(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 804 502**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/24 (2006.01)
H04L 29/12 (2006.01)
H04W 4/00 (2008.01)
H04W 8/00 (2009.01)
H04L 12/28 (2006.01)
H04L 12/46 (2006.01)
H04W 76/12 (2008.01)
H04W 76/32 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.12.2015 PCT/RO2015/050013**

(87) Fecha y número de publicación internacional: **16.06.2016 WO16093724**

(96) Fecha de presentación y número de la solicitud europea: **11.12.2015 E 15837215 (1)**

(97) Fecha y número de publicación de la concesión europea: **15.04.2020 EP 3231156**

(54) Título: **Sistemas y métodos para detección automática de dispositivo, gestión de dispositivo y asistencia remota**

(30) Prioridad:

11.12.2014 US 201462090547 P
16.06.2015 US 201562180390 P
11.09.2015 US 201562717310 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.02.2021

(73) Titular/es:

BITDEFENDER IPR MANAGEMENT LTD. (100.0%)
Kreontos 12
1076 Nicosia , CY

(72) Inventor/es:

CEBERE, BOGDAN-CONSTANTIN y
MIRCESCU, DANIEL-ALEXANDRU

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistemas y métodos para detección automática de dispositivo, gestión de dispositivo y asistencia remota

Solicitudes relacionadas

La presente solicitud reivindica el beneficio de la fecha de presentación de las solicitudes de patente provisionales de EE. UU. No. 62/090,547, presentada el 11 de diciembre de 2014, titulada "*Systems and Methods for Securing Network Endpoints*", No. 62/180,390, presentada el 16 de junio de 2015, titulada "*Systems and Methods for Automatic Device Detection, Device Management, and Remote Assistance*", y No. 62/217,310, presentada el 11 de septiembre de 2015, titulada "*Systems and Methods for Automatic Network Service Takeover*".

Antecedentes

La invención se refiere a sistemas y métodos para asegurar puntos extremos de red contra amenazas a la seguridad informática, y a sistemas y métodos para la detección automática de dispositivos y la gestión remota de dispositivos.

El software malicioso, también conocido como malware, afecta a una gran cantidad de sistemas informáticos en todo el mundo. En sus diversas formas como, por ejemplo, virus informáticos, *exploits* y programas espía, el malware presenta un grave riesgo para millones de usuarios de ordenadores, haciéndolos vulnerables a la pérdida de datos e información confidencial, al robo de identidad y a la pérdida de productividad, entre otros.

Actualmente, una gran variedad de dispositivos, a los que se hace referencia informalmente como Internet de las cosas (IoT, por sus siglas en inglés), se están conectando a redes de comunicación e Internet. Dichos dispositivos incluyen, entre otros, teléfonos inteligentes, relojes inteligentes, televisores y otros dispositivos multimedia, consolas de juegos, electrodomésticos y diversos sensores domésticos como, por ejemplo, termostatos. A medida que se conectan más dispositivos de este tipo, se convierten en objetivos de amenazas a la seguridad. Por lo tanto, existe una creciente necesidad de proteger dichos dispositivos contra malware, así como de proteger las comunicaciones hacia y desde dichos dispositivos. Un ejemplo de dicha protección se describe en la publicación de preconcesión de EE. UU. No. 2011/122774 A1, a favor de Hassan y otros, que muestra un enrutador configurado para determinar si una conexión segura entre el enrutador y un servidor remoto ha fallado, y posteriormente intentar restablecer la respectiva conexión. El documento US2008172476 A1 describe un método, donde un servidor de red se hace cargo de la tarea DHCP de un enrutador.

Además, la proliferación de dichos dispositivos inteligentes en entornos como, por ejemplo, hogares y oficinas, crea un problema creciente de gestión de dispositivos y redes. Cuando cada dispositivo utiliza una interfaz de configuración distinta y requiere configuraciones de conexión separadas, la gestión de una gran cantidad de dichos dispositivos puede convertirse en una carga, especialmente para un usuario doméstico típico que no tiene experiencia en gestión de redes. Por lo tanto, existe un interés creciente en desarrollar sistemas y métodos para la detección y configuración automática de dispositivos, con especial énfasis en la seguridad.

Compendio

Según un aspecto, un regulador de red comprende un procesador de hardware y una memoria, el procesador de hardware configurado, en respuesta a la recepción de un conjunto de configuraciones de seguridad de un servidor de configuración remota, para configurar el regulador de red según las configuraciones de seguridad, en donde la configuración del regulador de red según la configuración de seguridad hace que el regulador de red proteja múltiples sistemas cliente contra amenazas a la seguridad informática, en donde los múltiples sistemas cliente están conectados a una red local, y en donde un enrutador provee un servicio de red que comprende asignar direcciones de red a los múltiples sistemas cliente. El procesador de hardware se configura, además, en respuesta a la conexión al enrutador en la red local, para configurar un túnel que conecta el regulador de red al servidor de configuración, en donde la configuración del túnel comprende configurar el regulador de red para redirigir al enrutador una comunicación recibida a través del túnel, la comunicación configurada para provocar una interrupción del servicio de red. El procesador de hardware se configura, además, en respuesta a la interrupción, para hacerse cargo del servicio de red del enrutador.

Según otro aspecto, un servidor de configuración comprende al menos un procesador de hardware y una memoria, el al menos un procesador de hardware configurado para transmitir un conjunto de configuraciones de seguridad a un regulador de red conectado a una red remota, en donde la configuración del regulador de red según las configuraciones de seguridad hace que el regulador de red proteja múltiples sistemas cliente contra amenazas a la seguridad informática, en donde los múltiples sistemas cliente están conectados a la red remota, y en donde un enrutador provee un servicio de red que comprende asignar direcciones de red a los múltiples sistemas cliente. El al menos un procesador de hardware se configura además para transmitir una comunicación al regulador de red a través de un túnel configurado por el regulador de red, cuyo túnel conecta el regulador de red al servidor de configuración, en donde la configuración del túnel comprende configurar el regulador de red para redirigir la comunicación al enrutador, y en donde la comunicación se configura para provocar una interrupción del servicio de red.

Según otro aspecto, un medio legible por ordenador no transitorio almacena instrucciones que, cuando se ejecutan por al menos un procesador de hardware de un regulador de red, hacen que el regulador de red, en respuesta a la recepción de un conjunto de configuraciones de seguridad de un servidor de configuración remota, configure el regulador de red según la configuración de seguridad, en donde la configuración del regulador de red según la configuración de seguridad hace que el regulador de red proteja múltiples sistemas cliente contra amenazas a la seguridad informática, en donde los múltiples sistemas cliente están conectados a una red local, y en donde un enrutador provee un servicio de red que comprende asignar direcciones de red a los múltiples sistemas cliente. Las instrucciones además hacen que el regulador de red, en respuesta a la conexión al enrutador en la red local, configure un túnel que conecte el regulador de red al servidor de configuración, en donde la configuración del túnel comprende configurar el regulador de red para redirigir al enrutador una comunicación recibida a través del túnel del servidor de configuración, la comunicación configurada para provocar una interrupción del servicio de red. Las instrucciones además hacen que el regulador de red, en respuesta a la interrupción, se haga cargo del servicio de red del enrutador. La invención se describe en las reivindicaciones adjuntas.

Breve descripción de los dibujos

Los aspectos y las ventajas anteriores de la presente invención se entenderán mejor tras leer la siguiente descripción detallada y al hacer referencia a los dibujos donde:

La Figura 1-A muestra una configuración a modo de ejemplo de sistemas cliente interconectados por una red local, y un regulador de red que protege los sistemas cliente contra amenazas a la seguridad de los ordenadores según algunas realizaciones de la presente invención.

La Figura 1-B muestra una configuración alternativa de sistemas cliente y regulador de red según algunas realizaciones de la presente invención.

La Figura 2 muestra un conjunto de servidores remotos que colaboran con el regulador de red según algunas realizaciones de la presente invención.

La Figura 3 ilustra una configuración de hardware a modo de ejemplo de un sistema cliente según algunas realizaciones de la presente invención.

La Figura 4 ilustra una configuración de hardware a modo de ejemplo de un regulador de red según algunas realizaciones de la presente invención.

La Figura 5 ilustra una configuración de hardware a modo de ejemplo de un dispositivo de administración según algunas realizaciones de la presente invención.

La Figura 6 muestra un conjunto de componentes de software a modo de ejemplo que se ejecutan en un sistema cliente protegido según algunas realizaciones de la presente invención.

La Figura 7 muestra un conjunto a modo de ejemplo de componentes de software que se ejecutan en el regulador de red según algunas realizaciones de la presente invención.

La Figura 8 ilustra un software a modo de ejemplo que se ejecuta en el enrutador según algunas realizaciones de la presente invención.

La Figura 9 muestra un software a modo de ejemplo que se ejecuta en el dispositivo de administración según algunas realizaciones de la presente invención.

La Figura 10 muestra una secuencia a modo de ejemplo de etapas ejecutadas por el regulador de red según algunas realizaciones de la presente invención.

La Figura 11 muestra un intercambio de datos a modo de ejemplo entre el enrutador, el regulador de red y el servidor de configuración, llevado a cabo durante un procedimiento de adquisición de servicio de red según algunas realizaciones de la presente invención.

La Figura 12 muestra una secuencia a modo de ejemplo de etapas llevadas a cabo por el regulador de red durante un procedimiento de adquisición de servicio de red, según algunas realizaciones de la presente invención.

La Figura 13 muestra un intercambio de datos alternativo llevado a cabo durante una adquisición de servicio de red según algunas realizaciones de la presente invención.

La Figura 14 muestra una secuencia a modo de ejemplo de etapas llevadas a cabo por el regulador de red en colaboración con el servidor de configuración para llevar a cabo una adquisición de servicio de red según algunas realizaciones de la presente invención.

La Figura 15 muestra un intercambio de datos entre el enrutador, el regulador de red y un sistema cliente, llevado a cabo durante otro ejemplo de procedimiento de adquisición de servicio de red según algunas realizaciones de la presente invención.

La Figura 16 muestra otra secuencia a modo de ejemplo de etapas llevadas a cabo por el regulador de red durante un procedimiento de adquisición de servicio de red, según algunas realizaciones de la presente invención.

La Figura 17 ilustra un intercambio de datos a modo de ejemplo entre un sistema cliente, el regulador de red y el servidor de configuración, como parte de la instalación del agente específico del dispositivo.

La Figura 18 ilustra una secuencia a modo de ejemplo de etapas llevadas a cabo por el regulador de red durante un procedimiento de instalación del agente, según algunas realizaciones de la presente invención.

La Figura 19-A ilustra una realización de la presente invención, en donde una parte del tráfico de una red se escanea en el servidor de seguridad según algunas realizaciones de la presente invención.

La Figura 19-B muestra una realización de la presente invención, en donde una parte del tráfico de una red se escanea por el regulador de red según algunas realizaciones de la presente invención.

La Figura 20 muestra un intercambio de datos a modo de ejemplo entre un sistema cliente, el regulador de red y el servidor de configuración como parte de la configuración de un agente de utilidad de red privada virtual (VPN, por sus siglas en inglés) y una conexión segura para un sistema cliente protegido, según algunas realizaciones de la presente invención.

La Figura 21 ilustra una secuencia a modo de ejemplo de etapas llevadas a cabo por el sistema cliente para operar un agente VPN según algunas realizaciones de la presente invención.

Descripción detallada de realizaciones preferidas

En la siguiente descripción, se entiende que todas las conexiones descritas entre estructuras pueden ser conexiones operativas directas o conexiones operativas indirectas a través de estructuras intermedias. Un conjunto de elementos incluye uno o más elementos. Se entiende que cualquier descripción de un elemento se refiere a al menos a un elemento. Múltiples elementos incluyen al menos dos elementos. A menos que se requiera lo contrario, las etapas del método descritas no tienen que llevarse a cabo necesariamente en un orden ilustrado particular. Un primer elemento (por ejemplo, datos) derivado de un segundo elemento abarca un primer elemento igual al segundo elemento, así como un primer elemento generado al procesar el segundo elemento y opcionalmente otros datos. El llevar a cabo una determinación o decisión según un parámetro incluye tomar la determinación o decisión según el parámetro y opcionalmente según otros datos. A menos que se especifique lo contrario, un indicador de cierta cantidad/datos puede ser la cantidad/datos en sí, o un indicador diferente de la cantidad/datos en sí. La seguridad informática abarca la protección de usuarios y equipos contra el acceso involuntario o no autorizado a datos y/o hardware, contra modificaciones involuntarias o no autorizadas de datos y/o hardware, y contra la destrucción de datos y/o hardware. Un programa de ordenador es una secuencia de instrucciones del procesador que lleva a cabo una tarea. Los programas de ordenador descritos en algunas realizaciones de la presente invención pueden ser entidades o subentidades de software independientes (por ejemplo, subrutinas, bibliotecas) de otros programas de ordenador. Se dice que dos dispositivos están conectados o pertenecen a la misma red local cuando sus direcciones de red pertenecen a la misma subred y/o cuando ambos tienen la misma dirección de difusión. Un túnel es una conexión virtual de punto a punto entre dos entidades conectadas a una red de comunicación. Los medios legibles por ordenador incluyen medios no transitorios como, por ejemplo, medios de almacenamiento magnéticos, ópticos y de semiconductores (por ejemplo, discos duros, discos ópticos, memoria flash, DRAM), así como enlaces de comunicación como, por ejemplo, cables conductores y enlaces de fibra óptica. Según algunas realizaciones, la presente invención provee, entre otros, sistemas de ordenador que comprenden hardware (por ejemplo, uno o más microprocesadores) programado para llevar a cabo los métodos descritos en la presente memoria, así como instrucciones de codificación de medios legibles por ordenador para llevar a cabo los métodos descritos en la presente memoria.

La siguiente descripción ilustra realizaciones de la invención a modo de ejemplo y no necesariamente a modo de limitación:

Las Figuras 1-A-B muestran configuraciones 10a-b de red a modo de ejemplo según algunas realizaciones de la presente invención, en donde múltiples sistemas cliente 12a-f están interconectados por una red 14 local, y además están conectados a una red 16 extendida como, por ejemplo, Internet. Los sistemas cliente 12a-f pueden representar cualquier dispositivo electrónico que tenga un procesador, una memoria y una interfaz de comunicación. Sistemas cliente 12a-f a modo de ejemplo incluyen ordenadores personales, ordenadores portátiles, tabletas, dispositivos de telecomunicaciones móviles (por ejemplo, teléfonos inteligentes), reproductores multimedia, televisores, consolas de juegos, electrodomésticos (por ejemplo, neveras, termostatos, sistemas inteligentes de calefacción y/o iluminación) y dispositivos que pueden llevarse puestos (por ejemplo, relojes inteligentes, equipos deportivos y de fitness), entre otros. La red 14 local puede comprender una red de área local (LAN, por sus siglas en inglés). Las redes 14 locales a modo de ejemplo pueden incluir una red doméstica y una red corporativa, entre otras.

El enrutador 19 comprende un dispositivo electrónico que permite la comunicación entre sistemas cliente 12a-f y/o acceso de sistemas cliente 12a-f a la red 16 extendida. En algunas realizaciones, el enrutador 19 actúa como una pasarela entre la red 14 local y la red 16 extendida, y provee un conjunto de servicios de red a los sistemas cliente 12a-f. A menos que se especifique lo contrario, el término servicios de red se usa en la presente memoria para denotar servicios que permiten la intercomunicación de los sistemas cliente 12a-f, así como la comunicación entre sistemas cliente 12a-f y otras entidades. Dichos servicios pueden incluir, por ejemplo, distribuir parámetros de configuración de red (por ejemplo, direcciones de red) a los sistemas cliente 12a-f, y encaminar la comunicación entre puntos extremos participantes. Los servicios de red a modo de ejemplo implementan un protocolo de configuración dinámica de host (DHCP por sus siglas en inglés).

Las Figuras 1-A-B muestran además un regulador 18 de red conectado a la red 14 local. En algunas realizaciones, regulador 18 de red comprende un aparato de red configurado para llevar a cabo diversos servicios para sistemas cliente 12a-f. Dichos servicios incluyen, entre otros, servicios de seguridad informática (por ejemplo, antimalware, detección de intrusos, antispyware, etc.), gestión de dispositivos (por ejemplo, configuración remota de sistemas cliente 12a-f), servicios de control parental, servicios de comunicación segura (por ejemplo, redes privadas virtuales - VPN) y asistencia técnica remota (por ejemplo, resolución de problemas de dispositivos y/o redes).

En una aplicación típica según algunas realizaciones de la presente invención, el regulador 18 de red se introduce en una red local ya configurada y gestionada por el enrutador 19. En algunas realizaciones, en la instalación, el regulador 18 se hace cargo de los servicios de red como, por ejemplo, DHCP del enrutador 19, y se instala en una posición de pasarela entre la red 14 local y la red 16 extendida, de modo que al menos una parte del tráfico entre sistemas cliente 12a-f y la red 16 extendida atraviesa el regulador 18 de red (es preciso ver la Figura 1-A). La colocación del regulador 18 de red en una posición de pasarela puede ser preferible porque, en algunas realizaciones, el regulador 18 provee servicios de seguridad informática al redirigir al menos parte del tráfico (por ejemplo, solicitudes HTTP) de los sistemas cliente 12a-f a un servidor de seguridad. El tener el regulador 18 en una posición de pasarela puede facilitar la intercepción de dicho tráfico.

En algunas realizaciones como, por ejemplo, el ejemplo de la Figura 1-B, el enrutador 19 puede continuar operando como pasarela para la red 14 local después de la instalación del regulador 18 pero, en dichos casos, el regulador 18 de red se posiciona preferiblemente entre los sistemas cliente 12a-f y la pasarela existente (a saber, el enrutador 19), de modo que el regulador 18 pertenece a la misma red local que los sistemas cliente 12a-f. Dicha posición se prefiere porque, en algunas realizaciones, el regulador 18 de red está configurado para colaborar con un servidor remoto para detectar el tipo de cada sistema cliente (por ejemplo, teléfono inteligente frente a PC) y, en respuesta, para entregar un agente de utilidad específico del dispositivo a algunos de los sistemas cliente 12a-f. Las configuraciones en donde el regulador 18 no es un miembro de la red 14 local (por ejemplo, mediante la colocación del regulador 18 entre el enrutador 19 y la red 16 extendida) puede dificultar la detección del dispositivo y la entrega del agente.

En algunas realizaciones, los sistemas cliente 12a-f se monitorean, gestionan y/o configuran remotamente por un usuario/administrador, mediante el uso de software que se ejecuta en un dispositivo 20 de administración conectado a la red 16 extendida (por ejemplo, Internet). Dispositivos 20 de administración a modo de ejemplo incluyen teléfonos inteligentes y sistemas de ordenadores personales, entre otros. El dispositivo 20 puede exponer una interfaz gráfica de usuario (GUI, por sus siglas en inglés) que permite a un usuario configurar y/o gestionar de manera remota el funcionamiento de los sistemas cliente 12a-f, por ejemplo, para establecer opciones de configuración y/o recibir notificaciones sobre episodios que ocurren en los respectivos sistemas cliente.

En algunas realizaciones, el regulador 18 de red puede colaborar con un conjunto de sistemas informáticos remotos para llevar a cabo diversos servicios para sistemas cliente 12a-f. Sistemas informáticos remotos a modo de ejemplo incluyen un servidor 50 de seguridad y un servidor 52 de configuración, ilustrados en la Figura 2. Los servidores 50 y 52 pueden comprender máquinas individuales o grupos de múltiples sistemas informáticos interconectados. En algunas realizaciones, el regulador 18 de red redirige parte o la totalidad del tráfico que se dirige a y/o de los sistemas cliente 12a-f al servidor 50 de seguridad. El servidor 50 luego puede llevar a cabo operaciones de detección de amenazas (por ejemplo, detección de malware, bloqueo de acceso a sitios web maliciosos o fraudulentos, prevención de intrusiones, etc.), para proteger los sistemas cliente 12a-f contra amenazas a la seguridad informática. El servidor 50 de seguridad puede además estar conectado a una base de datos 55 de episodios que comprende múltiples registros de seguridad, y cada registro de seguridad incluye datos indicativos de un episodio de seguridad, así como un indicador de una asociación entre el episodio respectivo y un sistema cliente protegido.

Una ventaja de encaminar el tráfico hacia/desde un sistema cliente protegido a través del servidor 50 de seguridad es que permite que el sistema cliente respectivo abandone la red 14 local, sin dejar de beneficiarse de la protección. Dichas configuraciones se describen con todo detalle más abajo.

En algunas realizaciones, el servidor 52 de configuración colabora con el dispositivo 20 de administración para configurar la gestión del dispositivo y/o la configuración de seguridad del regulador 18, enrutador 19 y/o de un sistema cliente 12 protegido. El servidor 52 puede estar conectado comunicativamente a una base de datos 54 de abonados y a una base de datos 56 de características del dispositivo. La base de datos 54 de abonados puede

almacenar múltiples registros de abono, cada registro de abono indicativo de un conjunto de sistemas cliente bajo gestión de dispositivos según algunas realizaciones de la presente invención. En una realización, cada registro de abono está asociado de manera única a un regulador 18 de red distinto. En dichas realizaciones, todos los sistemas cliente 12 configurados y/o a los que se proveen servicios de otro modo mediante el uso del regulador de red respectivo (por ejemplo, sistemas cliente 12a-f conectados a la red 14 local en la Figura 1-A) están asociados al mismo registro de abono. Cada registro de abono puede incluir un indicador de un período de abono y/o un conjunto de parámetros de abono que describen, por ejemplo, un nivel deseado de seguridad o una selección de servicios del abono. Los abonos pueden gestionarse según un acuerdo de nivel de servicio (SLA, por sus siglas en inglés).

En algunas realizaciones, la base de datos 56 de características del dispositivo comprende un conjunto de registros que indican características configurables de cada sistema cliente 12 y/o ajustes de configuración actuales para cada sistema cliente. La base de datos 56 puede comprender además un conjunto completo de registros que se pueden usar para determinar el tipo de dispositivo del sistema cliente 12. Dichos registros pueden incluir entradas correspondientes a varios tipos de dispositivos (por ejemplo, enrutadores, teléfonos inteligentes, dispositivos que pueden ponerse, etc.), marcas y modelos, de varios fabricantes, mediante el uso de varios sistemas operativos (por ejemplo, Windows® vs. Linux®). Una entrada a modo de ejemplo puede comprender, entre otros, indicadores de si el tipo de dispositivo respectivo usa un protocolo de red particular para comunicarse (por ejemplo, HTTP, Bonjour®), un indicador de un diseño de una interfaz de inicio de sesión expuesta por el tipo de dispositivo respectivo, etc.

Las Figuras 3-4-5 muestran configuraciones de hardware a modo de ejemplo del sistema cliente 12, regulador 18 de red y dispositivo 20 de administración, respectivamente. Sin pérdida de generalidad, las configuraciones ilustradas corresponden a sistemas informáticos (Figuras 3-4) y a un teléfono inteligente (Figura 5). La configuración de hardware de otros sistemas (por ejemplo, tabletas) puede diferir de las ilustradas en las Figuras 3-4-5. Cada uno de los procesadores 22, 122, y 222 comprende un dispositivo físico (por ejemplo, microprocesador, circuito integrado multinúcleo formado en un sustrato semiconductor) configurado para ejecutar operaciones computacionales y/o lógicas con un conjunto de señales y/o datos. Las unidades 24, 124, y 224 de memoria pueden comprender medios legibles por ordenador no permanentes (por ejemplo, RAM) que almacenan datos/señales a los que los procesadores 22, 122, y 222, respectivamente, acceden o generan en el curso de la realización de operaciones.

Los dispositivos 26, 226 de entrada pueden incluir teclados de ordenador, ratones y micrófonos, entre otros, incluidas las respectivas interfaces y/o adaptadores de hardware que permiten a un usuario introducir datos y/o instrucciones en el sistema respectivo. Los dispositivos 28, 228 de salida pueden incluir dispositivos de visualización como, por ejemplo, monitores y altavoces, entre otros, así como interfaces/adaptadores de hardware como, por ejemplo, tarjetas gráficas, que permiten que el sistema respectivo comunique datos a un usuario. En algunas realizaciones, los dispositivos de entrada y salida comparten una pieza de hardware común (por ejemplo, pantalla táctil). Los dispositivos 32, 132, y 232 de almacenamiento incluyen medios legibles por ordenador que permiten el almacenamiento permanente, la lectura y escritura de instrucciones y/o datos de software. Los dispositivos de almacenamiento a modo de ejemplo incluyen discos magnéticos y ópticos y dispositivos de memoria flash, así como medios extraíbles como, por ejemplo, discos y unidades de CD y/o DVD.

Los adaptadores 34, 134 de red habilitan el sistema cliente 12 y el regulador 18 de red, respectivamente, para conectarse a una red de comunicación electrónica como, por ejemplo, la red 14 local, y/o a otros dispositivos/sistemas informáticos. Los dispositivos 40 de comunicación (Figura 5) habilitan el dispositivo 20 de administración para conectarse a la red 16 extendida (por ejemplo, Internet), y pueden incluir hardware de telecomunicaciones (emisores/receptores de ondas electromagnéticas, antena, etc.). Dependiendo del tipo de dispositivo y de la configuración, el dispositivo 20 de administración puede incluir además un dispositivo 42 de geolocalización (por ejemplo, receptor GPS) y un conjunto de dispositivos 136 de detección (por ejemplo, sensores de movimiento, sensores de luz, etc.).

Los concentradores 30, 130, 230 de controlador representan los múltiples buses de sistema, periféricos y/o conjuntos de chips, y/o todos los demás circuitos que permiten la comunicación entre el procesador de cada sistema respectivo y el resto de los componentes de hardware. En un sistema cliente 12 a modo de ejemplo (Figura 3), el concentrador 30 puede comprender un controlador de memoria, un controlador de entrada/salida (E/S) y un controlador de interrupción. Dependiendo del fabricante del hardware, algunos de dichos controladores pueden incorporarse en un solo circuito integrado y/o pueden integrarse con el procesador.

La Figura 6 muestra componentes de software a modo de ejemplo que se ejecutan en el sistema cliente 12 según algunas realizaciones de la presente invención. Dicho software puede incluir un sistema operativo (SO) 40 que provee una interfaz entre el hardware del sistema cliente 12 y un conjunto de aplicaciones de software que se ejecutan en el sistema cliente respectivo. Las aplicaciones de software incluyen un agente 41 de utilidad configurado para proveer diversos servicios al sistema cliente respectivo como, por ejemplo, servicios de seguridad, servicios de gestión de dispositivos, servicios de control parental, servicios de comunicación segura (por ejemplo, redes privadas virtuales - VPN), etc. En algunas realizaciones, el agente 41 de utilidad está configurado para acceder y/o modificar un conjunto de opciones de configuración del sistema cliente 12 (por ejemplo, parámetros de configuración de red, parámetros de gestión de energía, parámetros de seguridad, parámetros específicos del dispositivo como, por ejemplo, la temperatura deseada en el caso de un termostato controlado de forma remota, o una selección de luces en el caso de un administrador de iluminación del hogar controlado de forma remota, etc.). En algunas realizaciones,

la instalación del agente 41 en el sistema cliente 12 se inicia y/o facilita por el regulador 18 de red, como se muestra con más detalle más abajo.

La Figura 7 muestra un conjunto de componentes de software que se ejecutan en el regulador 18 de red según algunas realizaciones de la presente invención. Dichos componentes pueden incluir, entre otros, un módulo 42 de detección de dispositivos y un módulo 43 DHCP. En algunas realizaciones, el módulo 43 provee servicios DHCP para la red 14 local. Dichos servicios pueden incluir la entrega de información de configuración del protocolo de Internet (IP, por sus siglas en inglés) a los clientes que solicitan acceso a la red 14 local y/o a la red 16 extendida. El módulo 42 de detección de dispositivos puede configurarse para colaborar con un servidor de configuración remota para detectar un tipo de dispositivo de sistema cliente 12, como se muestra más abajo. En algunas realizaciones, el regulador 18 ejecuta además un módulo 44 de interrupción de red configurado para llevar a cabo una adquisición del servicio de red como se muestra en detalle más abajo.

La Figura 8 muestra un conjunto a modo de ejemplo de componentes de software que se ejecutan en el enrutador 19, según algunas realizaciones de la presente innovación. Dichos componentes de software pueden incluir un sistema 140 operativo y un conjunto de aplicaciones, las cuales incluyen un servidor 45 DHCP. El servidor 45 se puede usar para distribuir parámetros de configuración de red (por ejemplo, direcciones IP) a sistemas cliente 12a-f, para configurar la red 14 local.

La Figura 9 muestra un conjunto a modo de ejemplo de componentes de software que se ejecutan en el dispositivo 20 de administración (por ejemplo, un teléfono inteligente), según algunas realizaciones de la presente invención. Dichos componentes de software pueden incluir un sistema 240 operativo y un conjunto de aplicaciones. Las aplicaciones incluyen una aplicación 46 de administración configurada para permitir que un usuario configure de forma remota los sistemas cliente 12a-f. La configuración de los sistemas 12a-f puede incluir, entre otros, configurar ajustes de seguridad específicos del cliente, configurar parámetros de acceso a la red específicos del cliente (por ejemplo, velocidad de conexión, etc.) e iniciar tareas de mantenimiento (por ejemplo, actualizaciones de software, operaciones de limpieza de disco, etc.). La aplicación 46 de administración puede exponer una interfaz 48 gráfica de usuario (GUI) de administración a un usuario del dispositivo 20 de administración.

La Figura 10 muestra una secuencia de etapas ejecutadas por el regulador 18 de red según algunas realizaciones de la presente invención. Dicha secuencia puede ejecutarse, por ejemplo, tras la instalación del regulador 18 de red o cuando el regulador 18 se presenta por primera vez en la red 14 local. En una etapa 300, el regulador 18 detecta automáticamente el enrutador 19, que en la presente memoria representa al proveedor existente de servicios de red. En algunas realizaciones, el regulador 18 luego se hace cargo de algunos de los servicios de red del enrutador 19. Dicha adquisición puede comprender el apagado o la incapacidad de alguna manera de algunas de las funciones del enrutador 19, y el reemplazo del enrutador 19 como proveedor de al menos una parte de los servicios de red asociados a la red 14 local. En una realización alternativa, la adquisición del servicio puede comprender ofrecer un conjunto alternativo de servicios de red además de los gestionados por el enrutador 19, sin realmente incapacitar a este último. En algunas realizaciones, la etapa 302 comprende además instalar el regulador 18 de red en una posición de pasarela entre la red 14 local y la red 16 extendida, de modo que al menos una parte del tráfico de red entre sistemas cliente 12a-f y la red 16 extendida atraviesa el regulador 18.

En una secuencia de las etapas 304-306, el regulador 18 de red puede detectar automáticamente dispositivos que pertenecen a la red 14 local (a saber, sistemas cliente 12a-f) y distribuir agentes 41 de utilidad específicos del dispositivo a al menos a algunos de los sistemas cliente 12a-f. Una etapa 308 adicional lleva a cabo un conjunto de servicios de seguridad informática para sistemas cliente 12a-f. Las etapas 300-308 se describen con más detalle más abajo.

Adquisición de servicio de red

En algunas realizaciones de la presente invención, los servicios DHCP del enrutador 19 pueden apagarse o de otra manera incapacitarse por el regulador 18 de red. Este efecto se puede obtener a través de varios métodos, algunos de los cuales se ejemplifican más abajo. Los servicios de DHCP se usan en la presente memoria solo como un ejemplo; los sistemas y métodos descritos más abajo pueden adaptarse para hacerse cargo de otros servicios de red.

En un escenario a modo de ejemplo, conocido como hambre DHCP, el regulador 18 de red puede usar el módulo 44 de interrupción de la red para hacerse pasar por múltiples dispositivos ficticios y solicitar direcciones de red para cada dispositivo ficticio del enrutador 19. El recuento de dichos dispositivos ficticios se puede elegir para que ocupe por completo el conjunto disponible de direcciones IP ofrecidas en arrendamiento por el servidor 45 DHCP del enrutador 19. De esta manera, aunque el servidor 45 continúa operando, el servidor 45 ya no puede proveer direcciones IP a los sistemas cliente en la red 14 local. En algunas realizaciones, el regulador 18 de red entonces puede usar el módulo 43 DHCP para transmitir su propia oferta de arrendamiento de DHCP y, de esta manera, formar efectivamente a los sistemas cliente 12a-f a que usen el regulador 18 como el servidor DHCP por defecto y el dispositivo de pasarela para al menos parte del tráfico entre los sistemas cliente 12a-f y la red 16 extendida.

Otro conjunto a modo de ejemplo de métodos de adquisición de servicios DHCP comprende detectar automáticamente un proveedor de servicios DHCP existente (por ejemplo, el enrutador 19) y deshabilitar el dispositivo respectivo, por ejemplo, mediante la reconfiguración automática de su red y/u otros parámetros funcionales. Uno de dichos escenarios involucra al regulador 18 de red que colabora con el servidor 52 de configuración en la manera ilustrada en las Figuras 11-12.

En algunas realizaciones, una etapa 320 solicita y luego recibe permiso de un usuario para reconfigurar el enrutador 19. El usuario respectivo puede ser propietario o administrador del regulador 18 y/o de la red 14 local, como se enumera, por ejemplo, en la base de datos 54 de abonados mantenida por el servidor 52 de configuración (es preciso ver la Figura 2). La obtención del permiso puede incluir, por ejemplo, enviar una notificación al dispositivo 20 de administración, lo cual puede llevar a cabo el regulador 18 o el servidor 52 de configuración. La GUI 48 de administración del dispositivo 20 luego puede exponer un campo de entrada que permite al usuario indicar si él/ella permite reconfigurar los parámetros del enrutador 19. La etapa 320 puede incluir además la obtención de credenciales de inicio de sesión (por ejemplo, nombre de usuario, contraseña, etc.) para el enrutador 19, directamente del usuario a través del dispositivo 20 de administración, o de un registro de abonos almacenado en la base de datos 54.

En una etapa 322, el regulador 18 de red recopila información indicativa del tipo de dispositivo sobre el enrutador 19, por ejemplo, mediante el análisis de los datos recibidos del enrutador 19 durante un intercambio de solicitud/respuesta de DHCP. Dichos datos pueden incluir, entre otros, una dirección de control de acceso al medio (MAC, por sus siglas en inglés) del enrutador 19 y un encabezamiento de autenticación. En algunas realizaciones, el regulador 18 de red puede además intentar exponer una interfaz de inicio de sesión del enrutador 19, y además extraer datos indicativos del tipo de dispositivo de la interfaz respectiva (por ejemplo, determinar si la interfaz es un documento HTML o no, y determinar una dirección de red de la interfaz respectiva). Algunas realizaciones del regulador 18 pueden incluso extraer ciertas características visuales de la interfaz respectiva, por ejemplo, mediante el uso de un algoritmo de procesamiento de imágenes.

Los datos 61 indicativos del tipo de dispositivo luego se envían al servidor 52 de configuración (etapa 324), el cual puede identificar un tipo de dispositivo del enrutador 19 (por ejemplo, fabricante, modelo, familia, subfamilia, versión de firmware, etc.) según dichos datos y/o según los datos almacenados en la base de datos 56 de características del dispositivo (Figura 2). El servidor 52 de configuración luego puede configurar una prueba 60 de inicio de sesión adaptada para el tipo de dispositivo particular del enrutador 19 según los datos indicativos del tipo de dispositivo recibidos del regulador 18, y puede transmitir datos de prueba de inicio de sesión al regulador 18.

En algunas realizaciones, el regulador 18 de red puede repetir un bucle de etapas 326-334 en un intento iterativo de prueba y error para iniciar sesión en el enrutador 19. Las etapas 328-330 pueden exponer la interfaz de inicio de sesión del enrutador 19 y transmitir datos 60 de prueba de inicio de sesión y/o credenciales de usuario al enrutador 19. Un indicador de si el inicio de sesión se ha llevado a cabo con éxito se devuelve al servidor 52 (etapa 332); el indicador de éxito puede usarse para identificar además un tipo de dispositivo de enrutador 19.

Una vez que se logró un inicio de sesión exitoso, en una etapa 336, el regulador 18 de red puede obtener un conjunto de comandos 63 de configuración del enrutador del servidor 52 de configuración, comandos **63** diseñados específicamente según el tipo de enrutador identificado y dirigidos a incapacitar al enrutador 19, o al menos a algunos servicios de red ofrecidos por el enrutador 19. Los comandos 63 de configuración del enrutador a modo de ejemplo pueden ordenar al enrutador 19 que se apague, que se reinicie, que exponga una interfaz de configuración y que cambie un ajuste de configuración, entre otros. Otro comando 63 de configuración a modo de ejemplo comprende una solicitud HTTP configurada para exponer una interfaz de configuración del enrutador 19. En algunas realizaciones, los comandos 63 pueden completar automáticamente un conjunto de campos de la interfaz expuesta. En algunas realizaciones, los comandos 63 comprenden un conjunto de valores de parámetros para completar un conjunto de campos de una interfaz de configuración del enrutador 19.

En una etapa 338, el regulador 18 de red puede transmitir comandos 63 de configuración al enrutador 19. Para completar la adquisición de servicios DHCP del enrutador 19, el regulador 18 puede emplear el módulo 43 DHCP (Figura 7) para transmitir su propia oferta de arrendamiento de DHCP a los sistemas cliente 12a-f.

En algunas realizaciones, el regulador 18 de red puede transmitir otro conjunto de comandos al enrutador 19 en el caso en el que el propietario/administrador del regulador 18 decide desinstalar el regulador 18. En dicho ejemplo, el regulador 18 puede ordenar al enrutador 19 que invierta los ajustes, los cuales eran efectivos antes de la instalación del regulador 18 de red.

Las Figuras 13-14 ilustran un método alternativo de adquisición de servicios de red por parte del regulador 18 de red según algunas realizaciones de la presente invención. El método ilustrado comprende una variación del método descrito más arriba en relación con las Figuras 11-12. En lugar de emplear un regulador 18 de red para reconfigurar activamente la configuración de red y/o deshabilitar (parcialmente) el enrutador 19, en el método ilustrado en las Figuras 13-14, dichas acciones se llevan a cabo directamente por el servidor 52 de configuración, mientras que el regulador 18 se usa como un proxy o retransmisión. Algunas realizaciones llevan a cabo la configuración remota del enrutador 19 mediante el uso de túneles, a saber, conexiones/canales de comunicación seguros de punto a punto.

En respuesta a la instalación dentro de la red 14 local, el regulador 18 de red puede transmitir un mensaje de registro a los servidores 50-52, el cual incluye indicadores de identificación únicos para el respectivo regulador de red, enrutador 19 y sistemas cliente conectados a la red local respectiva. Por lo tanto, los servidores 50-52 pueden identificar selectivamente cada dispositivo individual y asociar cada sistema cliente 12 y enrutador 19 a un abono y/o a un regulador de red respectivo. Este proceso de registro en el servidor 52 de configuración permite al servidor 52 aceptar conexiones de túnel del regulador 18.

En respuesta a la obtención del permiso del usuario para reconfigurar la red local (etapa 340), el regulador 18 de red puede abrir un túnel 69 de comunicación que conecta el regulador 18 al servidor 52. Un túnel a modo de ejemplo comprende un túnel de caparazón seguro (SSH, por sus siglas en inglés), a saber, un túnel configurado mediante el uso de una versión del protocolo SSH. En algunas realizaciones, el regulador 18 de red emplea una estrategia de reenvío de puertos para redirigir el tráfico de red recibido a través del túnel 69 hacia el enrutador 19, y/o redirigir las comunicaciones recibidas del enrutador 19 hacia el servidor 52 a través del túnel 69. Dicho reenvío de puertos se puede lograr mediante el uso de cualquier método conocido en la técnica de redes, por ejemplo, mediante el uso de proxy, un cliente SOCKS, traducción de direcciones de red (NAT, por sus siglas en inglés), etc.

Mediante el uso del reenvío de puertos, algunas realizaciones del servidor 52 de configuración por lo tanto, pueden configurar el enrutador 19 de forma remota a través del túnel 69. Dicha configuración remota puede incluir algunas de las operaciones descritas más arriba en relación con las Figuras 11-12 como, por ejemplo, determinar un tipo de dispositivo de enrutador 19, enviar comandos de configuración al enrutador 19, etc.

En respuesta a la determinación de un tipo de dispositivo de enrutador 19, el servidor 52 puede enviar una solicitud 68 de túnel al regulador 18, cuya solicitud de túnel ordena al regulador 18 de red que configure el túnel 69 (etapa 346). El túnel se puede configurar con reenvío de puertos, de modo que una comunicación enviada por el servidor 52 al regulador 18 se reenviará al enrutador 19. En una etapa 348, el servidor 52 luego puede transmitir datos de inicio de sesión y/o comandos de configuración del enrutador a través del túnel 69 para ordenar al enrutador 19 que deshabilite o de otra manera reconfigure los servicios DHCP del enrutador 19.

Las Figuras 15-16 ilustran incluso otro método para hacerse cargo de los servicios de red del enrutador 19 según algunas realizaciones de la presente invención. Cuando se introduce en la red 14 local, el regulador 18 puede enviar una solicitud 70 de dirección al proveedor de servicios de red actual (por ejemplo, el enrutador 19), por medio de la cual solicita una dirección de red (etapa 350). En respuesta, el enrutador 19 puede devolver una oferta 72 de dirección al regulador 18. La solicitud 70 y la devolución 72 pueden formar parte de un protocolo estándar de asignación de direcciones, por ejemplo, DHCP. La etapa 352 puede comprender además aceptar la oferta 72 de dirección y configurar el regulador 18 de red para usar la dirección de red respectiva y/u otros parámetros de red (por ejemplo, pasarela, servidor DNS, etc.).

A continuación, en una etapa 354, el regulador 18 puede obtener permiso de un operador humano para llevar a cabo el procedimiento de adquisición del servicio de red (es preciso ver más arriba, en relación con la Figura 12). En respuesta a la obtención de permiso, en una etapa 356, el regulador 18 de red puede determinar un conjunto objetivo de direcciones de red según los parámetros de la oferta 72 de dirección recibida previamente. En algunas realizaciones que usan DHCP, la oferta 72 comprende un indicador de un conjunto de direcciones (por ejemplo, un rango de valores de dirección) gestionado por y/o disponible para su asignación por el proveedor de servicios de red actual. El regulador 18 puede seleccionar el conjunto objetivo de direcciones de red del grupo de direcciones respectivo. En algunas realizaciones, el conjunto objetivo incluye todas las direcciones del grupo. En otras realizaciones, el conjunto objetivo incluye todas las direcciones del grupo, excepto la dirección actualmente asignada al enrutador 19.

Una etapa 358 puede configurar el regulador 18 de red para usar todas las direcciones del conjunto objetivo. En algunas realizaciones, la etapa 358 comprende crear un conjunto de dispositivos ficticios (alias) y asignar un subconjunto del conjunto objetivo de direcciones de red a cada dispositivo ficticio. A continuación, en una secuencia de etapas 360-366, el regulador 18 de red puede explotar un mecanismo de detección de conflicto de direcciones (ACD, por sus siglas en inglés) para forzar progresivamente a los clientes 12a-f para que renuncien a sus direcciones de red asignadas actualmente. Mientras tanto, el regulador 18 puede usar el módulo 36 DHCP para ofrecer un nuevo conjunto de direcciones de red y/u otros parámetros de configuración a los sistemas cliente 12a-f y, por consiguiente, completar el procedimiento de adquisición del servicio de red.

Un mecanismo ACD a modo de ejemplo se describe en la Solicitud de Comentarios de Detección de Conflicto de Direcciones IPv4 (RFC5227) emitida por el Grupo de Trabajo de Red de Apple®, Inc., en julio de 2008. El mecanismo ACD descrito requiere que, como parte de la asignación de dirección de red (que ocurre, por ejemplo, tras la oferta inicial de arrendar una dirección de red, o al renovar el arrendamiento de la dirección de red respectiva), cada cliente y/o su proveedor de servicios de red respectivo verifican si la dirección de red respectiva está disponible, a saber, si no está ya en uso por otro dispositivo. Dichas verificaciones pueden usar herramientas y/o mecanismos descritos en el protocolo de resolución de direcciones (ARP, por sus siglas en inglés) y el protocolo de descubrimiento de vecinos (NDP, por sus siglas en inglés), entre otros. Una verificación a modo de ejemplo comprende que el cliente y/o proveedor respectivo envía una sonda (por ejemplo, un paquete de red especialmente configurado, un ping, un arping, etc.) a la dirección de red que se está verificando actualmente. Cuando el cliente y/o

proveedor que han enviado la sonda no recibe respuesta a la sonda respectiva, la dirección respectiva se considera disponible y puede (re)asignarse al cliente respectivo. Por el contrario, cuando el cliente y/o proveedor recibe una respuesta a la sonda respectiva, la dirección respectiva se considera tomada y ya no se (re)asigna al cliente respectivo.

El mecanismo ACD descrito más arriba se explota por algunas realizaciones del regulador 18 de red para fines de adquisición, como se muestra en las Figuras 15-16. En una secuencia de etapas 360-362, el regulador 18 puede escuchar las sondas 64a-b de disponibilidad de direcciones, emitidas por el sistema 12 del cliente y/o enrutador 19, respectivamente. En respuesta a la detección de dicha sonda, una etapa 364 determina si la dirección sondeada coincide con algún miembro del conjunto objetivo de direcciones de red determinado en la etapa 356. Cuando no, el regulador 18 vuelve a escuchar las sondas de disponibilidad de direcciones.

Cuando la dirección sondeada coincide con un miembro del conjunto objetivo de direcciones, en una etapa 366, el regulador 18 puede devolver una respuesta 66a-b de sonda al remitente de la sonda respectiva, la respuesta de sonda configurada para indicar que la dirección de red respectiva no está disponible. En algunas realizaciones, la etapa 366 comprende un dispositivo ficticio (alias) creado por el regulador 18 de red mediante la emisión de una respuesta de sonda configurada con los detalles del dispositivo ficticio respectivo. Cuando el sistema 12 cliente está configurado para admitir la detección de conflictos, la recepción de dicha sonda de retorno puede determinar que el sistema 12 cliente deja de usar la dirección de red respectiva y solicita una nueva dirección. Estas nuevas solicitudes fallarán para todas las direcciones en el conjunto objetivo de direcciones, ya que activarán una nueva ejecución de etapas 360-366. Al repetir la secuencia de etapas 360-366 para cada sistema cliente 12a-f, el regulador 18 de red, por lo tanto, puede deshabilitar progresivamente los servicios de red ofrecidos por el enrutador 19 y forzar a los sistemas cliente 12a-f a que utilicen un nuevo conjunto de direcciones de red emitidas por el regulador 18.

Descubrimiento automático de dispositivos y provisión de agentes

Habiéndose instalado como pasarela y/o proveedor de servicios de red para la red 14 local, el regulador 18 de red puede proceder a distribuir agentes 41 de utilidad (por ejemplo, la Figura 6) a sistemas cliente 12a-f conectados a la red 14 local. La Figura 17 muestra un intercambio de datos a modo de ejemplo entre el sistema cliente 12, el regulador 18 de red y el servidor 52 de configuración del cliente según algunas realizaciones de la presente invención, el intercambio ocurriendo durante el descubrimiento del dispositivo y la provisión del agente. Dichos intercambios pueden ocurrir al instalar el regulador 18 de red, así como cuando un nuevo sistema cliente se introduce por primera vez en la red 14 local.

Una secuencia de etapas a modo de ejemplo llevada a cabo por el regulador 18 de red para entregar un agente de utilidad específico del dispositivo se ilustra en la Figura 18. En algunas realizaciones, el regulador 18 puede esperar las solicitudes de conexión de los sistemas cliente locales (etapa 400) Una solicitud de conexión a modo de ejemplo comprende una solicitud HTTP. Cuando el sistema cliente 12 intenta acceder a una dirección en la red 16 extendida, el regulador 18 puede forzar al sistema cliente respectivo a instalar el agente 41 de utilidad. En algunas realizaciones, el regulador 18 puede redirigir la solicitud de acceso a la red actual al servidor 52 de configuración, que puede servir a un instalador 75 de agente al sistema cliente respectivo (Figura 17). En una realización alternativa, el regulador 18 puede obtener el instalador 75 de agente del servidor 52, y luego empujar el instalador 75 al respectivo sistema cliente.

En algunas realizaciones, el instalador 75 está configurado para determinar el sistema cliente 12 (o dispositivo 20 de administración) para exponer una interfaz de confirmación a un usuario, por medio de la cual se solicita al usuario que acepte instalar el agente 41. El instalador 75 además puede solicitar al usuario que confirme que el usuario está de acuerdo con los términos del abono respectivo (por ejemplo, como se detalla en un SLA). Cuando el usuario indica acuerdo, el instalador 75 puede instalar y ejecutar el agente 41. En algunas realizaciones, el instalador 75 y/o el regulador 18 de red pueden registrar el sistema cliente respectivo con el servidor 52 de configuración de cliente (etapa 418 en la Figura 18). Dicho registro puede incluir que el servidor 52 asocia el sistema cliente respectivo a un registro de abonos adjunto al regulador 18 de red.

Teniendo en cuenta la gran diversidad de dispositivos que actualmente se conectan a las redes de comunicación e Internet, puede ser preferible que los agentes 41 de utilidad entregados a sistemas cliente 12a-f protegidos se adapten al tipo de dispositivo de cada sistema cliente (por ejemplo, teléfono inteligente, tableta, reloj inteligente, sistema operativo Windows® o iOS®, etc.). Las etapas 400-406 a modo de ejemplo (Figura 18) ilustran un método a modo de ejemplo para determinar un tipo de dispositivo de sistema cliente 12. El regulador 18 de red puede obtener datos indicativos del tipo de dispositivo mediante la extracción de un indicador de agente de usuario de una solicitud HTTP (el indicador de agente de usuario generalmente contiene información sobre el tipo de navegador y el sistema operativo del remitente de la solicitud HTTP). El regulador 18 puede detectar además un conjunto de aplicaciones, protocolos y/o servicios utilizados por los respectivos sistemas cliente, por ejemplo, mediante la exploración de los respectivos servicios y/o protocolos (etapa 404). Dicha exploración puede incluir enviar una sonda a un puerto particular del sistema cliente respectivo y escuchar una respuesta. Los protocolos y servicios detectados pueden incluir, entre otros, Bonjour®, protocolo simple de administración de red (SNMP, por sus siglas en inglés) y mapeador de redes (Nmap). El regulador 18 de red luego puede determinar un tipo de dispositivo de sistema cliente 12 localmente, según dichos datos indicativos del tipo de dispositivo, mediante el uso de un conjunto de reglas, un

árbol de decisión y/o un algoritmo de aprendizaje automático. En una realización alternativa, los datos indicativos del tipo de dispositivo se envían al servidor 52 de configuración (etapa 406), que identifica el tipo de dispositivo según los datos recibidos y según la información almacenada en la base de datos 56 de características del dispositivo. Por ejemplo, el servidor 52 puede intentar hacer coincidir las características del sistema cliente 12 con varias entradas de la base de datos 56, en donde cada entrada puede corresponder a un tipo de dispositivo distinto (posiblemente incluidas versiones distintas de un producto, sistemas operativos distintos, etc.). El descubrimiento de dispositivos puede proceder de manera iterativa: el servidor 52 puede llevar a cabo una determinación preliminar de un tipo de dispositivo según la información disponible sobre el sistema cliente. En respuesta a la determinación preliminar, el servidor 52 puede solicitar más datos indicativos del tipo de dispositivo sobre el sistema cliente al regulador 18 de red. Progresivamente, más datos indicativos del tipo de dispositivo se envían al servidor 52 de configuración, hasta que una identificación positiva del tipo de dispositivo del sistema cliente 12 se consigue. Cuando el tipo de dispositivo se ha identificado con éxito, el servidor 52 puede enviar una notificación al regulador 18. En respuesta a la recepción de la notificación (etapa 408), el regulador 18 puede redirigir la solicitud de conexión de red interceptada en la etapa 400 a una aplicación de instalador de agente.

Un escenario alternativo de descubrimiento de dispositivos y/o provisión de agente puede implicar un túnel, de manera similar a la descrita más arriba en relación con la detección automática del enrutador 19 (Figuras 13-14). En un ejemplo, el regulador 18 abre un túnel de comunicación (por ejemplo, un túnel SSH) que conecta el regulador 18 con el servidor 52. El túnel respectivo puede configurarse con reenvío de puertos, de modo que las comunicaciones recibidas del servidor 52 se redirigen por el regulador 18 de red al sistema cliente 12 respectivo. El servidor 52 entonces puede entregar directamente un instalador de agente al sistema cliente 12 a través del túnel, y puede además ordenar al sistema cliente ***12*** que instale el agente respectivo. El servidor 52 también puede usar el túnel SSH para obtener información indicativa del tipo de dispositivo del sistema cliente 12, mediante el uso de cualquiera de los métodos descritos más arriba.

Se puede proveer una amplia variedad de agentes de utilidad mediante el uso de los sistemas y métodos descritos en la presente memoria. Un agente 41 de utilidad a modo de ejemplo configurado para proveer servicios de seguridad puede llevar a cabo una evaluación de seguridad del sistema cliente 12 (por ejemplo, un análisis de malware local) y puede enviar datos de evaluación de seguridad al servidor 52 de configuración o al servidor 50 de seguridad. El(los) servidor(es) puede(n) entonces reenviar un indicador de seguridad al dispositivo 20 de administración para mostrar al usuario/administrador. Los indicadores de seguridad a modo de ejemplo que se muestran al usuario/administrador pueden incluir, entre otros, un indicador de si un objeto de software particular (por ejemplo, el sistema operativo) que se está ejecutando en el sistema cliente 12 está actualizado, y un indicador de la seguridad de una contraseña utilizada para proteger el sistema cliente 12. Otras acciones a modo de ejemplo llevadas a cabo por un agente de seguridad incluyen la actualización de software y/o políticas de seguridad para el sistema cliente respectivo. En algunas realizaciones, el agente 41 está configurado para filtrar el tráfico de red hacia/desde el sistema cliente 12 mediante el uso de un algoritmo de inspección de paquetes de red para determinar, por ejemplo, si el sistema cliente 12 está sujeto a un ataque malicioso. La funcionalidad adicional de un agente de utilidad que provee servicios de seguridad informática se detalla más abajo.

Un agente 41 de utilidad a modo de ejemplo configurado para proveer servicios de comunicación segura incluye un agente de red privada virtual (VPN). Dichos agentes pueden proteger el sistema cliente 12 cuando el sistema cliente 12 abandona la red 14 local (por ejemplo, cuando el usuario sale de su casa con su teléfono móvil). Dicho agente puede colaborar con el regulador 18 de red y/o servidor 52 de configuración para abrir un túnel de comunicación segura y/o configurar una VPN entre el sistema cliente respectivo y el servidor 50 de seguridad (más detalles más abajo).

Un agente 41 de utilidad a modo de ejemplo configurado para proveer servicios de control parental puede monitorear el uso del sistema cliente 12, e informar patrones de uso a un usuario supervisor (por ejemplo, padre) a través del dispositivo 20 de administración. El agente 41 puede además evitar que el sistema cliente 12 acceda a ciertos recursos remotos (por ejemplo, direcciones IP, sitios web, etc.) o que use ciertas aplicaciones instaladas localmente (por ejemplo, juegos). Dicho bloqueo se puede aplicar de forma permanente o según una planificación específica del usuario.

Un agente 41 de utilidad a modo de ejemplo configurado para proveer asistencia técnica remota puede configurar y/o abrir automáticamente un canal de comunicación segura (por ejemplo, un túnel SSH) entre el sistema cliente 12 y el servidor 52 de configuración. Los comandos de configuración y/o solución de problemas pueden entonces transmitirse del servidor 52 al sistema cliente 12, posiblemente sin la participación o asistencia explícita de un usuario del sistema cliente 12.

Es posible que algunos sistemas cliente como, por ejemplo, electrodomésticos, dispositivos que pueden ponerse, etc., no puedan instalar un agente de utilidad como se indica más arriba. Sin embargo, dichos dispositivos pueden incluir configuración integrada y/o agentes de gestión de dispositivos que permitan un comando remoto de los dispositivos respectivos. Algunas realizaciones de la presente invención pueden usar los agentes de gestión existentes y protocolos específicos del dispositivo y/o métodos de comunicación para comunicar actualizaciones de valores de parámetros a dichos dispositivos. Incluso para dichos dispositivos, la identificación correcta del tipo de dispositivo habilita al servidor 52 de configuración a formatear y comunicar correctamente los comandos de

configuración a los respectivos sistemas cliente. Para facilitar la determinación del tipo de dispositivo de dichos sistemas cliente, el regulador 18 de red puede analizar activamente las comunicaciones recibidas del sistema cliente respectivo o redirigir las comunicaciones respectivas al servidor 52 de configuración.

En algunas realizaciones, el regulador 18 de red puede condicionar el acceso del sistema cliente 12 a la red 16 extendida a una instalación exitosa del agente 41 de utilidad. Como ilustra en la etapa 416 en la Figura 18, algunas realizaciones pueden permitir que el sistema cliente acceda a la red 16 extendida solo en respuesta a la instalación del agente. Dichas configuraciones pueden mejorar la seguridad del sistema cliente 12 y/o de la red 14 local.

Gestión de dispositivos

Una vez que los agentes 41 de utilidad son funcionales, se pueden usar para llevar a cabo diversas tareas de gestión de dispositivos, por ejemplo, para configurar de forma remota los respectivos sistemas cliente 12a-f. Las tareas de configuración a modo de ejemplo incluyen, entre otras, encender o apagar un sistema cliente (por ejemplo, armar o desarmar un sistema de seguridad del hogar, encender y apagar luces), establecer un valor de un parámetro funcional de un sistema cliente (por ejemplo, configurar una temperatura deseada en un termostato inteligente), configurar la red y/o características de seguridad (por ejemplo, bloquear o permitir el acceso de ciertos sistemas cliente a la red 14, configurar parámetros de cortafuegos, configurar aplicaciones y/o funciones de control parental), llevar a cabo actualizaciones de software para componentes que se ejecutan en el sistema cliente respectivo y llevar a cabo tareas de asistencia técnica/resolución de problemas en relación con el sistema cliente respectivo.

En algunas realizaciones, un usuario/administrador puede gestionar remotamente el sistema cliente 12 a través de la GUI 48 de administración expuesta por el dispositivo 20 de administración (por ejemplo, un teléfono inteligente que ejecuta una aplicación de administración). Tras el registro del regulador 18 de red con el servidor 52 de configuración, el servidor 52 puede asociar de forma única el regulador 18 y el dispositivo 20 de administración a un abono. El abono respectivo también permite asociar de forma única el regulador 18 al conjunto de sistemas cliente 12a-f protegido por el respectivo regulador de red. Por lo tanto, el usuario del dispositivo 20 de administración puede seleccionar un sistema cliente específico para gestionar de forma remota desde la GUI 48 de administración, con la asistencia del servidor 52 de configuración. La gestión real del dispositivo (por ejemplo, el establecimiento de valores de parámetros) puede comprender la transmisión de datos y/o comandos de configuración entre el dispositivo 20 de administración y el sistema cliente respectivo.

En algunas realizaciones, la transmisión de datos/comandos de configuración a un sistema cliente objetivo utiliza una variación de los sistemas y métodos descritos más arriba, en relación con la configuración del enrutador 19 (Figuras 13-14) y con el descubrimiento de dispositivos. En respuesta a la recepción de una solicitud de gestión de dispositivo del dispositivo 20 de administración, el servidor 52 puede enviar una notificación al regulador 18 de red, la notificación haciendo que el regulador 18 y/o el sistema cliente objetivo abran un túnel de comunicación (por ejemplo, túnel SSH) entre el servidor 52 y el regulador 18 y/o entre el servidor 52 y el sistema cliente objetivo. El túnel se puede configurar con reenvío de puertos como se describe más arriba. Dicho túnel se puede entonces usar para transmitir comandos de configuración del servidor 52 al sistema cliente objetivo, los comandos respectivos diseñados, por ejemplo, para cambiar los ajustes de configuración del sistema cliente respectivo. En algunas realizaciones, dichos comandos de configuración se ejecutan por el agente 41 de utilidad. Cuando el sistema cliente objetivo carece de un agente de utilidad o no puede instalar dicho agente, los comandos de configuración están dirigidos al software de gestión nativo del dispositivo respectivo.

En una aplicación a modo de ejemplo, un usuario puede solicitar asistencia técnica/solución de problemas de un sistema cliente objetivo particular mediante el uso de los métodos descritos más arriba. La asistencia técnica puede entonces proceder automáticamente, sin mayor participación del usuario respectivo. Como parte de la resolución de problemas, algunas realizaciones del servidor 52 pueden determinar el sistema cliente objetivo para instalar un agente de utilidad dedicado configurado para resolver un problema técnico en particular.

Protección de seguridad informática

Las Figuras 19-A-B muestran realizaciones a modo de ejemplo en donde el regulador 18 de red colabora con el servidor 50 de seguridad para proteger los sistemas cliente 12a-f de amenazas a la seguridad informática como, por ejemplo, malware, adware, spyware e intrusión en la red. En la realización de la Figura 19-A, el regulador 18 de red redirige parte o la totalidad del tráfico de datos (en la presente memoria ilustrado por el paquete 80 de red) entre el sistema cliente 12 protegido y un sistema informático externo a la red local a través del servidor 50 de seguridad. Dicho reencaminamiento puede lograrse, por ejemplo, mediante la instalación de un regulador 18 de red como pasarela entre la red 14 local y la red 16 extendida, y mediante el uso del regulador 18 para interceptar el tráfico de red y redirigirlo activamente al servidor 50. En realizaciones como la ilustrada en la Figura 19-A, la detección de amenazas se lleva a cabo por el servidor 50 de seguridad, mediante el uso de cualquier método conocido en la técnica (por ejemplo, mediante el análisis de paquetes 80 de red para determinar si contienen malware o si son indicativos de una intrusión en la red).

En algunas realizaciones, como se ilustra en la Figura 19-B, la detección de amenazas se lleva a cabo por el regulador 18 de red. Dicha detección local puede comprender, por ejemplo, filtrado de contenido de paquetes. El regulador 18 puede mantener actualizados los algoritmos de detección de malware mediante la descarga de un conjunto de parámetros 82 de filtro (por ejemplo, firmas indicativas de malware) del servidor 50 de seguridad. Algunas realizaciones pueden combinar la detección de amenazas en el regulador 18 con la detección de amenazas en el servidor 50 de seguridad. En un ejemplo, el regulador 18 de red puede llevar a cabo un análisis preliminar del tráfico de datos, mediante el uso de, por ejemplo, métodos relativamente económicos. El regulador 18 luego puede enviar paquetes de red sospechosos para mayor análisis al servidor 50.

El reencaminamiento del tráfico a través del servidor 50 de seguridad (Figura 19-A) puede tener varias ventajas sobre la realización de un análisis de seguridad local (Figura 19-B). El servidor 50 puede comprender múltiples sistemas informáticos de alto caudal diseñados especialmente y, por lo tanto, puede llevar a cabo un análisis de tráfico computacionalmente intensivo como, por ejemplo, la inspección profunda de paquetes, de manera mucho más eficiente que el regulador 18. La instalación de dichas capacidades en el regulador 18 de red aumentará sustancialmente el precio, la complejidad y la superficie de ataque del regulador 18. Otra ventaja de tener un análisis de datos centralizado es que dichas configuraciones eliminan la necesidad de distribuir actualizaciones de firmas de identificación de malware y de otros datos utilizados en el análisis de paquetes de red a una gran cantidad de reguladores 18 de red distribuidos. Los sistemas de seguridad centralizados también suelen estar mejor equipados para responder a las amenazas recientemente descubiertas.

Una aplicación a modo de ejemplo de dichos sistemas y métodos de seguridad informática comprende bloquear el acceso de un sistema cliente protegido a páginas web maliciosas o fraudulentas. En un ejemplo, una solicitud de acceso a un recurso remoto (por ejemplo, una solicitud HTTP de un sistema cliente protegido) se intercepta y analiza para determinar si el acceso al recurso remoto, la página web, etc., representa un riesgo de seguridad informática. Dicho análisis puede usar cualquier método conocido en la técnica, por ejemplo, comparar una dirección del recurso respectivo con una lista negra de páginas web maliciosas o fraudulentas conocidas, analizar el diseño de la página web respectiva, etc. El análisis puede llevarse a cabo en el servidor 50 de seguridad (por ejemplo, en una configuración como se muestra en la Figura 19-A) o en el regulador 18 de red 18 (por ejemplo, como se muestra en la Figura 19-B). Cuando el análisis establece que el acceso al recurso remoto no representa un riesgo para la seguridad de la computadora, el respectivo sistema cliente tiene acceso al recurso remoto respectivo. Cuando el acceso se considera riesgoso, el sistema cliente solicitante puede bloquearse para acceder al recurso respectivo. Además de bloquear el acceso, algunas realizaciones del servidor 50 de seguridad envían una notificación de episodio al dispositivo 20 de administración, e informan al usuario/administrador del regulador 18 de red que ha ocurrido un episodio de seguridad. La notificación puede incluir un indicador del sistema cliente involucrado en el episodio respectivo y un indicador de un tipo de episodio (por ejemplo, acceso a un sitio web fraudulento).

Otra aplicación a modo de ejemplo de un sistema de seguridad informática según algunas realizaciones de la presente invención se ilustra en las Figuras 20-21. Como se muestra más arriba, un sistema cliente puede estar protegido contra amenazas a la seguridad informática mientras está conectado al regulador 18 de red en la red 14 local. El abandono de la red 14 (como sucede, por ejemplo, cuando un usuario abandona su hogar con su teléfono móvil), sin embargo, puede exponer el sistema cliente respectivo a varios riesgos de seguridad. Algunas realizaciones aseguran que, una vez registrado para la protección con el regulador 18 y servidor 52 de configuración, el sistema cliente respectivo está protegido en todo momento.

Para lograr dicha protección, algunas realizaciones instalan un agente 41 de utilidad en el sistema cliente respectivo (por ejemplo, teléfono móvil, tableta), agente 41 de utilidad configurado para gestionar una red privada virtual (VPN) que conecta el sistema cliente respectivo con el servidor 50 de seguridad. Cuando el sistema cliente respectivo tiene un agente VPN incorporado, algunas realizaciones pueden optar por configurar el agente VPN existente, en lugar de instalar el agente 41 de utilidad. Una conexión VPN (túnel) al servidor 50 de seguridad puede iniciarse, por ejemplo, cuando el sistema cliente respectivo abandona la red 14 local. Al mantener una conexión con el servidor 50 de seguridad incluso cuando está lejos de la red 14 local, algunas realizaciones pueden continuar utilizando los métodos de seguridad informática descritos más arriba (por ejemplo, para redirigir el tráfico a través del servidor 50 de seguridad) para proteger el sistema cliente respectivo.

La Figura 20 muestra un intercambio de datos a modo de ejemplo entre el sistema cliente 12, el regulador 18 de red y el servidor 52 de configuración, el intercambio ocurriendo como parte de la operación de un agente de utilidad VPN y una conexión segura asociada con el servidor 50 de seguridad. La Figura 21 muestra una secuencia a modo de ejemplo de etapas llevadas a cabo por el sistema cliente 12 que opera el agente de utilidad VPN según algunas realizaciones de la presente invención.

El agente de utilidad VPN que se ejecuta en el sistema cliente 12 puede obtener parámetros 88 de conexión para establecer un túnel VPN con el servidor 50 de seguridad del servidor 52 de configuración. Dichos parámetros pueden adaptarse al tipo de dispositivo del sistema cliente 12, como se describe más arriba. En algunas realizaciones, una secuencia de etapas 502-504 determina si el sistema cliente 12 actualmente es parte de la red 14 local (a saber, la red local atendida por el regulador 18 de red). La etapa 502 puede proceder según cualquier método conocido en la técnica, por ejemplo, mediante el mantenimiento de un flujo de mensajes 84 de mantenimiento de conexión entre el regulador 18 y el sistema cliente respectivo. Mientras el sistema cliente 12

permanece conectado a la red 14 local, el sistema cliente 12 puede usar el regulador 18 como pasarela para acceder a la red 16 externa, encontrándose protegida contra amenazas a la seguridad informática según los métodos descritos más arriba.

Cuando el sistema cliente 12 detecta que ya no está conectado a la red 14 local, en una etapa 510, el agente VPN que se ejecuta en el sistema cliente 12 puede abrir un túnel 90 VPN al servidor 50 de seguridad, y configurar, de esta manera, el túnel 90 según los parámetros 88 de VPN. El sistema cliente 12 puede, a partir de entonces, usar el túnel 90 VPN para la comunicación como, por ejemplo, navegación por Internet, mensajería, etc. En una realización alternativa, el regulador 18 de red puede determinar que el sistema cliente 12 ha abandonado la red 14 local y, en respuesta, notificar al servidor de 50 seguridad. El establecimiento del túnel 90 entonces puede iniciarse por el servidor 50.

Cuando el sistema cliente 12 vuelve a la proximidad del regulador 18 de red (por ejemplo, cuando el usuario vuelve a casa con su teléfono móvil), el sistema cliente 12 puede detectar una oferta de servicios de red (por ejemplo, una oferta de DHCP) del regulador 18 de red. Cuando recibe dicha oferta para conectarse a la red 14 local, en una secuencia de etapas 514-516, el agente de utilidad VPN que se ejecuta en el sistema cliente respectivo puede cerrar el túnel 90 VPN y conectarse a la red 14 local.

Los sistemas y métodos a modo de ejemplo descritos en la presente memoria permiten proteger múltiples sistemas cliente contra amenazas a la seguridad informática como, por ejemplo, software malicioso e intrusión en la red. Además de proteger los sistemas informáticos convencionales, los sistemas y métodos descritos son particularmente adecuados para proteger un ecosistema diverso de dispositivos inteligentes conectados a Internet como, por ejemplo, los dispositivos conocidos colectivamente en la cultura popular como Internet de las Cosas (IoT). Ejemplos de dichos dispositivos incluyen, entre otros, dispositivos que pueden ponerse (por ejemplo, relojes inteligentes, bandas de ejercicio, joyas interactivas), dispositivos de entretenimiento para el hogar (televisores, reproductores multimedia, consolas de juegos), electrodomésticos (neveras, termostatos, sistemas de iluminación inteligentes, sistemas de seguridad para el hogar). Algunas realizaciones permiten, por ejemplo, proteger todos los dispositivos electrónicos en un hogar mediante el uso de una solución unificada e integrada.

Algunas realizaciones incluyen un regulador de red configurado para configurar y gestionar una red local que interconecta los múltiples sistemas cliente protegidos. El regulador de red puede instalarse en una posición de pasarela entre la red local y una red extendida como, por ejemplo, Internet. En algunas realizaciones, la protección se logra por el regulador de red que redirige al menos una parte del tráfico de datos intercambiado entre un sistema cliente protegido y una entidad fuera de la red local a través de un servidor de seguridad remoto. Luego, se puede analizar el tráfico en busca de malware y bloquear el acceso a recursos riesgosos (por ejemplo, sitios web maliciosos o fraudulentos).

Algunas realizaciones aseguran que la protección contra amenazas a la seguridad informática continúe incluso cuando el sistema cliente respectivo abandone la red local. Por ejemplo, cuando un usuario sale de su casa con su teléfono móvil, el teléfono conserva la protección. En algunas realizaciones, dicha protección se logra al detectar automáticamente que un sistema cliente protegido ha abandonado la red local y, en respuesta, se activa automáticamente un túnel (por ejemplo, una conexión VPN punto a punto) al servidor de seguridad, cuyo túnel se utiliza para transportar tráfico de datos hacia/desde el dispositivo respectivo mientras el dispositivo está lejos de la red local.

En algunas realizaciones, el regulador de red está asociado de forma exclusiva a un abono de servicio, que permite una gestión unificada de la seguridad y otros aspectos para todos los sistemas cliente protegidos, por ejemplo, para todos los dispositivos inteligentes dentro de un hogar. Un episodio de seguridad como, por ejemplo, un intento por un sistema cliente protegido de acceder a un sitio web fraudulento, puede, por consiguiente, asociarse automáticamente a una cuenta de abono e informarse a una persona de contacto/administrador de la cuenta respectiva. La notificación de episodios de seguridad puede comprender el envío de una notificación a un dispositivo de administración (por ejemplo, teléfono móvil) del administrador. En algunas realizaciones, dichas notificaciones son centralizadas por el servidor de seguridad y agrupadas por usuario y/o por dispositivo. Una interfaz gráfica de usuario (GUI) que se ejecuta en el dispositivo de administración puede mostrar información sobre cada episodio de seguridad, datos estadísticos, etc. Algunas realizaciones de la presente invención, por lo tanto, permiten una solución centralizada para gestionar la seguridad informática para un gran número de clientes/cuentas, cada una de dichas cuentas asociada a su propio grupo diverso de dispositivos.

Aparte de garantizar la protección de los sistemas cliente conectados a la red local, algunas realizaciones proveen una solución unificada para la configuración automática, la resolución de problemas/asistencia técnica y la gestión remota de los sistemas cliente protegidos. Algunas realizaciones instalan un agente de utilidad en cada dispositivo protegido, y el agente de utilidad colabora con servidores remotos para recibir datos de configuración y/o código ejecutable. El usuario/administrador del sistema cliente puede gestionar de forma remota el dispositivo respectivo a través de una interfaz de usuario que se muestra en un dispositivo de administración (por ejemplo, teléfono móvil). Dicha gestión puede incluir, por ejemplo, la configuración de parámetros operativos (una temperatura deseada en el hogar, una configuración de control parental, etc.), la aplicación de actualizaciones de software y la resolución de problemas.

Algunas realizaciones de la presente invención están diseñadas específicamente para facilitar su uso, de modo que no requieran conocimientos especializados de ingeniería informática o administración de redes. Por ejemplo, después de la instalación, el regulador de red puede adquirir automáticamente algunos servicios de red de un enrutador existente, para convertirse en el proveedor por defecto de acceso a Internet para la red local.

Para una persona con experiencia en la técnica será claro que las realizaciones de más arriba pueden alterarse de muchas maneras sin apartarse del alcance de la invención. Por consiguiente, el alcance de la invención debe determinarse por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un regulador [18] de red conectado a múltiples sistemas cliente [12a-f] en una red [14] local, en donde un enrutador [19] provee un servicio de red que comprende asignar direcciones de red a los múltiples sistemas cliente [12a-f], el regulador [18] de red comprendiendo un procesador de hardware y una memoria, el procesador de hardware está configurado para:

en respuesta a la recepción de un conjunto de configuraciones de seguridad de un servidor [52] de configuración remota, configurar el regulador [18] de red según las configuraciones de seguridad, en donde la configuración del regulador [18] de red según las configuraciones de seguridad hace que el regulador [18] de red proteja los múltiples sistemas cliente [12a-f] contra amenazas a la seguridad informática; caracterizado por que

en respuesta a la conexión al enrutador [19] en la red [14] local, configurar un túnel que conecta el regulador [18] de red al servidor [52] de configuración remota, en donde la configuración del túnel comprende configurar el regulador [18] de red para redirigir al enrutador [19] una comunicación recibida a través del túnel, la comunicación configurada para provocar una interrupción del servicio de red; y

en respuesta a la interrupción, adquirir el servicio de red del enrutador [19].

2. El regulador [18] de red de la reivindicación 1, en donde la interrupción del servicio de red comprende incapacitar al enrutador [19].

3. El regulador [18] de red de la reivindicación 1, en donde la comunicación comprende un conjunto de instrucciones que, cuando se ejecutan por el enrutador [19], provocan la interrupción del servicio de red.

4. El regulador [18] de red de la reivindicación 1, en donde la comunicación comprende una solicitud para exponer una interfaz de configuración del enrutador [19].

5. El regulador [18] de red de la reivindicación 1, en donde la comunicación se configura para completar automáticamente un conjunto de campos de una interfaz de configuración del enrutador [19] con un conjunto de valores, el conjunto de valores seleccionados para provocar la interrupción del servicio de red.

6. El regulador [18] de red de la reivindicación 1, en donde la comunicación comprende un conjunto de credenciales de usuario para iniciar sesión en una interfaz de configuración del enrutador [19].

7. El regulador [18] de red de la reivindicación 1, en donde el servidor [52] de configuración se configura, en preparación para transmitir la comunicación, para:

adquirir a través del túnel un conjunto de datos de tipo de dispositivo indicativos de un tipo de dispositivo del enrutador [19]; y

en respuesta a la adquisición del conjunto de datos del tipo de dispositivo, configurar la comunicación según el tipo de dispositivo del enrutador [19].

8. El regulador [18] de red de la reivindicación 1, en donde el servidor [52] de configuración se configura para determinar un tipo de dispositivo del enrutador [19] según una respuesta a la comunicación.

9. El regulador [18] de red de la reivindicación 1, en donde el procesador de hardware se caracteriza además por estar configurado, en respuesta a la adquisición del servicio de red, para:

recibir una solicitud de túnel del servidor [52] de configuración, la solicitud de túnel indicando un sistema cliente [12] objetivo de los múltiples sistemas cliente [12a-f]; y

en respuesta a la recepción de la solicitud de túnel, configurar un segundo túnel que conecte el regulador [18] de red al servidor [52] de configuración, en donde la configuración del segundo túnel comprende configurar el regulador [18] de red para redirigir al sistema cliente [12] objetivo una segunda comunicación recibida a través del segundo túnel desde el servidor [52] de configuración.

10. El regulador [18] de red de la reivindicación 9, en donde la segunda comunicación comprende un instalador de agente configurado para instalar un agente de utilidad en el sistema cliente [12] objetivo.

11. El regulador [18] de red de la reivindicación 9, en donde la segunda comunicación comprende un conjunto de valores de parámetros para ajustar un conjunto de parámetros operativos del sistema cliente [12] objetivo.

12. El regulador [18] de red de la reivindicación 9, en donde el servidor [52] de configuración se configura, en preparación para transmitir la segunda comunicación, para:

adquirir a través del segundo túnel un conjunto de datos de tipo de dispositivo indicativos de un tipo de dispositivo del sistema cliente [12] objetivo; y

en respuesta a la adquisición del conjunto de datos del tipo de dispositivo, configurar la segunda comunicación según el tipo de dispositivo del sistema cliente [12] objetivo.

13. El regulador [18] de red de la reivindicación 1, en donde la protección de los múltiples sistemas cliente [12a-f] contra las amenazas a la seguridad informática comprende redirigir una solicitud para acceder a un recurso a un servidor [50] de seguridad remoto, la solicitud recibida de un sistema cliente [12] de los múltiples sistemas cliente [12a-f], en donde el servidor [50] de seguridad se configura para determinar si el otorgamiento de acceso al recurso expone el sistema cliente [12] a una amenaza a la seguridad informática.

14. El regulador [18] de red de la reivindicación 1, en donde el túnel se configura según un protocolo de carcasa segura (SSH).

15. Un medio no transitorio legible por ordenador que almacena instrucciones que,

cuando se ejecutan por al menos un procesador de hardware de un regulador [18] de red, en donde el regulador de red está conectado a múltiples sistemas cliente en una red local y en donde un enrutador provee un servicio de red que comprende asignar direcciones de red a los múltiples sistemas cliente, hacen que el regulador [18] de red:

en respuesta a la recepción de un conjunto de ajustes de seguridad de un servidor [52] de configuración remota, configure el regulador [18] de red según los ajustes de seguridad, en donde la configuración del regulador [18] de red según los ajustes de seguridad hace que el regulador [18] de red proteja múltiples sistemas cliente [12q-f] contra amenazas a la seguridad informática;

caracterizado por que en respuesta a la conexión al enrutador [19] en la red [14] local, configure un túnel que conecta el regulador [18] de red al servidor [52] de configuración remota, en donde la configuración del túnel comprende configurar el regulador [18] de red para redirigir al enrutador [19] una comunicación recibida a través del túnel desde el servidor [52] de configuración, la comunicación configurada para provocar una interrupción del servicio de red; y

en respuesta a la interrupción, adquiera el servicio de red del enrutador [19].

16. Un método, llevado a cabo por un regulador [18] de red, para proteger múltiples sistemas cliente [12a-f] contra las amenazas a la seguridad informática, los múltiples sistemas cliente [12a-f] conectados a una red [14] local, en donde un enrutador [19] conectado a la red [14] local lleva a cabo un servicio de red que comprende asignar direcciones de red a los múltiples sistemas cliente [12a-f], el método comprendiendo:

en respuesta a la recepción de un conjunto de configuraciones de seguridad de un servidor [52] de configuración remota, configurar el regulador [18] de red según los ajustes de seguridad, en donde la configuración del regulador [18] de red según los ajustes de seguridad hace que el regulador [18] de red proteja los múltiples sistemas cliente [12a-f] contra amenazas a la seguridad informática; caracterizado por que

en respuesta a la conexión al enrutador [18] en la red [14] local, emplear el regulador [18] de red para configurar un túnel que conecta el regulador [18] de red al servidor [52] de configuración remota, en donde la configuración del túnel comprende configurar el regulador [18] de red para redirigir al enrutador [19] una comunicación recibida a través del túnel desde el servidor [52] de configuración, la comunicación configurada para provocar una interrupción del servicio de red; y

en respuesta a la interrupción, emplear el regulador [18] de red para hacerse cargo del servicio de red del enrutador [19].

17. El regulador [18] de red de la reivindicación 1, en donde la adquisición del servicio de red del enrutador [19] comprende que el regulador de red se configura además para instalarse como una pasarela entre la red local y una red extendida, estando fuera de la red local, en donde al menos una parte del tráfico de red entre el sistema cliente [12] y la red [14] extendida atraviesa el regulador [18] de red.

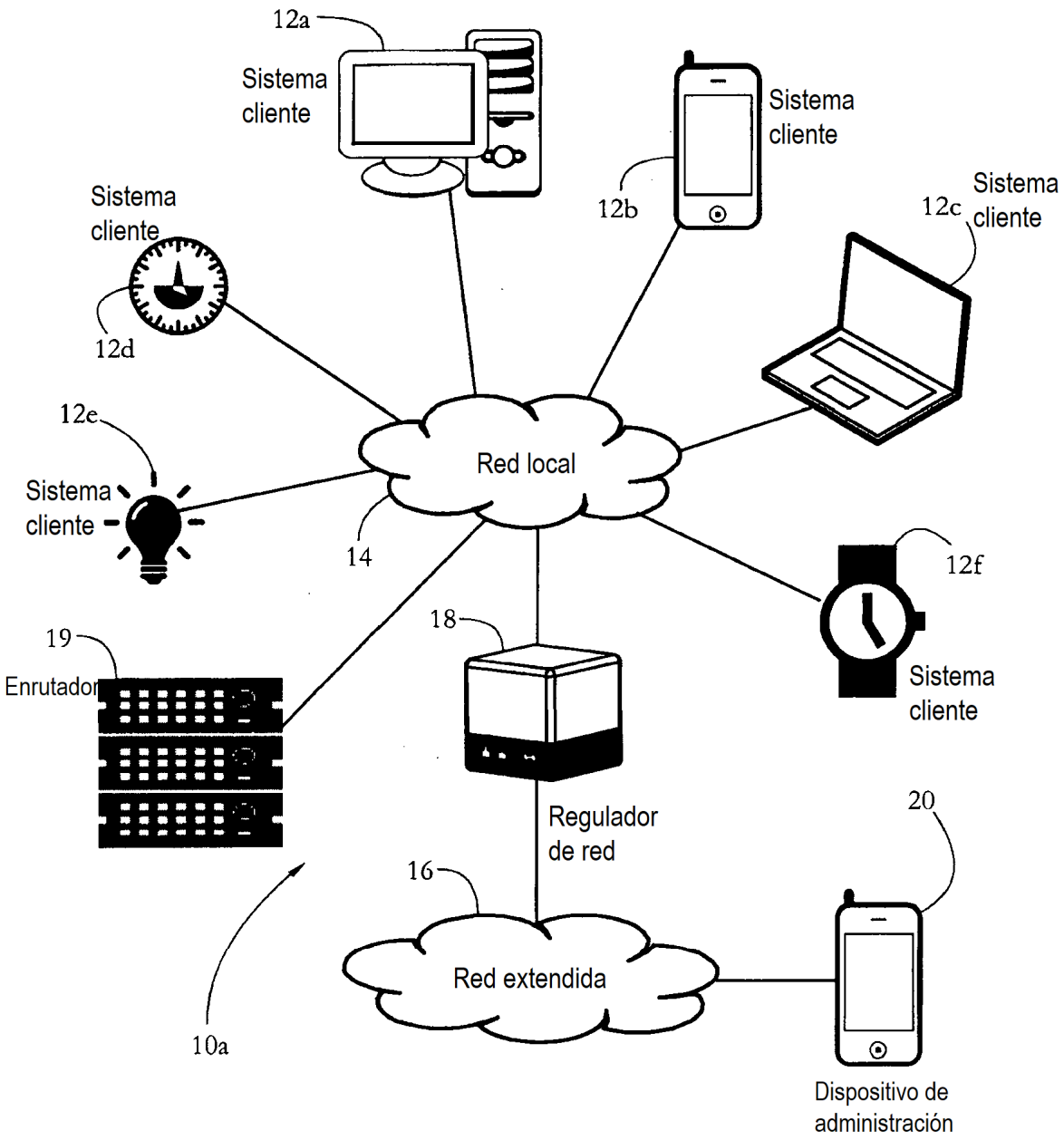
12a
Sistema cliente
Sistema cliente
12b
12c
Sistema cliente
Sistema cliente
12d
12e
Sistema cliente
Red local
14
12f
Sistema cliente
19
Enrutador
18
Regulador de red
16
20
Red extendida
10a
Dispositivo de administración

FIG. 1-A

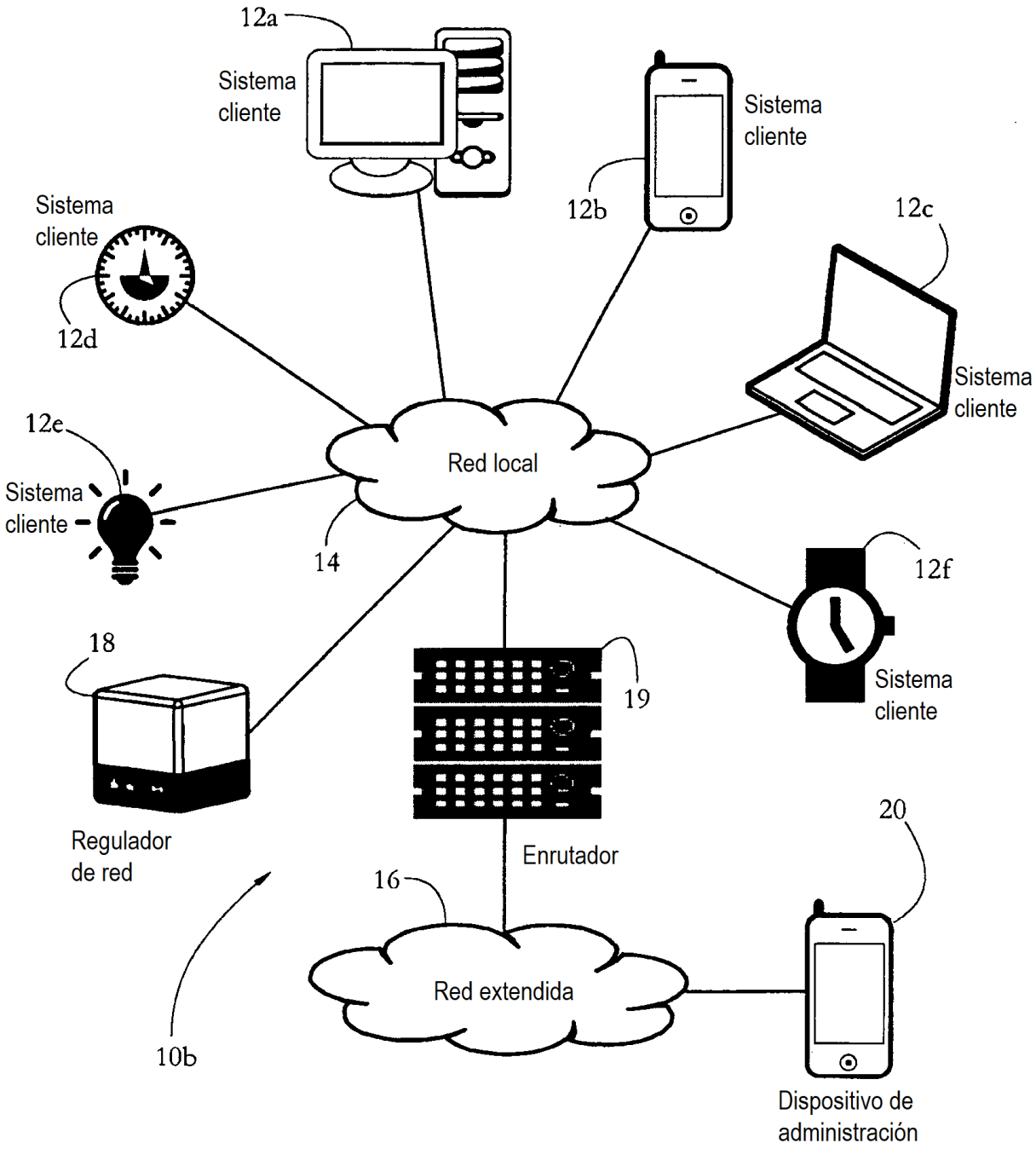
12a
Sistema cliente
Sistema cliente
12b
12c
Sistema cliente
Sistema cliente
12d
12e
Sistema cliente
Red local
14
12f
Sistema cliente
18
19
Regulador de red
Enrutador
20
16
Red extendida
10b
Dispositivo de administración

FIG. 1-B

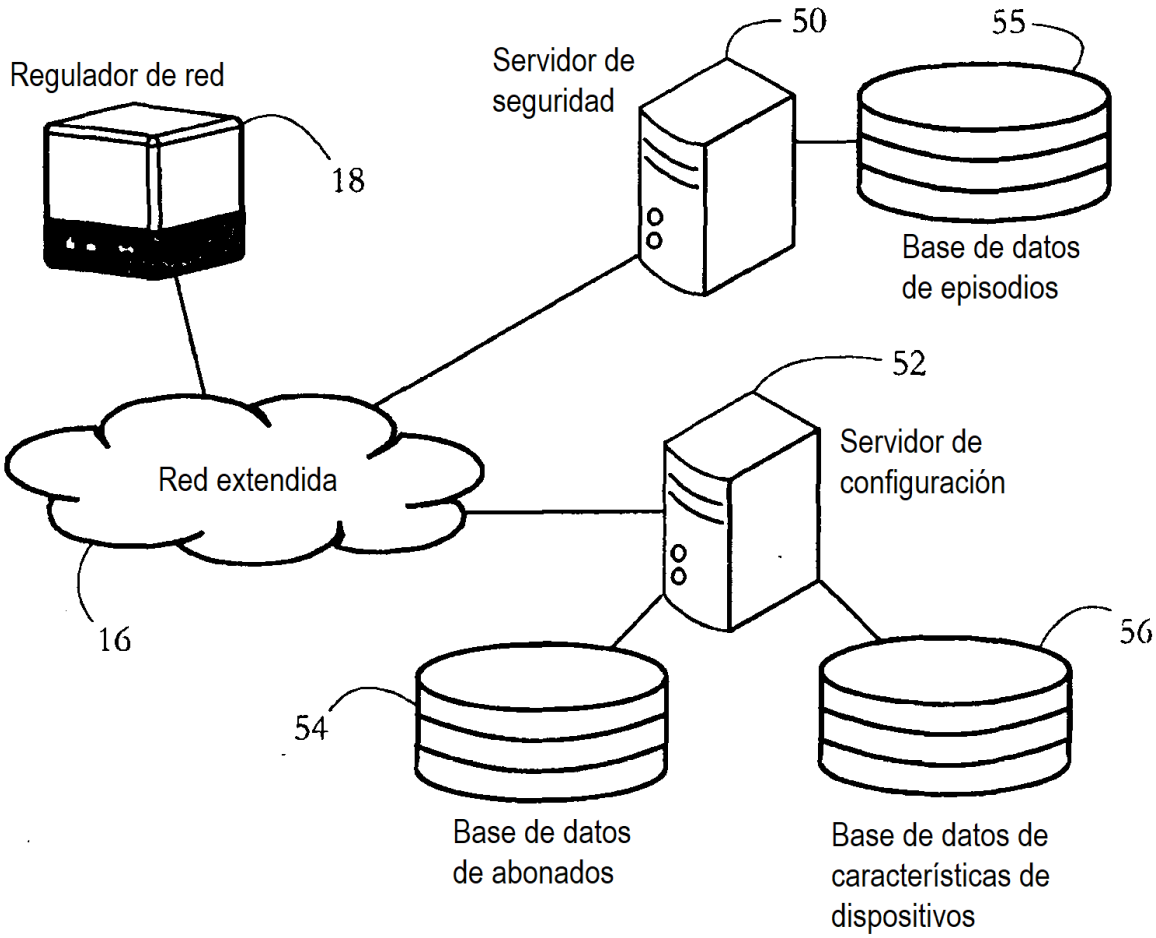
Regulador de red
18
Servidor de seguridad
50
55
Base de datos de episodios
52
Servidor de configuración
Red extendida
16
54
56
Base de datos de abonados
Base de datos de características de dispositivos

FIG. 2

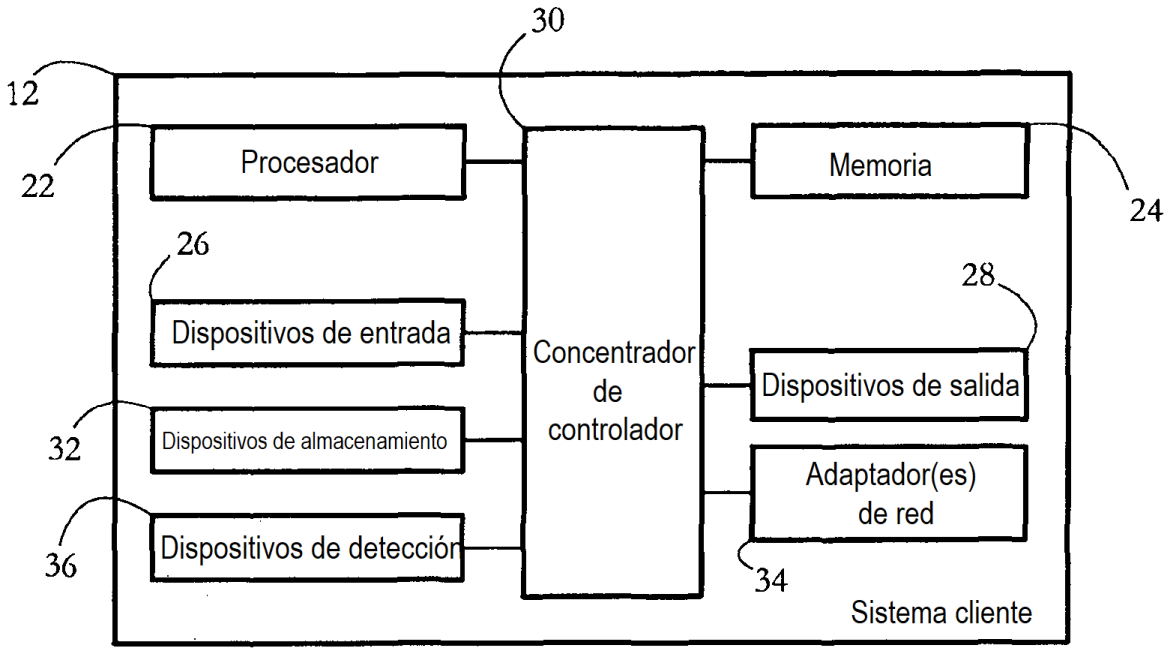
12
30
22
Procesador
Memoria
24
26
28
Dispositivos de entrada
Concentrador de controlador
Dispositivos de salida
32
Dispositivos de almacenamiento
Adaptador(es) de red
36
Dispositivos de detección
34
Sistema cliente

FIG. 3

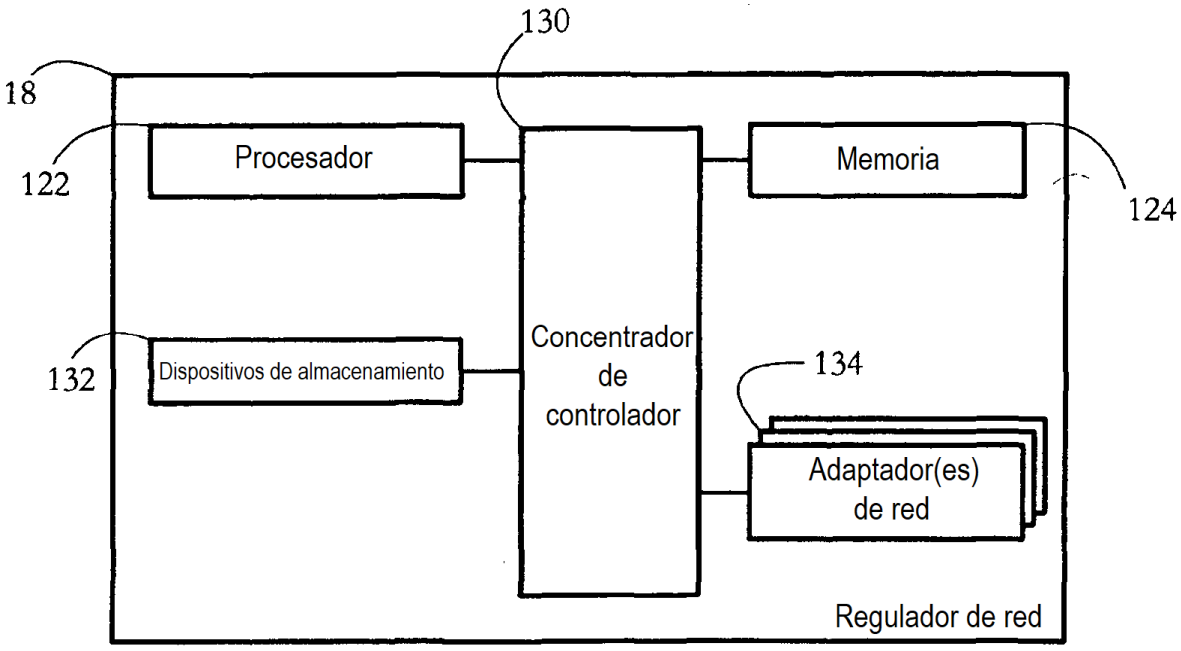
130
18
122
Procesador
Memoria
124
132
Dispositivos de almacenamiento
Concentrador de controlador
134
Adaptador(es) de red
Regulador de red

FIG. 4

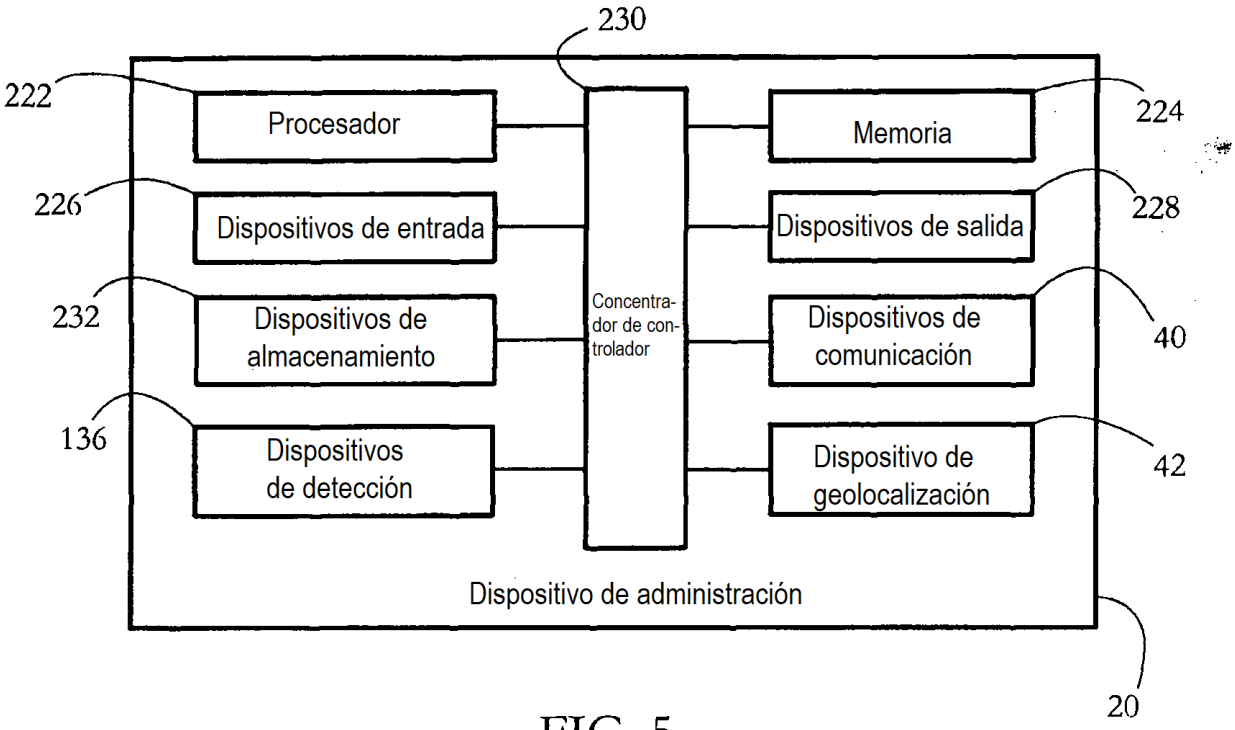
230
222
Procesador
224
Memoria
226
Dispositivos de entrada
228
Dispositivos de salida
232
Dispositivos de almacenamiento
Concentra-dor de con-trolador
Dispositivos de comunicación
40
136
Dispositivos de detección
Dispositivo de geolocalización
42
Dispositivo de administración
20

FIG. 5

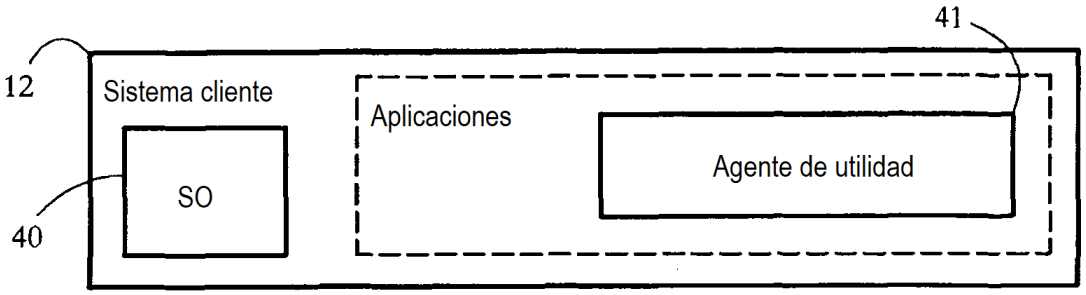

FIG. 6

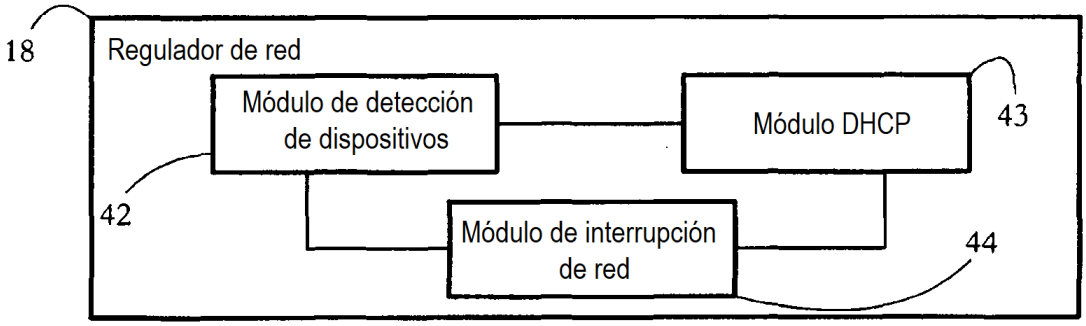

FIG. 7

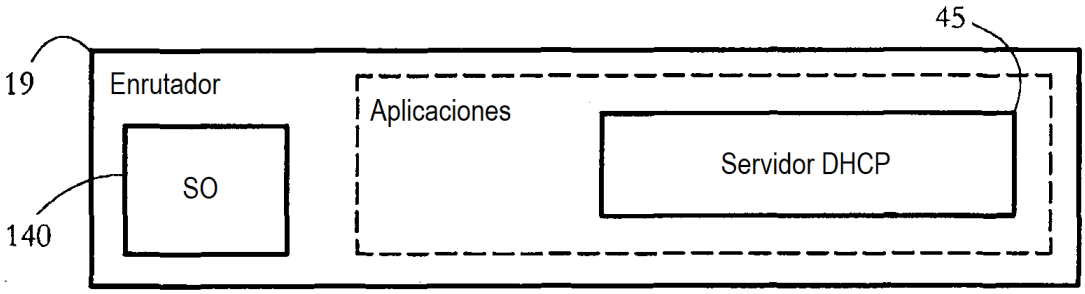

FIG. 8

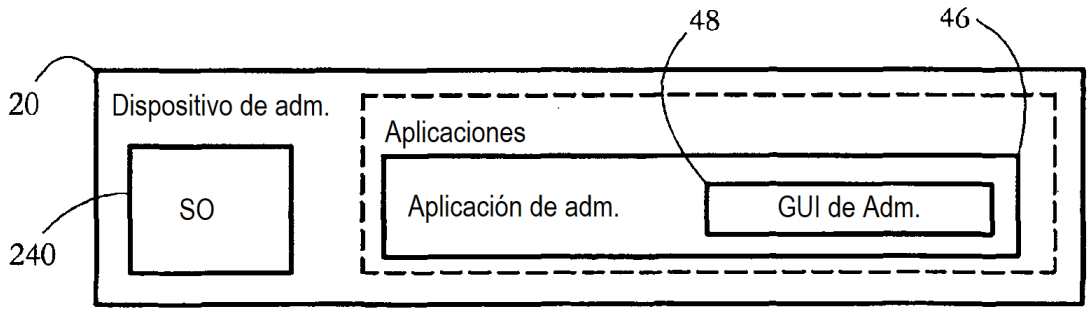

FIG. 9

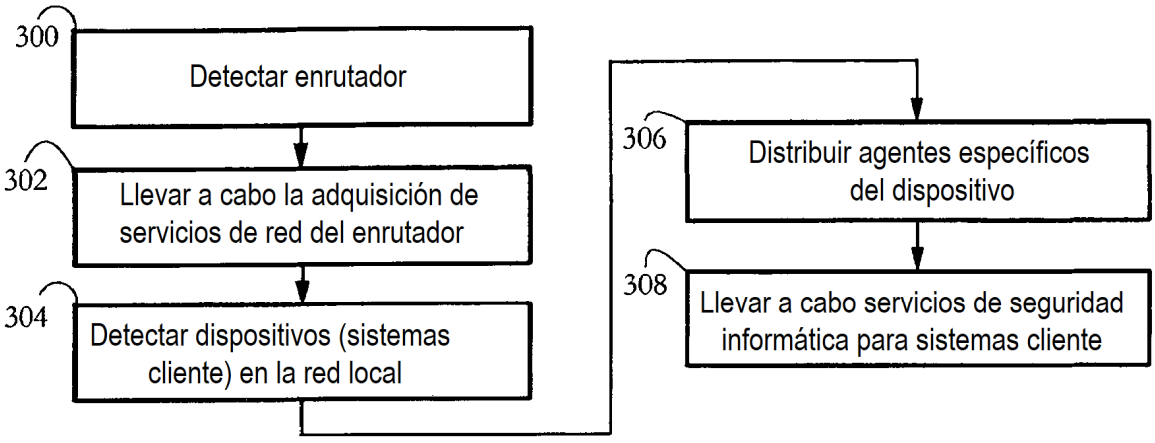
300
Detectar enrutador
302
Llevar a cabo la adquisición de servicios de red del enrutador
304
Detectar dispositivos (sistemas cliente) en la red local
306
Distribuir agentes específicos del dispositivo
308
Llevar a cabo servicios de seguridad informática para sistemas cliente

FIG. 10

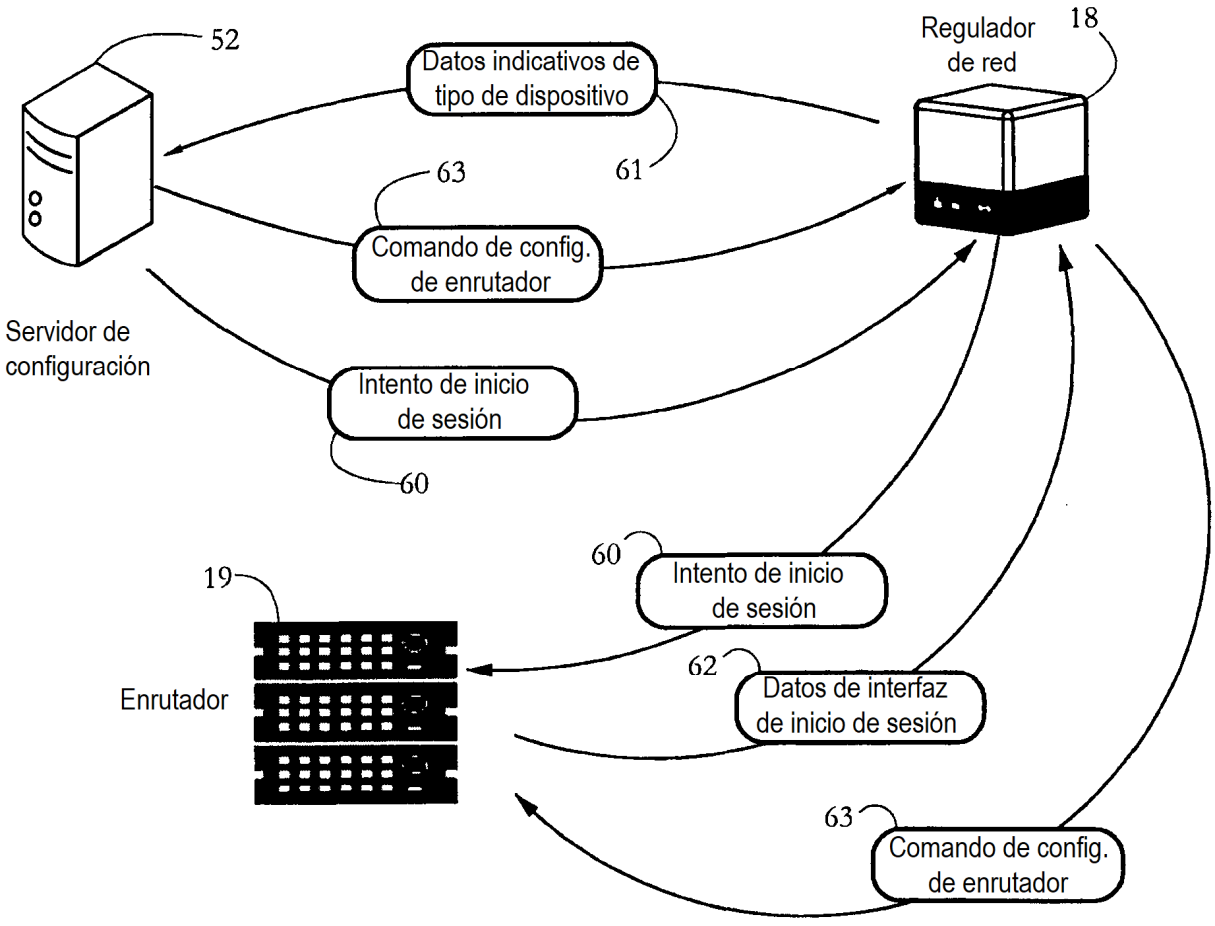
52
Datos indicativos de tipo de dispositivo
61
Regulador de red
18
63
Comando de config. de enrutador
Servidor de configuración
Intento de inicio de sesión
60
60
Intento de inicio de sesión
19
Enrutador
62
Datos de interfaz de inicio de sesión
63
Comando de config. de enrutador

FIG. 11

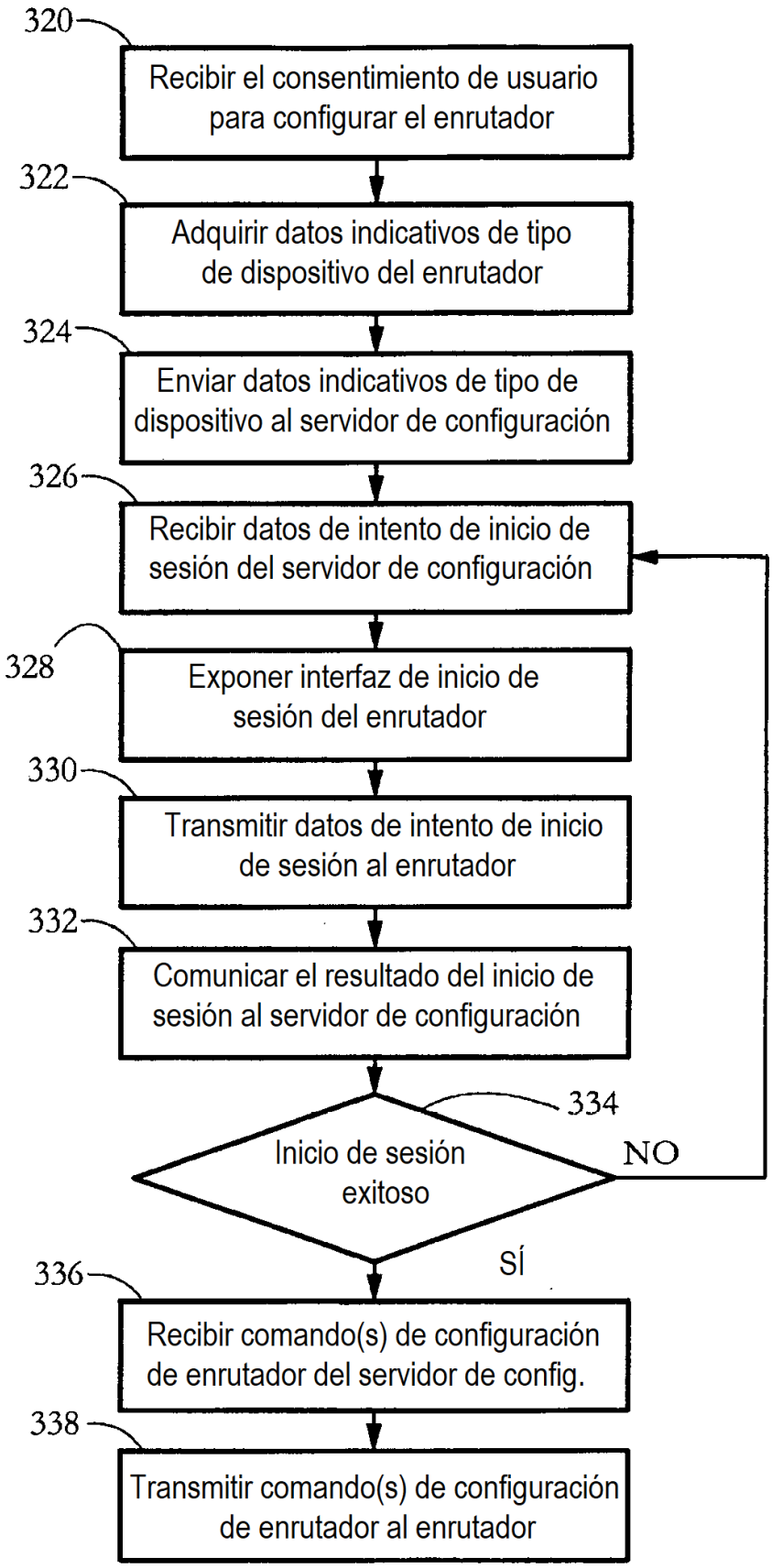
320
Recibir el consentimiento de usuario para configurar el enrutador
322
Adquirir datos indicativos de tipo de dispositivo del enrutador
324
Enviar datos indicativos de tipo de dispositivo al servidor de configuración
326
Recibir datos de intento de inicio de sesión del servidor de configuración
328
Exponer interfaz de inicio de sesión del enrutador
330
Transmitir datos de intento de inicio de sesión al enrutador
332
Comunicar el resultado del inicio de sesión al servidor de configuración
334
Inicio de sesión exitoso
NO
SÍ
336
Recibir comando(s) de configuración de enrutador del servidor de config.
338
Transmitir comando(s) de configuración de enrutador al enrutador

FIG. 12

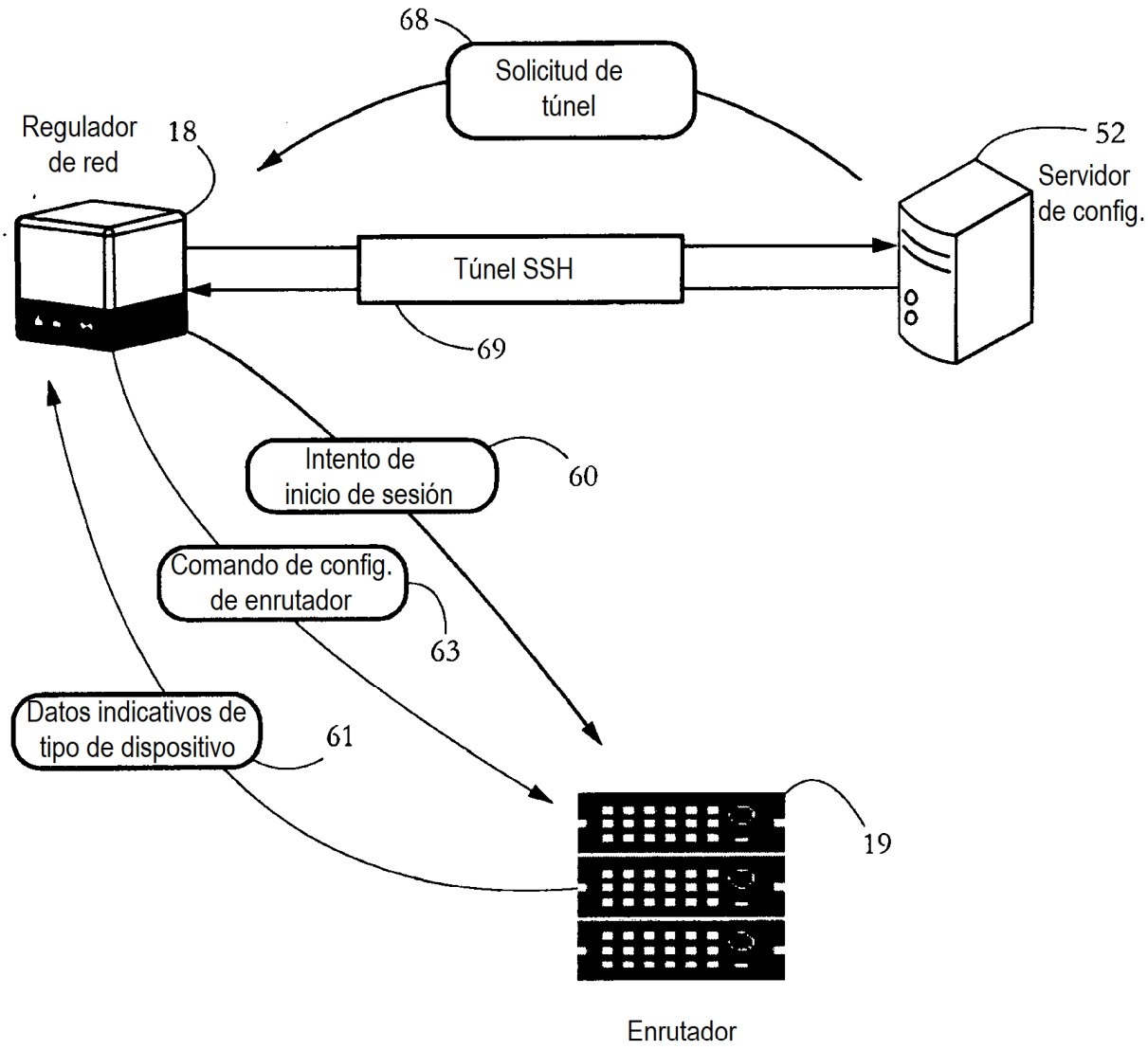
68
Solicitud de túnel
Regulador de red
18
52
Servidor de config.
Túnel SSH
69
Intento de inicio de sesión
60
Comando de config. de enrutador
63
Datos indicativos de tipo de dispositivo
61
19
Enrutador

FIG. 13

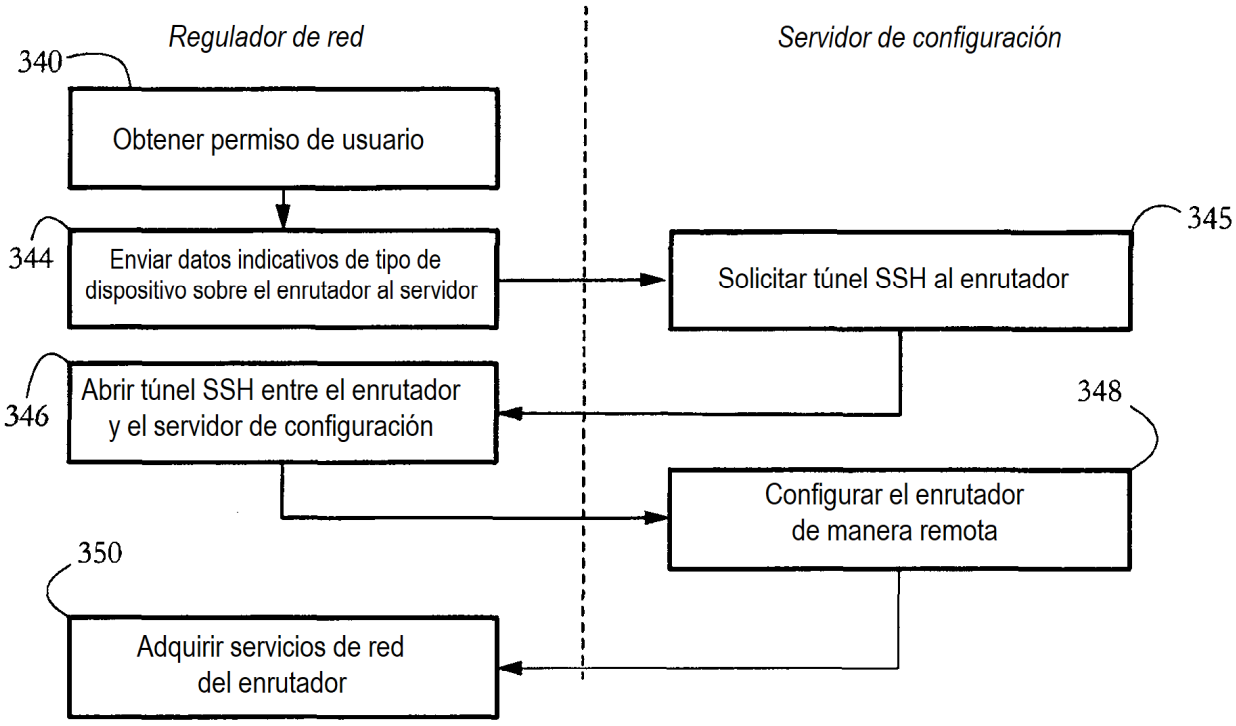
Regulador de red
Servidor de configuración
340
Obtener permiso de usuario
344
Enviar datos indicativos de tipo de dispositivo sobre el enrutador al servidor
345
Solicitar túnel SSH al enrutador
346
Abrir túnel SSH entre el enrutador y el servidor de configuración
348
Configurar el enrutador de manera remota
350
Adquirir servicios de red del enrutador

FIG. 14

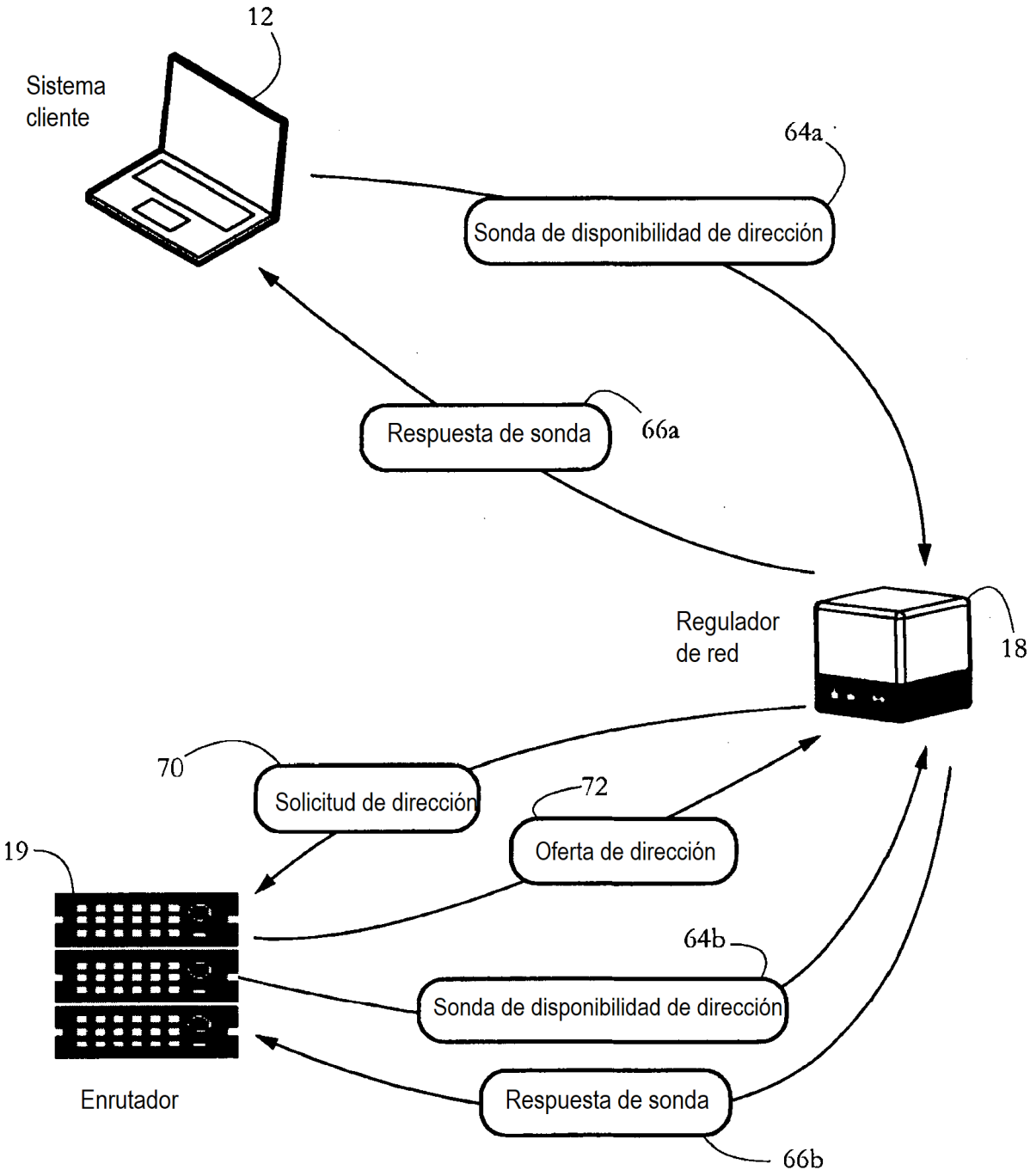
12
Sistema cliente
64a
Sonda de disponibilidad de dirección
Respuesta de sonda
66a
Regulador de red
18
70
Solicitud de dirección
72
Oferta de dirección
19
64b
Sonda de disponibilidad de dirección
Enrutador
Respuesta de sonda
66b

FIG. 15

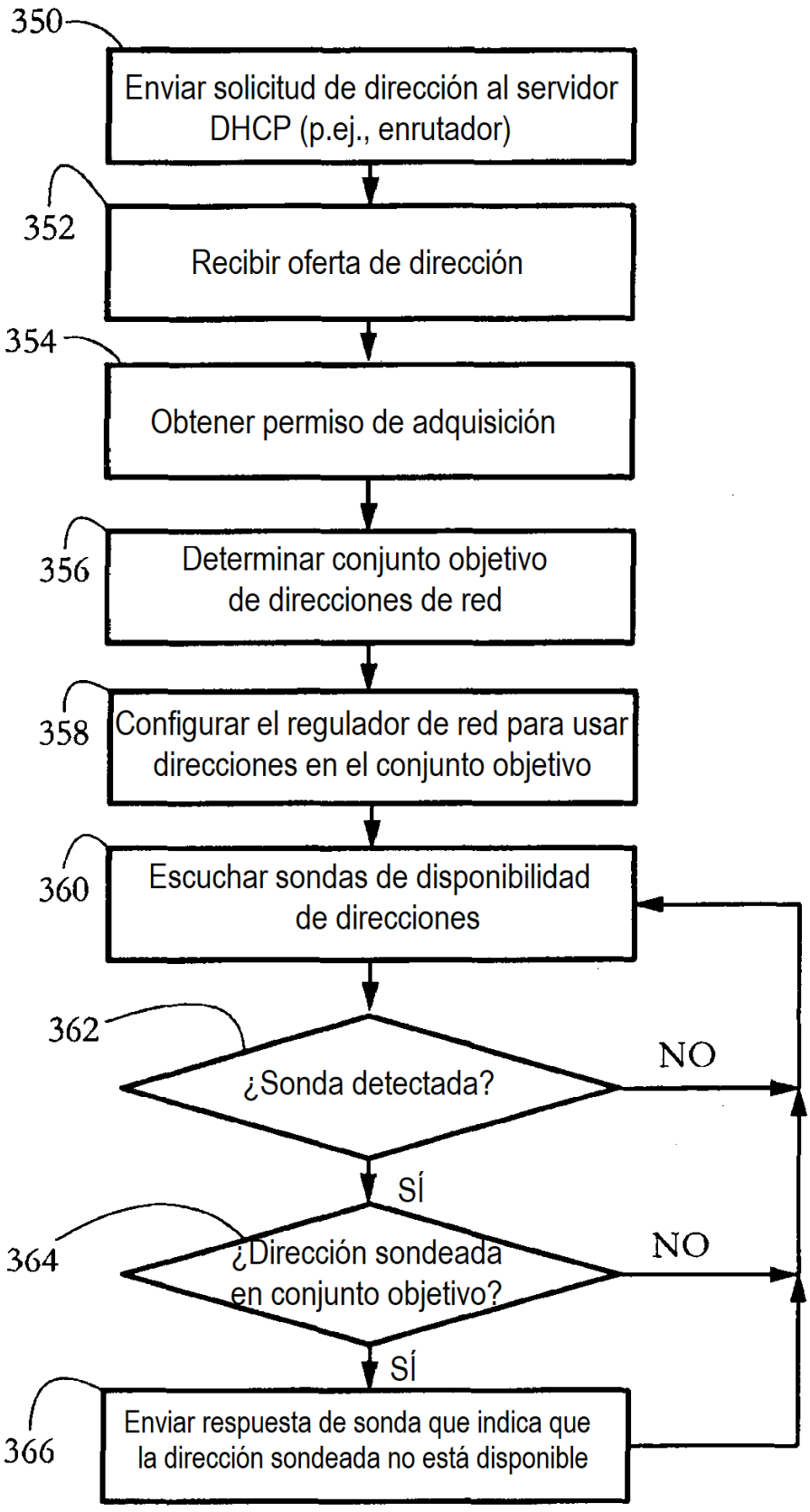
350
Enviar solicitud de dirección al servidor DHCP (p.ej., enrutador)
352
Recibir oferta de dirección
354
Obtener permiso de adquisición
356
Determinar conjunto objetivo de direcciones de red
358
Configurar el regulador de red para usar direcciones en el conjunto objetivo
360
Escuchar sondas de disponibilidad de direcciones
362
¿Sonda detectada?
NO
SÍ
364
¿Dirección sondeada en conjunto objetivo?
NO
SÍ
366
Enviar respuesta de sonda que indica que la dirección sondeada no está disponible

FIG. 16

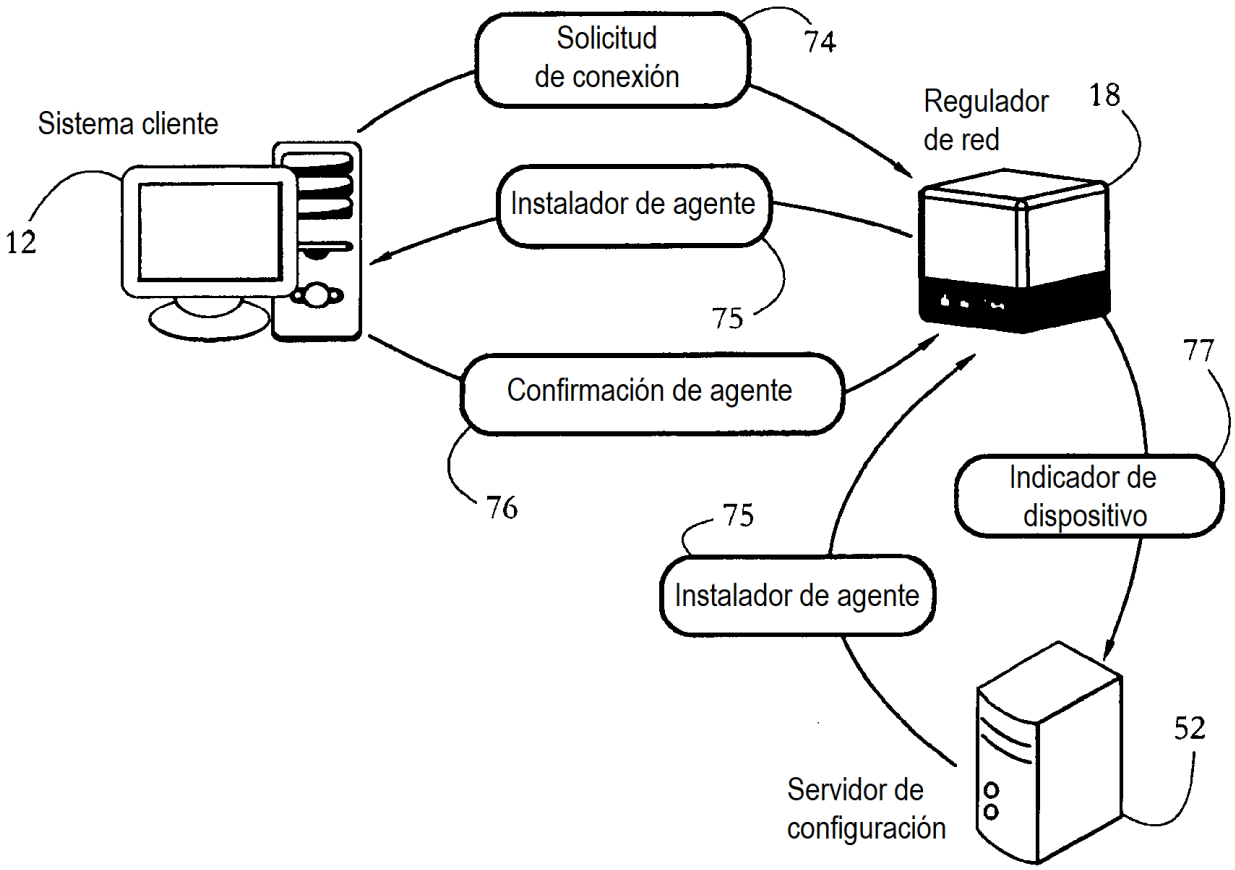
Solicitud
de conexión
74
Sistema cliente
12
Regulador
de red
18
Instalador de agente
75
Confirmación de agente
76
77
Indicador de
dispositivo
75
Instalador de agente
52
Servidor de
configuración

FIG. 17

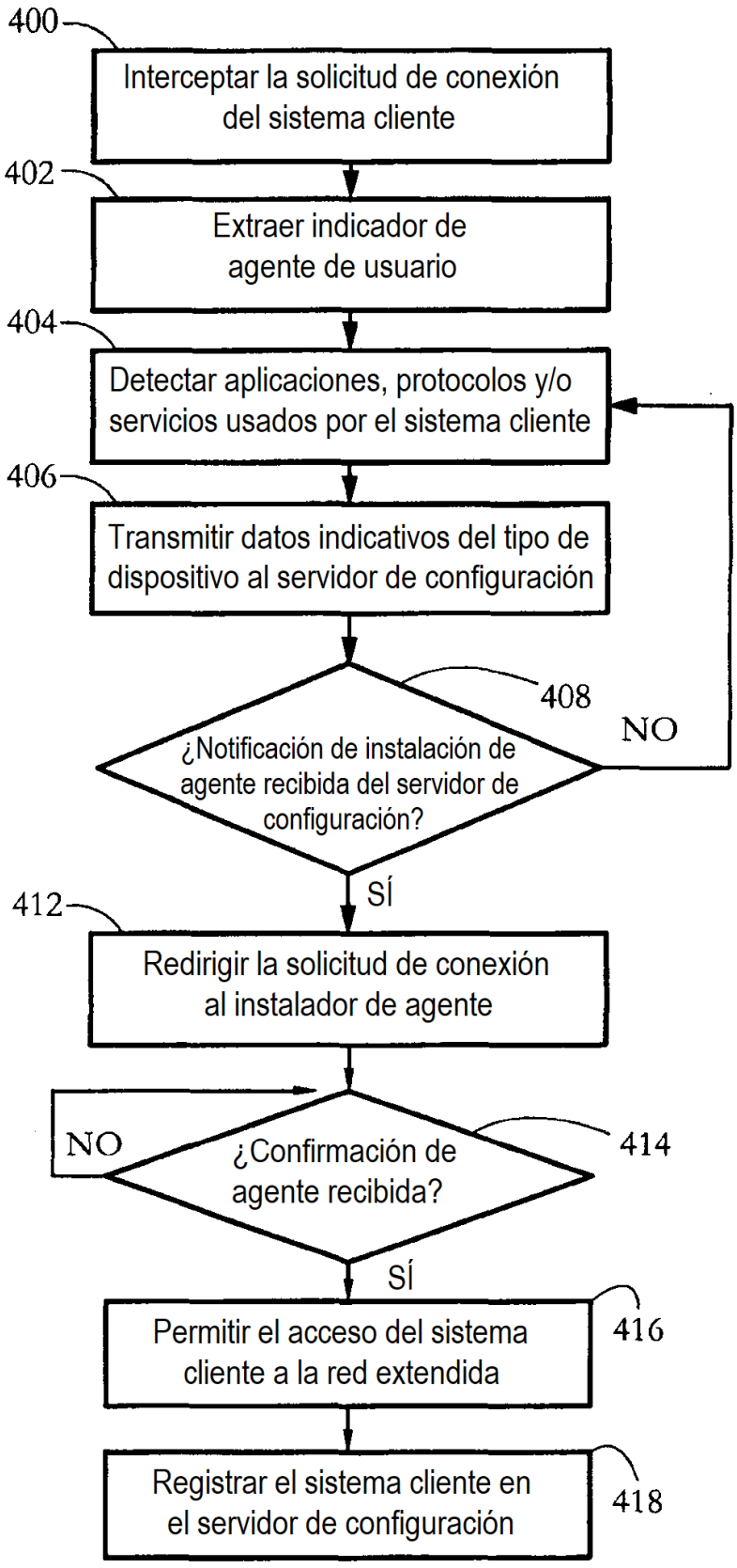
400
Interceptar la solicitud de conexión del sistema cliente
402
Extraer indicador de agente de usuario
404
Detectar aplicaciones, protocolos y/o servicios usados por el sistema cliente
406
Transmitir datos indicativos del tipo de dispositivo al servidor de configuración
408
¿Notificación de instalación de agente recibida del servidor de configuración?
NO
SÍ
412
Redirigir la solicitud de conexión al instalador de agente
NO
¿Confirmación de agente recibida?
414
SÍ
Permitir el acceso del sistema cliente a la red extendida
416
Registrar el sistema cliente en el servidor de configuración
418

FIG. 18

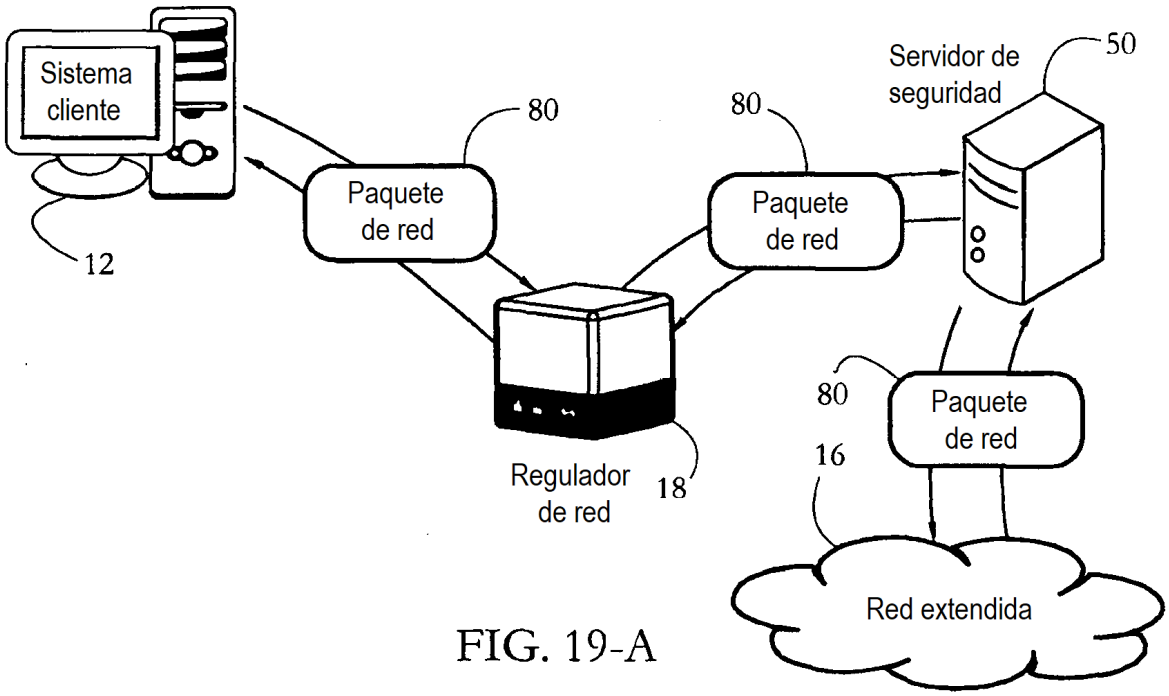

FIG. 19-A

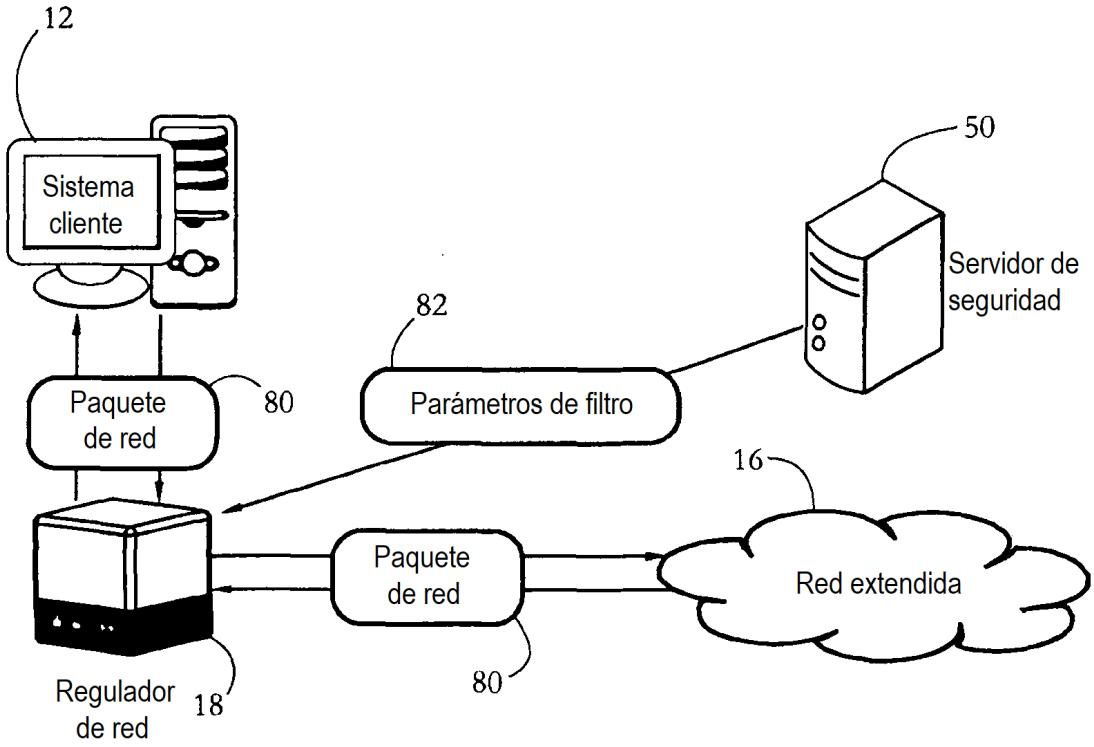

FIG. 19-B

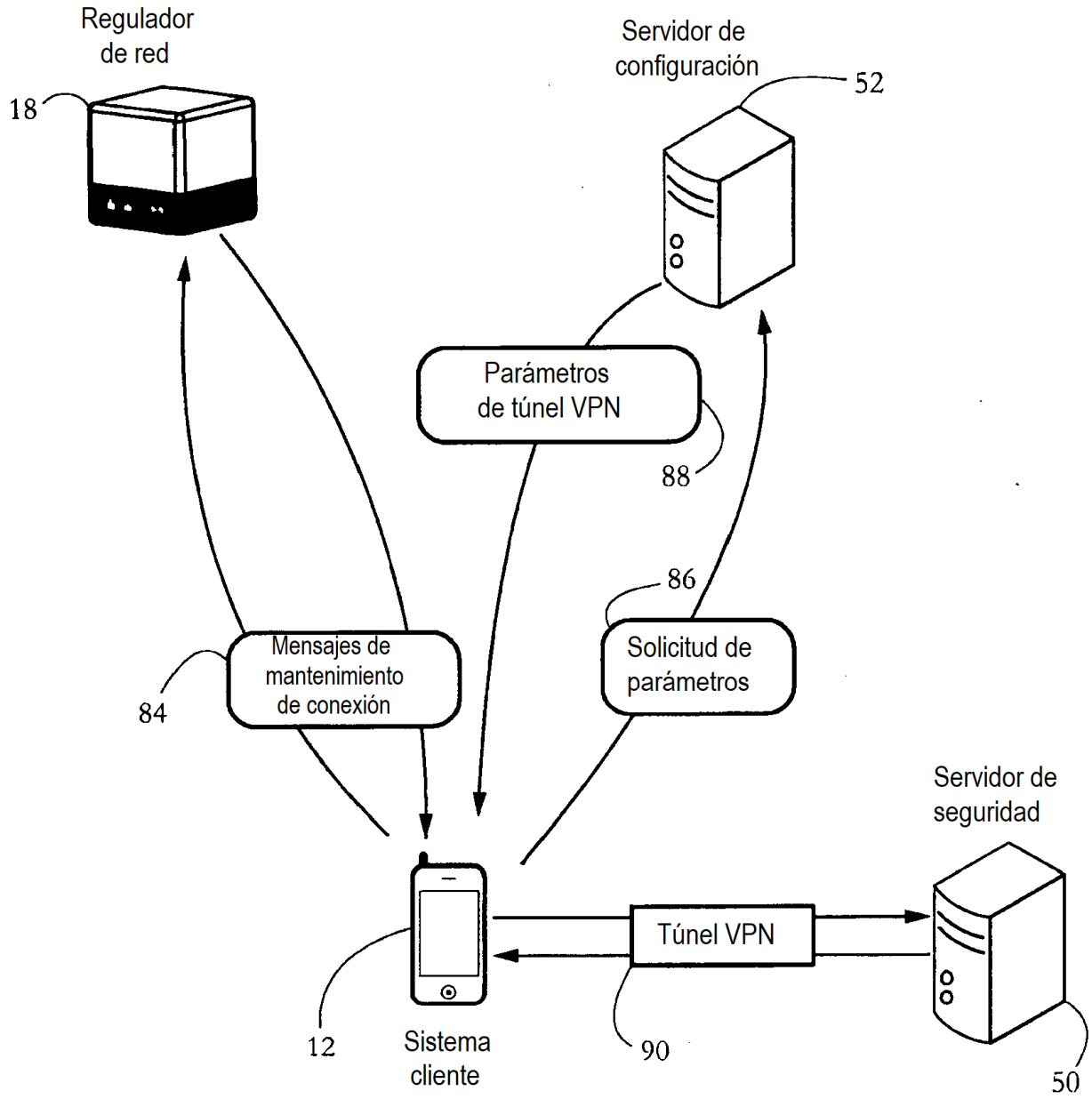
Regulador
de red
18
Servidor de
configuración
52
Parámetros
de túnel VPN
88
86
Mensajes de
mantenimiento
de conexión
84
Solicitud de
parámetros
Servidor de
seguridad
Túnel VPN
12
Sistema
cliente
90
50

FIG. 20

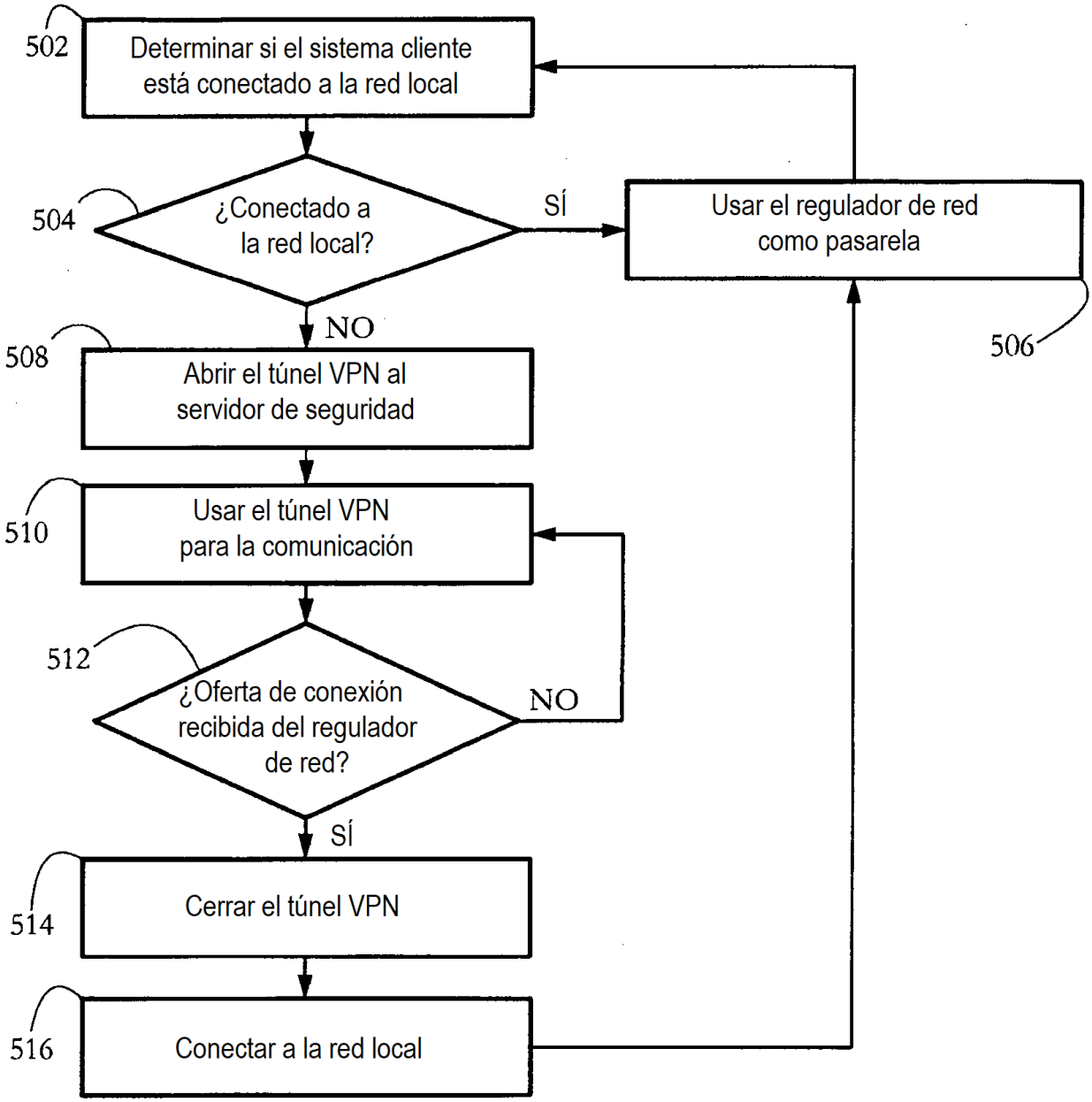
502
Determinar si el sistema cliente está conectado a la red local
504
¿Conectado a la red local?
SÍ
Usar el regulador de red como pasarela
506
NO
508
Abrir el túnel VPN al servidor de seguridad
510
Usar el túnel VPN para la comunicación
512
¿Oferta de conexión recibida del regulador de red?
NO
SÍ
514
Cerrar el túnel VPN
516
Conectar a la red local

FIG. 21