de redes de retorno adecuadas. Una estación móvil inalámbrica típica puede incluir un teléfono portátil o un ordenador portátil. El sistema de comunicación inalámbrica 100 puede emplear cualquiera de varias técnicas de acceso múltiple tales como acceso múltiple por división de código (CDMA), acceso múltiple por división de tiempo (TDMA), acceso múltiple por división de frecuencia (FDMA), acceso múltiple por división de espacio (SDMA), acceso múltiple por división de polarización (PDMA), u otras técnicas de modulación conocidas en la técnica.

[0031] Los expertos en la técnica entenderán que la información y las señales se pueden representar usando cualquiera de una variedad de tecnologías y técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips de información que se puedan haber mencionado a lo largo de la descripción anterior se pueden representar por tensiones, corrientes, ondas

electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos, o cualquier combinación de los mismos.

[0032] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con los modos de realización divulgados en el presente documento se pueden implementar como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito en general diversos componentes, bloques, módulos, circuitos y etapas ilustrativos en lo que respecta a su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de la aplicación particular y de las restricciones de diseño impuestas al sistema global. Los expertos en la técnica pueden implementar la funcionalidad descrita de formas distintas para cada aplicación particular, pero no debería interpretarse que dichas decisiones de implementación suponen apartarse del alcance de la presente invención.

[0033] Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con los modos de realización divulgados en el presente documento se pueden implementar o realizar con un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro dispositivo de lógica programable, lógica de puertas o transistores discretos, componentes de hardware discretos o con cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también se puede implementar como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

[0034] Las etapas de un procedimiento o algoritmo descrito en relación con los modos de realización divulgados en el presente documento se pueden incorporar directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo de software puede residir en memoria RAM, memoria *flash*, memoria ROM, memoria EPROM, memoria EEPROM, registros, un disco duro, un disco extraíble, un CD-ROM o cualquier otra forma de medio de almacenamiento conocida en la técnica. Un medio de almacenamiento ejemplar está acoplado al procesador de modo que el procesador puede leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

[0035] En uno o más modos de realización ejemplares, las funciones descritas se pueden implementar en hardware, software, firmware o en cualquier combinación de los mismos. Si se implementan en software como producto de programa informático, las funciones pueden almacenarse o transmitirse como una o varias instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios no transitorios de almacenamiento legibles por ordenador como medios de comunicación, incluido cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que se pueda acceder mediante un ordenador. A modo de ejemplo y no de limitación, dichos medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otros dispositivos de almacenamiento en disco óptico, de almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que se pueda usar para llevar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que se pueda acceder mediante un ordenador. Además, cualquier conexión recibe apropiadamente la denominación de medio legible por ordenador. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea digital de abonado (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas, tales como infrarrojos, radio y microondas, se incluyen en la definición de medio. Los discos, como se usan en el presente documento, incluyen el disco compacto (CD), el disco láser, el disco óptico, el disco versátil digital (DVD), el disco flexible y el disco Blu-ray, donde algunos discos reproducen habitualmente datos magnéticamente y otros discos reproducen datos ópticamente con láseres. Las combinaciones de lo anterior también se deben incluir dentro del alcance de los medios legibles por ordenador.

[0036] La descripción anterior de los modos de realización divulgados se proporciona para permitir que cualquier experto en la técnica realice o use la presente invención. Varias modificaciones a estos modos de realización serán fácilmente evidentes para los expertos en la técnica. Por tanto, la presente invención no se pretende limitar a los modos de realización mostrados en el presente documento, sino que se le ha de conceder el alcance más amplio consecuente con los principios y características novedosos divulgados en el presente documento.

REIVINDICACIONES

1. Un procedimiento para conectarse de forma segura a un servidor remoto, que comprende:

recibir, por parte de un cliente, una solicitud para conectarse a un servidor remoto asociado con un nombre de dominio;

en respuesta a recibir la solicitud para conectarse a un servidor remoto asociado con el nombre de dominio, obtener por parte del cliente una resolución de nombre de dominio de un servidor de Sistema de Nombres de Dominio, DNS, en el que la resolución de nombre de dominio incluye una dirección de Protocolo de Internet, IP, para el servidor remoto y un registro de servicio DNS para el nombre de dominio que incluye al menos un parámetro que indica que el servidor remoto soporta al menos un protocolo de seguridad de capa IP;

determinar, por parte del cliente, que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP basado en el al menos un parámetro que indica que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP incluido en el registro de servicio DNS incluido en la resolución DNS obtenida del servidor DNS;

realizar, por parte del cliente, un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP; y

conectarse, por parte del cliente, al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP para establecer una conexión segura entre el cliente en un punto extremo de la conexión segura y el servidor remoto en otro punto extremo de la conexión segura.

2. El procedimiento de acuerdo con la reivindicación 1, en el que las comunicaciones con el servidor DNS usan un protocolo DNS seguro.

3. Un aparato para conectarse de forma segura a un servidor remoto, que comprende:

un medio para recibir una solicitud para conectarse a un servidor remoto asociado con un nombre de dominio;

un medio para, en respuesta a recibir la solicitud para conectarse a un servidor remoto asociado con el nombre de dominio, obtener por parte del cliente una resolución de nombre de dominio de un servidor de Sistema de Nombres de Dominio, DNS, en el que la resolución de nombre de dominio incluye una dirección de Protocolo de Internet, IP, para el servidor remoto y un registro de servicio DNS para el nombre de dominio que incluye al menos un parámetro que indica que el servidor remoto soporta al menos un protocolo de seguridad de capa IP;

un medio para determinar para determinar que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP basado en el al menos un parámetro que indica que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP incluido en el registro de servicio DNS incluido en la resolución DNS obtenida del servidor DNS;

un medio para realizar un protocolo de intercambio de claves con el servidor remoto para generar al menos un secreto compartido en respuesta a la determinación de que el servidor remoto soporta el al menos un protocolo de seguridad de capa IP; y

un medio para conectarse al servidor remoto usando el al menos un secreto compartido en el al menos un protocolo de seguridad de capa IP para establecer una conexión segura entre el aparato en un punto extremo de la conexión segura y el servidor remoto en otro punto extremo de la conexión segura.

4. El aparato de acuerdo con la reivindicación 3, en el que las comunicaciones con el servidor DNS usan un protocolo DNS seguro.

5. Un medio legible por ordenador, que comprende un código que, cuando se ejecuta en un dispositivo, emprende el procedimiento de acuerdo con la reivindicación 1 o 2.

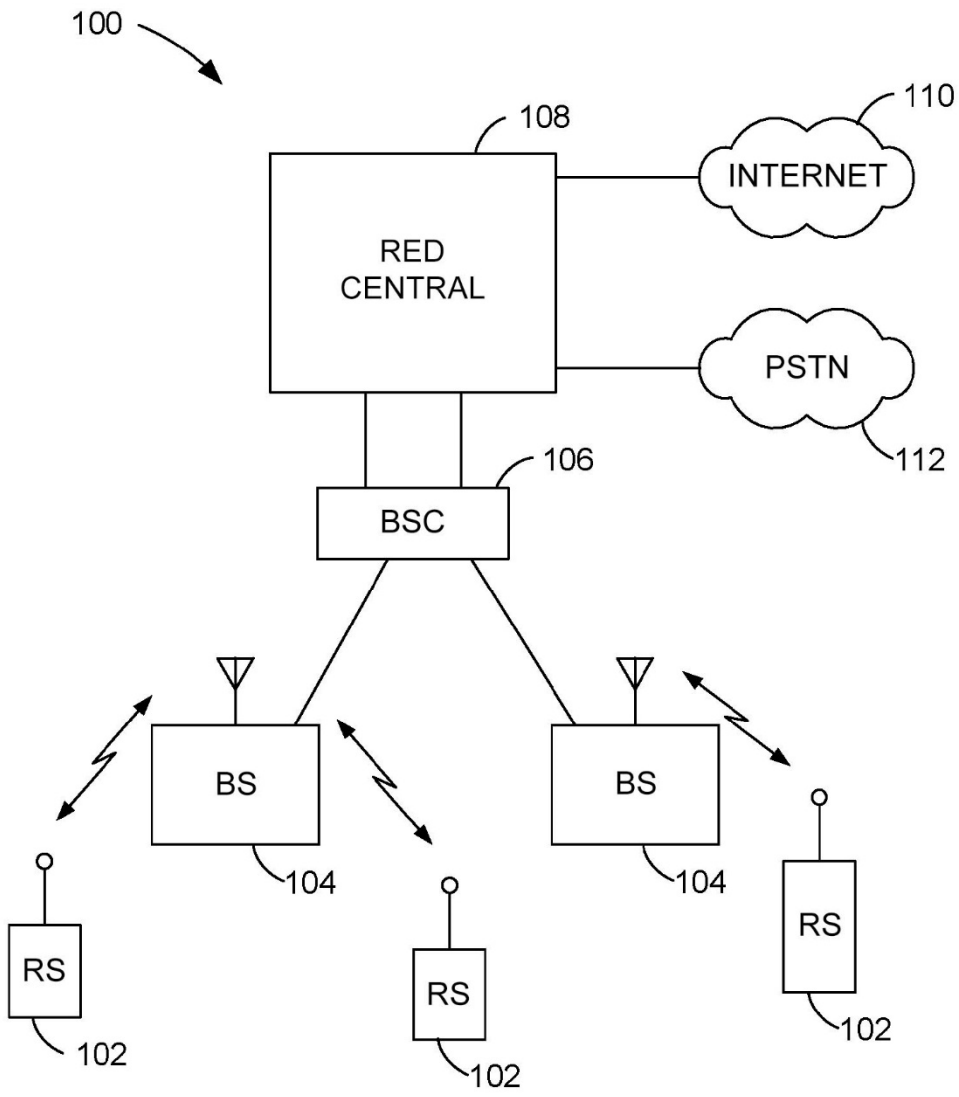
100
108
110
INTERNET
RED
CENTRAL
PSTN
112
106
BSC
BS
BS
104
104
RS
RS
RS
102
102
102

FIG. 1

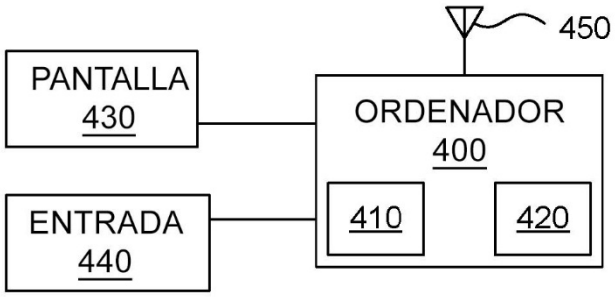
450
PANTALLA
430
ORDENADOR
400
ENTRADA
440
410
420

FIG. 4

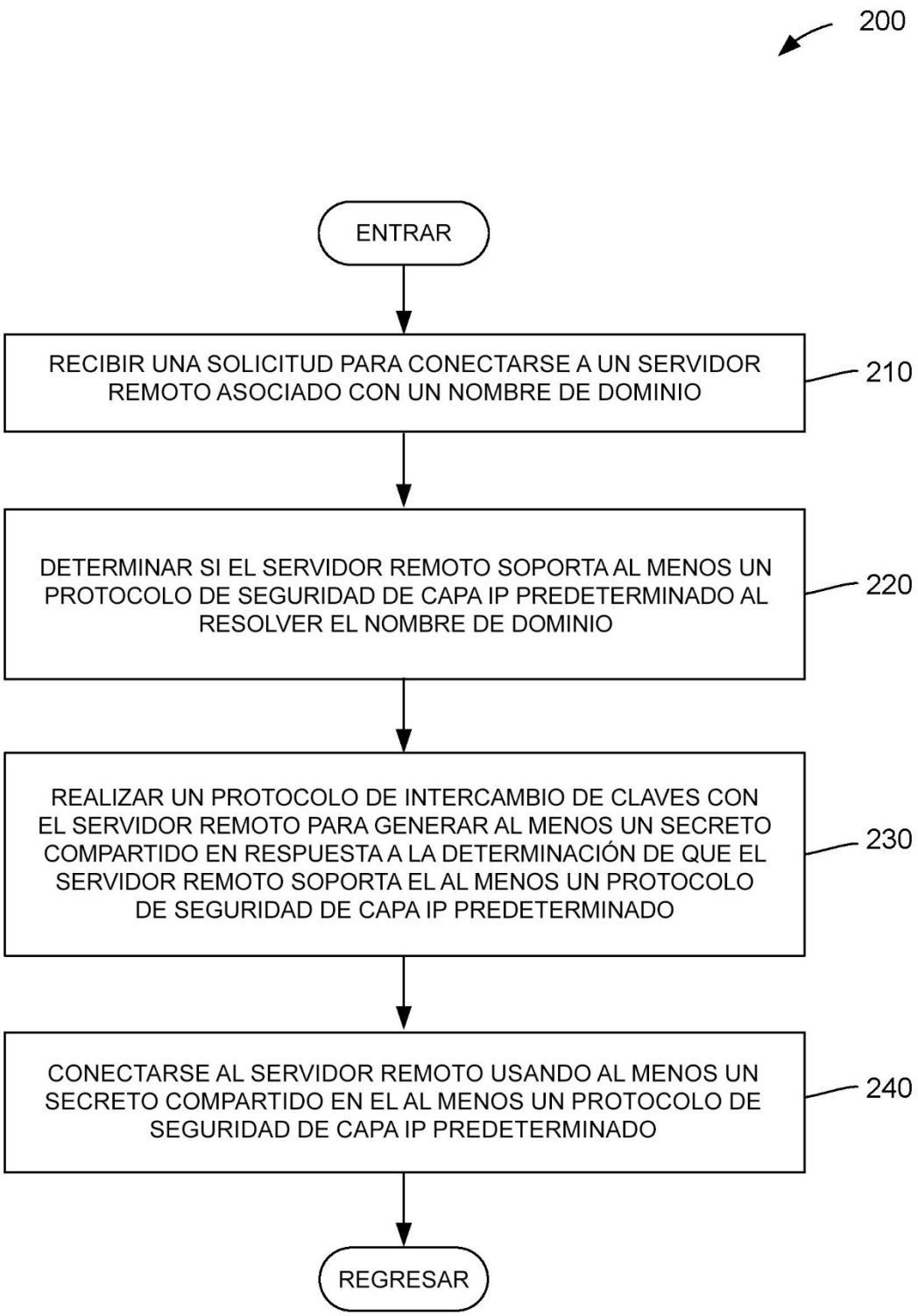
200
ENTRAR
RECIBIR UNA SOLICITUD PARA CONECTARSE A UN SERVIDOR REMOTO ASOCIADO CON UN NOMBRE DE DOMINIO
210
DETERMINAR SI EL SERVIDOR REMOTO SOPORTA AL MENOS UN PROTOCOLO DE SEGURIDAD DE CAPA IP PREDETERMINADO AL RESOLVER EL NOMBRE DE DOMINIO
220
REALIZAR UN PROTOCOLO DE INTERCAMBIO DE CLAVES CON EL SERVIDOR REMOTO PARA GENERAR AL MENOS UN SECRETO COMPARTIDO EN RESPUESTA A LA DETERMINACIÓN DE QUE EL SERVIDOR REMOTO SOPORTA EL AL MENOS UN PROTOCOLO DE SEGURIDAD DE CAPA IP PREDETERMINADO
230
CONECTARSE AL SERVIDOR REMOTO USANDO AL MENOS UN SECRETO COMPARTIDO EN EL AL MENOS UN PROTOCOLO DE SEGURIDAD DE CAPA IP PREDETERMINADO
240
REGRESAR

FIG. 2

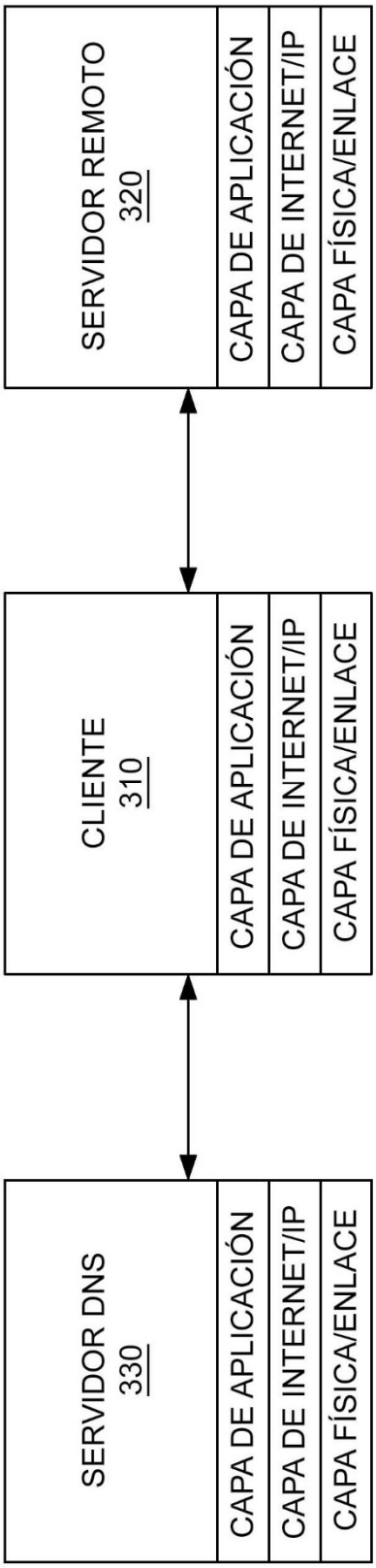
SERVIDOR DNS
330
CAPA DE APLICACIÓN
CAPA DE INTERNET/IP
CAPA FÍSICA/ENLACE
CLIENTE
310
CAPA DE APLICACIÓN
CAPA DE INTERNET/IP
CAPA FÍSICA/ENLACE
SERVIDOR REMOTO
320
CAPA DE APLICACIÓN
CAPA DE INTERNET/IP
CAPA FÍSICA/ENLACE

FIG. 3

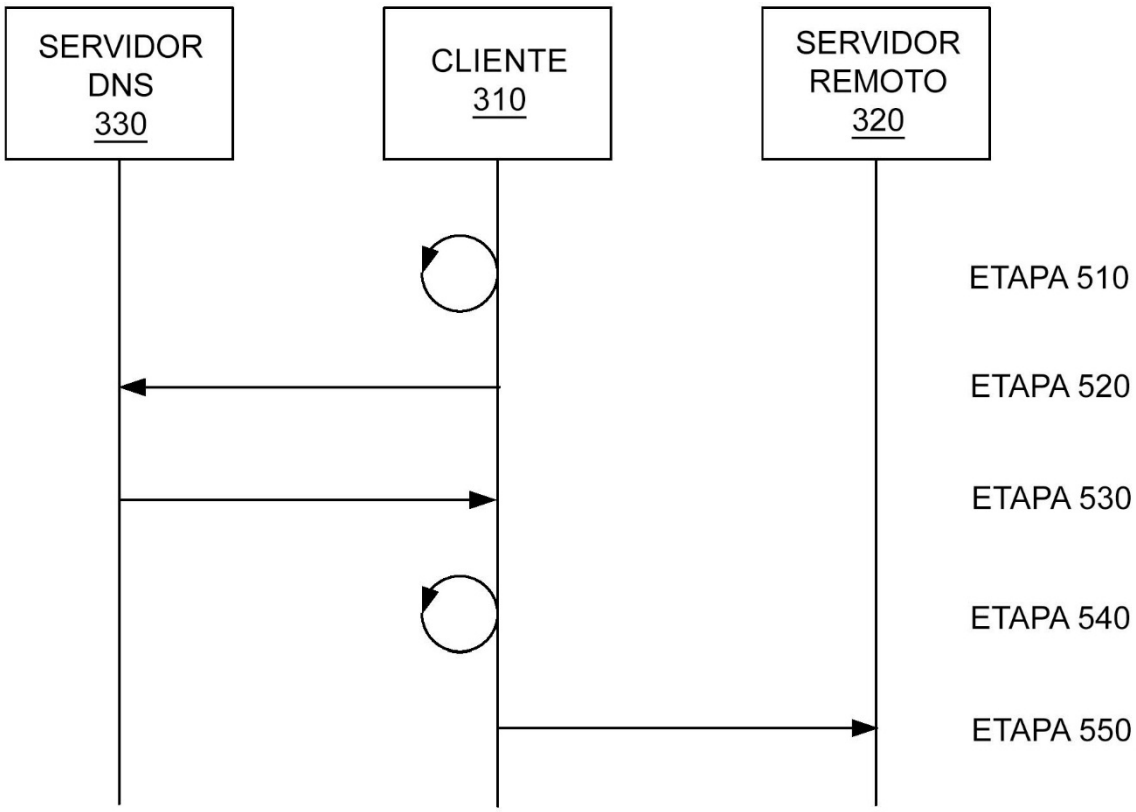
SERVIDOR DNS 330
CLIENTE 310
SERVIDOR REMOTO 320
ETAPA 510
ETAPA 520
ETAPA 530
ETAPA 540
ETAPA 550

FIG. 5

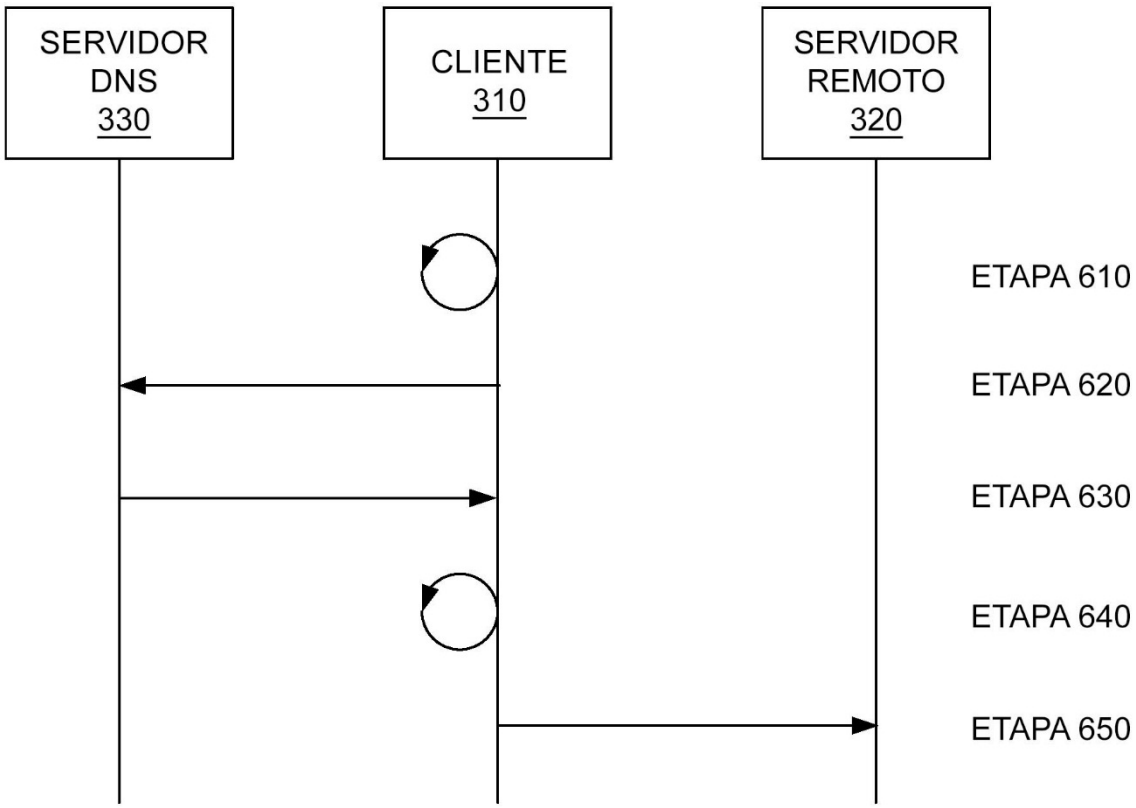
SERVIDOR DNS 330
CLIENTE 310
SERVIDOR REMOTO 320
ETAPA 610
ETAPA 620
ETAPA 630
ETAPA 640
ETAPA 650

FIG. 6

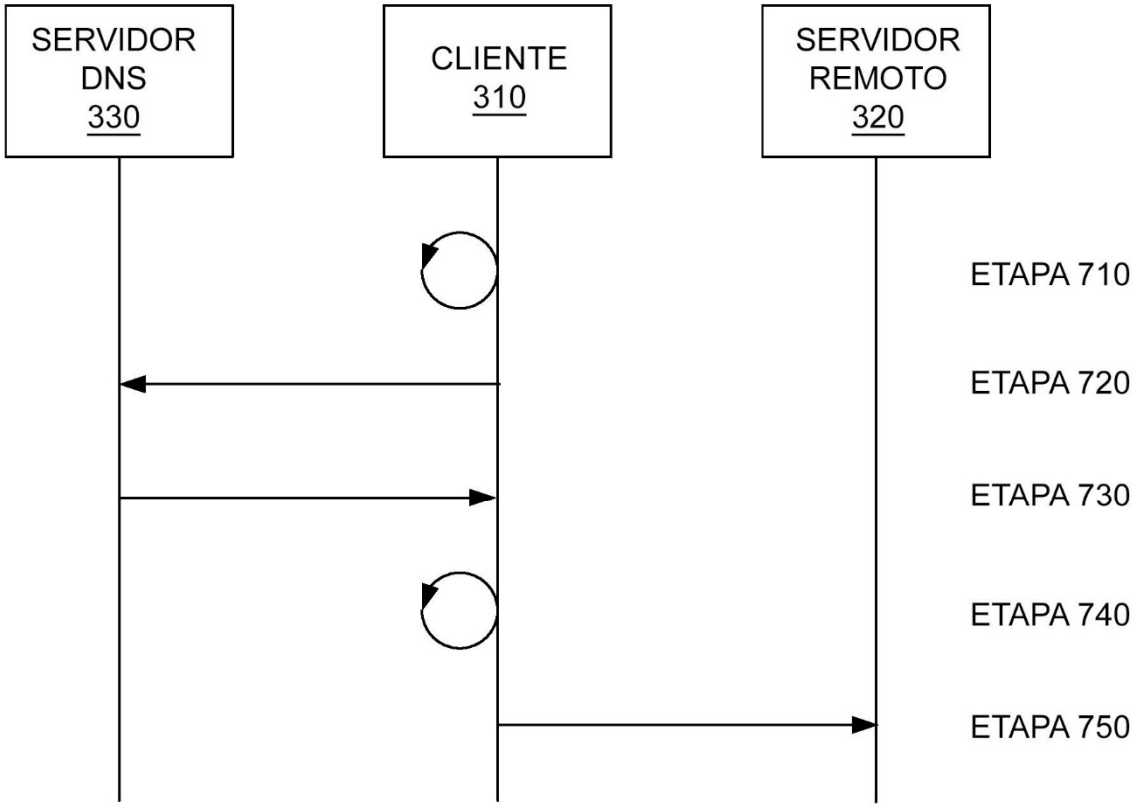
SERVIDOR DNS 330
CLIENTE 310
SERVIDOR REMOTO 320
ETAPA 710
ETAPA 720
ETAPA 730
ETAPA 740
ETAPA 750

FIG. 7