(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 549 069**

(51) Int. CI.:

H04L 12/58 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.04.2002 E 02762088 (9)**

(97) Fecha y número de publicación de la concesión europea: **12.08.2015 EP 1388068**

(54) Título: **Sistema y método para proporcionar protección contra programas maliciosos para redes**

(30) Prioridad:

13.04.2001 US 283757 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.10.2015

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

SMITH, GREGORY J.

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Sistema y método para proporcionar protección contra programas maliciosos para redes

Campo de la invención

La presente invención se refiere a la seguridad de red informática, y en particular, a la protección contra programas maliciosos para redes.

Antecedentes

La Internet conecta millones de nodos localizados en todo el mundo. Con el clic de un botón, un usuario en una parte del mundo puede acceder a un archivo en otro ordenador a miles de kilómetros de distancia. Además, la Internet ha facilitado el intercambio de información en forma de mensajes electrónicos conocidos como correo electrónico. Aunque, primero se usaba para transferir mensajes de texto cortos, ahora el correo electrónico puede usarse para enviar imágenes digitales, archivos de sonido, documentos, hojas de cálculo, programas ejecutables y otros archivos electrónicos. Enviar este tipo de archivos es tan fácil como adjuntarles a un mensaje de correo electrónico y hacer clic en un botón de envío.

La facilidad de transmitir información, sin embargo, también se ha aprovechado por algunos para otros fines. Uno de los primeros casos muy publicitados de aprovechamiento involucró el uso de servidores de correo electrónico para propagar un programa. Una vez que un servidor de correo electrónico se convierte en "infectado" con el programa, comenzará el envío de mensajes de correo electrónico que contienen el programa a otros servidores de correo electrónico de los que era consciente. Como un virus, el programa se propaga desde un servidor de correo electrónico a un servidor de correo con una velocidad increíble. Aunque el programa no borra los archivos o daña los datos en los servidores de correo electrónico, debido al volumen de mensajes de correo electrónico enviados por los servidores de correo electrónico infectados, el programa provoca que la recuperación de mensajes de correo electrónico desde los servidores de correo electrónico se ralentice a un ritmo insoportable.

Actualmente, las noticias informan de programas similares a virus (en adelante en el presente documento "programas maliciosos") prácticamente de manera diaria. Algunos de estos programas maliciosos son relativamente benignos; otros destruyen los datos o capturan información sensible. A menos que se proteja adecuadamente contra estos programas maliciosos pueden tener a sus pies la red o el sistema de correo electrónico de una empresa o robar información sensible, incluso si solo unos pocos ordenadores están infectados.

El método más común para hacer frente a estos programas maliciosos es instalar un software de protección antivirus en todos los ordenadores. Tan pronto como se libera una versión de software de protección antivirus, aquellos que tratan de eludir el software de protección antivirus crean nuevos programas maliciosos que no se reconocen por el software de protección antivirus.

Esto lleva a los desarrolladores de software de protección antivirus a crear actualizaciones de su software de protección antivirus para detectar estos nuevos programas maliciosos. Anteriormente, actualizar el software de protección antivirus en cada equipo requería obtener las actualizaciones en disco y pasar de un ordenador a otro para instalar las actualizaciones. Ahora, el software de protección antivirus permite a los usuarios de ordenadores descargar las actualizaciones usando Internet. Ya que la instalación de actualizaciones requiere un esfuerzo por parte de cada usuario (o un equipo de soporte informático), muy a menudo el software de protección de virus no está al día en todos los equipos. Además, a menudo existe un retraso significativo entre la introducción de un nuevo virus y la creación y distribución de una actualización destinada a proteger contra el nuevo virus. Además, el software de protección antivirus normalmente no protege contra la clase más general de programas similares a los virus conocidos como programas maliciosos.

La solicitud de patente del Reino Unido Nº 2.357.939 y la solicitud PCT Nº WO02/05072 describen ambas un sistema que explora los correos electrónicos en busca de virus por el método descrito en las mismas.

Sumario

De acuerdo con un primer aspecto de la invención, se proporciona un sistema para proporcionar protección a los dispositivos conectados a una red, que comprende: un componente de exploración adaptado para determinar si un mensaje incluye un programa malicioso; y un componente de cuarentena acoplado al componente de exploración y adaptado para retener el mensaje cuando el mensaje incluye un programa malicioso; estando el sistema caracterizado por: el componente de exploración que además está adaptado para: examinar cada mensaje que recibe para buscar una firma digital que indique que el mensaje examinado no debería reenviarse; y reenviar el mensaje examinado al componente de cuarentena cuando se encuentra una firma digital.

El componente de exploración podría adaptarse para examinar los mensajes salientes.

El componente de exploración podría adaptarse además, para reenviar el mensaje examinado al componente de cuarentena junto con la información en cuanto a quién ha enviado el mensaje, el momento en que se ha enviado el mensaje y otros datos relacionados con el mensaje.

El sistema podría comprender además: (a) un filtro de contenidos que está adaptado para: recibir un mensaje que se dirige a al menos uno de los dispositivos y que incluye un encabezamiento, un cuerpo y un anexo; determinar una encapsulación que se ha aplicado al anexo antes de que el sistema reciba el mensaje; y desencapsular el anexo; y (b) un componente de descompresión que está acoplado al filtro de contenidos y que está adaptado para realizar al menos una descompresión del anexo cuando el anexo está comprimido.

El componente de exploración podría adaptarse además para determinar si el anexo incluye un programa malicioso.

El sistema podría comprender además un cliente que está adaptado para aplicar de manera automática una actualización a al menos uno de entre el filtro de contenidos, el componente de descompresión, el componente de exploración, y el componente de cuarentena para permitir la detección de al menos un programa malicioso.

El cliente podría adaptarse para determinar cuándo la actualización está disponible adaptándose para sondear los servidores asociados con los proveedores de software de protección de programas maliciosos.

El cliente podría adaptarse para recuperar de manera automática la actualización disponible.

El componente de exploración podría adaptarse para emplear al menos dos aplicaciones de protección de programas maliciosos por separado para determinar si el anexo incluye un programa malicioso.

El filtro de contenidos, el componente de descompresión, el componente de exploración, y el componente de cuarentena podrían cada uno implementarse en software.

El filtro de contenidos, el componente de descompresión, el componente de exploración, y el componente de cuarentena podrían todos incluirse en al menos uno de entre un cortafuegos, un router, un switch, y un gestor de tráfico.

La encapsulación puede incluir al menos uno de entre extensiones multipropósito de correo de internet, Base 64, y uuencode.

El componente de cuarentena podría adaptarse para eliminar el programa malicioso del mensaje que se ha determinado que incluye un programa malicioso y reenviar dicho mensaje hacia un destinatario de dicho mensaje.

De acuerdo con un segundo aspecto de la invención, se proporciona un método para proporcionar protección a los dispositivos conectados a una red, que comprende: recibir un mensaje en un nodo, siendo dicho nodo un nodo que recibe los mensajes que se dirigen a cualquiera de los dispositivos y que provoca que cada uno de dichos mensajes se explore en busca de un programa malicioso mediante un componente de exploración antes de reenviar los mensajes respectivos hacia al menos uno de los dispositivos y que retiene los mensajes respectivos mediante un componente de cuarentena cuando los mensajes respectivos incluyen unos programas maliciosos respectivos; caracterizado por: examinar, mediante el componente de exploración, el mensaje en busca de una firma digital que indique que no debería reenviarse el mensaje examinado; y reenviar el mensaje examinado al componente de cuarentena cuando se encuentra una firma digital.

El mensaje examinado en busca de una firma digital podría ser un mensaje saliente.

El mensaje examinado podría reenviarse al componente de cuarentena junto con la información en cuanto a quién ha enviado el mensaje, el momento en que se ha enviado el mensaje y otros datos relacionados con el mensaje.

El método podría comprender además: recibir un mensaje adicional en el que el mensaje adicional incluye una cabecera; determinar si la cabecera incluye un programa malicioso; y cuando la cabecera del mensaje adicional incluya el programa malicioso, poner en cuarentena el mensaje adicional, en el que la cabecera incluye un campo que tiene un tamaño definido y en el que la cabecera incluye el programa malicioso cuando un tamaño de datos en el campo es distinto que el tamaño definido.

El mensaje adicional podría incluir un anexo, que comprende además: desencapsular el anexo cuando el anexo está encapsulado; y descomprimir el anexo al menos una vez cuando el anexo está comprimido.

El método podría comprender además, eliminar el programa malicioso y reenviar el mensaje adicional hacia al menos uno de los dispositivos.

Estas y otras diversas características así como ventajas que caracterizan la presente solicitud, serán evidentes a partir de una lectura de la siguiente descripción detallada y una revisión de los dibujos asociados.

Breve descripción de los dibujos

Las figuras 1-3 muestran los componentes de un entorno a modo de ejemplo en el que puede ponerse en práctica la invención;
La figura 4 ilustra un entorno a modo de ejemplo en el que funciona un sistema para proporcionar protección a una red contra un programa malicioso;
La figura 5 ilustra los componentes de un cortafuegos que pueden funcionar para proporcionar protección contra un programa malicioso; y
La figura 6 ilustra un diagrama de flujo para detectar programas maliciosos de acuerdo con la invención.

Descripción detallada

En la siguiente descripción detallada de unas realizaciones a modo de ejemplo de la invención, se hace referencia a los dibujos anexos, que forman parte de la misma, y que se muestran a modo de ilustración, realizaciones a modo de ejemplo específicas en las que la invención puede ponerse en práctica. Estas realizaciones se describen con suficiente detalle para permitir a los expertos en la materia practicar la invención, y debe entenderse que otras realizaciones pueden utilizarse, y que otros cambios pueden realizarse, sin alejarse del espíritu o alcance de la presente invención. Por lo tanto, la siguiente descripción detallada no debe tomarse en un sentido limitativo, y el alcance de la presente invención se define por las reivindicaciones adjuntas.

En la siguiente descripción, se dan primero unas definiciones de algunos términos que se usan a lo largo del presente documento. A continuación, se divulgan los componentes ilustrativos de un entorno de funcionamiento ilustrativo en el que puede practicarse la invención. A continuación, se divulga un entorno de funcionamiento ilustrativo en el que puede ponerse en práctica la invención. Finalmente, se proporciona un método para detectar y eliminar los programas maliciosos.

Definiciones

Las definiciones de esta sección se aplican al presente documento, a menos que el contexto indique claramente lo contrario. La frase "el presente documento" se refiere a la memoria descriptiva, las reivindicaciones, y el resumen de esta solicitud.

"Que incluye" significa que incluye pero no limitado a. Por lo tanto, una lista que incluye a A no impide que incluya a B.

Un "paquete" se refiere a una cantidad arbitraria o seleccionable de datos que puede representarse por una secuencia de uno o más bits. Un paquete puede corresponder a una unidad de datos encontrada en cualquier capa del modelo de interconexión de sistemas abiertos (OSI), tal como un segmento, un mensaje, un paquete, un datagrama, una trama, un flujo de símbolos, o un flujo, una combinación de unidades de datos encontrada en el modelo OSI, o una unidad de datos no OSI.

"Cliente" se refiere a un proceso o conjunto de procesos que se ejecutan en uno o más dispositivos electrónicos, tal como el dispositivo informático 300 de la figura 3. Un cliente no está restringido para funcionar en una estación de trabajo; también puede ejecutarse en un servidor como un servidor de WWW, un servidor de archivos, u otro servidor, otro dispositivo informático, o distribuirse en un grupo de este tipo de dispositivos. Cuando proceda, el término "cliente" debería interpretarse, además o en lugar de la definición anterior, para ser un dispositivo o dispositivos en los que se ejecutan uno o más procesos de cliente, por ejemplo, un dispositivo informático, tal como el dispositivo informático 300, configurado para funcionar como un servidor de World Wide Web (de WWW), un dispositivo informático configurado como un router, un pasarela, una estación de trabajo, etc.

De manera similar, "servidor" se refiere a un proceso o conjunto de procesos que se ejecutan en uno o más dispositivos electrónicos, tales como el dispositivo informático 300 configurado como un servidor de WWW. Similar a un cliente, un servidor no se limita a funcionar en un dispositivo informático que está configurado para proporcionar predominantemente servicios a otros dispositivos informáticos. Más bien, también puede ejecutarse en lo que normalmente se consideraría un ordenador cliente, tal como el dispositivo informático 300 configurado como estación de trabajo del usuario, o distribuirse entre diversos dispositivos electrónicos, en los que cada dispositivo puede incluir uno o más procesos que en conjunto constituyen una aplicación de servidor. Cuando proceda, el término "servidor" debería interpretarse, además o en lugar de la definición anterior, para ser un dispositivo o dispositivos en los que se ejecutan uno o más procesos de servidor, por ejemplo, un dispositivo informático configurado para operar como un servidor de WWW, un router, una pasarela, una estación de trabajo, etc.

Un programa malicioso es cualquier procedimiento y/o software que puede usarse para acceder de manera inadecuada a un ordenador a través del correo electrónico. Los programas maliciosos incluyen lo que se conoce comúnmente como virus informáticos, pero puede incluir también otros métodos para obtener acceso de manera inapropiada a un ordenador. Por ejemplo, los virus informáticos se incluyen normalmente en un anexo de un mensaje de correo electrónico. Algunos programas maliciosos, sin embargo, están contenidos en el encabezamiento

o el cuerpo de un mensaje de correo electrónico. Por ejemplo, algunos programas maliciosos intentan desbordar las memorias intermedias asignadas para las partes o la totalidad de un encabezamiento o cuerpo de un mensaje de correo electrónico. En los bytes de datos contenidos en el desbordamiento, estos programas maliciosos a menudo contienen código ejecutable. Este código ejecutable está dispuesto de tal manera como para ejecutarse por el ordenador anfitrión. A continuación, el código ejecutable puede acceder de manera inadecuada a los datos y/o ejecutar programas no autorizados en el ordenador anfitrión.

Haciendo referencia a los dibujos, los mismos números indican partes similares en todas las figuras y en el presente documento.

Las definiciones de los términos se encuentran también a lo largo del presente documento. Estas definiciones no necesitan introducirse usando "medios" o "se refiere" al lenguaje y puede introducirse por un ejemplo y/o una función realizada. Tales definiciones se aplicarán también al presente documento, a menos que el contexto indique claramente lo contrario.

Entorno de funcionamiento ilustrativo

Las figuras 1-3 muestran unos componentes de un entorno a modo de ejemplo en el que puede ponerse en práctica la invención. No todos los componentes pueden ser necesarios para practicar la invención, y pueden hacerse variaciones en la disposición y el tipo de los componentes sin alejarse del alcance de la invención.

La figura 1 muestra las redes inalámbricas 105 y 110, las redes telefónicas 115 y 120, interconectadas a través de las pasarelas 130A-130D, respectivamente, a la red de área amplia / red de área local 200. Cada una de las pasarelas 130A-130D incluye de manera opcional un componente de cortafuegos, tales como los cortafuegos 140A-140D, respectivamente. Las letras FW en cada una de las pasarelas 130A-130D significa cortafuegos.

Las redes inalámbricas 105 y 110 transportan información y comunicaciones de voz desde y hacia los dispositivos capaces de una comunicación inalámbrica, tales como los teléfonos móviles, los teléfonos inteligentes, los buscapersonas, los walkie talkies, los dispositivos de radiofrecuencia (RF), los dispositivos de infrarrojos (IR), los CB, los dispositivos integrados que combinan uno o más de los dispositivos anteriores, y similares. Las redes inalámbricas 105 y 110 también pueden transportar información a otros dispositivos que tienen unas interfaces para conectarse a las redes inalámbricas, tal como una PDA, un Pocket PC, un ordenador portátil, los ordenadores personales, los sistemas multiprocesador, la electrónica de consumo basada en microprocesadores o programable, los PC de red, y otros dispositivos adecuadamente equipados. Las redes inalámbricas 105 y 110 pueden incluir tanto componentes inalámbricos como cableados. Por ejemplo, la red inalámbrica 110 puede incluir una torre móvil (no mostrada) que esté enlazada a una red telefónica por cable, tal como la red telefónica 115. Por lo general, la torre móvil lleva la comunicación desde y hacia los teléfonos móviles, los buscapersonas y otros dispositivos inalámbricos, y la red telefónica por cable lleva la comunicación a los teléfonos regulares, los enlaces de comunicaciones de larga distancia, y similares.

Del mismo modo las redes telefónicas 115 y 120 transportan información y comunicaciones de voz desde y hacia los dispositivos capaces de comunicaciones por cable, tales como los teléfonos regulares y los dispositivos que incluyen módems o alguna otra interfaz para comunicarse con una red telefónica. Una red telefónica, tal como una red telefónica 120, puede incluir también tanto componentes inalámbricos como cableados. Por ejemplo, una red telefónica puede incluir enlaces de microondas, enlaces por satélite, enlaces de radio, y otros enlaces inalámbricos para interconectar las redes de cable.

Las pasarelas 130A-130D interconectan las redes inalámbricas 105 y 110 y las redes telefónicas 115 y 120 a una WAN/LAN 200. Una pasarela, tal como la pasarela 130A, transmite datos entre redes, tal como la red inalámbrica 105 y la WAN/LAN 200. En la transmisión de datos, la pasarela puede trasladar los datos a un formato adecuado para la red receptora. Por ejemplo, un usuario que usa un dispositivo inalámbrico puede comenzar su búsqueda de Internet llamando a un número determinado, sintonizar a una frecuencia particular, o seleccionar una función de navegación del dispositivo. Tras la recepción de la información dirigida o formateada de manera apropiada, la red inalámbrica 105 puede configurarse para enviar datos entre el dispositivo inalámbrico y la pasarela 130A. La pasarela 130A puede trasladar las peticiones de las páginas web desde el dispositivo inalámbrico a unos mensajes de protocolo de transferencia de hipertexto (HTTP) que pueden a continuación enviarse a la WAN/LAN 200. A continuación, la pasarela 130A puede trasladar las respuestas a este tipo de mensajes en una forma compatible con el dispositivo inalámbrico. La pasarela 130A puede transformar también otros mensajes enviados desde los dispositivos inalámbricos en un mensaje adecuado para la WAN/LAN 200, tal como un correo electrónico, una comunicación de voz, unas bases de datos de contactos, calendarios, citas, y otros mensajes.

Antes o después de la traslación de los datos en cualquier dirección, la pasarela puede pasar los datos a través de un cortafuegos, tal como, por ejemplo, el cortafuegos 140A, para seguridad, filtrar, o por otras razones. Un cortafuegos, tal como el cortafuegos 140A, puede incluir o enviar mensajes a un detector de programas maliciosos. Los cortafuegos y su funcionamiento en el contexto de las realizaciones de la invención se describen con más detalle junto con las figuras 4-6. Brevemente, una pasarela puede pasar datos a través de un cortafuegos para

determinar si debería reenviar los datos a una red receptora. El cortafuegos puede pasar algunos datos, tal como los mensajes de correo electrónico, a través de un detector de programas maliciosos que puede detectar y eliminar los programas maliciosos de los datos. Si los datos contienen un programa malicioso, el cortafuegos puede impedir que los datos pasen a través de la pasarela.

En otras realizaciones de la invención, los detectores de programas maliciosos están localizados en unos componentes separados de las pasarelas y/o de los cortafuegos. Por ejemplo, en algunas realizaciones de la invención, un detector de programas maliciosos puede estar incluido dentro de un router en el interior de una red inalámbrica, tal como la red inalámbrica 105, que recibe mensajes dirigidos a y procedentes de la red inalámbrica, tal como la red inalámbrica 105. Esto puede negar o hacer redundante un detector de programas maliciosos en una pasarela entre redes, tal como la pasarela 130A. Idealmente, los detectores de programas maliciosos se colocan en localizaciones de entrada a una red de manera que todos los dispositivos dentro de la red están protegidos de los programas maliciosos. Los detectores de programas maliciosos pueden, sin embargo, localizarse en otros lugares dentro de una red, integrados con otros dispositivos tales como switches, hubs, routers, servidores, gestores de tráfico, etc., o separados de dichos dispositivos.

En otra realización de la invención, un detector de programas maliciosos es accesible desde un dispositivo que busca proporcionar protección contra los programas maliciosos, tal como una pasarela. Accesible, en este contexto, puede significar que el protector contra los programas maliciosos se localiza físicamente en el servidor o en el dispositivo informático que implementa la pasarela o que el detector de programas maliciosos está en otro servidor o dispositivo informático accesible desde la pasarela. En esta realización, una pasarela, puede acceder al detector de programas maliciosos a través de una interfaz de programación de aplicaciones (API). Idealmente, un dispositivo que busca protección contra los programas maliciosos dirige todos los mensajes a través de un detector de programas maliciosos asociado de manera que el detector de programas maliciosos está "lógicamente" entre las redes que interconecta el dispositivo. En algunos casos, un dispositivo no puede enviar todos los mensajes a través de un detector de programas maliciosos. Por ejemplo, un detector de programas maliciosos puede desactivarse o ciertos mensajes pueden designarse explícita o implícitamente para evitar el detector de programas maliciosos.

Por lo general, la WAN/LAN 200 transmite información entre dispositivos informáticos, como se describe con más detalle en relación con la figura 2. Un ejemplo de una WAN es la Internet que conecta a millones de ordenadores a través de un anfitrión de pasarelas, routers, switches, hubs, y similares. Un ejemplo de una LAN es una red que se usa para conectar ordenadores en una sola oficina. Una WAN puede usarse para conectar múltiples LAN.

Se reconocerá que las distinciones entre redes WAN/LAN, redes telefónicas y redes inalámbricas se están difuminando. Es decir, cada uno de estos tipos de redes puede incluir una o más partes que lógicamente pertenecerían a uno o más de los otros tipos de redes. Por ejemplo, la WAN/LAN 200 puede incluir algunas líneas telefónicas analógicas o digitales para transmitir información entre unos dispositivos informáticos. La red telefónica 120 puede incluir componentes inalámbricos y componentes basados en paquetes, tal como la voz sobre IP. La red inalámbrica 105 puede incluir componentes cableados y/o componentes basados en paquetes. Red significa una WAN/LAN, una red telefónica, una red inalámbrica, o cualquier combinación de las mismas.

La figura 2 muestra una pluralidad de redes de área local ("LAN") 220 y una red de área amplia ("WAN") 230 interconectadas por routers 210. Los routers 210 son dispositivos intermediarios en una red de comunicaciones que agilizan la entrega de paquetes. En una sola red que une muchos ordenadores a través de una malla de conexiones posibles, un router recibe unos paquetes transmitidos y los reenvía a sus destinos correctos a través de las rutas disponibles. En un conjunto interconectado de redes LAN, que incluyen a las basadas en diferentes arquitecturas y protocolos, un router actúa como un enlace entre las redes LAN, permitiendo que los paquetes se envíen de una a otra. Un router puede implementarse usando hardware de propósito especial, un dispositivo informático que ejecute el software apropiado, tal como el dispositivo informático 300 como se describe junto con la figura 3, o a través de cualquier combinación de los anteriores.

Los enlaces de comunicaciones en las redes LAN incluyen normalmente par trenzado, fibra óptica o cable coaxial, mientras que los enlaces de comunicaciones entre redes pueden utilizar las líneas telefónicas analógicas, las líneas digitales dedicadas completas o fraccionadas incluyendo T1, T2, T3 y T4, las redes digitales de servicios integrados (RDSI), las líneas de abonado digitales (DSL), los enlaces inalámbricos, u otros enlaces de comunicaciones conocidos por los expertos en la materia. Además, los ordenadores, tal como el ordenador remoto 240, y otros dispositivos electrónicos relacionados pueden conectarse de manera remota a cualquiera de las redes LAN 220 o WAN 230 a través de un módem y de un enlace de teléfono temporal. El número de las WAN, LAN y routers en la figura 2 puede aumentarse o disminuirse de manera arbitraria sin alejarse del alcance de esta invención.

Por lo tanto, se apreciará que la propia Internet puede estar formada por un gran número de este tipo de redes interconectadas, ordenadores y routers. En general, el término "Internet" se refiere a la recopilación mundial de redes, pasarelas, routers y ordenadores que utilizan el protocolo de control de transmisión/protocolo de Internet ("TCP/IP") de la suite de protocolos para comunicarse entre sí. En el corazón de la Internet está una red troncal de líneas de comunicación y datos de alta velocidad entre los principales nodos u ordenadores principales, incluyendo miles de sistemas informáticos comerciales, gubernamentales, educativos y otros, que encaminan datos y paquetes.

Una realización de la invención puede practicarse a través de la Internet sin alejarse del alcance de la invención.

Los medios usados para transmitir información en los enlaces de comunicaciones como se ha descrito anteriormente ilustra un tipo de medios legibles por ordenador, es decir, los medios de comunicación. En general, los medios legibles por ordenador incluyen cualquier medio que pueda accederse mediante un dispositivo informático. Los medios legibles por ordenador pueden incluir medios de almacenamiento informáticos, medios de comunicación, o cualquier combinación de los mismos.

Los medios de comunicación incorporan normalmente unas instrucciones legibles por ordenador, unas estructuras de datos, unos módulos de programa, u otros datos en una señal de datos modulada tal como una onda portadora u otro mecanismo de transporte e incluyen cualquier medio de entrega de información. El término "señal de datos modulada" significa una señal que tiene una o más de sus características fijadas o cambiadas de una manera tal como para codificar información en la señal. A modo de ejemplo, los medios de comunicación incluyen medios cableados tales como par trenzado, cable coaxial, fibra óptica, guías de onda, y otros medios cableados y medios inalámbricos tales como medios acústicos, de RF, infrarrojos y otros medios inalámbricos.

La Internet ha visto recientemente un crecimiento explosivo en virtud de su capacidad de enlazar los ordenadores localizados en todo el mundo. A medida que la Internet ha crecido, también lo ha hecho la WWW. En general, la WWW es el conjunto total de documentos de hipertexto interenlazados que residen en los servidores de HTTP (protocolo de transporte de hipertexto) en todo el mundo. Los documentos en la WWW, llamados páginas o páginas web, se escriben normalmente en HTML (lenguaje de marcado de hipertexto) o algún otro lenguaje de marcas, identificado por las URL (localizador de recursos uniforme) que especifican la máquina y el nombre de ruta específicos, mediante los cuales puede accederse a un archivo, y transmitidas desde el servidor al usuario final usando HTTP. Los códigos, denominados etiquetas, integrados en un documento HTML asocian palabras e imágenes específicas en el documento con las URL de manera que un usuario pueda acceder a otro archivo, que puede estar, literalmente, al otro lado del mundo, con solo pulsar una tecla o un clic del ratón. Estos archivos pueden contener texto (en varias fuentes y estilos), imágenes gráficas, archivos de películas, clips multimedia, y sonidos, así como applets de JAVA, controles ActiveX, u otros programas de software integrados que se ejecutan cuando el usuario los activa. Un usuario que visita una página web también puede ser capaz de descargar archivos desde un sitio FTP y enviar paquetes a otros usuarios a través de correo electrónico usando enlaces en la página Web.

Un dispositivo informático que puede proporcionar un sitio de WWW se describe en más detalle junto con la figura 3. Cuando se usa para proporcionar un sitio de WWW, un dispositivo informático de este tipo se denomina normalmente como un servidor de WWW. Un servidor de WWW es un dispositivo informático conectado a la Internet que tiene unos servicios de almacenamiento para almacenar documentos de hipertexto de un sitio de WWW y que ejecuta el software de administración para manejar las solicitudes de los documentos de hipertexto almacenados. Un documento de hipertexto normalmente incluye una serie de hiperenlaces, es decir, resaltado partes de texto que enlazan el documento a otro documento de hipertexto posiblemente almacenado en un sitio de WWW en otro lugar en la Internet. Cada hiperenlace se asocia con una URL que proporciona la localización del documento enlazado en un servidor conectado a la Internet y que describe el documento. Por lo tanto, cada vez que se recupera un documento de hipertexto desde cualquier servidor de WWW, el documento se considera que se recupera desde la WWW. Como es sabido por los expertos en la materia, un servidor de WWW puede incluir también servicios para almacenar y transmitir programas de aplicación, tales como los programas de aplicación escritos en el lenguaje de programación JAVA de Sun Microsystems, para su ejecución en un ordenador remoto. Del mismo modo, un servidor de WWW puede incluir también servicios para la ejecución de scripts y otros programas de aplicación en el propio servidor de WWW.

Un usuario puede recuperar documentos de hipertexto desde la WWW a través de un programa de aplicación de navegador de WWW localizado en un dispositivo cableado o inalámbrico. Un navegador de WWW, tal como NAVIGATOR® de Netscape o INTERNET EXPLORER® de Microsoft, es un programa de aplicación de software para proporcionar una interfaz gráfica de usuario a la WWW. Tras una solicitud del usuario a través del navegador de WWW, el navegador de WWW accede y recupera el documento hipertexto deseado del servidor de WWW apropiado usando la URL del documento y HTTP. HTTP es un protocolo de más alto nivel que TCP/IP y está diseñado específicamente para los requisitos de la WWW. HTTP se usa para llevar las peticiones de un navegador a un servidor Web y para transportar las páginas desde los servidores Web de vuelta al navegador o cliente solicitante. El navegador de WWW puede recuperar también los programas de aplicación del servidor de WWW, tal como los applets de JAVA, para su ejecución en un equipo cliente.

La figura 3 muestra un dispositivo informático. Tal dispositivo puede usarse, por ejemplo, como un servidor, una estación de trabajo, un dispositivo de red, un router, un bridge, un cortafuegos, un detector de programas maliciosos, una pasarela, y/o como un dispositivo de gestión del tráfico. Cuando se usa para proporcionar un sitio de WWW, el dispositivo informático 300 transmite las páginas de WWW al programa aplicación de navegador de WWW que se ejecuta solicitando unos dispositivos para realizar este proceso. Por ejemplo, el dispositivo informático 300 puede transmitir páginas y formularios para recibir información acerca de un usuario, tal como una dirección, un número de teléfono, una información de facturación, un número de tarjeta de crédito, etc. Por otra parte, el dispositivo informático 300 puede transmitir las páginas de WWW a un dispositivo que solicita que se permita a un consumidor

participar en un sitio de WWW. Las transacciones pueden tener lugar a través de la Internet, la WAN/LAN 100, o alguna otra red de comunicaciones conocida por los expertos en la materia.

Se apreciará que el dispositivo informático 300 puede incluir muchos más componentes que los mostrados en la figura 3. Sin embargo, los componentes mostrados son suficientes para divulgar un entorno ilustrativo para la práctica de la presente invención. Como se muestra en la figura 3, el dispositivo informático 300 puede estar conectado a la WAN/LAN 200, o a otra red de comunicaciones, a través de la unidad de interfaz de red 310. La unidad de interfaz de red 310 incluye la circuitería necesaria para conectar el dispositivo informático 300 a la WAN/LAN 200, y está construido para usarse con diversos protocolos de comunicación, incluyendo el protocolo TCP/IP. Normalmente, la unidad de interfaz de red 310 es una tarjeta contenida dentro del dispositivo informático 300.

El dispositivo informático 300 incluye también una unidad de procesamiento 312, un adaptador de pantalla de vídeo 314, y una memoria masiva, todos conectados a través del bus 322. La memoria masiva, en general, incluye una memoria de acceso aleatorio ("RAM") 316, una memoria de solo lectura ("ROM") 332, y uno o más dispositivos de almacenamiento masivo permanentes, tal como la unidad de disco duro 328, una unidad de cinta (no mostrada), una unidad óptica 326, tal como una unidad de CD-ROM/DVDROM, y/o una unidad de disco flexible (no mostrada). La memoria masiva almacena el sistema operativo 320 para controlar el funcionamiento del dispositivo informático 300. Se apreciará que este componente puede comprender un sistema operativo de propósito general, que incluye, por ejemplo, UNIX, LINUX, o uno producido por Microsoft Corporation de Redmond, Washington. También se proporciona un sistema de entrada/salida básico ("BIOS") 318 para controlar el funcionamiento de bajo nivel del dispositivo informático 300.

La memoria masiva como ha descrito anteriormente ilustra otros tipos de medios legibles por ordenador, es decir, unos medios de almacenamiento informáticos. Los medios de almacenamiento informáticos pueden incluir medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Ejemplos de medios de almacenamiento informático incluyen RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos digitales versátiles (DVD) u otro almacenamiento óptico, casetes magnéticos, cintas magnéticas, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y que pueda accederse por un dispositivo informático.

La memoria masiva también puede almacenar un código de programa y los datos para proporcionar un sitio de WWW. Más específicamente, la memoria masiva puede almacenar aplicaciones que incluyan software de propósito especial 330, y otros programas 334. El software de propósito especial 330 puede incluir un programa de aplicación de servidor de WWW que incluya instrucciones ejecutables por ordenador que, cuando se ejecutan por el dispositivo informático 300, generan pantallas de navegador de WWW, incluyendo la realización de la lógica descrita anteriormente. El dispositivo informático 300 puede incluir una máquina virtual de JAVA, una aplicación manejadora de SMTP para transmitir y recibir correo electrónico, una aplicación manejadora de HTTP para recibir y manejar las solicitudes HTTP, los applets de JAVA para su transmisión a un navegador de WWW que se ejecutan en un ordenador cliente, y una aplicación manejadora de HTTPS para manejar las conexiones seguras. La aplicación manejadora de HTTPS puede usarse para la comunicación con una aplicación de seguridad externa para enviar y recibir información sensible, tal como la información de una tarjeta de crédito, de una manera segura.

El dispositivo informático 300 puede comprender también una interfaz de entrada/salida 324 para comunicar con los dispositivos externos, tal como un ratón, un teclado, un escáner, u otros dispositivos de entrada que no se muestran en la figura 3. En algunas realizaciones de la invención, el dispositivo informático no incluye componentes de entrada/salida de usuario. Por ejemplo, el dispositivo informático 300 puede o no estar conectado a un monitor. Además, el dispositivo informático 300 puede o no tener un adaptador de pantalla de vídeo 314 o un interfaz de entrada/salida 324. Por ejemplo, el dispositivo informático 300 puede implementar un aparato de red, tal como un router, una pasarela, un dispositivo de gestión del tráfico, etc., es decir, conectado a una red y que no necesita estar conectado directamente a los dispositivos de entrada/salida de usuario. Un dispositivo de este tipo puede ser accesible, por ejemplo, en una red.

El dispositivo informático 300 puede comprender además unos servicios adicionales de almacenamiento masivo tales como una unidad óptica 326 y una unidad de disco duro 328. La unidad de disco duro 328 se utiliza por el dispositivo informático 300 para almacenar, entre otras cosas, programas de aplicaciones, bases de datos, y datos de programas usados por una aplicación de servidor de WWW que se ejecuta en el dispositivo informático 300. Una aplicación de servidor de WWW puede almacenarse como un software de propósito especial 330 y/u otros programas 334. Además, pueden almacenarse también las bases de datos de clientes, las bases de datos de productos, las bases de datos de imágenes, y las bases de datos relacionales en la memoria masiva o en la RAM 316.

Como se reconocerá a continuación a partir de la siguiente exposición, los aspectos de la invención pueden realizarse en los routers 210, en el dispositivo informático 300, en una pasarela, en un cortafuegos, en otros

dispositivos, o en alguna combinación de los anteriores. Por ejemplo, las etapas de programación que protegen contra los programas maliciosos pueden estar contenidas en un software de propósito especial 330 y/o en otros programas 334.

Ejemplo de configuración del sistema para la protección contra programa maliciosos

La figura 4 ilustra un ejemplo de entorno en el que un sistema funciona para proporcionar protección contra los programas maliciosos en una red, de acuerdo con una realización de la invención. El sistema incluye una red externa 405, un cortafuegos 500, un aparato de red 415, una estación de trabajo 420, un servidor de archivos 425, un servidor de correo 430, un dispositivo móvil 435, un servidor de aplicaciones 440, un dispositivo telefónico 445, y una red 450. La red 450 acopla el cortafuegos 500 al aparato de red 415, a la estación de trabajo 420, al servidor de archivos 425, al servidor de correo 430, al dispositivo móvil 435, al servidor de aplicaciones 440, y al dispositivo telefónico 445. El cortafuegos 500 acopla la red 450 a la red externa 405.

El aparato de red 415, la estación de trabajo 420, el servidor de archivos 425, el servidor de correo 430, el dispositivo móvil 435, el servidor de aplicaciones 440, y el dispositivo telefónico 445 son dispositivos capaces de conectarse con la red 450. El conjunto de tales dispositivos puede incluir dispositivos que se conectan normalmente usando unos medios de comunicaciones cableados tales como los ordenadores personales, los sistemas multiprocesador, las electrónicas de consumo basadas en microprocesadores o programables, los PC de red, y similares. El conjunto de tales dispositivos puede incluir también dispositivos que se conectan normalmente usando unos medios de comunicaciones inalámbricas tales como los teléfonos móviles, los teléfonos inteligentes, los buscapersonas, los walkie talkies, los dispositivos de radiofrecuencia (RF), los dispositivos de infrarrojos (IR), los CB, los dispositivos integrados que combinan uno o más de los dispositivos anteriores, y similares. Algunos dispositivos pueden ser capaces de conectarse a la red 450 usando unos medios de comunicaciones cableadas o inalámbricas, tales como una PDA, un Pocket PC, un ordenador portátil u otro dispositivo mencionado anteriormente que está equipado para usar unos medios de comunicaciones cableados y/o inalámbricos. Un dispositivo a modo de ejemplo que puede implementar cualquiera de los dispositivos anteriores es el dispositivo informático 300 de la figura 3 configurado con el hardware y/o software apropiados.

El aparato de red 415 puede ser, por ejemplo, un router, un switch, o algún otro dispositivo de red. La estación de trabajo 420 puede ser un ordenador usado por un usuario para acceder a otros ordenadores y recursos accesibles a través de la red 450, incluyendo la red externa 405. El servidor de archivos 425 puede, por ejemplo, proporcionar acceso a dispositivos de almacenamiento masivo. El servidor de correo 430 puede almacenar y proporcionar acceso a los mensajes de correo electrónico. El dispositivo móvil 435 puede ser un teléfono móvil, una PDA, un ordenador portátil o algún otro dispositivo usado por un usuario para acceder a los recursos alcanzables a través de la red 450. El servidor de aplicaciones 440 puede almacenar y proporcionar acceso a las aplicaciones, tales como las aplicaciones de bases de datos, las aplicaciones de contabilidad, etc. El dispositivo telefónico 445 puede proporcionar medios para transmitir voz, fax, y otros mensajes a través de la red 450. Cada uno de estos dispositivos puede representar muchos otros dispositivos capaces de conectarse con la red 450 sin alejarse del alcance de la invención.

La red exterior 405 y la red 450 son redes como se han definido anteriormente en el presente documento. La red exterior puede ser, por ejemplo, la Internet o alguna otra WAN/LAN.

El cortafuegos 500 proporciona un camino para que los mensajes de la red exterior 405 alcancen la red 450. El cortafuegos 500 puede o no puede proporcionar el único camino para ese tipo de mensajes. Además, puede haber otros dispositivos informáticos (no mostrados) en el camino entre la red exterior 405 y la red 450 sin alejarse del alcance de la invención. El cortafuegos puede incluirse en una pasarela, un router, un switch, u otro dispositivo informático o simplemente ser accesible a tales dispositivos.

El cortafuegos 500 puede proporcionar protección contra los programas maliciosos a los dispositivos acoplados a la red 450 incluyendo y/o accediendo a un detector de programas maliciosos (no mostrado) como se describe en más detalle junto con la figura 5. El cortafuegos 500 puede estar configurado para enviar ciertos tipos de mensajes a través de un detector de programas maliciosos. Por ejemplo, el cortafuegos 500 puede configurarse para realizar el procesamiento normal en los datos no de email mientras pasan todos los mensajes de correo electrónico a través de un detector de programas maliciosos.

Ejemplo de detector de programas maliciosos

La figura 5 ilustra los componentes de un cortafuegos que pueden funcionar para proporcionar protección contra los programas maliciosos, de acuerdo con una realización de la invención. Los componentes del cortafuegos 500 incluyen un escucha de mensajes 505, un detector de programas maliciosos 510, un componente de salida 545, y otros componentes de cortafuegos 550. El detector de programas maliciosos 510 incluye una cola de mensajes 515, un filtro de contenidos 520, un componente de descompresión 525, un componente de exploración 530, un componente de cuarentena 535, y un eliminador de programas maliciosos 540. También se muestra el agente de transporte de mensajes 555.

El cortafuegos 500 puede recibir muchos tipos de mensajes enviados entre dispositivos acoplados a la red 450 y a la red exterior 405 de la figura 4. Algunos mensajes pueden estar relacionados con el tráfico de WWW o los datos transferidos entre dos equipos que participan en una comunicación, mientras que otros mensajes pueden estar relacionados con un correo electrónico. El escucha de mensajes 505 está a la escucha de un mensaje y, tras recibir un mensaje adecuado, tal como un correo electrónico o un archivo, envía el mensaje al detector de programas maliciosos 510 para explorar en busca de programas maliciosos. Algunos mensajes pueden ser inapropiados para la detección de programas maliciosos. Estos mensajes se pasan por el escucha de mensajes 505 a otros componentes de cortafuegos 550.

Cuando se procesan los mensajes de correo electrónico, un detector de programas maliciosos 510 proporciona protección contra los programas maliciosos, en parte, explorando y verificando los campos de un mensaje de correo electrónico. Un mensaje de correo electrónico incluye normalmente una cabecera (que puede incluir ciertos campos), un cuerpo (que por lo general contiene el texto de un correo electrónico), y uno o más anexos opcionales. Como se ha descrito anteriormente, algunos programas maliciosos se confeccionan para desbordar las memorias intermedias en un encabezamiento o en un cuerpo. Un detector de programas maliciosos 510 puede examinar las longitudes de los campos de un mensaje de correo electrónico para determinar si son más largas de lo que deberían ser. Pudiéndose definir "más largos de lo que deberían ser" por las normas, las especificaciones del servidor de correo, o seleccionarse por un administrador del cortafuegos. Si un mensaje de correo electrónico incluye cualquier campo que sea más largo de lo que debería ser, el mensaje puede enviarse al componente de cuarentena 535 como se describe en más detalle a continuación.

El detector de programas maliciosos 510 puede utilizar un software de protección contra programas maliciosos de muchos vendedores. Por ejemplo, un cliente puede ejecutar el detector de programas maliciosos 510 que se conecta a un servidor de actualizaciones de protecciones antivirus. Periódicamente, el cliente puede sondear un servidor asociado con cada proveedor y buscar una indicación para ver si está disponible una actualización de protecciones contra programas maliciosos. Si existe una actualización disponible, el cliente puede recuperar de manera automática la actualización y comprobar la autenticidad. Por ejemplo, la actualización puede incluir una firma digital que incorpora un resumen criptográfico de los archivos enviados. La firma digital puede verificarse para asegurarse de que los archivos provienen de un remitente de confianza, y el resumen criptográfico puede usarse para asegurarse de que ninguno de los archivos se ha modificado en el tránsito. Otro proceso puede desempaquetar la actualización, detener la ejecución de un detector de programas maliciosos 510, instalar la actualización y reiniciar el detector de programas maliciosos 510.

El detector de programas maliciosos 510 puede configurarse para sondear en búsqueda de actualizaciones de protección contra programas maliciosos personalizadas creadas por, por ejemplo, un equipo de tecnología de la información. Este proceso puede ejecutarse de una manera similar a la del sondeo para las actualizaciones del proveedor descritas anteriormente.

Además, o en lugar de los sondeos, puede forzarse que un detector de programas maliciosos 510 busque las actualizaciones. Es decir, un cliente puede ejecutar el detector de programas maliciosos 510 que escucha para buscar las actualizaciones de los servidores de actualización de protección contra programas maliciosos. Para actualizar la protección contra programas maliciosos que se ejecuta en el cortafuegos 410, tales servidores pueden abrir una conexión con el cliente y enviar las actualizaciones de protección contra programas maliciosos. Un servidor que envía una actualización puede necesitar autenticarse a sí mismo. Además, el cliente puede comprobar la actualización enviada para asegurarse de que los archivos no han cambiado en el tránsito usando un resumen criptográfico como se ha descrito anteriormente.

A continuación, se explicarán los componentes de un detector de programas maliciosos 510. Tras la recepción de un mensaje para explorar un programa malicioso, un detector de programas maliciosos 510 almacena el mensaje en la cola de mensajes 515. El filtro de contenidos 520 procesa los mensajes de la cola de mensajes 515 para determinar los métodos de encapsulación que se han aplicado al mensaje antes de su entrada en el sistema. Por ejemplo, un mensaje puede encapsularse usando extensiones multipropósito de correo de internet (MIME), Base 64 y uuencode. El filtro de contenidos 520 también puede quitar anexos del correo electrónico con el fin de examinarles más de cerca. Un mensaje o anexo (en adelante en el presente documento, denominado cada uno como un "mensaje") que se emite desde el filtro de contenidos 520 se procesa a continuación por el componente de descompresión 525.

El componente de descompresión 525 determina si un mensaje está comprimido. Si el mensaje no está comprimido, los bits que componen el mensaje se envían en serie al componente de exploración 530. Si el mensaje está comprimido, el componente de descompresión 525 puede descomprimir el mensaje una o más veces antes de enviarlo al componente de exploración 530. Las descompresiones pueden estar hechas de una manera anidada si un mensaje se ha comprimido varias veces. Por ejemplo, un conjunto de archivos incluido en un mensaje puede primero comprimirse y a continuación empaquetarse con la orden "tar" de UNIX. Después de desempaquetar un archivo, el componente de descompresión 525 puede determinar que el archivo desempaquetado se ha comprimido anteriormente mediante un software de compresión como WinZip. Para obtener el archivo(s) descomprimido, el componente de descompresión 525 puede, a continuación, descomprimir el archivo desempaquetado. Puede haber

más de dos niveles de compresión que el componente de descompresión 525 puede descomprimir para obtener un archivo(s) descomprimido.

El componente de exploración 530 recibe los mensajes descomprimidos y los mensajes que no se han comprimido del componente de descompresión 525. El componente de exploración 530 incluye un software que explora el mensaje en busca de programas maliciosos. El componente de exploración 530 puede explorar los mensajes usando un software de protección contra programas maliciosos de muchos proveedores. Por ejemplo, el componente de exploración 530 puede pasar un mensaje a través de un software de proveedores de software de protección antivirus tales como Norton, McAfee, Network Associates, Inc., Kaspersky Lab, Sophos, etc. Además, el componente de exploración 530 puede aplicar algoritmos propietarios o definidos por el usuario al mensaje a explorar en busca de programas maliciosos. Por ejemplo, puede usarse una prueba de algoritmo definido por el usuario para los desbordamientos de memorias intermedias para detectar programa maliciosos.

El componente de exploración 530 puede incluir también un mecanismo interno que crea firmas digitales de los mensajes y contenidos que un administrador quiere evitar que se distribuyan fuera de una red. Por ejemplo, haciendo referencia a la figura 4, un usuario en uno de los dispositivos informáticos puede crear un mensaje o tratar de reenviar un mensaje que sea confidencial fuera de la red 405. El componente de exploración 530 puede examinar cada mensaje que recibe (incluidos los mensajes salientes) en busca de tales firmas digitales. Cuando se encuentra una firma digital que indica que el mensaje no debería reenviarse, el componente de exploración 530 puede reenviar el mensaje al componente de cuarentena junto con la información acerca de quién ha enviado el mensaje, el momento en que se ha enviado el mensaje, y otros datos relacionados con el mensaje.

Cuando se determina que un mensaje tiene un programa malicioso, el mensaje se envía al componente de cuarentena 535. El componente de cuarentena 535 puede almacenar los mensajes que contienen programas maliciosos para un examen adicional, por ejemplo, por un administrador de red. Además, el componente de cuarentena 535 puede enviar un mensaje infectado al eliminador de programas maliciosos 540 para eliminar un programa malicioso.

Cuando el componente de exploración 530 no encuentra un programa malicioso en un mensaje, el mensaje puede reenviarse al componente de salida 545. El componente de salida 545 reenvía un mensaje hacia su destinatario. El componente de salida 545 puede ser hardware y/o software que funcionen para reenviar mensajes a través de una red. Por ejemplo, el componente de salida 545 puede incluir una interfaz de red tal como una unidad de interfaz de red 310.

El eliminador de programas maliciosos 540 puede eliminar los programas maliciosos de un mensaje. Algunos programas maliciosos pueden eliminarse de un mensaje después de la detección dando un mensaje de limpieza. El mensaje limpio, ahora libre de programa maliciosos, puede a continuación enviarse a su destinatario. Después de limpiar un mensaje, el eliminador de programas maliciosos puede reenviar el mensaje al componente de salida 545. Si el eliminador de programas maliciosos no puede eliminar un programa malicioso, puede enviar de nuevo el mensaje al componente de cuarentena 535.

Un cortafuegos puede realizar otras tareas además de pasar mensajes a un detector de programas maliciosos. Por ejemplo, un cortafuegos puede bloquear los mensajes hacia o desde determinadas direcciones. Tales otras tareas pueden realizarse por otros componentes de cortafuegos 550. Cuando otros componentes de cortafuegos 550 determinan que un mensaje debería pasar a través del cortafuegos 500, otros componentes de cortafuegos 550 reenvían el mensaje al componente de salida 545.

El agente de transporte de mensajes 555 es un dispositivo informático que recibe correo electrónico. Los dispositivos de recepción de correo electrónico incluyen los servidores de correo. Ejemplos de servidores de correo incluyen Microsoft Exchange, Q Mail, LotusNotes, etc. Haciendo referencia a la figura 4, el cortafuegos 500 puede reenviar un mensaje al servidor de correo 430.

Método ilustrativo de explorar en busca de programa maliciosos

La figura 6 ilustra un diagrama de flujo para detectar programas maliciosos, de acuerdo con una realización de la invención. El proceso comienza en el bloque 605 cuando un escucha, tal como el escucha de mensajes 505 de la figura 5, está listo para recibir un mensaje.

En el bloque 610, se recibe el mensaje por un escucha. El escucha determina si el mensaje debería explorarse en busca de programas maliciosos. Si los mensajes se exploran en busca de programas maliciosos, el proceso continúa en el bloque 615; de lo contrario otro procesamiento (no mostrado) puede realizarse en el mensaje. Por ejemplo, haciendo referencia a la figura 5, se recibe un mensaje que incluye un mensaje de correo electrónico por el escucha de mensajes 505. El escucha de mensajes 505 determina que el mensaje debería explorarse en busca de programas maliciosos y envía el mensaje a la cola de mensajes 515.

Si es necesario, en el bloque 615 el mensaje se desencapsula. Un mensaje puede desencapsularse de muchas

maneras, incluyendo MIME, Base 64, y uuencode. Para recuperar el mensaje, el mensaje puede estar sin encapsular. Por ejemplo, haciendo referencia a la figura 5, el mensaje de correo electrónico puede incluir un anexo que se codifica usando MIME. El filtro de contenidos 520 puede desencapsular el anexo. Después del bloque 615, el proceso continúa en el bloque 620.

En el bloque 620, el mensaje y/o su anexo, si tiene alguno, pueden descomprimirse una o más veces. Por ejemplo, haciendo referencia a la figura 5, un mensaje de correo electrónico puede incluir un anexo que se ha comprimido mediante WinZip. El componente de descompresión 525 puede determinar el algoritmo de compresión usado y a continuación descomprimir el anexo. Después del bloque 620, el proceso continúa en el bloque 625.

En el bloque 625, se explora un mensaje en busca de programas maliciosos. El mensaje puede explorarse usando un software de detección de programas maliciosos convencional y/o un software de detección de programas maliciosos propietario o definido por el usuario. Por ejemplo, haciendo referencia a la figura 5, pueden explorarse los campos de cabecera, cuerpo, y anexo de un mensaje de correo electrónico para determinar si la longitud es menor que o igual que la máxima de tales campos. Además, los anexos de un correo electrónico, si los hay, pueden pasarse a través de un software de detección de virus de diversos proveedores para determinar si incluyen algún programa malicioso. Después del bloque 625, el proceso continúa en el bloque 630.

En el bloque 630, se realiza una determinación en cuanto a si la exploración ha detectado algún programa malicioso. Si se encuentran programas maliciosos, el proceso continúa en el bloque 635; de lo contrario el proceso continúa en el bloque 640.

En el bloque 635, un mensaje se pone en cuarentena y, de manera opcional, se eliminan uno o más programas maliciosos. Cuarentena puede significar que el mensaje se almacena junto con otra información sobre el mensaje, tal como quién ha enviado el mensaje, a quién se ha dirigido, y cuando ha llegado el mensaje. Esto puede hacerse para un examen o análisis posterior. Como alternativa, en cuarentena puede significar que se descarta el mensaje. Cuando los programas maliciosos se eliminan de un mensaje, el procesamiento puede continuar en el bloque 640; de lo contrario, el procesamiento termina para un mensaje específico y puede explorarse otro mensaje en busca de programas maliciosos. Por ejemplo, haciendo referencia a la figura 5, el componente de cuarentena recibe un correo electrónico que incluye programas maliciosos y almacena el correo electrónico para un examen adicional.

En el bloque 640, se reenvía un mensaje hacia su destinatario. El mensaje puede ser un mensaje original recibido por un detector de programas maliciosos o puede ser un mensaje del que se han eliminado programas maliciosos. Por ejemplo, haciendo referencia a la figura 5, el componente de salida 545 reenvía un mensaje al agente de transporte de mensajes 555.

En el bloque 645, el procesamiento termina. En este punto, se ha explorado un mensaje en busca de programas maliciosos. Si se ha encapsulado cualquier parte del mensaje, el mensaje se ha desencapsulado. Si el mensaje se comprime una o más veces, el mensaje se ha descomprimido una o más veces. Se ha producido una exploración en busca de programas maliciosos en el mensaje. Si se han encontrado programas maliciosos se han puesto en cuarentena y/o de manera opcional se han eliminado del mensaje. A continuación, el mensaje o mensaje limpio se ha reenviado hacia el destinatario. El proceso resumido anteriormente puede repetirse para cada mensaje recibido.

Las diversas realizaciones de la invención pueden implementarse como una secuencia de etapas implementadas en ordenador o módulos de programa que se ejecutan en un sistema informático y/o como circuitos lógicos de máquina interconectados o módulos de circuito dentro del sistema informático. La implementación es una cuestión de elección que depende de los requisitos de rendimiento del sistema informático que implementa la invención. A la luz de esta divulgación, se reconocerá por un experto en la materia que las funciones y el funcionamiento de las diversas realizaciones divulgadas pueden implementarse en software, en firmware, en lógica digital de propósito especial, o cualquier combinación de los mismos sin desviarse del alcance de la presente invención.

REIVINDICACIONES

1. Un sistema (500) para proporcionar protección a los dispositivos conectados a una red, que comprende:

un componente de exploración (530) adaptado para determinar si un mensaje incluye un programa malicioso; y
un componente de cuarentena (535) acoplado al componente de exploración y adaptado para retener el mensaje cuando el mensaje incluye un programa malicioso; estando el sistema **caracterizado por que**:

el componente de exploración está adaptado además para:

examinar en cada mensaje que se recibe si hay una firma digital que indique que no debería reenviarse el mensaje examinado; y
reenviar el mensaje examinado al componente de cuarentena cuando se encuentra una firma digital.

2. El sistema de la reivindicación 1, en el que el componente de exploración está adaptado para examinar los mensajes salientes.

3. El sistema de cualquiera de las reivindicaciones 1 o 2, en el que el componente de exploración está adaptado además para reenviar el mensaje examinado al componente de cuarentena junto con la información en cuanto a quién ha enviado el mensaje, el momento en que se ha enviado el mensaje y otros datos relacionados con el mensaje.

4. El sistema de la reivindicación 1, que comprende además:

(a) un filtro de contenidos (520) que está adaptado para:

recibir un mensaje que se dirige a al menos uno de los dispositivos y que incluye un encabezamiento, un cuerpo y un anexo;
determinar una encapsulación que se ha aplicado al anexo antes de que el sistema reciba el mensaje; y desencapsular el anexo; y

(b) un componente de descompresión (525) que está acoplado al filtro de contenidos y que está adaptado para realizar al menos una descompresión del anexo cuando el anexo está comprimido.

5. El sistema de la reivindicación 4, en el que el componente de exploración está adaptado además para determinar si el anexo incluye un programa malicioso.

6. El sistema de la reivindicación 5, que comprende además un cliente que está adaptado para aplicar de manera automática una actualización a al menos uno de entre el filtro de contenidos, el componente de descompresión, el componente de exploración y el componente de cuarentena para permitir la detección de al menos un programa malicioso.

7. El sistema de la reivindicación 6, en el que el cliente está adaptado para determinar cuándo la actualización está disponible adaptándose para sondear los servidores asociados con los proveedores de software de protección de programas maliciosos.

8. El sistema de la reivindicación 7, en el que el cliente está adaptado para recuperar de manera automática la actualización disponible.

9. El sistema de la reivindicación 6, en el que el componente de exploración está adaptado para emplear al menos dos aplicaciones de protección de programas maliciosos por separado para determinar si el anexo incluye un programa malicioso.

10. El sistema de la reivindicación 4, en el que el filtro de contenidos, el componente de descompresión, el componente de exploración y el componente de cuarentena se implementan cada uno en software.

11. El sistema de la reivindicación 4, en el que el filtro de contenidos, el componente de descompresión, el componente de exploración y el componente de cuarentena están todos incluidos en al menos uno de entre un cortafuegos, un router, un switch y un gestor de tráfico.

12. El sistema de la reivindicación 4, en el que la encapsulación incluye al menos uno de entre extensiones multipropósito de correo de internet, Base 64 y uuencode.

13. El sistema de la reivindicación 1, en el que el componente de cuarentena está adaptado para eliminar el programa malicioso del mensaje que se ha determinado que incluye un programa malicioso y reenviar dicho mensaje hacia un destinatario de dicho mensaje.

14. Un método para proporcionar protección a los dispositivos conectados a una red, que comprende:

recibir un mensaje en un nodo, siendo dicho nodo un nodo que recibe los mensajes que se dirigen a cualquiera de los dispositivos y que hace que cada uno de dichos mensajes sea explorado en busca de un programa malicioso mediante un componente de exploración antes de reenviar los mensajes respectivos hacia al menos uno de los dispositivos y que retiene los mensajes respectivos mediante un componente de cuarentena (530) cuando los mensajes respectivos incluyen unos programas maliciosos respectivos; **caracterizado por**:

examinar, mediante el componente de exploración, el mensaje en busca de una firma digital que indique que no debería reenviarse el mensaje examinado; y
reenviar el mensaje examinado al componente de cuarentena cuando se encuentra una firma digital.

15. El método de acuerdo con la reivindicación 14, en donde el mensaje examinado en busca de una firma digital es un mensaje saliente.

16. El método de cualquiera de las reivindicaciones 14 o 15, en el que el mensaje examinado se reenvía al componente de cuarentena junto con la información en cuanto a quién ha enviado el mensaje, el momento en que se ha enviado el mensaje y otros datos relacionados con el mensaje.

17. El método de acuerdo con cualquiera de las reivindicaciones 14 a 16, que comprende además:

recibir un mensaje adicional en donde el mensaje adicional incluye una cabecera;
determinar si la cabecera incluye un programa malicioso; y
cuando la cabecera del mensaje adicional incluya el programa malicioso, poner en cuarentena el mensaje adicional,

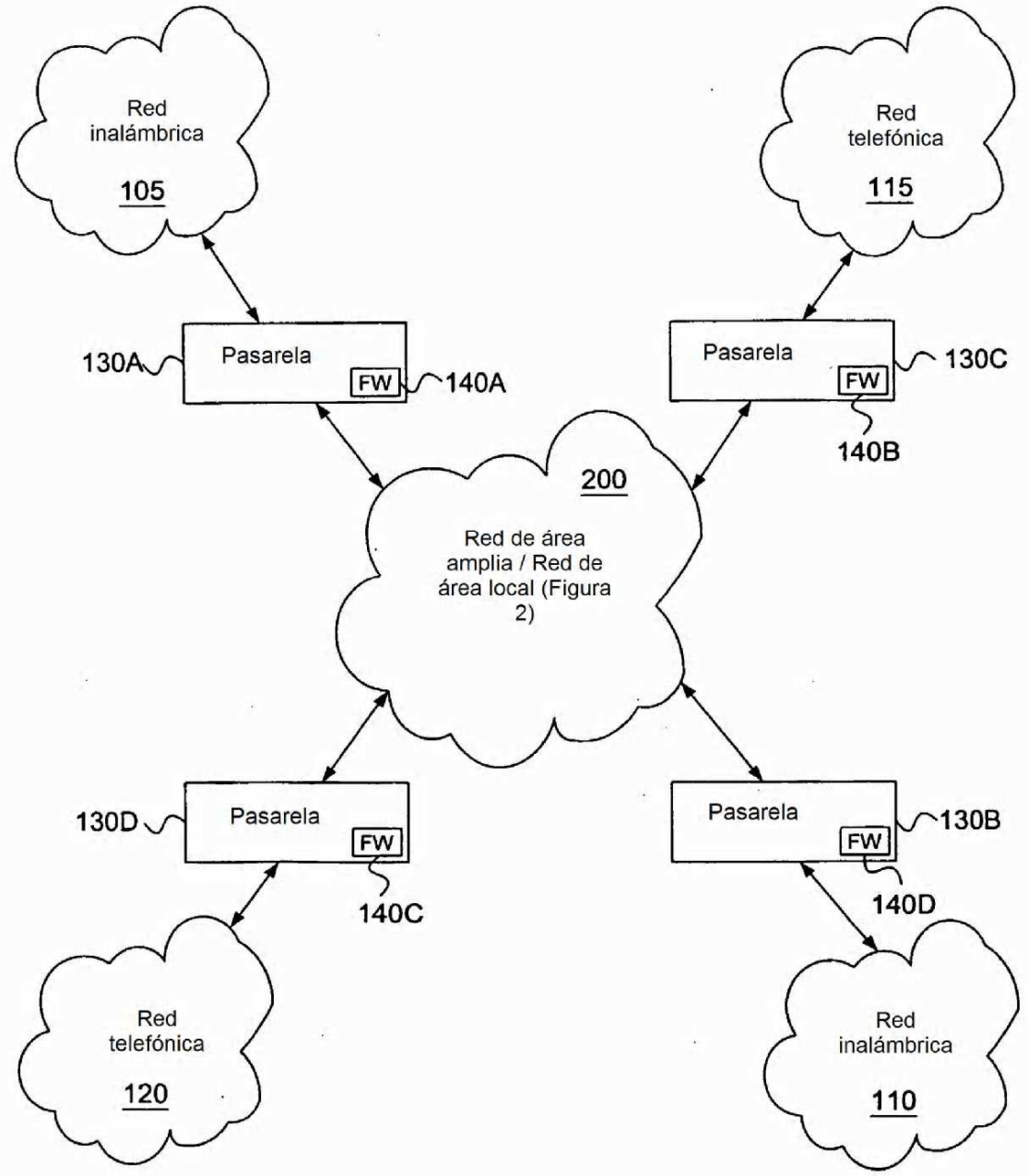
en el que la cabecera incluye un campo que tiene un tamaño definido y en el que la cabecera incluye el programa malicioso cuando un tamaño de datos en el campo es distinto al tamaño definido.

18. El método de la reivindicación 17, en el que el mensaje adicional incluye un anexo, que comprende además:

desencapsular el anexo cuando el anexo está encapsulado; y
descomprimir el anexo al menos una vez cuando el anexo está comprimido.

19. El método de la reivindicación 18, que comprende además eliminar el programa malicioso y reenviar el mensaje adicional hacia al menos uno de los dispositivos.

FIG. 1


Red inalámbrica
105
Red telefónica
115
130A
Pasarela
FW
140A
Pasarela
FW
130C
140B
200
Red de área amplia / Red de área local (Figura 2)
130D
Pasarela
FW
140C
Pasarela
FW
130B
140D
Red telefónica
120
Red inalámbrica
110

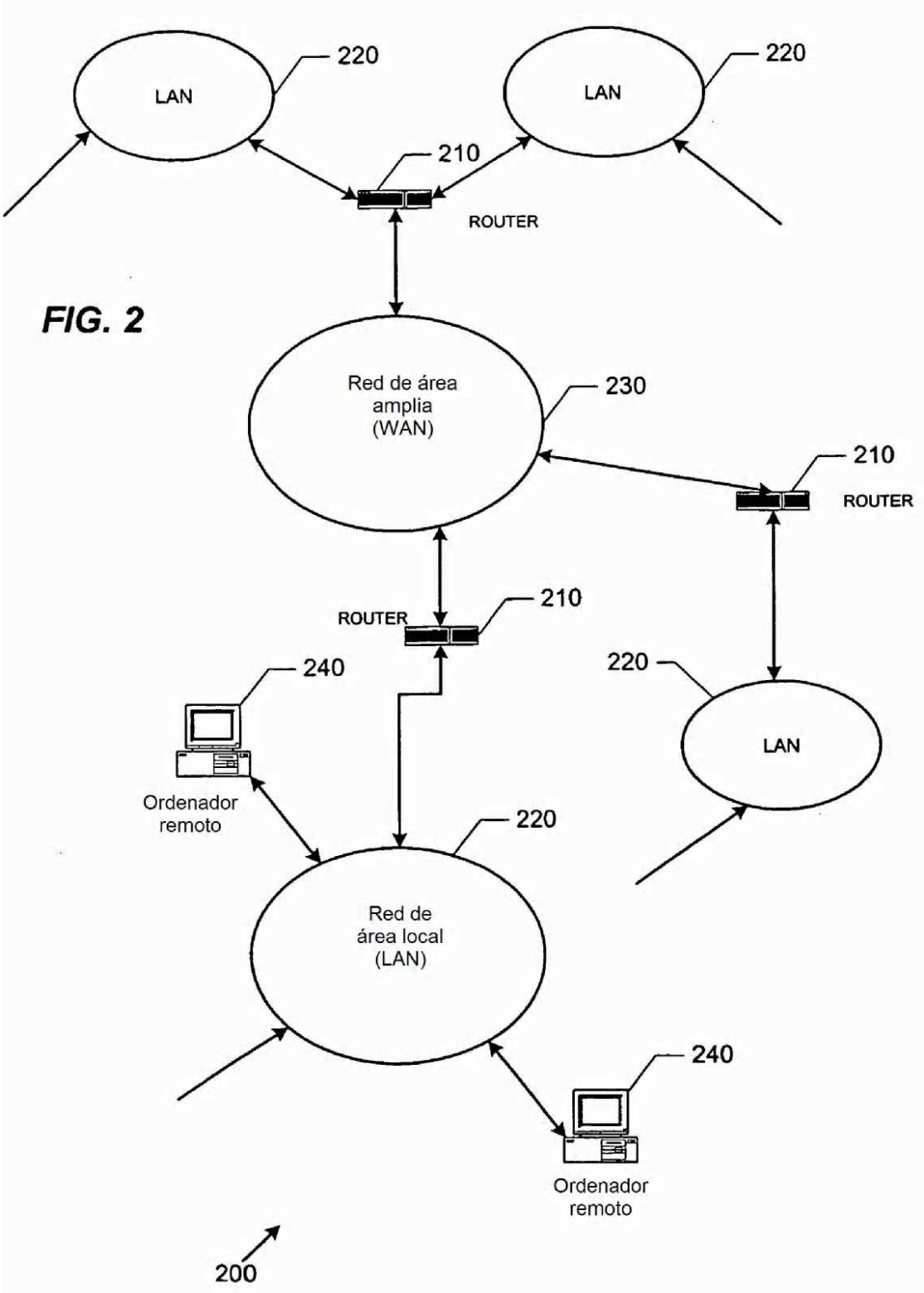

LAN
220
LAN
220
210
ROUTER
Red de área amplia (WAN)
230
210
ROUTER
ROUTER
210
240
220
LAN
Ordenador remoto
220
Red de área local (LAN)
240
Ordenador remoto
200

FIG. 2

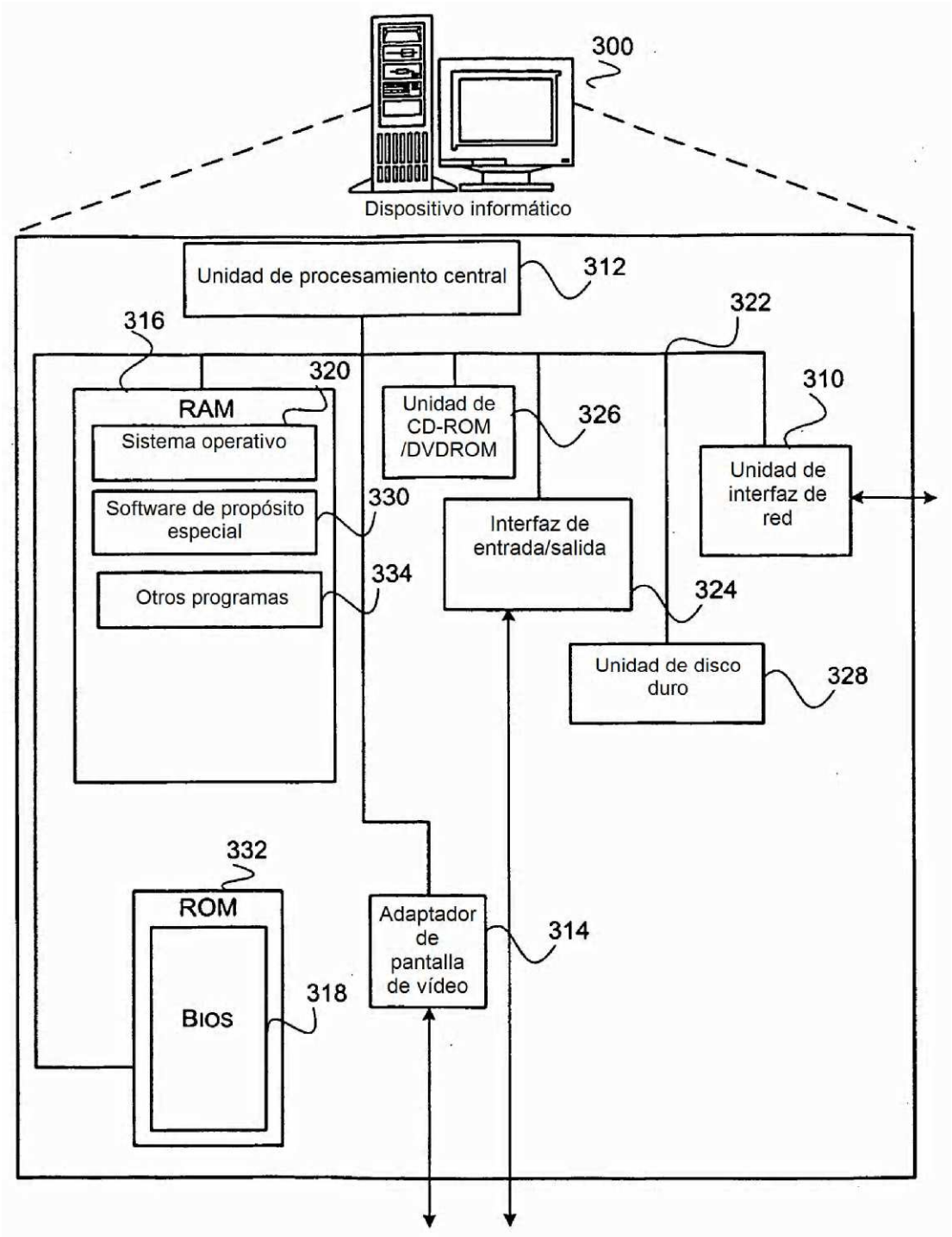

300
Dispositivo informático
Unidad de procesamiento central
312
316
322
320
RAM
Sistema operativo
Software de propósito especial
330
Otros programas
334
Unidad de CD-ROM /DVDROM
326
Interfaz de entrada/salida
324
Unidad de disco duro
328
310
Unidad de interfaz de red
332
ROM
BIOS
318
Adaptador de pantalla de vídeo
314

FIG. 3

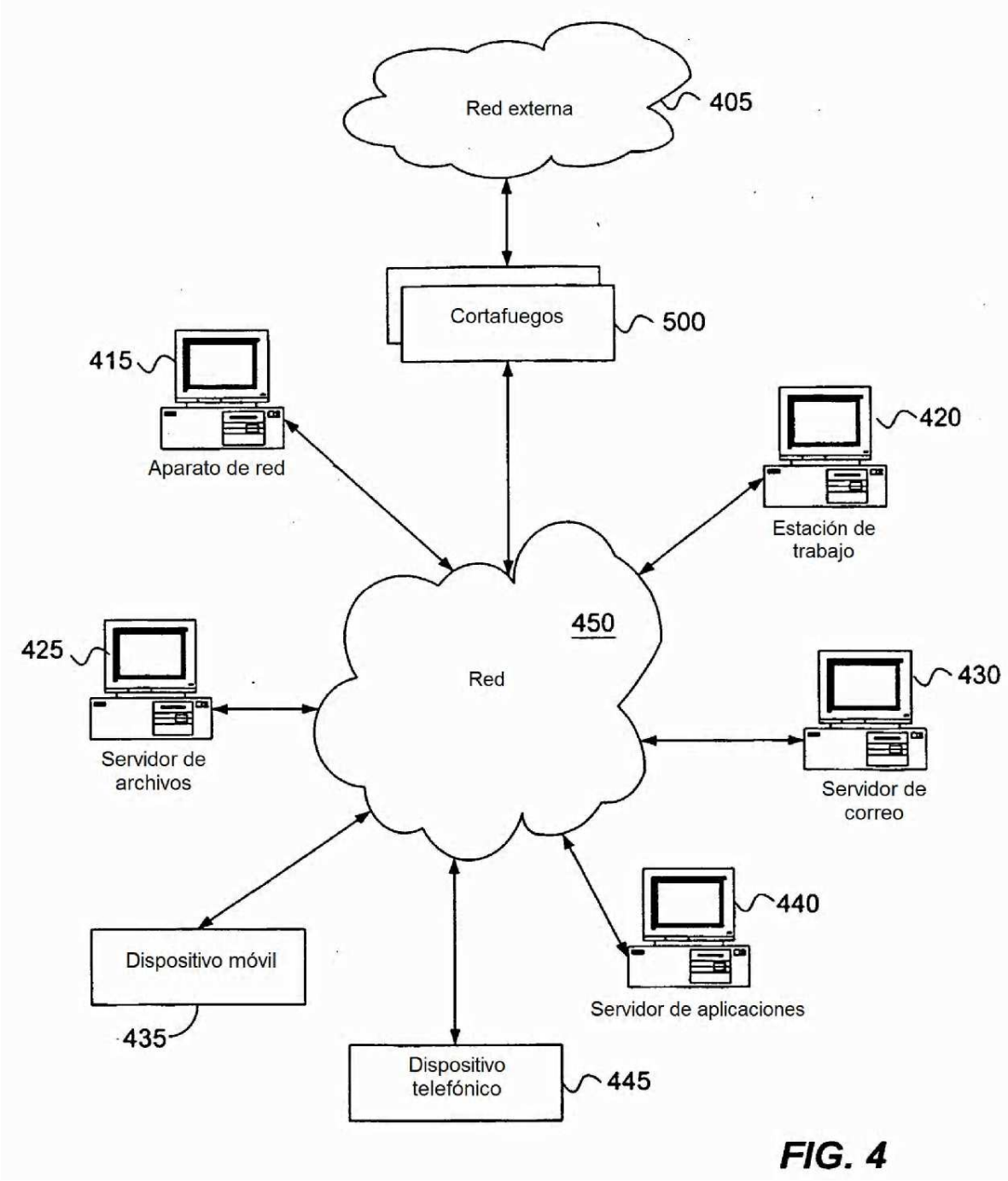

Red externa
405
Cortafuegos
500
415
Aparato de red
420
Estación de trabajo
450
Red
425
Servidor de archivos
430
Servidor de correo
440
Servidor de aplicaciones
Dispositivo móvil
435
Dispositivo telefónico
445

FIG. 4

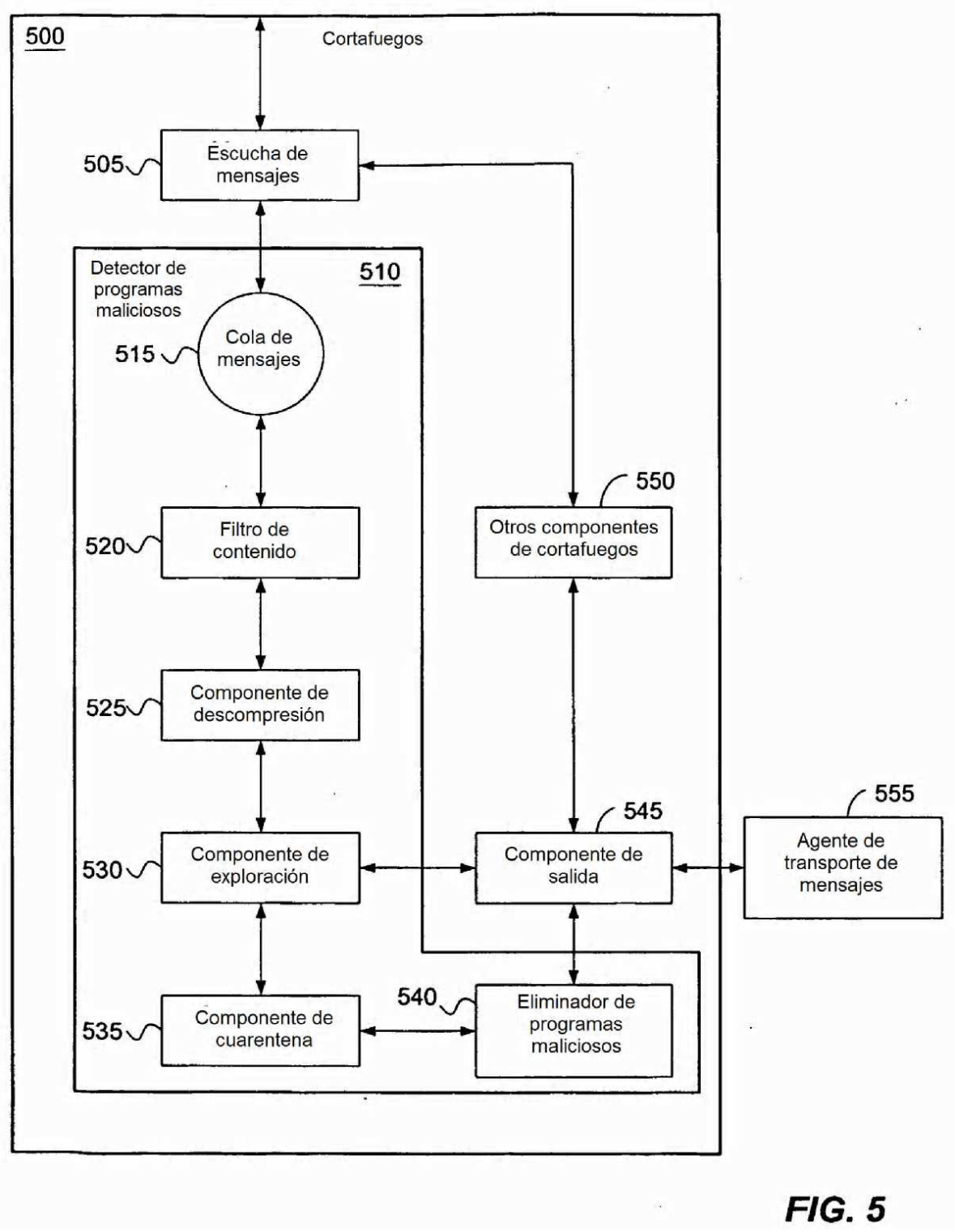

500
Cortafuegos
505
Escucha de mensajes
Detector de programas maliciosos
510
515
Cola de mensajes
520
Filtro de contenido
525
Componente de descompresión
530
Componente de exploración
535
Componente de cuarentena
540
Eliminador de programas maliciosos
550
Otros componentes de cortafuegos
545
Componente de salida
555
Agente de transporte de mensajes

FIG. 5

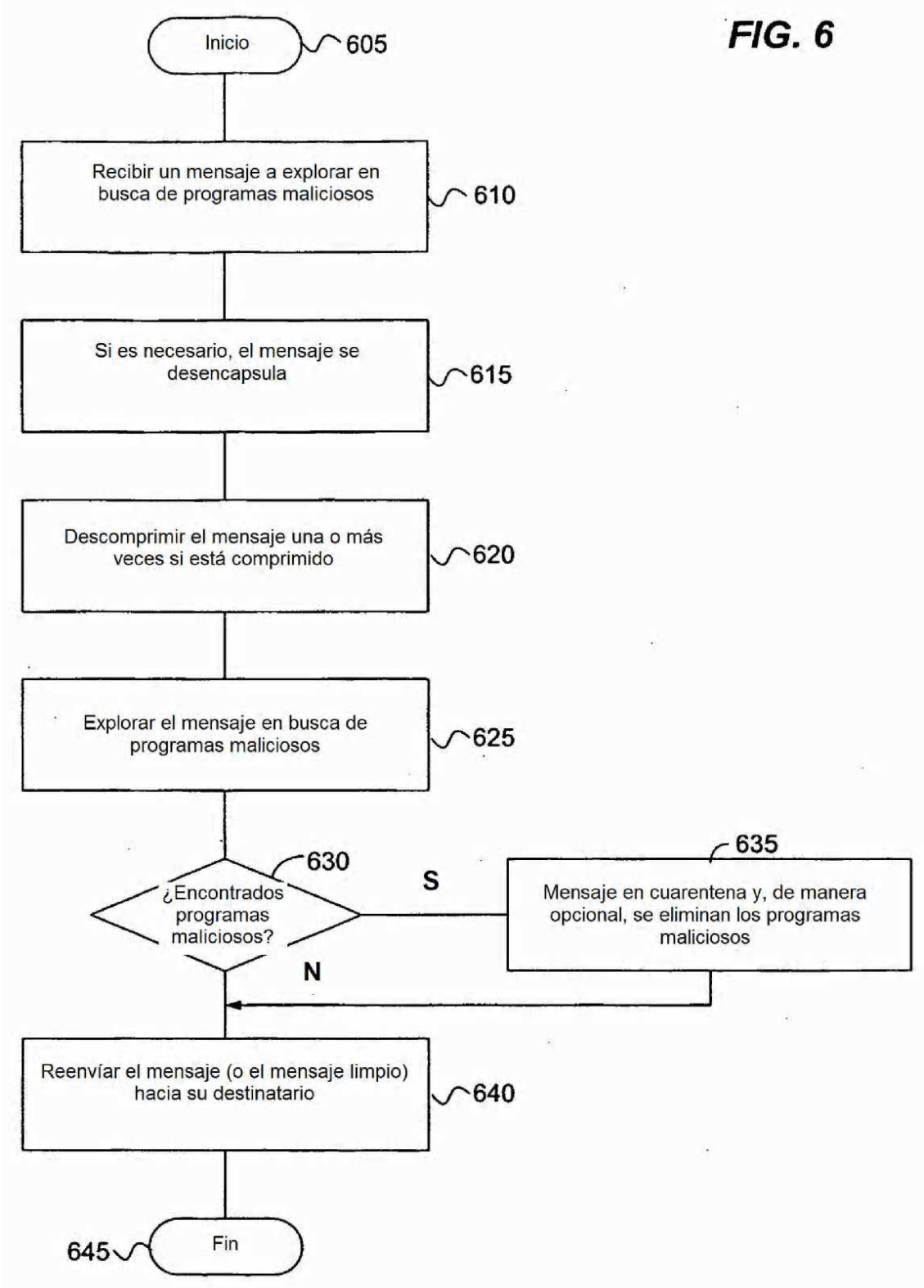

Inicio
605
Recibir un mensaje a explorar en busca de programas maliciosos
610
Si es necesario, el mensaje se desencapsula
615
Descomprimir el mensaje una o más veces si está comprimido
620
Explorar el mensaje en busca de programas maliciosos
625
630
¿Encontrados programas maliciosos?
S
N
635
Mensaje en cuarentena y, de manera opcional, se eliminan los programas maliciosos
Reenvíar el mensaje (o el mensaje limpio) hacia su destinatario
640
645
Fin

FIG. 6