(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 871 067**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/12 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2016 PCT/IB2016/057733**

(87) Fecha y número de publicación internacional: **29.06.2017 WO17109659**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2016 E 16820357 (8)**

(97) Fecha y número de publicación de la concesión europea: **21.04.2021 EP 3381168**

(54) Título: **Red doméstica asegurada**

(30) Prioridad:

21.12.2015 US 201514976441

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2021

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

STRANSKY-HEILKRON, PHILIPPE

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Red doméstica asegurada

Campo técnico

La presente divulgación se refiere en general a redes domésticas y de forma más específica se refiere a sistemas y métodos para proporcionar protección a redes domésticas.

Antecedentes

Muchas casas están equipadas con redes domésticas. De forma más frecuente, la red doméstica puede ser una red IEEE 802.11 (Wi-Fi) proporcionada por e instalada por un proveedor de televisión por cable, un proveedor de servicio de teléfono por fibra óptica, un proveedor de servicio de red por satélite, etc. Los dispositivos se pueden conectar en la red doméstica a través de un rúter, que proporciona conectividad con una o más redes externas. El rúter puede estar dotado de software de encriptación para encriptar mensajes con dispositivos compatibles que también emplean el mismo tipo de encriptación utilizando un cliente de encriptación, el documento US 2004/0268147 A1 divulga un dispositivo de red utilizado para proporcionar una seguridad de red que incluye una interfaz configurada para recibir datos transmitidos sobre una red. El dispositivo de red también incluye un cortafuegos, una lógica de detección de intrusión y una lógica de reenvío. El cortafuegos, la lógica de detección de intrusión y la lógica de reenvío procesan los datos recibidos para determinar si los datos contienen un contenido malicioso. Cuando los datos contienen un contenido malicioso, los datos se pueden eliminar antes de alcanzar un dispositivo de usuario al cual se envían los datos recibidos. De forma opcional, el dispositivo de red puede interactuar con un dispositivo externo con el fin de realizar una decisión de reenvío. Adicionalmente, el dispositivo de red puede suscribirse a servicios ofrecidos por el dispositivo externo para recibir una información de seguridad actualizada. El documento US 2014/0237599 A1 divulga un modelo basado en agente distribuido para una monitorización y respuesta de seguridad.

Desafortunadamente, las redes domésticas provistas de software de encriptación todavía pueden estar sujetas a ataques, llevando a los usuarios a sentir que su red doméstica está expuesta y es insegura. Es difícil para los usuarios de redes domésticas instalar y mantener herramientas disponibles para restaurar la confianza, por ejemplo, cortafuegos, antivirus, etc. Adicionalmente muchos usuarios no tienen una experiencia suficiente para instalar, mantener y configurar estas herramientas. Esto lleva a una desconfianza de usuario adicional cuando el usuario desea instalar dispositivos tales como cámaras de vigilancia de niños, cámaras web, sistemas de seguridad de puertas y ventanas, etc., que se pueden piratear. Los usuarios pueden estar muy dudosos de añadir dispositivos no asegurados a su red doméstica. Los usuarios no quieren que su cámara de vigilancia de niños o sistema de seguridad de puertas y ventanas sean jaqueados.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra una red de ejemplo en la cual pueden funcionar ejemplos de la presente descripción.

La figura 2 es un diagrama de bloques de los elementos de la figura 1 adaptados para añadir un dispositivo no asegurado a una red doméstica fiable, en donde los mensajes son enrutados a través de un dispositivo existente que tiene una lógica de detección de software malicioso en la red doméstica fiable.

La figura 3 es un diagrama de bloques de los elementos de la figura 1 adaptados para añadir un dispositivo no asegurado a una red doméstica fiable, en donde los mensajes son enrutados a través de un nuevo dispositivo que tiene una lógica de detección de software malicioso en la red doméstica fiable.

La figura 4 es un diagrama que ilustra un método de ejemplo para permitir a un dispositivo asegurado de la figura 1 recibir un mensaje desde un dispositivo no asegurado de una primera red y destinado a un dispositivo de destino de la red doméstica de la figura 1, en donde la determinación de la presencia de software malicioso se realiza mediante una lógica de detección de software malicioso ejecutada por un dispositivo de procesamiento (por ejemplo, un servidor de puerta de enlace).

La figura 5 es un diagrama que ilustra un método de ejemplo para permitir a un dispositivo asegurado de la figura 3 recibir un mensaje de un dispositivo no asegurado de una primera red y destinado a un dispositivo de destino de la red doméstica de la figura 1, en donde la determinación de la presencia de software malicioso se realiza mediante una lógica de detección de software malicioso en la nube del servidor informático en la nube.

La figura 6 es un diagrama que ilustra un método de ejemplo para configurar una sesión de comunicación segura entre dos dispositivos en la red de la figura 1, un primer dispositivo (por ejemplo, el servidor de puerta de enlace) que tiene una lógica de detección de software malicioso y un segundo dispositivo que tiene un cliente de seguridad.

La figura 7 es un diagrama que ilustra un método de ejemplo para añadir un dispositivo no asegurado a una red doméstica de la figura 2, en donde los mensajes son enrutados a través de un dispositivo existente (por ejemplo, un dispositivo de red) que tiene una lógica de detección de software malicioso en la red doméstica.

La figura 8 es un diagrama que ilustra un método de ejemplo para añadir un dispositivo no asegurado a la red doméstica de la figura 3, en donde los mensajes son enrutados a través de un nuevo dispositivo asegurado que tiene una lógica de detección de software malicioso en la red doméstica.

La figura 9 es un diagrama que ilustra un método de ejemplo para configurar una red doméstica para responder a una modificación de una configuración de un dispositivo asegurado (por ejemplo, el servidor de puerta de enlace) en la red doméstica de la figura 1.

La figura 10 ilustra una representación esquemática de una máquina en forma de ejemplo de un sistema informático dentro del cual se puede ejecutar un conjunto de instrucciones para provocar que la máquina realice una o más de las metodologías expuestas en el presente documento.

Descripción detallada

Tal y como se utiliza en el presente documento, un software malicioso puede referirse a cualquier software utilizado para interrumpir operaciones informáticas, recopilar información sensible o acceder a sistemas informáticos privados. El software malicioso puede definirse mediante su intención maliciosa, que actúa contra los requisitos del usuario informático y no incluye software que provoca un daño no intencionado debido a alguna deficiencia. “Software malicioso” es un término paraguas utilizado para referirse a una variedad de formas de software hostil o intrusivo, incluyendo, pero no limitadas a, virus informáticos, gusanos, caballos de Troya, software de petición de rescate, software espía, software de publicidad, software de intimidación y otros programas maliciosos. Puede tomar la forma de un código ejecutable, archivos de comandos, un contenido activo y otro software.

En la siguiente descripción, se establecen numerosos detalles. Será evidente, sin embargo, para un experto en la técnica, que la presente divulgación se puede llevar a la práctica sin estos detalles específicos. En algunos casos, estructuras y dispositivos bien conocidos se muestran en forma de diagrama de bloques, en lugar de en detalle, con el fin de evitar oscurecer la presente divulgación.

La figura 1 es un diagrama de bloques que ilustra una red 100 de ejemplo en la cual pueden funcionar ejemplos de la presente divulgación. La red 100 puede incluir un servidor/ anfitrión /dispositivo 102 de procesamiento (de aquí en adelante la “puerta 102 de enlace asegurada”) provista de una lógica 104 de detección de software malicioso, de acuerdo con ejemplos de la presente divulgación. Tal y como se utiliza en el presente documento, la lógica de detección de software malicioso puede referirse a una lógica de procesamiento destinada a detectar la presencia de un software malicioso. Los términos “ordenador”, “plataforma informática”, dispositivo de procesamiento, anfitrión, servidor están destinados a incluir cualquier dispositivo de procesamiento de datos, tal como un ordenador de sobremesa, un ordenador portátil, un ordenador de tableta, un ordenador central, un servidor, un dispositivo de mano, un procesador de señal digital (DSP), un procesador embebido (un ejemplo del cual se describe en conexión con la figura 10) o cualquier otro dispositivo capaz de procesar datos. La plataforma informática/ordenador está configurada para incluir uno o más microprocesadores conectados de forma comunicativa a uno o más medios legibles por ordenador no transitorios y una o más redes. El término “conectados de forma comunicativa” está destinado a incluir cualquier tipo de conexión, sea cableada o inalámbrica, en la cual se puedan comunicar datos. El término “conectado de forma comunicativa” está destinado a incluir, pero no está limitado a, una conexión entre dispositivos y programas con un único ordenador o entre dispositivos y/u ordenadores separados sobre una red. El término “red” está destinado a incluir, pero no está limitado a OTA (transmisión por aire, ATSC, DVB-T”, redes de conmutación de paquetes (TCP/IP, por ejemplo, Internet) un satélite (microondas, transmisión de transporte MPEG o IP), un satélite de retransmisión directa, sistemas de transmisión por cable analógicos (RF), un sistema de transmisión de video digital (ATSC, HD-SDI, HDMI, DVI, VGA), etc.

La puerta 102 de enlace asegurada puede conectarse de forma comunicativa a una red 106 externa no asegurada, tal como Internet, a uno o más dispositivos/anfitriones/servidores 111 de procesamiento no seguros y a un sistema/servidor 108 de computación en la nube (de aquí en adelante el “servidor 108 de computación en la nube”) que tenga una lógica 110 de detección de software malicioso en la nube en el mismo. La puerta 102 de enlace asegurada puede conectarse de forma comunicativa a una red 106 externa no asegurada mediante un rúter 112 provisto de un proveedor de servicios de Internet basado en cable, fibra, satélite, etc. El rúter 112 puede configurarse para tener uno o más protocolos de encriptación (no mostrados) y/un software de detección de software malicioso (no mostrado).

La red 100 puede además incluir una subred 114 doméstica asegurada (de aquí en adelante la “red 114 doméstica asegurada”) y una subred 116 doméstica no asegurada (de aquí en adelante la “red 116 doméstica no asegurada”) conectada de forma comunicativa a la red 106 externa no asegurada. La red 114 doméstica asegurada puede incluir uno o más dispositivos 118a-118n, en donde todos de los uno o más dispositivos 118a-118n asegurados están provistos de clientes 120a-120n de seguridad. La red 114 doméstica asegurada puede además estar provista de un dispositivo 122 de red que tiene una lógica 126 de detección de software malicioso, a través de la cual el uno o más dispositivos 118a-118n asegurados pueden comunicarse con la red 106 externa directamente o a través del rúter 112. La red 116 doméstica no asegurada puede incluir uno o más dispositivos 124a-124n no asegurados, en donde al menos uno de los dispositivos 124a-124n no fiable no está provisto de un cliente de seguridad y por tanto puede referirse como un dispositivo no asegurado (por ejemplo, 124a). El uno o más dispositivos 118a-118n asegurados y el

uno o más dispositivos 124a-124n no asegurados, pueden incluir, pero no están limitados a, sensores avanzados, cámaras, máquinas del Internet de las cosas, electrodomésticos, etc. La red 116 doméstica no asegurada puede incluir un dispositivo 128 de red que tiene una lógica 130 de detección de software malicioso, a través de la cual el uno o más dispositivos 124a-124n no asegurados se puede comunicar con la red 106 externa directamente o a través del rúter 112.

La lógica 104, 110, 126, 130 de detección de software malicioso y los clientes 120a-120n de seguridad pueden tener uno o más componentes de un tipo de cortafuegos y de capa de seguridad (de aquí en adelante una “pared de seguridad”) configurados para realizar una pluralidad de detecciones de software malicioso, protección y otras funciones de seguridad que incluyen, pero no están limitadas a, una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus, una inspección de paquetes profunda para la detección de ataques conocidos o una generación de alarmas. En un ejemplo, los clientes 120a-120n de seguridad pueden además configurarse para recibir únicamente mensajes encriptados. La lógica 104, 110, 126, 130 de detección de software malicioso y los clientes 120a-120n de seguridad pueden implementarse o bien en hardware como un dispositivo externo o en software como un módulo de complemento, instalado o descargado.

La pared de seguridad puede configurarse para proporcionar un proceso de inicio seguro, un proceso de descarga seguro y/un proceso de generación para generar una o más claves para mensajes de encriptación. La pared de seguridad puede configurarse para encriptar/desencriptar mensajes para crear un canal seguro entre clientes de seguridad equipados con una pared de seguridad menos potente (por ejemplo, 120a) para proporcionar canales de comunicación entre varias instancias de la pared de seguridad en la red 100, para una reacción dinámica y un reporte de amenaza, comunicada entre la pared de seguridad y los servicios en la nube proporcionados por la lógica 110 de detección de software malicioso en la nube que reside en el servidor 108 en la nube cuando se requiere una experiencia detallada y un enrutado de mensajes/transmisión a través de la lógica 110 de detección de software malicioso en la nube que reside en el servidor 108 en la nube para una detección de amenaza o una trasferencia de datos altamente sensibles.

La lógica 104 de detección de software malicioso ejecutada por un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que reside en la red 100 puede configurarse para recibir un mensaje de un dispositivo no asegurado (por ejemplo, el rúter 112) de la primera red (por ejemplo, la red 106 externa no fiable) destinada a un dispositivo de destino (por ejemplo, 118a o 102) de la red doméstica (por ejemplo, la red 114 doméstica asegurada). El dispositivo de destino (por ejemplo 118a o 102) puede comprender un cliente de seguridad (por ejemplo, 120a). La lógica 104 de detección de software malicioso puede configurarse para establecer un canal de comunicación segura entre la lógica 104 de detección de software malicioso y el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) y el cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a o 102). La lógica 104 de detección de software malicioso puede configurarse para ejecutar una comprobación de validación en el mensaje para determinar que el mensaje incluye un software malicioso. La lógica de detección de software malicioso puede configurarse para reportar una alarma al cliente de seguridad (por ejemplo 120a) del dispositivo de destino (por ejemplo, 118a o 102). La lógica 104 de detección de software malicioso puede configurarse para trasmitir una información relacionada con el software malicioso a la lógica 110 de detección del software malicioso en la nube de servidor 108 de computación en la nube. La lógica 104 de detección de software malicioso puede configurarse para evitar que una aplicación asociada con el dispositivo de destino (por ejemplo, 118a o 102) procese el mensaje.

El dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede trasmitir el mensaje sobre la red 114 doméstica asegurada al dispositivo de destino (por ejemplo, 118a). Antes de transmitir el mensaje, la lógica 104 de detección de software malicioso puede encriptar el mensaje.

En otro ejemplo, la aplicación puede residir en el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada).

La lógica 104 de detección de software malicioso puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos. La lógica 104 de detección de software malicioso puede trasmitir una indicación de la presencia del software malicioso a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La lógica 104 de detección de software malicioso puede trasmitir una alarma indicativa de la presencia del software malicioso al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a).

La lógica 104 de detección de software malicioso puede funcionar para proporcionar uno o más de, un proceso de inicio seguro, un proceso de descarga seguro o un proceso de generación para generar una o más claves para la encriptación del mensaje.

El dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede configurarse para recibir un mensaje de un dispositivo no asegurado (por ejemplo, el rúter 112) de una primera red (por ejemplo, la red 106 externa no asegurada) destinada a un dispositivo de destino (por ejemplo, 118a o 102) de la red doméstica (por ejemplo, la red

114 doméstica asegurada), en donde la determinación de la presencia de software malicioso se realiza por la lógica 110 de detección de software malicioso en la nube del servidor 108 de ordenador en la nube. La lógica 104 de detección de software malicioso ejecutada por el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que reside en la red 100 puede recibir el mensaje destinado al dispositivo de destino (por ejemplo, 118a o 102) de la red 100. Si la lógica 104 de detección de software malicioso decide no determinar si el mensaje incluye un software malicioso, entonces la lógica 104 de detección de software malicioso puede configurarse para trasmitir el mensaje a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La lógica 104 de detección de software malicioso puede determinar que el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) tiene una potencia de procesamiento insuficiente o necesita más experiencia para determinar si el mensaje incluye un software malicioso. En un ejemplo, la lógica 104 de detección de software malicioso puede recibir una indicación (por ejemplo, de uno del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada, el servidor 108 de computación en la nube, el dispositivo 124 de red o uno de los clientes 120a-120n) de seguridad) de que ha aumentado una alerta del nivel de la red 114 doméstica asegurada. La determinación de si el mensaje incluye un software malicioso puede basarse en la sensibilidad de seguridad de uno de, el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada), el servidor 108 de computación en la nube, el dispositivo 124 de red o uno de los clientes 120a-120n de seguridad.

La lógica 104 de detección de software malicioso puede configurarse para recibir desde la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de que el mensaje contiene un software malicioso. La lógica 104 de detección de software malicioso puede configurarse para reportar una alarma al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a). La lógica 104 de detección de software malicioso puede configurarse para evitar que una aplicación (no mostrada) asociada con el dispositivo de destino (por ejemplo, 118a) procese el mensaje. La lógica 104 de detección de software malicioso puede configurarse para recibir desde la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de que el mensaje no contiene un software malicioso. Por consiguiente, la lógica 104 de detección de software malicioso puede configurarse para permitir que la aplicación asociada con el dispositivo de destino (por ejemplo, 118a) procese el mensaje.

El dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede trasmitir el mensaje sobre la red 114 doméstica asegurada al dispositivo de destino (por ejemplo, 118a). Antes de transmitir el mensaje, la lógica 104 de detección de software malicioso puede encriptar el mensaje. La aplicación puede residir en el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada).

La lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada y/o la lógica 110 de detección de software malicioso de la nube del servidor 108 de computación en la nube) puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos.

La lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede trasmitir una indicación de la presencia de software malicioso a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube. En un ejemplo, la lógica 104 de detección de software malicioso puede trasmitir una alarma indicativa de la presencia del software malicioso al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a).

La lógica 104 de detección de software malicioso puede funcionar para proporcionar uno o más de, un proceso de inicio seguro, un proceso de descarga seguro o un proceso de generación para generar una o más claves para la encriptación del mensaje.

La lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede configurarse para enrutar todos los mensajes entrantes recibidos del rúter 112 y que se originan en la red 106 externa no fiable a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube. En un ejemplo, la lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que enruta todos los mensajes entrantes puede ser el resultado de la sensibilidad del cliente de seguridad (por ejemplo, 120a) o debido a que aumentado el nivel de alerta de la red. Tal y como se utiliza en el presente documento, la sensibilidad se puede determinar por el tipo de dispositivo y/o por la consecuencia de un ataque exitoso. Por ejemplo, una cerradura de puerta tiene una sensibilidad más alta que una cámara web, debido a que un ataque exitoso en la cerradura de puerta puede resultar en la abertura de la puerta a intrusos. Un regulador de calefacción en Canadá puede tener una sensibilidad más alta en invierno que en verano. Si la calefacción se detiene en invierno, las tuberías de agua pueden congelarse y llegar a dañarse. El mismo regulador en Florida puede ser menos sensible. El nivel de alerta se puede aumentar mediante servicios de seguridad ubicados en el servidor 108 de computación en la nube como resultado de actividades de monitorización de la lógica 110 de detección de software malicioso en la nube.

Un primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que tiene una lógica 104 de detección de software malicioso puede configurar una sesión de comunicación segura con un segundo dispositivo

asegurado (por ejemplo, el dispositivo 118b) que tiene un cliente de seguridad (por ejemplo, 120b). La lógica 104 de detección de software malicioso ejecutada por el primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que reside en la red 100 puede recibir el mensaje destinado al segundo dispositivo asegurado (por ejemplo, 118b) de la red 100 desde un dispositivo no asegurado (por ejemplo, el servidor 111) de una red no fiable (por ejemplo, la red 106 externa). La lógica 104 de detección de software malicioso puede configurarse para establecer un canal de comunicación segura con el segundo dispositivo asegurado (por ejemplo, 118b) a la vista de un nivel de seguridad asociado con la lógica 104 de detección de software malicioso o un nivel de amenaza asociado con el mensaje. La lógica 104 de detección de software malicioso puede emplear al menos uno de, un mecanismo de creación de clave de sesión, creación de uno o más certificados, una clave de sesión generada en la nube o una o más claves de dominio doméstico.

La lógica 104 de detección de software malicioso puede configurarse para recibir una indicación de que el nivel de seguridad asociado con la lógica 104 de detección de software malicioso o el nivel de amenaza asociado con el mensaje ha cambiado. El cambio de nivel de seguridad puede ser el resultado de una o más alarmas activadas por la detección de la presencia de software malicioso en el mensaje o un cambio de la red 114 doméstica asegurada que requiere una nueva autentificación. La lógica 104 de detección de software malicioso puede configurarse para interrumpir una sesión asociada con el canal de comunicación segura a la vista de la indicación. La lógica 104 de detección de software malicioso puede configurarse para evitar que una aplicación (no mostrada) de un dispositivo asegurado (por ejemplo, el dispositivo 118b) procese el mensaje.

Si la lógica 104 de detección de software malicioso determina que la sesión asociada con el canal de comunicación segura va a continuar a la vista de la indicación, entonces la lógica 104 de detección de software malicioso puede permitir que la aplicación del segundo dispositivo asegurado (por ejemplo, el dispositivo 118b) procese el mensaje. La puerta 102 de enlace asegurada puede transmitir el mensaje sobre la red 114 doméstica asegurada al segundo dispositivo asegurado (por ejemplo, el dispositivo 118b). En un ejemplo, antes de que el primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) transmita el mensaje, la lógica 104 de detección de software malicioso puede encriptar el mensaje.

La lógica 104 de detección de software malicioso puede configurarse para reportar la creación de la sesión a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube. La lógica 104 de detección de software malicioso puede configurarse para proporcionar una aprobación para el comienzo de sesión. En un ejemplo, proporcionar la aprobación puede basarse en un nivel de seguridad de la red 114 doméstica asegurada o una sensibilidad de seguridad del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) o el segundo dispositivo asegurado (por ejemplo, el dispositivo 118b).

Durante la sesión, la lógica 104 de detección de software malicioso de la puerta 102 de enlace asegurada puede ser informada sobre el nivel de seguridad de sus correspondientes (por ejemplo, 118a-118n) y puede decidir si la sesión puede continuar o si la sesión va a ser interrumpida basándose en el nivel de seguridad. Por ejemplo, el nivel de seguridad puede ser una consecuencia de alarmas activadas durante la ejecución de la configuración en los ejemplos anteriores. En otro ejemplo, el nivel de seguridad puede cambiar si hay un cambio en el entorno que requiere una nueva autentificación. El cambio en el entorno puede ser activado por mensajes obtenidos por la lógica 110 de detección de software malicioso en la nube.

La figura 2 es un diagrama de bloques de los elementos de la figura 1 adaptados para añadir un dispositivo 132 no asegurado a la red 114 doméstica asegurada, en donde los mensajes son enrutados a través de un dispositivo asegurado existente (por ejemplo, el dispositivo 122 de red) que tiene una lógica 126 de detección de software malicioso en la red 114 doméstica asegurada. En un ejemplo, la lógica 126 de detección de software malicioso del dispositivo asegurado existente (por ejemplo, el dispositivo 124 de red) en la red 114 doméstica asegurada puede configurarse para recibir un identificador asociado con un dispositivo no asegurado (por ejemplo, 132) de la red 114 doméstica asegurada. La lógica 126 de detección de software malicioso puede configurarse para informar a uno o más de los otros dispositivos asegurados (por ejemplo, 118a-118n, 102) en la red 114 doméstica asegurada para volver a enrutar mensajes a través de la lógica 126 de detección de software malicioso del dispositivo existente (por ejemplo, el dispositivo 122 de red) en la red 114 doméstica asegurada a la vista del identificador. La lógica 126 de detección de software malicioso puede recibir un mensaje destinado al dispositivo no asegurado (por ejemplo, 132) de uno o más de los otros dispositivos asegurados (por ejemplo, 118a) en la red 114 doméstica asegurada. La lógica 126 de detección de software malicioso puede configurarse para ejecutar una comprobación de validación en el mensaje para determinar si el mensaje incluye un software malicioso. La lógica 126 de detección de software malicioso puede transmitir el mensaje a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube y recibir de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de si el mensaje incluye un software malicioso. La lógica 126 de detección de software malicioso puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos. La lógica 126 de detección de software malicioso puede transmitir una indicación de la presencia del software malicioso a un servidor 108 de computación en la nube.

Si la lógica 126 de detección de software malicioso determina que el mensaje no incluye un software malicioso, entonces la lógica 126 de detección de software malicioso puede transmitir el mensaje sobre la red 114 doméstica

asegurada al dispositivo no asegurado (por ejemplo, 132). Si la lógica 126 de detección de software malicioso determina que el mensaje no incluye un software malicioso, entonces la lógica 126 de detección de software malicioso no transmite el mensaje sobre la red 114 doméstica asegurada al dispositivo no asegurado (por ejemplo, 132).

La lógica 126 de detección de software malicioso puede reportar la presencia del dispositivo no asegurado (por ejemplo, 132) a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

Antes de que la lógica 126 de detección de software malicioso transmita el mensaje al dispositivo no asegurado (por ejemplo, 132), la lógica 126 de detección de software malicioso puede configurarse para encriptar el mensaje.

La lógica 126 de detección de software malicioso puede enrutar todas las comunicaciones a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube, para grabación, inspección, registro, etc.

La figura 3 es un diagrama de bloques de los elementos de la figura 1 adaptados para añadir un dispositivo 134 asegurado a la red 114 doméstica asegurada, en donde los mensajes son enrutados a través de un dispositivo asegurado (por ejemplo, 136) que tiene una lógica de detección de software malicioso (por ejemplo, 138) en la red 114 doméstica asegurada. Un dispositivo no asegurado (por ejemplo, 132), por ejemplo, una cámara de vigilancia de niños) se puede insertar en la red 114 doméstica asegurada. El dispositivo asegurado (por ejemplo, 136) que tiene una lógica de detección de software malicioso (por ejemplo, 138) se añade a la red 114 doméstica asegurada. La lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede configurarse para recibir un identificador asociado con el dispositivo 134 no asegurado insertado en la red 114 doméstica asegurada. La lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede configurarse para informar a uno o más de los otros dispositivos asegurados (por ejemplo, 118a-118n) en la red 114 doméstica asegurada para volver a enrutar mensajes a través de la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) a la vista del identificador. La lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede configurarse para recibir un mensaje destinado al dispositivo 134 no asegurado desde uno o más de los otros dispositivos asegurados (por ejemplo, 118a) en la red 114 doméstica asegurada. La lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede configurarse para ejecutar una comprobación de validación en el mensaje para determinar si el mensaje incluye un software malicioso.

Si la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) determina que el mensaje no incluye un software malicioso, entonces la lógica 138 de detección de software malicioso del dispositivo 136 asegurado transmite el mensaje sobre la red 114 doméstica asegurada al dispositivo 134 no asegurado. Si la lógica 138 de detección de software malicioso del dispositivo 136 asegurado determina que el mensaje no incluye un software malicioso, entonces la lógica 138 de detección de software malicioso del nuevo dispositivo 136 asegurado no transmite el mensaje sobre la red 114 doméstica asegurada al dispositivo 134 no asegurado. La lógica 138 de detección de software malicioso puede configurarse para reportar la presencia del nuevo dispositivo 136 de red a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La lógica 138 de detección de software malicioso puede transmitir el mensaje a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube y recibir de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de si el mensaje incluye un software malicioso.

Antes de que la lógica 138 de detección de software malicioso del dispositivo 134 asegurado transmita el mensaje, la lógica 138 de detección de software malicioso del nuevo dispositivo 136 asegurado puede configurarse para encriptar el mensaje.

La lógica 138 de detección de software malicioso del dispositivo 136 asegurado puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos.

La lógica 138 de detección de software malicioso puede transmitir una indicación de la presencia del software malicioso a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

Con referencia a la figura 1, una configuración de un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede cambiar en la red 114 doméstica asegurada. La lógica de detección de software malicioso (por ejemplo, 104) ejecutada por el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) en la red 114 doméstica asegurada puede configurarse para recibir una indicación de que una primera firma asociada con el dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada) ha cambiado a la vista de un cambio en la configuración del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada). La lógica de detección de software malicioso (por ejemplo, 104) ejecutada por un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede configurarse para calcular una segunda firma asociada con el dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada) a la vista de la indicación. La lógica de detección de software malicioso (por

ejemplo, 104) puede configurarse para transmitir la segunda firma a la lógica 110 de detección de software malicioso del servidor 108 de computación en la nube. La lógica de detección de software malicioso (por ejemplo, 104) puede configurarse para recibir de la lógica 110 de detección de software malicioso del servidor 108 de computación en la nube una actualización de un estado de seguridad del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) a la vista de la segunda firma.

La primera firma puede determinarse basándose en una configuración del dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada), una o más características del dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada) o uno o más comportamientos del dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada). La lógica 110 de detección de software malicioso del servidor 108 de computación en la nube recibe y prohíbe comunicaciones adicionales con el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada).

La lógica 110 de detección de software malicioso del servidor 108 de computación en la nube puede informar a otros dispositivos asegurados (por ejemplo, 118a-118n) en la red 114 doméstica asegurada sobre el cambio en el estado de seguridad del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada). Como resultado, los otros dispositivos asegurados (por ejemplo, 118a-118n) en la red 114 doméstica asegurada pueden tomar una o más acciones individuales. Un ejemplo de cuáles acciones pueden tomar los otros dispositivos asegurados (por ejemplo, 118a-118n) puede incluir, pero no está limitado a, decidir detener la comunicación con el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada), reinicializar la comunicación con el dispositivo asegurado, (por ejemplo, la puerta 102 de enlace asegurada), reiniciarse a sí mismos y/o volver a una configuración conocida o a parámetros conocidos, etc. La acción individual puede llevar a la lógica 110 de detección de software malicioso del servidor 108 de computación en la nube a prohibir cualquier comunicación adicional (por ejemplo, por otros dispositivos asegurados (118a-118n)) con el dispositivo asegurado que fue modificado (por ejemplo, la puerta 102 de enlace asegurada).

La figura 4 es un diagrama que ilustra un método 400 de ejemplo para permitir a un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) de la figura 1 recibir un mensaje de un dispositivo no asegurado (por ejemplo, el servidor 111) de una primera red (por ejemplo, la red 106 externa no fiable) y destinada a un dispositivo de destino (por ejemplo, 118a o 102) de la red doméstica (por ejemplo, la red 114 doméstica asegurada), en donde la determinación de la presencia de software malicioso se realiza por la lógica 104 de detección de software malicioso ejecutada por un dispositivo de procesamiento de un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada). El método 400 se puede realizar por la lógica de detección de software malicioso (por ejemplo, 104) del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) de la figura 1 y puede comprender hardware (por ejemplo, una circuitería, una lógica dedicada, una lógica programable, un microcódigo, etc.), software (por ejemplo, instrucciones ejecutadas en un dispositivo de procesamiento) o una combinación de los mismos.

Tal y como se muestra en la figura 4, en el bloque 405, la lógica 104 de detección de software malicioso ejecutada por el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que reside en la red 100, puede recibir el mensaje destinado al dispositivo de destino (por ejemplo, 118a o 102) de la red 100. El dispositivo de destino (por ejemplo, 118a o 102) puede comprender un cliente de seguridad (por ejemplo, 120a). En el bloque 410, la lógica 104 de detección de software malicioso puede establecer un canal de comunicación segura entre la lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) y el cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a). En el bloque 415, la lógica 104 de detección de software malicioso puede ejecutar una comprobación de validación del mensaje para determinar si el mensaje incluye un software malicioso. Si, en el bloque 420, la lógica 104 de detección de software malicioso determina que el mensaje incluye un software malicioso, entonces en el bloque 425, la lógica 104 de detección de software malicioso puede reportar una alarma al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a). La lógica 104 de detección de software malicioso puede trasmitir información relacionada con el software malicioso a un servidor 108 de computación en la nube. En el bloque 430, la lógica 104 de detección de software malicioso puede evitar que una aplicación (no mostrada) asociada con el dispositivo de destino (por ejemplo, 118a) procese (por ejemplo, reciba, lea, extraiga información de y/o ejecute porciones de, etc.) El mensaje. Si, en el bloque 420, la lógica 104 de detección de software malicioso determina que el mensaje no incluye un software malicioso, entonces en el bloque 435, la lógica 104 de detección de software malicioso puede permitir que la aplicación asociada con el dispositivo de destino (por ejemplo, 118a) procese el mensaje.

Permitir a la aplicación procesar el mensaje puede comprender transmitir, mediante el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada), el mensaje sobre la red 114 doméstica asegurada al dispositivo de destino (por ejemplo, 118a). Antes de transmitir el mensaje, la lógica 104 de detección de software malicioso puede encriptar el mensaje. La aplicación puede residir en el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada).

La lógica 104 de detección de software malicioso puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos. En otro ejemplo, la lógica 104 de detección de software malicioso puede trasmitir una indicación de la presencia del software malicioso a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La lógica 104 de detección de software malicioso puede trasmitir una alarma indicativa de la presencia del software malicioso al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a).

La lógica 104 de detección de software malicioso puede proporcionar uno o más de, un proceso de inicio seguro, un proceso de descarga seguro o un proceso de generación para generar una o más claves para la encriptación del mensaje.

La figura 5 es un diagrama que ilustra un método 500 de ejemplo para permitir al dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada de la figura 1) gestionar una comunicación entre un dispositivo no asegurado (por ejemplo, 122) de una primera red (por ejemplo, la red 106 externa) y un dispositivo de destino (por ejemplo, 118a) de una red doméstica (por ejemplo, la red 114 doméstica asegurada). El método 500 puede realizarse mediante la lógica de detección de software malicioso (por ejemplo, 104) del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) de la figura 1 y puede comprender hardware (por ejemplo, una circuitería, una lógica dedicada, una lógica programable, un microcódigo, etc.), software (por ejemplo, instrucciones ejecutadas en un dispositivo de procesamiento) o una combinación de los mismos.

Tal y como se muestra en la figura 5, en el bloque 505, una lógica 104 de detección de software malicioso ejecutada por un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que reside en una red doméstica (por ejemplo, la red 114 doméstica asegurada) recibe un mensaje destinado al dispositivo de destino (por ejemplo, 118a o 102) de la red doméstica (por ejemplo, la red 114 doméstica asegurada). En el bloque 510, la lógica 104 de detección de software malicioso decide no determinar si el mensaje incluye software malicioso. En el bloque 915, la lógica 104 de detección de software malicioso puede trasmitir el mensaje a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La lógica 104 de detección de software malicioso puede determinar que el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada tiene una potencia de procesamiento insuficiente o necesita más experiencia para determinar si el mensaje incluye un software malicioso. La lógica 104 de detección de software malicioso puede recibir una indicación (por ejemplo, de uno de, el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada), el servidor 108 de computación en la nube, el dispositivo 124 de red o uno de los clientes 120a-120n de seguridad) de que ha aumentado un nivel de alerta de la red 114 doméstica asegurada. La determinación de si el mensaje incluye software malicioso puede basarse en la sensibilidad de seguridad de uno de, el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada), el servidor 108 de computación en la nube, el dispositivo 124 de red o uno de los clientes 120a-120n de seguridad.

Si, en el bloque 520, la lógica 104 de detección de software malicioso recibe de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de que el mensaje contiene un software malicioso, entonces en el bloque 525, la lógica 104 de detección de software malicioso puede reportar una alarma al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a). En el bloque 530, la lógica 104 de detección de software malicioso puede evitar que una aplicación (no mostrada) asociada con el dispositivo de destino (por ejemplo, 118a) procese el mensaje. Si, en el bloque 520, la lógica 104 de detección de software malicioso recibe de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de que el mensaje no contiene un software malicioso, entonces en el bloque 535, la lógica 104 de detección de software malicioso puede permitir que la aplicación asociada con el dispositivo de destino (por ejemplo, 118a) procese el mensaje.

Un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede trasmitir el mensaje sobre la red 114 doméstica asegurada al dispositivo de destino (por ejemplo, 118a). En un ejemplo, antes de transmitir, el mensaje, la lógica 104 de detección de software malicioso puede encriptar el mensaje. La aplicación puede recibir en el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada).

La lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) y/o la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos.

La lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede trasmitir una indicación de la presencia del software malicioso a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube. En un ejemplo, la lógica 104 de detección de software malicioso puede trasmitir una alarma indicativa de la presencia del software malicioso al cliente de seguridad (por ejemplo, 120a) del dispositivo de destino (por ejemplo, 118a).

La lógica 104 de detección de software malicioso puede funcionar para proporcionar uno o más de, un proceso de inicio seguro, un proceso de descarga seguro o un proceso de generación para generar una o más claves para la encriptación del mensaje.

La lógica 104 de detección de software malicioso del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede configurarse para enrutar todos los mensajes entrantes recibidos desde el rúter 112 y que se

originan en la red 106 externa no asegurada de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube. En un ejemplo, enrutar todos los mensajes entrantes puede ser el resultado de la sensibilidad del cliente de seguridad (por ejemplo, 120a) o debido a que ha aumentado el nivel de alerta en la red. El nivel de alerta puede aumentarse por los servicios de seguridad ubicados en el servidor 108 de computación en la nube como resultado de actividades de monitorización de la lógica 110 de detección de software malicioso en la nube.

La figura 6 es un diagrama que ilustra un método 600 de ejemplo para configurar una sesión de comunicación segura entre dos dispositivos asegurados en la red de la figura 1, un primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que tiene una lógica 104 de detección de software malicioso y un segundo dispositivo asegurado (por ejemplo, el dispositivo 118b) que tiene un cliente de seguridad (por ejemplo, 120b). El método 600 puede realizarse mediante una lógica de detección de software malicioso (por ejemplo, 104) del primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) de la figura 1 y puede comprender hardware (por ejemplo, una circuitería, una lógica dedicada, una lógica programable, un microcódigo, etc.), software (por ejemplo, instrucciones ejecutadas en un dispositivo de procesamiento) o una combinación de los mismos.

Tal y como se muestra en la figura 6, para configurar una sesión de comunicación segura entre los dispositivos asegurados en la red de la figura 1, en el bloque 605, la lógica 104 de detección de software malicioso ejecutada por el primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) que reside en la red 100, puede recibir el mensaje destinado al segundo dispositivo asegurado (por ejemplo, 118b) de la red 100 desde un dispositivo no asegurado (por ejemplo, 122) de una red no fiable (por ejemplo, la red 106 externa). En el bloque 610, la lógica 104 de detección de software malicioso puede establecer un canal de comunicación segura con el dispositivo no asegurado (por ejemplo, el servidor 111) a la vista de un nivel de seguridad asociado con la lógica 104 de detección de software malicioso o un nivel de amenaza asociado con el mensaje. La lógica 104 de detección de software malicioso puede emplear al menos uno de, un mecanismo de creación de clave de sesión, crear uno o más certificados, una clave de sesión generada en la nube o una o más claves de dominio doméstico.

En el bloque 615, la lógica 104 de detección de software malicioso puede recibir una indicación de que ha cambiado el nivel de seguridad asociado con la lógica 104 de detección de software malicioso o el nivel de amenaza asociado con el mensaje. El cambio de nivel de seguridad puede ser el resultado de una o más alarmas activadas por la detección de la presencia de software malicioso en el mensaje o un cambio en la red 114 doméstica asegurada que requiere una nueva autentificación. En el bloque 620, la lógica 104 de detección de software malicioso puede interrumpir una sesión asociada con el canal de comunicación segura a la vista de la indicación. En el bloque 625, la lógica 104 de detección de software malicioso puede evitar que una aplicación (no mostrada) del segundo dispositivo asegurado (por ejemplo, 118b) procese el mensaje.

Si la lógica 104 de detección de software malicioso determina que la sesión asociada con el canal de comunicación seguro va a continuar a la vista de la indicación, entonces la lógica 104 de detección de software malicioso puede permitir que la aplicación del segundo dispositivo asegurado (por ejemplo, 118b) procese el mensaje. El primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede trasmitir el mensaje sobre la red 114 doméstica asegurada al segundo dispositivo asegurado (por ejemplo, 118b). En un ejemplo, antes de que el primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) transmita el mensaje, la lógica 104 de detección de software malicioso puede encriptar el mensaje.

La lógica 104 de detección de software malicioso puede reportar la creación de la sesión a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube. La lógica 104 de detección de software malicioso puede dar una aprobación al inicio de sesión. El hecho de dar la aprobación puede basarse en un nivel de seguridad de la red 114 doméstica asegurada o una sensibilidad de seguridad de la puerta 102 de enlace asegurada o el segundo dispositivo 118b asegurado.

Durante la sesión, la lógica 104 de detección de software malicioso del primer dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) puede informarse sobre el nivel de seguridad a sus correspondientes (por ejemplo, 118a-118n) y puede decidir si la sesión puede continuar y/o si la sesión se va a interrumpir basándose en el nivel de seguridad. Por ejemplo, el nivel de seguridad puede ser una consecuencia de alarmas activadas durante la ejecución de la configuración de las figuras 2 o 3. En otro ejemplo, el nivel de seguridad puede cambiar si hay un cambio en el entorno que puede requerir una nueva autentificación.

La figura 7 es un diagrama que ilustra un método 700 de ejemplo para añadir un dispositivo no asegurado (por ejemplo, 122) a una red doméstica (por ejemplo, la red 114 doméstica asegurada) de la figura 2, en donde los mensajes son enrutados a través de un dispositivo asegurado (por ejemplo, el dispositivo 124 de red) que tiene una lógica de detección de software malicioso (por ejemplo, 116) en la red doméstica (por ejemplo, la red 114 doméstica asegurada). El método 600 puede realizarse mediante una lógica de detección de software malicioso (por ejemplo, 116) del dispositivo asegurado (por ejemplo, el dispositivo 124 de red) de la figura 2 y puede comprender hardware (por ejemplo, una circuitería, una lógica dedicada, una lógica programable, un microcódigo, etc.), software (por ejemplo, instrucciones ejecutadas en un dispositivo de procesamiento) o una combinación de los mismos.

Tal y como se muestra en la figura 7, en el bloque 705, la lógica 126 de detección de software malicioso del dispositivo asegurado (por ejemplo, el dispositivo 124 de red) en la red 114 doméstica asegurada puede recibir un identificador

asociado con un dispositivo no asegurado (por ejemplo, 128) insertado en la red 114 doméstica asegurada. En el bloque 710, la lógica 126 de detección de software malicioso puede informar a uno o más de los otros dispositivos asegurados (por ejemplo, 118a-118n, 102) en la red 114 doméstica asegurada para enrutar mensajes a través de la lógica 126 de detección de software malicioso del dispositivo asegurado (por ejemplo, el dispositivo 124 de red) en la red 114 doméstica asegurada a la vista del identificador. En el bloque 715, la lógica 126 de detección de software malicioso puede recibir un mensaje destinado al dispositivo no asegurado (por ejemplo, 128) desde uno o más de los otros dispositivos asegurados (por ejemplo, 118a) en la red 114 doméstica asegurada. En el bloque 720, la lógica 126 de detección de software malicioso puede ejecutar una comprobación de validación en el mensaje para determinar si el mensaje incluye un software malicioso. La lógica 126 de detección de software malicioso puede transmitir el mensaje a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube y recibir de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de si el mensaje incluye un software malicioso. La lógica 126 de detección de software malicioso puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos. La lógica 126 de detección de software malicioso puede trasmitir una indicación de la presencia del software malicioso a un servidor 108 de computación en la nube.

Si, en el bloque 725, la lógica 126 de detección de software malicioso determina que el mensaje no incluye software malicioso, entonces en el bloque 730, la lógica 126 de detección de software malicioso puede trasmitir el mensaje sobre la red 114 doméstica asegurada al dispositivo no asegurado (por ejemplo, 128). Si, en el bloque 725, la lógica 126 de detección de software malicioso determina que el mensaje no incluye un software malicioso, entonces en el bloque 735, la lógica 126 de detección de software malicioso no transmite el mensaje sobre la red 114 doméstica asegurada al dispositivo no asegurado (por ejemplo, 128).

La lógica 126 de detección de software malicioso puede reportar la presencia del dispositivo no asegurado (por ejemplo, 128) a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

Antes de que la lógica 126 de detección de software malicioso transmita el mensaje al dispositivo no asegurado (por ejemplo, 128), la lógica 126 de detección de software malicioso puede configurarse para encriptar el mensaje.

La lógica 126 de detección de software malicioso puede enrutar todas las comunicaciones de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube, para grabación, inspección, registro, etc.

La figura 8 es un diagrama que ilustra un método 800 de ejemplo para añadir un dispositivo no asegurado (por ejemplo, 132) a una red doméstica (por ejemplo, la red 114 doméstica asegurada), en donde los mensajes son enrutados a través de un nuevo dispositivo asegurado (por ejemplo, 136) que tiene una lógica de detección de software malicioso (por ejemplo, 132) en la red doméstica (por ejemplo, la red 114 doméstica asegurada). El método 800 se puede realizar mediante el dispositivo asegurado (por ejemplo, 136) que tiene una lógica de detección de software malicioso (por ejemplo, 134) de la figura 3 y puede comprender hardware (por ejemplo, una circuitería, una lógica dedicada, una lógica programable, un microcódigo, etc.), software (por ejemplo, instrucciones ejecutadas en un dispositivo de procesamiento) o una combinación de los mismos.

Tal y como se muestra en la figura 8, en el bloque 805, un dispositivo no asegurado (por ejemplo, 132, por ejemplo, una cámara de vigilancia de niños) se inserta en la red 114 doméstica asegurada. En el bloque 810, el dispositivo asegurado (por ejemplo, 136) que tiene una lógica de detección de software malicioso (por ejemplo, 138) se añade a la red 114 doméstica asegurada. En el bloque 815, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede recibir un identificador asociado con el dispositivo 132 no asegurado insertado en la red 114 doméstica asegurada. En el bloque 820, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) pueden informar a uno o más de los otros dispositivos asegurados (por ejemplo, 118a-118n) en la red 114 doméstica asegurada para volver a enrutar mensajes a través de la lógica de detección de software malicioso (por ejemplo, 138) del nuevo dispositivo asegurado (por ejemplo, 136) a la vista del identificador. En el bloque 825, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede recibir un mensaje destinado al dispositivo 132 no asegurado de uno de los uno o más otros dispositivos asegurados (por ejemplo, 118a) en la red 114 doméstica asegurada. En el bloque 830, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede ejecutar una comprobación de validación en el mensaje para determinar si el mensaje incluye un software malicioso.

Si, en el bloque 835, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) determina que el mensaje no incluye un software malicioso, entonces en el bloque 840, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede trasmitir el mensaje sobre la red 114 doméstica asegurada al dispositivo no asegurado 132. Si, en el bloque 835, la lógica de detección de software malicioso (por ejemplo, 138) del nuevo dispositivo asegurado (por ejemplo, 136) determina que el mensaje no incluye un software malicioso, entonces en el bloque 845, la lógica de detección de software malicioso (por ejemplo, 138) del nuevo dispositivo asegurado (por ejemplo, 136) no transmite el mensaje sobre la red 114

doméstica asegurada al dispositivo 132 no asegurado. La lógica de detección de software malicioso (por ejemplo, 138) puede configurarse para reportar la presencia del nuevo dispositivo asegurado (por ejemplo, 136) a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La lógica de detección de software malicioso (por ejemplo, 138) puede transmitir el mensaje a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube y recibir de la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube una indicación de si el mensaje incluye un software malicioso.

Antes de que la lógica de detección de software malicioso (por ejemplo, 138) del nuevo dispositivo asegurado (por ejemplo, 136) transmita el mensaje, la lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede configurarse para encriptar el mensaje.

La lógica de detección de software malicioso (por ejemplo, 138) del dispositivo asegurado (por ejemplo, 136) puede realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus o una inspección de paquetes profunda para la detección de ataques conocidos.

La lógica de detección de software malicioso (por ejemplo, 138) puede transmitir una indicación de la presencia del software malicioso a la lógica 110 de detección de software malicioso en la nube del servidor 108 de computación en la nube.

La figura 9 es un diagrama que ilustra un método 900 de ejemplo de una red doméstica (la red 114 doméstica asegurada) que responde a un cambio en la configuración de un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) en la red doméstica (por ejemplo, la red 114 doméstica asegurada). El método 900 puede realizarse mediante una lógica de detección de software malicioso (por ejemplo, 104) ejecutada por un dispositivo de procesamiento (por ejemplo, de la puerta 102 de enlace asegurada) de la figura 1 y puede comprender hardware (por ejemplo, una circuitería, una lógica dedicada, una lógica programable, un microcódigo, etc.), software (por ejemplo, instrucciones ejecutadas en un dispositivo de procesamiento) o una combinación de los mismos.

Tal y como se muestra en la figura 9, en el bloque 905, la lógica de detección de software malicioso (por ejemplo, 104) ejecutada mediante un dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) en la red 114 doméstica asegurada puede recibir una indicación de que ha cambiado una primera señal asociada con el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) a la vista de una modificación de una configuración del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada). En el bloque 910, la lógica de detección de software malicioso (por ejemplo, 104) ejecutada por un dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada) puede calcular una segunda firma asociada con el dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada) a la vista de la indicación. En el bloque 915, la lógica de detección de software malicioso (por ejemplo, 104) puede transmitir la segunda firma a la lógica 110 de detección de software malicioso del servidor 108 de computación en la nube. En el bloque 920, la lógica de detección de software malicioso (por ejemplo, 104) puede recibir de la lógica 110 de detección de software malicioso del servidor 108 de computación en la nube una actualización de un estado de seguridad del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) a la vista de la segunda firma.

La primera firma puede determinarse basándose en una configuración del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) una o más características del dispositivo asegurado (por ejemplo, de la puerta 102 de enlace asegurada) o uno o más comportamientos del segundo dispositivo (por ejemplo, de la puerta 102 de enlace asegurada).

La lógica 110 de detección de software malicioso del servidor 108 de computación en la nube puede que no permita comunicaciones adicionales con el dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada) a la vista del estado de seguridad actualizado.

La lógica 110 de detección de software malicioso del servidor 108 de computación en la nube puede informar a otros dispositivos asegurados (por ejemplo, 118a-118n) en la red 114 doméstica asegurada sobre el cambio en el estado de seguridad del dispositivo asegurado (por ejemplo, la puerta 102 de enlace asegurada). Como resultado, los otros dispositivos asegurados (por ejemplo, 118a-118n) en la red 114 doméstica asegurada pueden tomar acciones individuales. La acción individual puede llevar a que la lógica 110 de detección de software malicioso del servidor 108 de computación en la nube no permita ninguna comunicación adicional (por ejemplo, por los otros dispositivos asegurados (118a-118n) con el dispositivo asegurado que fue modificado (por ejemplo, la puerta 102 de enlace asegurada).

La figura 10 ilustra una representación esquemática de una máquina en forma de ejemplo de un sistema 1000 informático dentro del cual se pueden ejecutar un conjunto de instrucciones para provocar que la máquina realice cualquiera o más de las metodologías expuestas en el presente documento. En algunos ejemplos, la máquina se puede conectar (por ejemplo, conectar en red) a otras máquinas en una LAN, una intranet, una extranet o Internet. La máquina puede funcionar con la capacidad de una máquina de servidor en un entorno de red cliente-servidor. La máquina puede ser un ordenador personal (PC), un decodificador (STB), un servidor, un rúter de red, un conmutador

o puente o cualquier máquina capaz de ejecutar un conjunto de instrucciones (secuenciales o de otro modo) que especifican acciones que se van a tomar por esa máquina. Además, aunque sólo se ilustra una única máquina, el término “máquina” se considerará también que incluye cualquier colección de máquinas que ejecuten de forma individual o conjunta un conjunto (o múltiples conjuntos) de instrucciones para realizar cualquiera o más de las metodologías expuestas en el presente documento.

El sistema 1000 informático de ejemplo incluye un dispositivo 1002 de procesamiento (procesador), una memoria 1004 principal (por ejemplo, una memoria de sólo lectura (ROM), una memoria flash, una memoria de acceso aleatorio dinámico (DRAM) tal como una DRAM síncrona (SDRAM)), una memoria 1006 estática (por ejemplo, una memoria flash, una memoria de acceso aleatorio estático (SRAM)) y un dispositivo 1016 de almacenamiento de datos, que se comunican entre sí a través de un bus 1008.

El procesador 1002 representa uno o más dispositivos de procesamiento de propósito general tales como un microprocesador, una unidad de procesamiento central o similares. De forma más particular, el procesador 702 puede ser un microprocesador de computación con conjunto de instrucciones complejas (CISC), un microprocesador de computación con conjunto de instrucciones reducidas (RISC), un microprocesador de palabra de instrucción muy larga (VLIW) o un procesador que implemente otros conjuntos de instrucciones o procesadores que implementen una combinación de conjuntos de instrucciones. El procesador 1002 puede también ser uno o más dispositivos de procesamiento de propósito especial tal como un circuito integrado de aplicación específica (ASIC), una matriz de puerta programable en campo (FPGA), un procesador de señal digital (DSP), un procesador de red o similares. La lógica 104, 110, 126, 130, 138 de detección de software malicioso en las figuras 1 y 3 puede ejecutarse por el procesador 1002 configurado para realizar las operaciones y etapas expuestas en el presente documento.

El sistema 1000 informático puede además incluir un dispositivo 1022 de interfaz de red. El sistema 1000 informático también puede incluir una unidad 1010 de visualización de vídeo (por ejemplo, una pantalla de cristal líquido (LCD) o un tubo de rayos catódicos (CRT)), un dispositivo 1012 de entrada alfanumérico (por ejemplo, un teclado), un dispositivo 1014 de control de cursor (por ejemplo, un ratón) y un dispositivo 1020 de generación de señal (por ejemplo, un altavoz).

Una unidad 1016 de disco puede incluir un medio 1024 legible por ordenador en el cual se almacena uno o más conjuntos de instrucciones (por ejemplo, instrucciones de la lógica 104, 110, 126, 130, 138 de detección de software malicioso en las figuras 1 y 3) que implementa cualquiera o más de las metodologías o funciones descritas en el presente documento. Las instrucciones de la lógica 104, 110, 126, 130, 138 de detección de software malicioso en las figuras 1 y 3 también puede residir, de forma completa o al menos parcialmente, dentro de la memoria 1004 principal y/o dentro del procesador 1002 durante la ejecución de la misma por el sistema 1000 informático, la memoria 1004 principal y el procesador 1002 que constituyen también medios legibles por ordenador. Las instrucciones de la lógica 104, 110, 126, 130, 138 de detección de software malicioso en las figuras 1 y 3 también pueden transmitirse o recibirse sobre una red 1026 a través del dispositivo 1022 de interfaz de red.

Aunque el medio 1024 de almacenamiento legible por ordenador se muestra en un ejemplo para ser un medio único, el término “medio de almacenamiento legible por ordenador” debería considerarse que incluye un único medio no transitorio o medio no transitorio múltiple (por ejemplo, una base de datos centralizada o distribuida y/o cachés y servidores asociados) que almacenan el uno o más conjuntos de instrucciones. El término “medio de almacenamiento legible por ordenador) también se considerará que incluye cualquier medio que es capaz de almacenar, codificar o transportar un conjunto de instrucciones para la ejecución mediante la máquina y que provoca que la máquina realice cualquiera o más de las metodologías de la presente divulgación. El término “medio de almacenamiento legible por ordenador” se considerará por consiguiente que incluye, pero no está limitado a, memorias en estado sólido, medios ópticos y medios magnéticos.

En la descripción anterior, se establecen numerosos detalles. Es evidente, sin embargo, para el experto en la técnica que tiene el beneficio de esta divulgación, que se pueden llevar a cabo ejemplos de la divulgación sin estos detalles específicos. En algunos casos, estructuras y dispositivos bien conocidos se muestran en forma de diagrama de bloques en lugar de en detalle, con el fin de evitar oscurecer la descripción.

Algunas porciones de la descripción detallada son presentadas en términos de algoritmos y representaciones simbólicas de operaciones en bits de datos dentro de una memoria informática. Estas descripciones y representaciones de algoritmo son los medios utilizados por los expertos en la técnica en el procesamiento de datos para transportar de la forma más efectiva la esencia de su trabajo a otros expertos en la técnica. Un algoritmo es en este caso y en general, concebido para ser una secuencia autoconsistente de etapas que llevan a un resultado deseado. Las etapas son aquellas que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no de forma necesaria, estas cantidades toman la forma de señales eléctricas o magnéticas capaces de ser almacenadas, trasferidas, combinadas, comparadas y de otro modo manipuladas. Se ha comprobado que es conveniente algunas veces, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares.

Se debería tener en cuenta, sin embargo, que todos estos términos y términos similares van a estar asociados con las cantidades físicas apropiadas y son meramente etiquetas convenientes aplicadas a estas cantidades. A menos que

se establezca de forma específica lo contrario como es evidente a partir de la exposición anterior, se aprecia que a lo largo de toda la descripción, las exposiciones que utilizan términos tales como “que recibe”, “que escribe”, “que mantiene” o similares se refieren a las acciones y procesos de un sistema informático o un dispositivo informático electrónico similar que manipula y transforma datos representados como cantidades físicas (por ejemplo, electrónicas) dentro de los registros y memorias del sistema informático en otros datos representados de forma similar como cantidades físicas dentro de las memorias o registros del sistema informático u otros dispositivos de almacenamiento de transmisión o de visualización de información de este tipo.

Ejemplos de la divulgación se refieren también a un aparato para realizar las operaciones en el presente documento. Este aparato puede construirse de forma específica para los propósitos requeridos o puede comprender un ordenador de propósito general activado o reconfigurado de forma selectiva mediante un programa informático almacenado en el ordenador. Dicho programa informático puede estar almacenado en un medio de almacenamiento legible por ordenador tal como, pero no limitado a, cualquier tipo de disco que incluye discos flexibles, discos ópticos, CDROM y discos magnético-ópticos, memorias de sólo lectura (ROM), memorias de acceso aleatorio (RAM), EPROM, EEPROM, tarjetas magnéticas u ópticas o cualquier tipo de medios adecuados para el almacenamiento de instrucciones electrónicas.

Los algoritmos y visualizaciones presentadas en el presente documento no están relacionados de forma inherente con ningún ordenador particular u otro aparato. Se pueden utilizar varios sistemas de propósito general con programas de acuerdo con las enseñanzas del presente documento o puede que sea conveniente construir un aparato más especializado para realizar las etapas del método requeridas. Una estructura de ejemplo para una variedad de estos sistemas aparece de la descripción del presente documento. Adicionalmente, la presente divulgación no se describe con referencia a ningún lenguaje de programación particular. Se apreciará que se puede utilizar una variedad de lenguajes de programación para implementar las enseñanzas de la divulgación tal y como se describen en el presente documento.

Por consiguiente, un método y un sistema eficientes proporcionan una protección a redes domésticas. La innovación reside en el uso de un servidor de computación en la nube y grupos de dispositivos que tienen una lógica de detección de software malicioso para incrementar la capacidad de detectar ataques e intrusiones y evitar los ataques y las intrusiones. El desarrollo de la lógica de detección de software malicioso de un dispositivo dedicado ayuda a hacer seguros los dispositivos que están expuestos, tales como dispositivos del Internet de las cosas (IoT) (por ejemplo, cámaras web, dispositivos multimedia, etc.).

Se ha de entender que la descripción anterior está destinada a ser ilustrativa y no restrictiva. Muchos otros ejemplos serán evidentes para los expertos en la técnica tras la lectura y la comprensión de la descripción anterior. El alcance de la divulgación por lo tanto debería determinarse con referencia a las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método que comprende:

recibir, mediante una lógica (104, 110, 126, 130) de detección de software malicioso ejecutada por un dispositivo (102) asegurado que reside en una red (100) doméstica, un mensaje desde un dispositivo (112) no asegurado de una primera red (106) y destinado a un dispositivo (118a o 102) de destino de la red doméstica, el dispositivo (118a o 102) de destino que comprende un cliente (120a-120n) de seguridad;

en donde el método está caracterizado por:

establecer, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, un canal de comunicación segura entre la lógica (104, 110, 126, 130) de detección de software malicioso del dispositivo (102) asegurado y el cliente (120a-120n) de seguridad del dispositivo (118a o 102) de destino;

ejecutar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, una comprobación de validación en el mensaje para determinar que el mensaje incluye un software malicioso;

reportar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, una alarma al cliente (120a-120n) de seguridad del dispositivo (118a o 102) de destino, siendo la alarma indicativa de la presencia del software malicioso; y

evitar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, que una aplicación asociada al dispositivo (118a o 102) de destino procese el mensaje.

2. El método de la reivindicación 1, que comprende además antes de transmitir, encriptar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, el mensaje

3. El método de la reivindicación 1, en donde la aplicación reside en el dispositivo (102) asegurado.

4. El método de la reivindicación 1, en donde la determinación de que el mensaje incluye software malicioso comprende realizar una o más comprobaciones de validación que comprenden al menos una de, una verificación de puerto, una verificación de contenido para la detección de virus, o una inspección de paquetes profunda para la detección de ataques conocidos.

5. El método de la reivindicación 1, que comprende además transmitir, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, una indicación de la presencia del software malicioso a un servidor (108) de computación en la nube.

6. El método de la reivindicación 1, en donde la lógica (104, 110, 126, 130) de detección de software malicioso va a proporcionar uno o más de un proceso de inicio seguro, un proceso de descarga seguro, o un proceso de generación para generar una o más claves para encriptar el mensaje.

7. Un sistema que comprende:

una memoria para almacenar instrucciones; y

un dispositivo de procesamiento conectado de forma operativa a la memoria;

el dispositivo de procesamiento que es para una red doméstica, el dispositivo de procesamiento adaptado para:

recibir un mensaje de un dispositivo (112) no asegurado de una primera red (106) y destinado a un dispositivo (118a o 102) de destino de la red doméstica, el dispositivo (118a o 102) de destino que comprende un cliente (120a-120n) de seguridad;

en donde el sistema está caracterizado por que comprende medios para:

establecer, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, un canal de comunicación segura entre la lógica (104, 110, 126, 130) de detección de software malicioso, del dispositivo (102) asegurado y el cliente (120a-120n) de seguridad del dispositivo (118a o 102) de destino;

ejecutar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, una comprobación de validación en el mensaje para determinar que el mensaje incluye un software malicioso;

reportar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, una alarma al cliente (120a-120n) de seguridad del dispositivo (118a o 102) de destino, siendo indicativa la alarma de una presencia del software malicioso; y

evitar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, que una aplicación asociada con el dispositivo (118a o 102) de destino procese el mensaje.

8. Un método que comprende:

recibir, mediante una lógica de detección de software malicioso ejecutada por un dispositivo asegurado que reside en una red doméstica, un mensaje desde un dispositivo (112) no asegurado de una primera red (106) y destinado al dispositivo (118a o 102) de destino de la red doméstica, el dispositivo (118a o 102) de destino que comprende un cliente (120a-120n) de seguridad;

en donde el método está caracterizado por:

determinar, mediante la lógica (104, 110, 126, 130) de detección de software malicioso y basándose en una característica del dispositivo (102) asegurado, no detectar si el mensaje incluye un software malicioso;

en respuesta a la lógica de detección de software malicioso determinar no detectar si el mensaje incluye un software malicioso;

transmitir, mediante la lógica de detección de software malicioso, el mensaje a un servidor (108) de computación en la nube;

en respuesta a la recepción, desde el servidor 108) de computación en la nube, de una indicación de que el mensaje incluye un software malicioso:

reportar, mediante la lógica de detección de software malicioso, una alarma al cliente (120a-120n) de seguridad (118a o 102) del dispositivo (118a o 102) de destino; y

evitar, mediante la lógica de detección de software malicioso, que una aplicación asociada con el dispositivo (118a o 102) de destino procese el mensaje.

9. El método de la reivindicación 8, que además comprende antes de transmitir, encriptar, mediante la lógica de detección de software malicioso, el mensaje.

10. El método de la reivindicación 8, que además comprende determinar que el dispositivo asegurado tiene una potencia de procesamiento suficiente o necesita más experiencia para determinar si el mensaje incluye un software malicioso en donde determinar no detectar si el mensaje incluye un software malicioso se basa en al menos uno de, el dispositivo (102) asegurado que tiene una potencia de procesamiento insuficiente o el dispositivo (102) asegurado que necesita más experiencia para determinar si el mensaje incluye un software malicioso.

11. EL método de la reivindicación 8, que además comprende recibir una indicación de que ha aumentado un nivel de alerta de la red (100) doméstica.

12. El método de la reivindicación 8, en donde la característica del dispositivo asegurado además incluye al menos una sensibilidad de seguridad del dispositivo (102) asegurado y en donde determinar no detectar si el mensaje incluye un software malicioso se hace a la vista de la sensibilidad de seguridad del dispositivo (102) asegurado.

13. El método de la reivindicación 8, en donde la aplicación reside en el dispositivo (102) asegurado.

14. El método de la reivindicación 8, que además comprende:

recibir, mediante la lógica de detección de software malicioso, un mensaje adicional; y

realizar, mediante la lógica de detección de software malicioso para el mensaje adicional, una o más comprobaciones de validación que comprenden al menos una de una verificación de puerto, verificación de contenido para la detección de virus, o una inspección de paquetes profunda para la detección de ataques conocidos.

15. El método de la reivindicación 8, que además comprende:

recibir, mediante la lógica de detección de software malicioso, un mensaje adicional;

determinar, mediante la lógica de detección de software malicioso, que el mensaje adicional incluye software malicioso; y

transmitir, mediante la lógica (104, 110, 126, 130) de detección de software malicioso, una indicación de la presencia del software malicioso a un servidor (108) de computación en la nube.

16. El método de la reivindicación 8, en donde la alarma es indicativa de una presencia del software malicioso.

17. El método de la reivindicación 8, en donde la lógica (104, 110, 126, 130) de detección de software malicioso se configura para proporcionar uno o más de un proceso de inicio seguro, un proceso de descarga seguro, o un proceso de generación para la generación de una o más claves para encriptar el mensaje.

18. Un sistema que comprende:

una memoria para almacenar instrucciones; y

un dispositivo de procesamiento conectado de forma operativa a la memoria; siendo el dispositivo de procesamiento para una red doméstica, el dispositivo de procesamiento adaptado para:

recibir un mensaje de un dispositivo (112) no asegurado de una primera red (106) y destinado a un dispositivo (118a o 102) de destino de la red doméstica, el dispositivo (118a o 102) de destino que comprende un cliente (120a-120n) de seguridad;

determinar, basándose en una característica del sistema, no detectar si el mensaje incluye un software malicioso;

en respuesta a una lógica (104, 110, 126, 130) de detección de software malicioso determinar no detectar si el mensaje incluye un software malicioso:

transmitir el mensaje a un servidor (108) de computación en la nube;

en respuesta a la recepción, desde el servidor (108) de computación en la nube, una indicación de que el mensaje contiene un software malicioso:

reportar una alarma al cliente (120a-120n) de seguridad del dispositivo (118a o 102) de destino; y evitar que una aplicación asociada con el dispositivo (118a o 102) de destino procese el mensaje.

19. El sistema de la reivindicación 18, que además comprende antes de transmitir, que el dispositivo de procesamiento además encripta el mensaje.

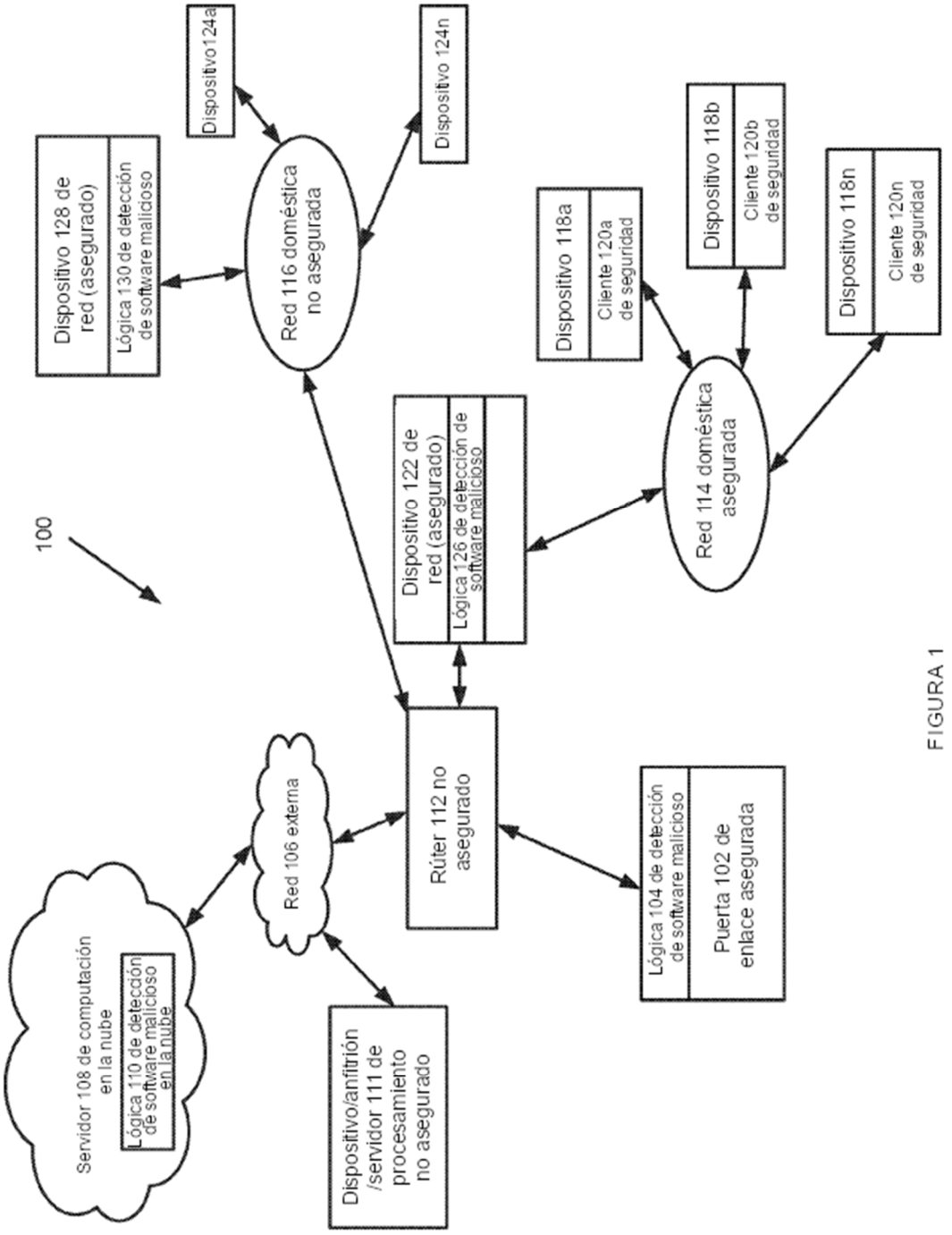
100
Dispositivo 128 de red (asegurado)
Lógica 130 de detección de software malicioso
Dispositivo124a
Dispositivo 124n
Red 116 doméstica no asegurada
Dispositivo 118a
Cliente 120a de seguridad
Dispositivo 118b
Cliente 120b de seguridad
Dispositivo 118n
Cliente 120n de seguridad
Dispositivo 122 de red (asegurado)
Lógica 126 de detección de software malicioso
Red 114 doméstica asegurada
Servidor 108 de computación en la nube
Lógica 110 de detección de software malicioso en la nube
Red 106 externa
Rúter 112 no asegurado
Lógica 104 de detección de software malicioso
Puerta 102 de enlace asegurada
Dispositivo/anfitrión /servidor 111 de procesamiento no asegurado

FIGURA 1

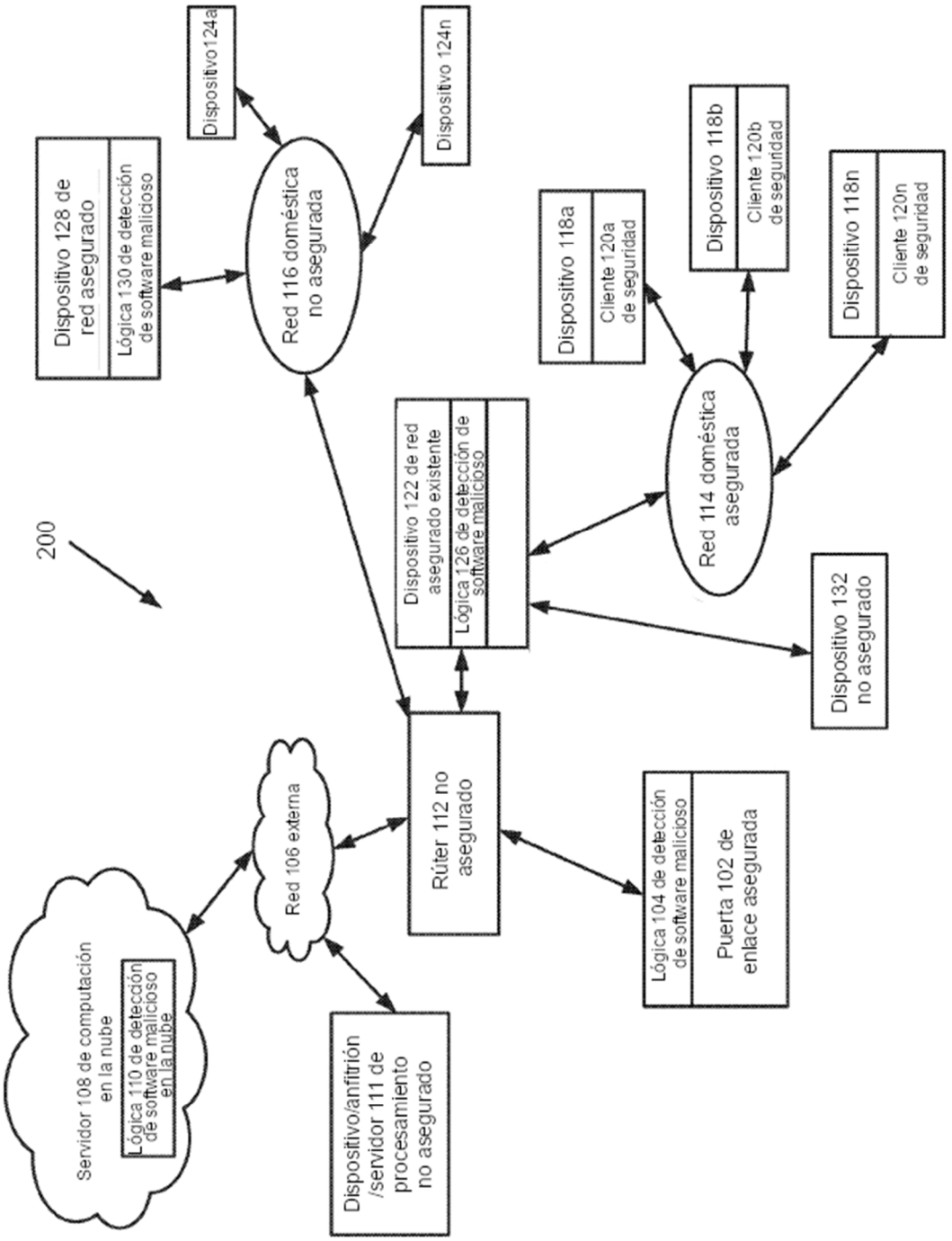
200
Servidor 108 de computación en la nube
Lógica 110 de detección de software malicioso en la nube
Red 106 externa
Dispositivo/anfitrión /servidor 111 de procesamiento no asegurado
Rúter 112 no asegurado
Lógica 104 de detección de software malicioso
Puerta 102 de enlace asegurada
Dispositivo 128 de red asegurado
Lógica 130 de detección de software malicioso
Red 116 doméstica no asegurada
Dispositivo124a
Dispositivo 124n
Dispositivo 122 de red asegurado existente
Lógica 126 de detección de software malicioso
Dispositivo 132 no asegurado
Red 114 doméstica asegurada
Dispositivo 118a
Cliente 120a de seguridad
Dispositivo 118b
Cliente 120b de seguridad
Dispositivo 118n
Cliente 120n de seguridad

FIGURA 2

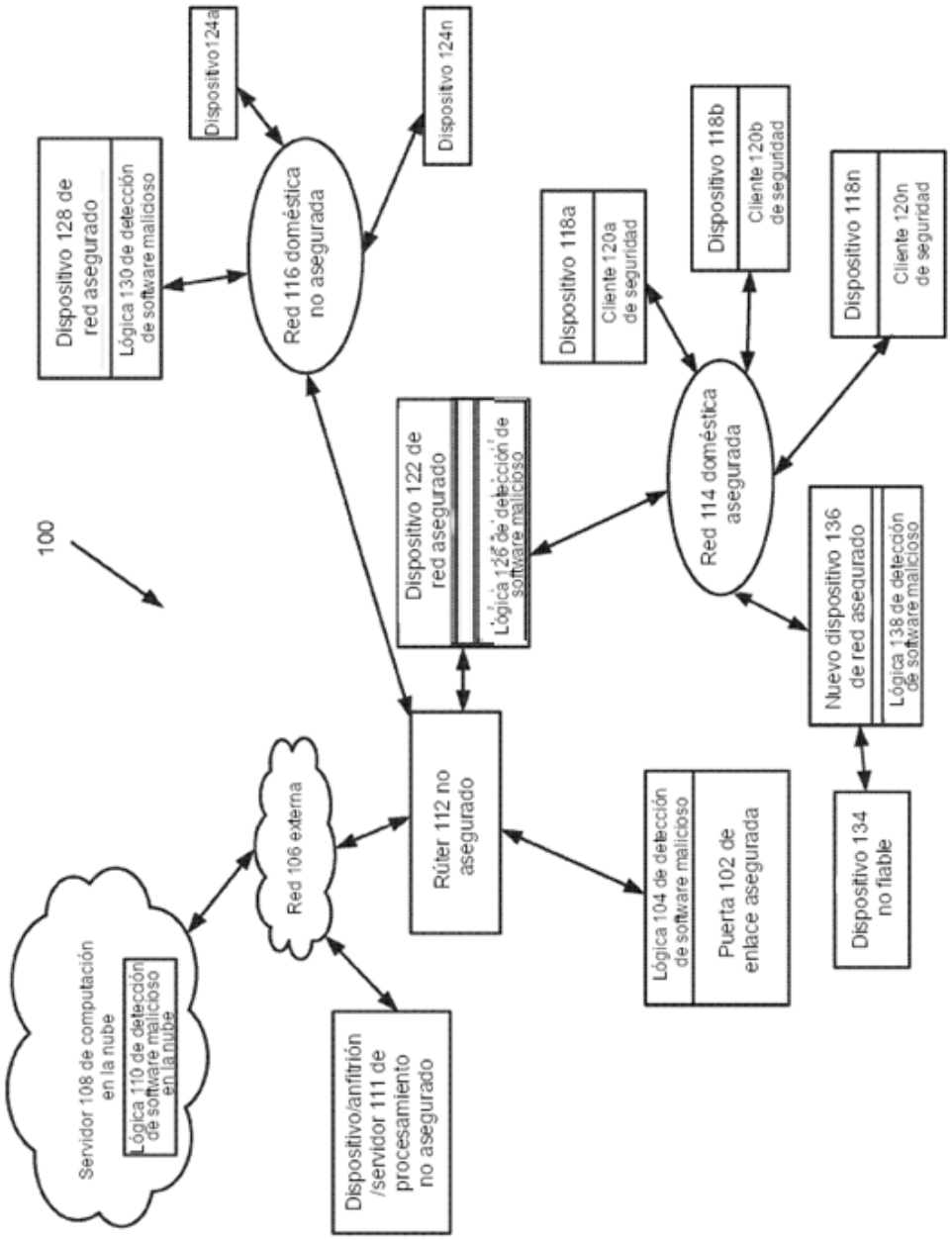
100
Servidor 108 de computación en la nube
Lógica 110 de detección de software malicioso en la nube
Red 106 externa
Dispositivo/anfitrión /servidor 111 de procesamiento no asegurado
Rúter 112 no asegurado
Lógica 104 de detección de software malicioso
Puerta 102 de enlace asegurada
Dispositivo 134 no fiable
Nuevo dispositivo 136 de red asegurado
Lógica 138 de detección de software malicioso
Red 114 doméstica asegurada
Dispositivo 122 de red asegurado
Lógica 126 de detección de software malicioso
Dispositivo 118a
Cliente 120a de seguridad
Dispositivo 118b
Cliente 120b de seguridad
Dispositivo 118n
Cliente 120n de seguridad
Red 116 doméstica no asegurada
Dispositivo 128 de red asegurado
Lógica 130 de detección de software malicioso
Dispositivo124a
Dispositivo 124n

FIGURA 3

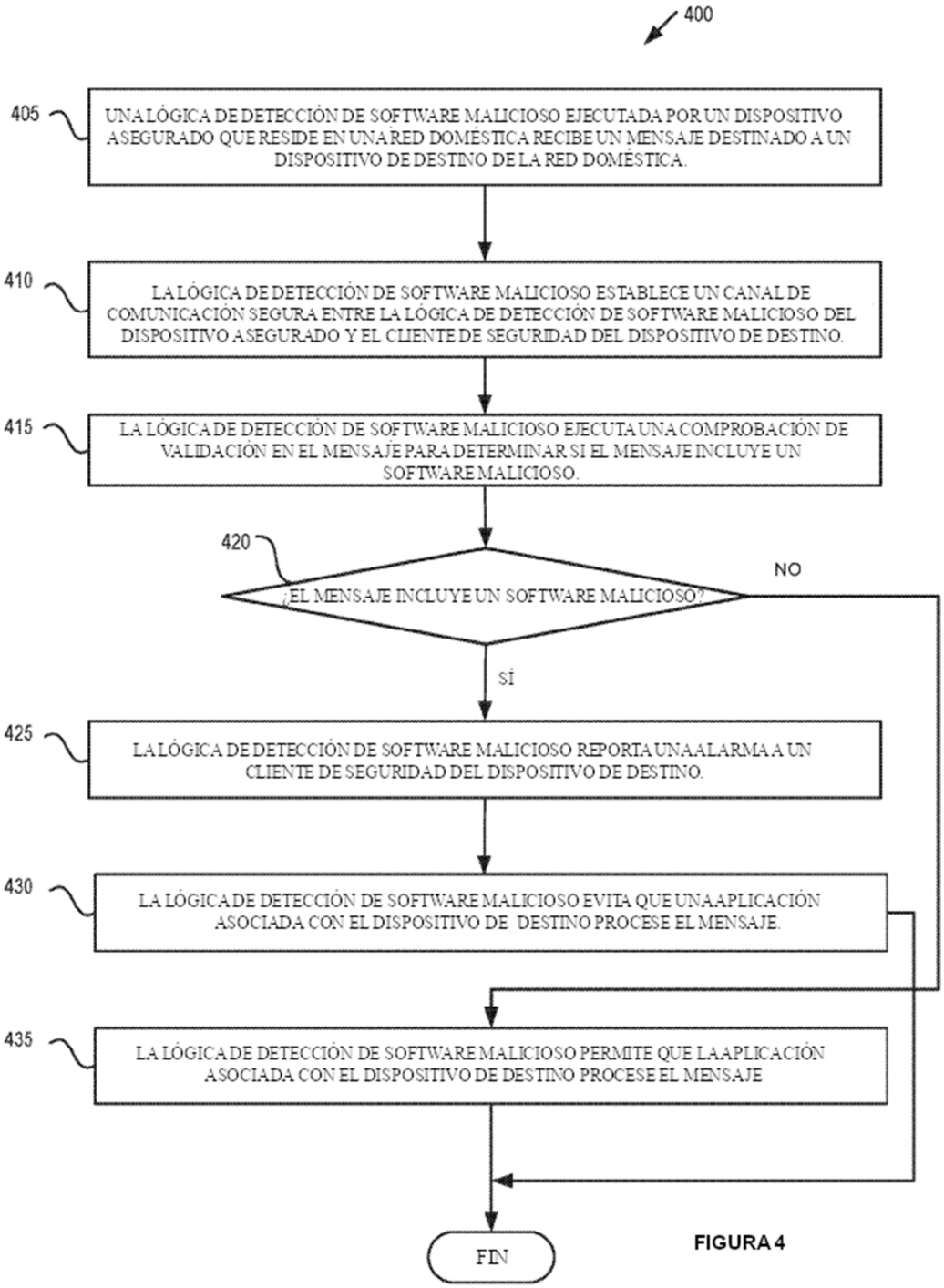
400
405
UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTADA POR UN DISPOSITIVO ASEGURADO QUE RESIDE EN UNA RED DOMÉSTICA RECIBE UN MENSAJE DESTINADO A UN DISPOSITIVO DE DESTINO DE LA RED DOMÉSTICA.
410
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO ESTABLECE UN CANAL DE COMUNICACIÓN SEGURA ENTRE LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL DISPOSITIVO ASEGURADO Y EL CLIENTE DE SEGURIDAD DEL DISPOSITIVO DE DESTINO.
415
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTA UNA COMPROBACIÓN DE VALIDACIÓN EN EL MENSAJE PARA DETERMINAR SI EL MENSAJE INCLUYE UN SOFTWARE MALICIOSO.
420
¿EL MENSAJE INCLUYE UN SOFTWARE MALICIOSO?
NO
SÍ
425
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO REPORTA UNA ALARMA A UN CLIENTE DE SEGURIDAD DEL DISPOSITIVO DE DESTINO.
430
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EVITA QUE UNA APLICACIÓN ASOCIADA CON EL DISPOSITIVO DE DESTINO PROCESE EL MENSAJE.
435
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO PERMITE QUE LA APLICACIÓN ASOCIADA CON EL DISPOSITIVO DE DESTINO PROCESE EL MENSAJE
FIN

FIGURA 4

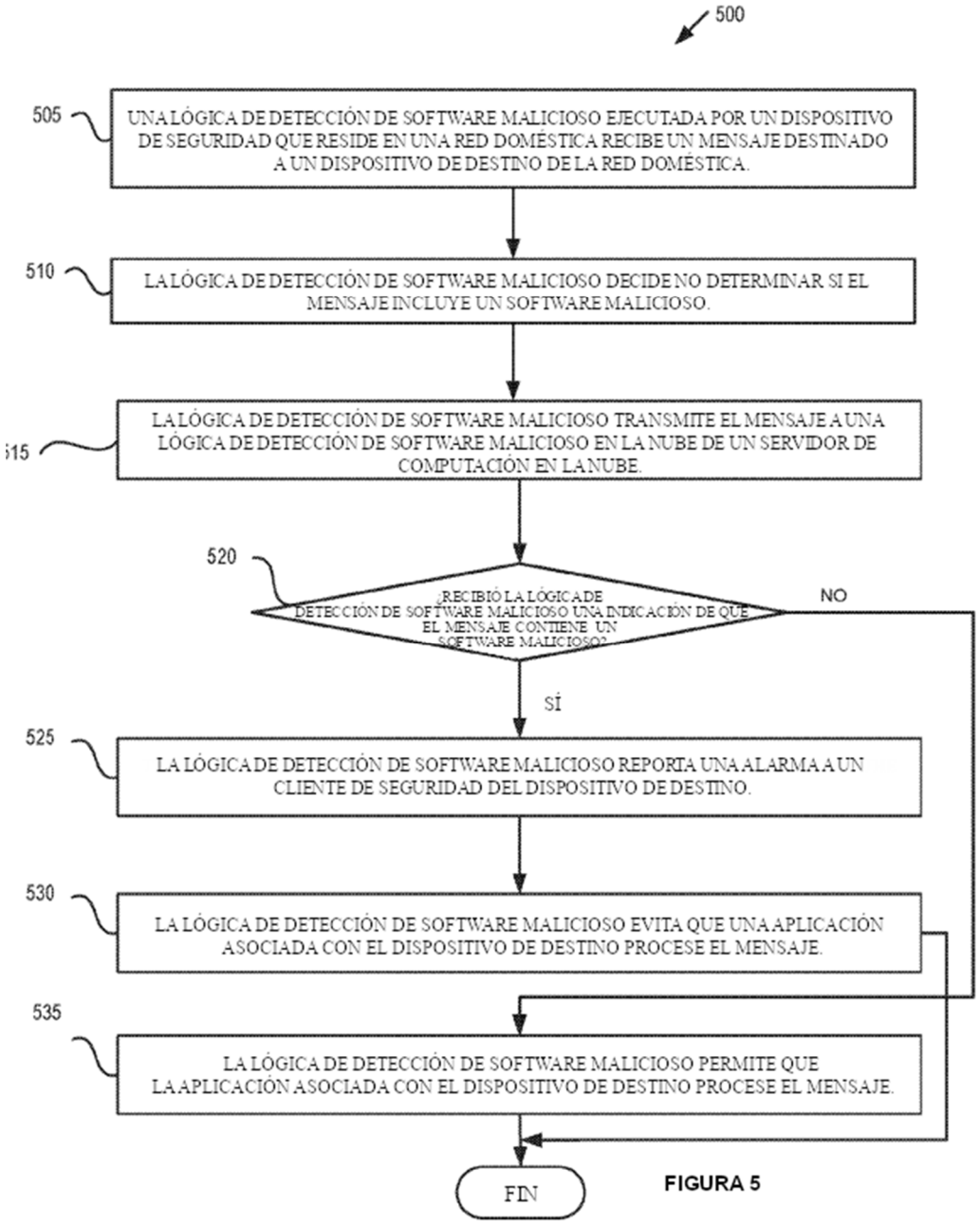
500
505
UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTADA POR UN DISPOSITIVO DE SEGURIDAD QUE RESIDE EN UNA RED DOMÉSTICA RECIBE UN MENSAJE DESTINADO A UN DISPOSITIVO DE DESTINO DE LA RED DOMÉSTICA.
510
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DECIDE NO DETERMINAR SI EL MENSAJE INCLUYE UN SOFTWARE MALICIOSO.
515
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO TRANSMITE EL MENSAJE A UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EN LA NUBE DE UN SERVIDOR DE COMPUTACIÓN EN LA NUBE.
520
¿RECIBIÓ LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO UNA INDICACIÓN DE QUE EL MENSAJE CONTIENE UN SOFTWARE MALICIOSO?
NO
SÍ
525
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO REPORTA UNA ALARMA A UN CLIENTE DE SEGURIDAD DEL DISPOSITIVO DE DESTINO.
530
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EVITA QUE UNA APLICACIÓN ASOCIADA CON EL DISPOSITIVO DE DESTINO PROCESE EL MENSAJE.
535
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO PERMITE QUE LA APLICACIÓN ASOCIADA CON EL DISPOSITIVO DE DESTINO PROCESE EL MENSAJE.
FIN

FIGURA 5

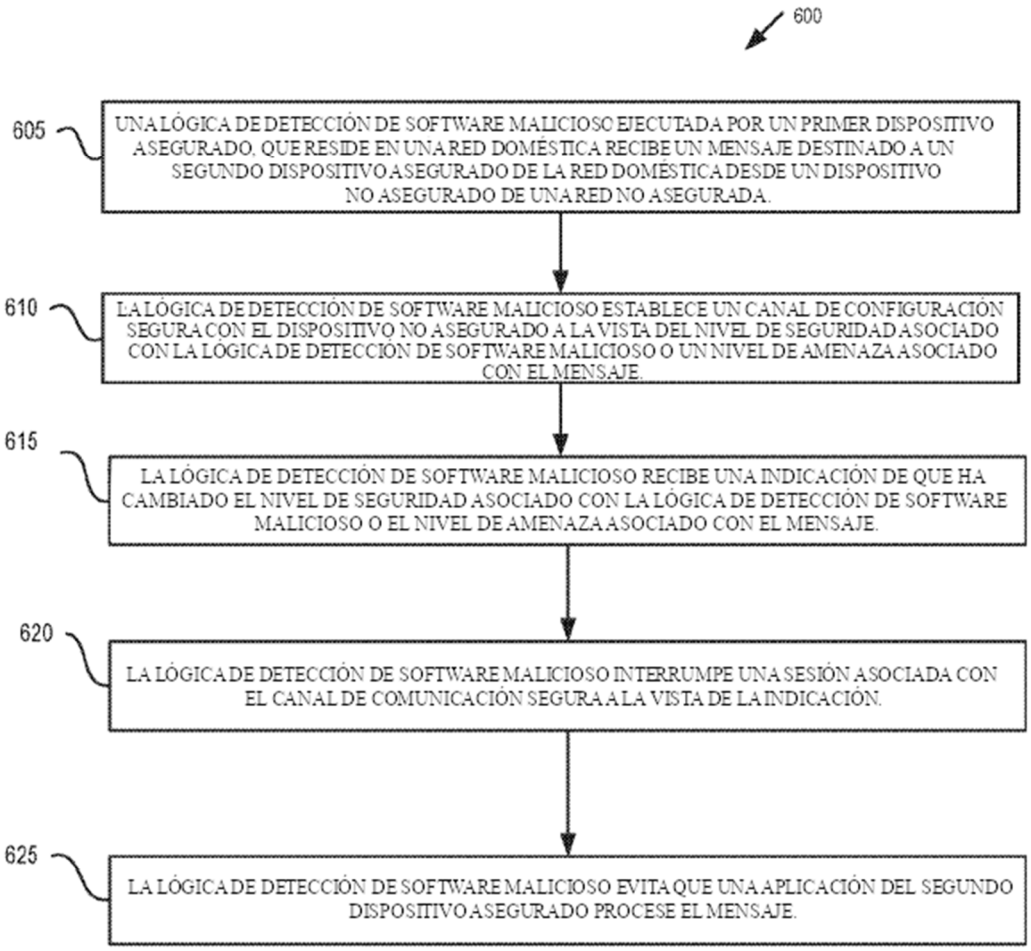
600
605
UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTADA POR UN PRIMER DISPOSITIVO ASEGURADO, QUE RESIDE EN UNA RED DOMÉSTICA RECIBE UN MENSAJE DESTINADO A UN SEGUNDO DISPOSITIVO ASEGURADO DE LA RED DOMÉSTICA DESDE UN DISPOSITIVO NO ASEGURADO DE UNA RED NO ASEGURADA.
610
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO ESTABLECE UN CANAL DE CONFIGURACIÓN SEGURA CON EL DISPOSITIVO NO ASEGURADO A LA VISTA DEL NIVEL DE SEGURIDAD ASOCIADO CON LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO O UN NIVEL DE AMENAZA ASOCIADO CON EL MENSAJE.
615
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO RECIBE UNA INDICACIÓN DE QUE HA CAMBIADO EL NIVEL DE SEGURIDAD ASOCIADO CON LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO O EL NIVEL DE AMENAZA ASOCIADO CON EL MENSAJE.
620
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO INTERRUMPE UNA SESIÓN ASOCIADA CON EL CANAL DE COMUNICACIÓN SEGURA A LA VISTA DE LA INDICACIÓN.
625
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EVITA QUE UNA APLICACIÓN DEL SEGUNDO DISPOSITIVO ASEGURADO PROCESE EL MENSAJE.

FIGURA 6

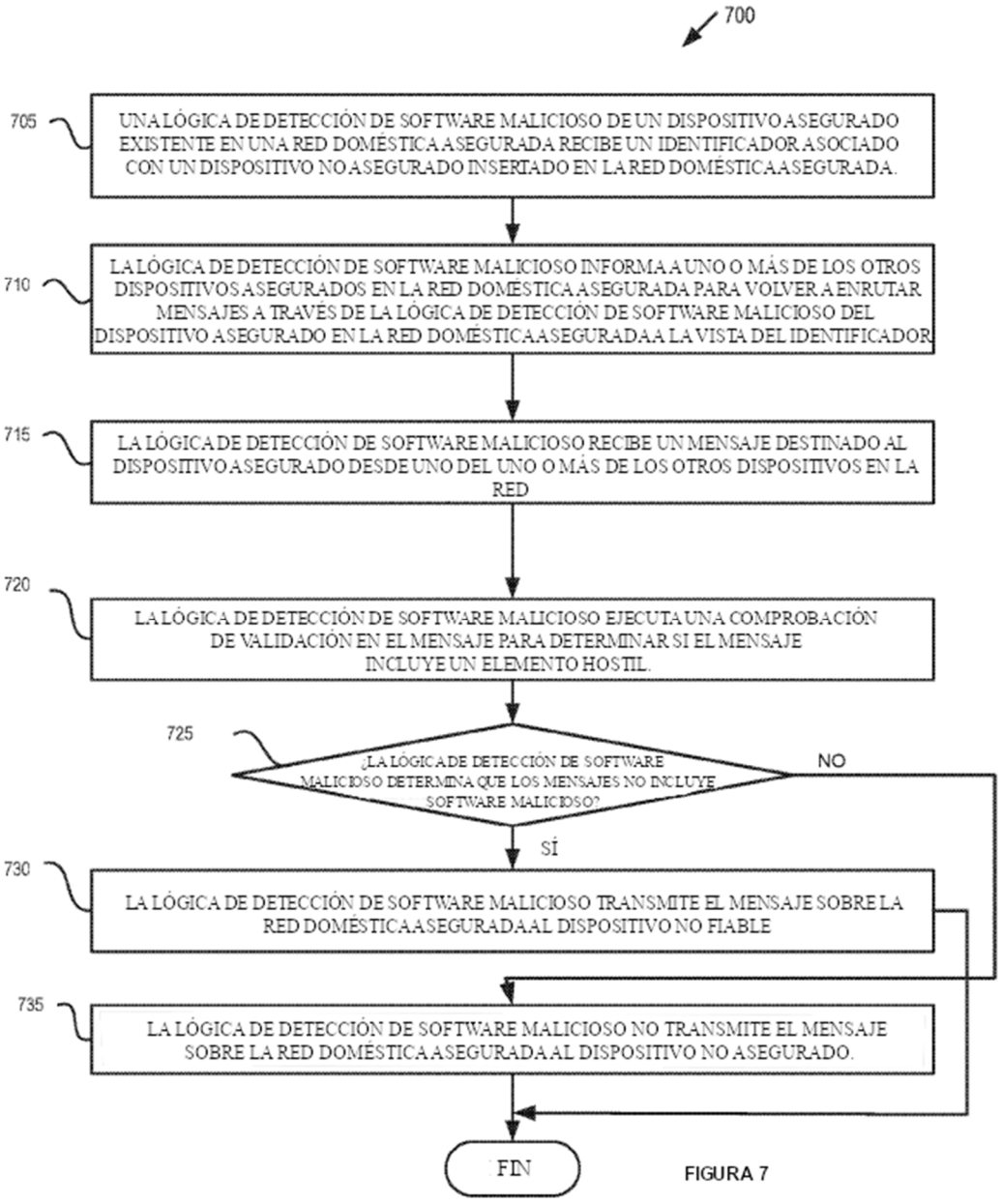
700
705
UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DE UN DISPOSITIVO ASEGURADO EXISTENTE EN UNA RED DOMÉSTICA ASEGURADA RECIBE UN IDENTIFICADOR ASOCIADO CON UN DISPOSITIVO NO ASEGURADO INSERTADO EN LA RED DOMÉSTICA ASEGURADA.
710
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO INFORMA A UNO O MÁS DE LOS OTROS DISPOSITIVOS ASEGURADOS EN LA RED DOMÉSTICA ASEGURADA PARA VOLVER A ENRUTAR MENSAJES A TRAVÉS DE LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL DISPOSITIVO ASEGURADO EN LA RED DOMÉSTICA ASEGURADA A LA VISTA DEL IDENTIFICADOR
715
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO RECIBE UN MENSAJE DESTINADO AL DISPOSITIVO ASEGURADO DESDE UNO DEL UNO O MÁS DE LOS OTROS DISPOSITIVOS EN LA RED
720
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTA UNA COMPROBACIÓN DE VALIDACIÓN EN EL MENSAJE PARA DETERMINAR SI EL MENSAJE INCLUYE UN ELEMENTO HOSTIL.
725
¿LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DETERMINA QUE LOS MENSAJES NO INCLUYE SOFTWARE MALICIOSO?
NO
SÍ
730
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO TRANSMITE EL MENSAJE SOBRE LA RED DOMÉSTICA ASEGURADA AL DISPOSITIVO NO FIABLE
735
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO NO TRANSMITE EL MENSAJE SOBRE LA RED DOMÉSTICA ASEGURADA AL DISPOSITIVO NO ASEGURADO.
FIN

FIGURA 7

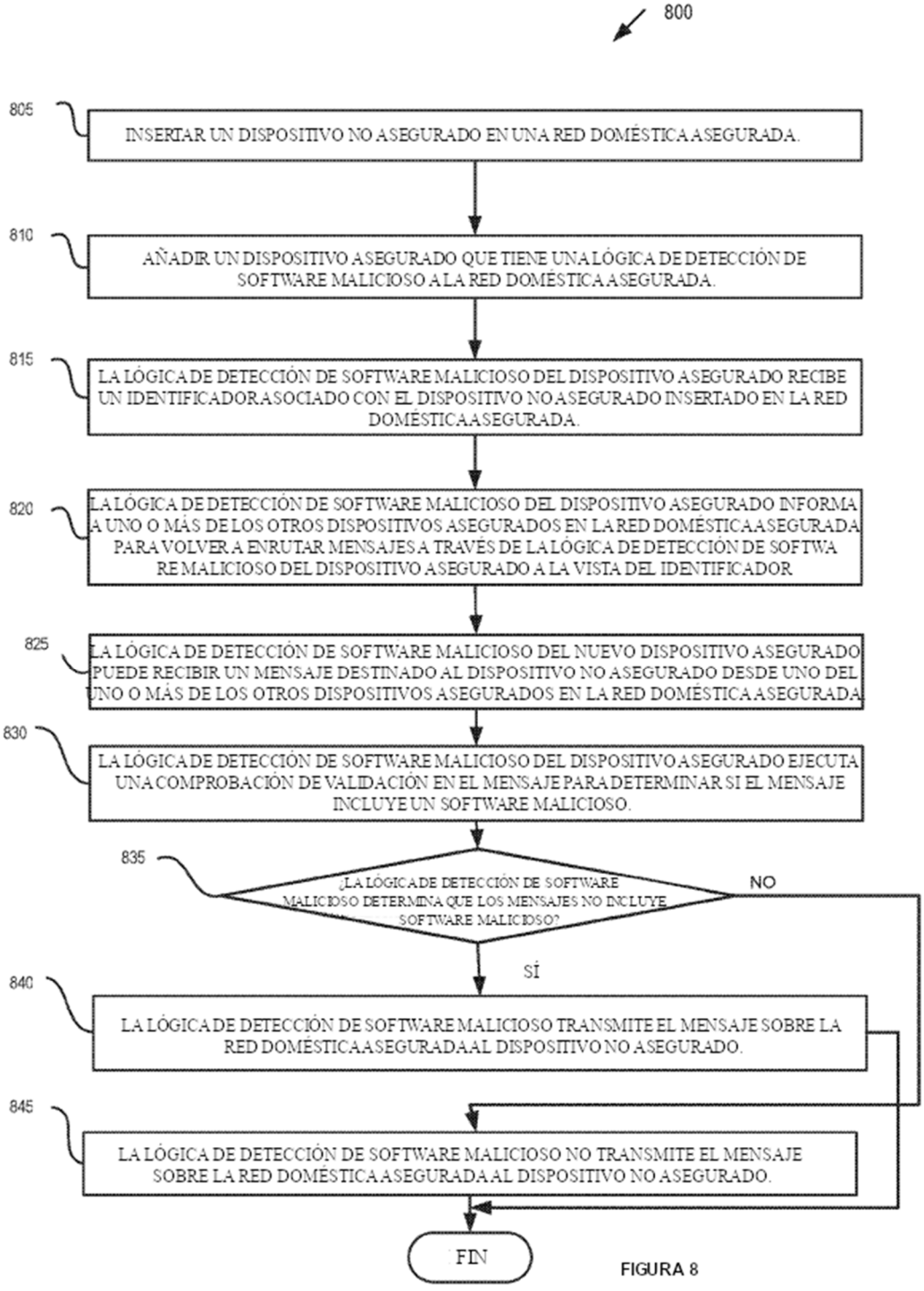
800
805
INSERTAR UN DISPOSITIVO NO ASEGURADO EN UNA RED DOMÉSTICA ASEGURADA.
810
AÑADIR UN DISPOSITIVO ASEGURADO QUE TIENE UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO A LA RED DOMÉSTICA ASEGURADA.
815
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL DISPOSITIVO ASEGURADO RECIBE UN IDENTIFICADOR ASOCIADO CON EL DISPOSITIVO NO ASEGURADO INSERTADO EN LA RED DOMÉSTICA ASEGURADA.
820
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL DISPOSITIVO ASEGURADO INFORMA A UNO O MÁS DE LOS OTROS DISPOSITIVOS ASEGURADOS EN LA RED DOMÉSTICA ASEGURADA PARA VOLVER A ENRUTAR MENSAJES A TRAVÉS DE LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL DISPOSITIVO ASEGURADO A LA VISTA DEL IDENTIFICADOR
825
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL NUEVO DISPOSITIVO ASEGURADO PUEDE RECIBIR UN MENSAJE DESTINADO AL DISPOSITIVO NO ASEGURADO DESDE UNO DEL UNO O MÁS DE LOS OTROS DISPOSITIVOS ASEGURADOS EN LA RED DOMÉSTICA ASEGURADA
830
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL DISPOSITIVO ASEGURADO EJECUTA UNA COMPROBACIÓN DE VALIDACIÓN EN EL MENSAJE PARA DETERMINAR SI EL MENSAJE INCLUYE UN SOFTWARE MALICIOSO.
835
¿LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DETERMINA QUE LOS MENSAJES NO INCLUYE SOFTWARE MALICIOSO?
NO
SÍ
840
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO TRANSMITE EL MENSAJE SOBRE LA RED DOMÉSTICA ASEGURADA AL DISPOSITIVO NO ASEGURADO.
845
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO NO TRANSMITE EL MENSAJE SOBRE LA RED DOMÉSTICA ASEGURADA AL DISPOSITIVO NO ASEGURADO.
FIN

FIGURA 8

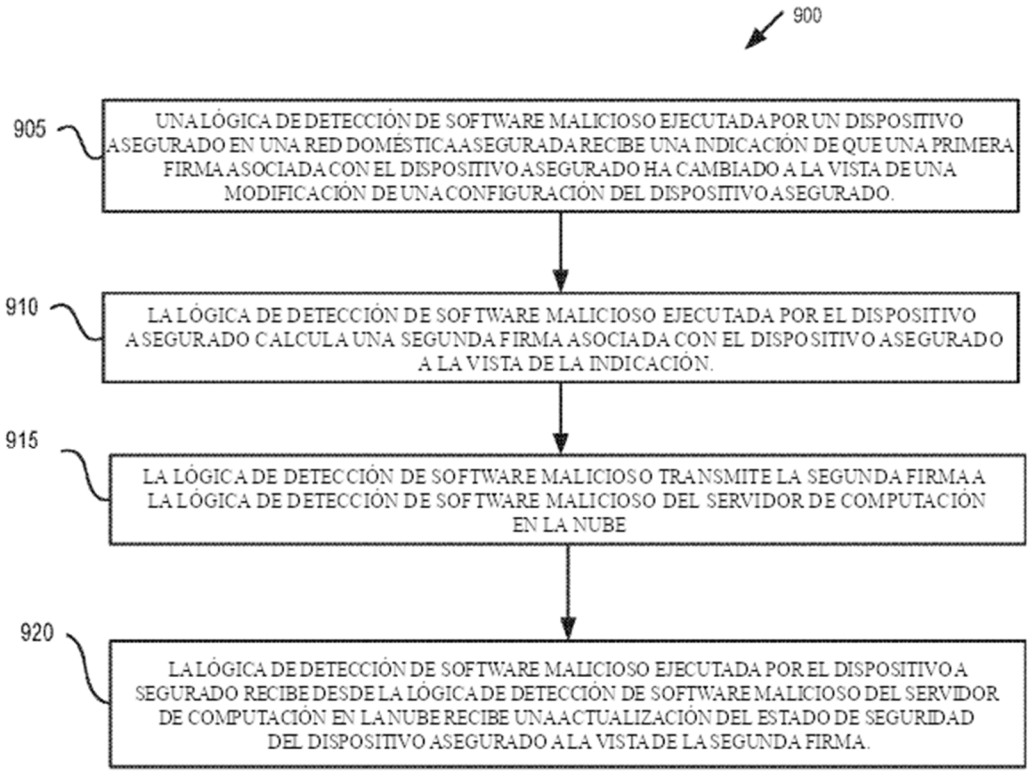
900
905
UNA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTADA POR UN DISPOSITIVO ASEGURADO EN UNA RED DOMÉSTICA ASEGURADA RECIBE UNA INDICACIÓN DE QUE UNA PRIMERA FIRMA ASOCIADA CON EL DISPOSITIVO ASEGURADO HA CAMBIADO A LA VISTA DE UNA MODIFICACIÓN DE UNA CONFIGURACIÓN DEL DISPOSITIVO ASEGURADO.
910
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTADA POR EL DISPOSITIVO ASEGURADO CALCULA UNA SEGUNDA FIRMA ASOCIADA CON EL DISPOSITIVO ASEGURADO A LA VISTA DE LA INDICACIÓN.
915
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO TRANSMITE LA SEGUNDA FIRMA A LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL SERVIDOR DE COMPUTACIÓN EN LA NUBE
920
LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO EJECUTADA POR EL DISPOSITIVO ASEGURADO RECIBE DESDE LA LÓGICA DE DETECCIÓN DE SOFTWARE MALICIOSO DEL SERVIDOR DE COMPUTACIÓN EN LA NUBE RECIBE UNA ACTUALIZACIÓN DEL ESTADO DE SEGURIDAD DEL DISPOSITIVO ASEGURADO A LA VISTA DE LA SEGUNDA FIRMA.

FIGURA 9

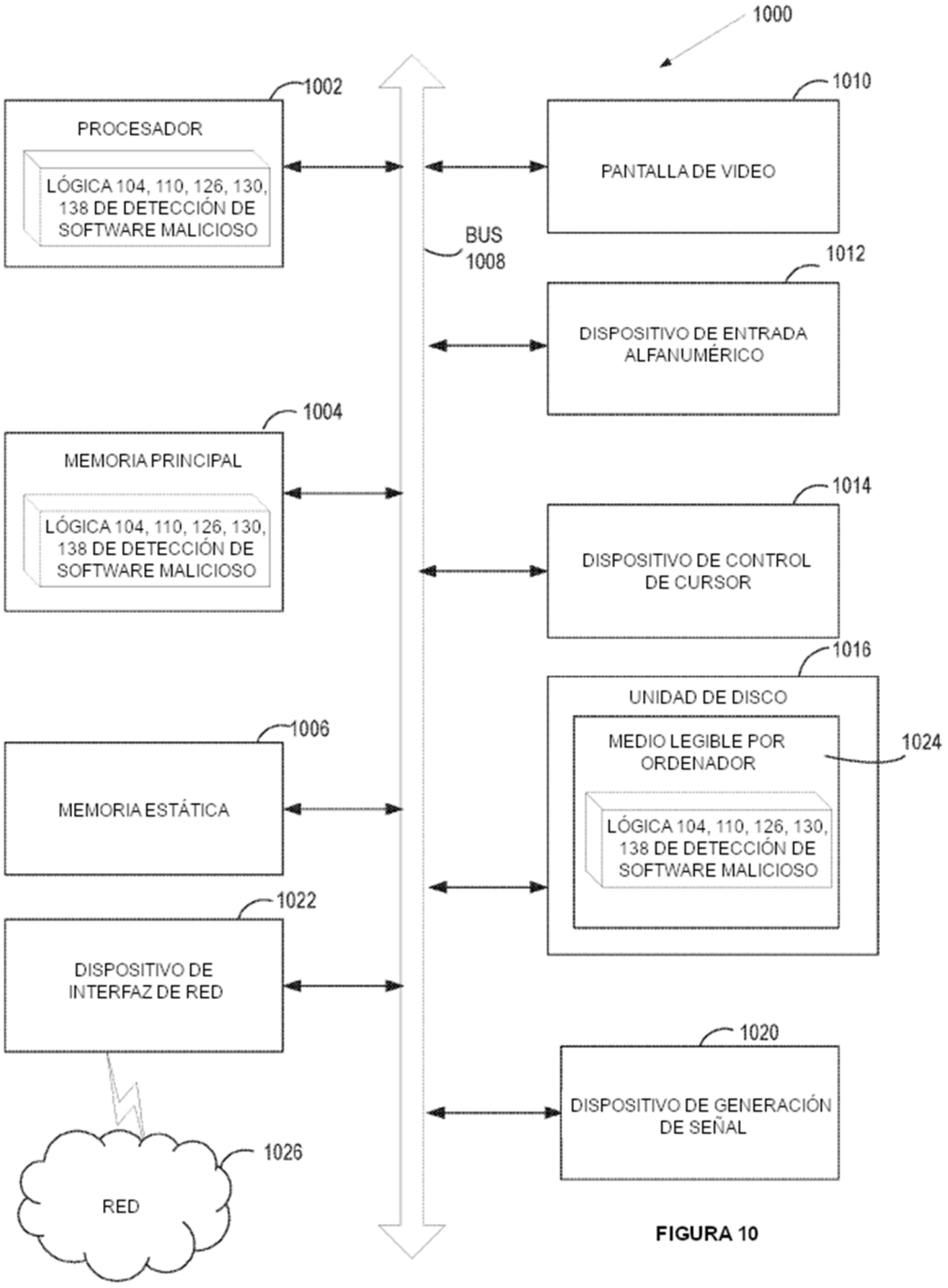
1000
1002
PROCESADOR
LÓGICA 104, 110, 126, 130, 138 DE DETECCIÓN DE SOFTWARE MALICIOSO
1010
PANTALLA DE VIDEO
BUS
1008
1012
DISPOSITIVO DE ENTRADA ALFANUMÉRICO
1004
MEMORIA PRINCIPAL
LÓGICA 104, 110, 126, 130, 138 DE DETECCIÓN DE SOFTWARE MALICIOSO
1014
DISPOSITIVO DE CONTROL DE CURSOR
1016
UNIDAD DE DISCO
MEDIO LEGIBLE POR ORDENADOR
1024
LÓGICA 104, 110, 126, 130, 138 DE DETECCIÓN DE SOFTWARE MALICIOSO
1006
MEMORIA ESTÁTICA
1022
DISPOSITIVO DE INTERFAZ DE RED
1020
DISPOSITIVO DE GENERACIÓN DE SEÑAL
1026
RED

FIGURA 10