(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 901**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.01.2002 PCT/US2002/02218**

(87) Fecha y número de publicación internacional: **01.08.2002 WO02060117**

(96) Fecha de presentación y número de la solicitud europea: **24.01.2002 E 02709175 (0)**

(97) Fecha y número de publicación de la concesión europea: **13.12.2017 EP 1356626**

(54) Título: **Verificación de la integridad de redes informáticas e implementación de contramedidas**

(30) Prioridad:

25.01.2001 US 770525

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.04.2018

(73) Titular/es:

NTT SECURITY (US) INC. (100.0%)
9420 Underwood Avenue
Omaha NE 68114, US

(72) Inventor/es:

HRABIK, MICHAEL;
GUILFOYLE, JEFFREY y
BEAVER, EDWARD, MAC

(74) Agente/Representante:

AZNÁREZ URBIETA, Pablo

DESCRIPCIÓN

Verificación de la integridad de redes informáticas e implementación de contramedidas

CAMPO DE LA INVENCIÓN

Esta invención se refiere a un procedimiento y a un aparato para verificar la integridad de un subsistema de seguridad informática con el fin de impedir ataques a los sistemas de seguridad de redes informáticas.

ANTECEDENTES DE LA INVENCIÓN

Simultáneamente con el desarrollo de la conectividad entre diversas redes informáticas y el correspondiente aumento en la dependencia de estos sistemas de información interconectados, se ha producido un aumento drástico en la necesidad de una seguridad robusta para imponer restricciones de acceso a sistemas de seguridad e impedir la intrusión en estos últimos. La topología de las redes interconectadas también se ha hecho cada vez más compleja y, con frecuencia, están involucradas redes abiertas tales como Internet, que exponen a los sistemas de seguridad a mayores amenazas de ataque. Por consiguiente, aún no se ha propuesto una sola solución que aborde todas las necesidades actuales para detectar intrusiones y dar respuesta a las mismas. En su lugar, se ha desarrollado un amplio surtido de dispositivos y técnicas de seguridad, que en general se han implementado de formas diferentes en sistemas individuales. Esto tiene como resultado un mosaico de seguridad global intrínsecamente susceptible a ataques y de sistemas individuales que implementan en sí mismos una mezcolanza de dispositivos y técnicas de seguridad diferentes.

Los intentos de conseguir el acceso no autorizado a redes informáticas aprovechan las lagunas intrínsecas de una topología de seguridad de red. Es sabido, por ejemplo, que, aunque un sistema de seguridad conectado a Internet pueda incluir cortafuegos y sistemas de detección de intrusiones para impedir el acceso no autorizado, con frecuencia se buscan y explotan con éxito puntos débiles de los componentes de seguridad individuales. La rápida introducción de nuevas tecnologías empeora el problema, creando o exponiendo otros puntos débiles que pueden no llegarse a conocer hasta que ya se ha producido un fallo de seguridad.

Un punto débil fundamental que comparten los sistemas de detección y respuesta a intrusiones actuales es su implementación “plana” o no jerárquica. La configuración mostrada en la Fig. 1 es un ejemplo de implementación de red típica de este tipo en una “red objetivo” hipotética. La red 10 incluye una pluralidad de servidores 14 de archivos, estaciones 16 de trabajo, un sistema 18 de detección de intrusiones (IDS, por sus siglas en inglés) de red, un servidor 20 de acceso remoto y un servidor web 22. Estos dispositivos están conectados entre sí a través de una red troncal 12 y forman una red de área local o de área amplia (LAN o WAN, por sus siglas en inglés). Un enrutador 26 está conectado directamente a una red abierta tal como Internet 30 y está conectado a los dispositivos de la red troncal 12 mediante un cortafuegos 24 de red.

El cortafuegos 24 y el IDS 18 son parte del sistema de seguridad de la red 10. El cortafuegos 24 puede configurarse y sirve para controlar el acceso por parte de los anfitriones de Internet a los recursos de la red. Éste protege la red 10 contra intrusos de fuera del cortafuegos, esencialmente filtrándolos. El IDS 18 explora paquetes de información transmitidos a través de la red troncal 12 y está configurado para detectar tipos específicos de transacciones que indican que un intruso está intentando conseguir o ha conseguido un acceso a la red 10. Así, el IDS protege la red contra intrusos tanto de dentro como de fuera del cortafuegos. Otros dispositivos de la red 10 pueden contribuir también a su seguridad, como el servidor 20 de acceso remoto, que permite acceder directamente a la red 10 desde ordenadores remotos (no mostrados), por ejemplo a través de un módem. El servidor 20 de acceso remoto debe implementar también ciertas funciones de seguridad, tales como una verificación de usuario y contraseña, para impedir que los intrusos consigan acceso a la red y eviten el cortafuegos 24.

En un escenario típico de intrusión en una red objetivo conectada a Internet, en primer lugar el intruso aprenderá tanto de la red objetivo como sea posible a partir de la información pública disponible. En esta fase, el intruso puede hacer una búsqueda “whois” o investigar tablas DNS o sitios web públicos asociados al objetivo. A continuación, el intruso pondrá en marcha diversas técnicas habituales para buscar información. El intruso puede hacer un barrido “ping” (búsqueda de direcciones de Internet) con el fin de saber qué máquinas de la red objetivo están en funcionamiento o puede emplear diversas herramientas de exploración bien conocidas en la técnica, como “rcpinfo”, “showmount” o “snmpwalk”, para descubrir información más detallada sobre la topología de la red objetivo. En esta fase, el intruso no ha causado daño al sistema, pero un IDS de red correctamente

configurado debería ser capaz, dependiendo de su lugar estratégico en la red, de detectar técnicas de vigilancia de intrusos que sigan patrones conocidos de actividad sospechosa e informar de las mismas. Estas definiciones estáticas, conocidas como “firmas de intrusión”, son eficaces sólo cuando el intruso toma una medida o una serie de medidas que siguen estrechamente las definiciones establecidas de actividad sospechosa. Por consiguiente, si el IDS no está actualizado, está desactivado o se encuentra con un método de ataque nuevo o desconocido, no responderá adecuadamente. Sin embargo, si no se toman medidas en este punto del ataque para impedir la posterior entrada en la red objetivo, el intruso puede realmente comenzar a invadir la red, explotando cualesquiera puntos débiles de seguridad (tales como el IDS, que puede no haber reaccionado previamente al intruso) y asegurando una posición en la red. Una vez atrincherado, el intruso puede ser capaz de modificar o desactivar cualquier dispositivo perteneciente a la red objetivo, incluyendo cualquier IDS o cortafuegos remanente.

Los métodos utilizados por los intrusos para conseguir un acceso no autorizado a las redes informáticas son cada vez más complejos siguiendo los avances en tecnología de seguridad. Sin embargo, es típico que los ataques con éxito a los sistemas de red comiencen frecuentemente atacando los subsistemas de seguridad existentes en la red objetivo que son responsables de detectar firmas de intrusión comunes, desactivando estos sistemas y destruyendo las pruebas de la intrusión.

La solicitud de patente WO 00/69120 A1 describe un sistema para administrar en remoto múltiples dispositivos de seguridad de red a través de un enlace seguro, utilizando uno o más dispositivos supervisores intermedios. El sistema permite que un dispositivo administrador reciba, analice y visualice toda la información de seguridad de red generada a partir de la información reunida por los dispositivos de seguridad. La patente US nº 5.916.644, de Kutzberg et al., describe un procedimiento para comprobar la integridad de sistemas de seguridad donde un sistema configurado específicamente, conectado directamente a una red informática objetivo, comprobará sistemáticamente la seguridad en la red simulando ataques a dispositivos de seguridad para verificar que éstos están operativos. Específicamente, el procedimiento descrito simula aleatoriamente un ataque a la red. Si se detecta el ataque, se supone que los subsistemas de seguridad están funcionando. Si no, se considera que éstos están comprometidos y que es posible que ya se esté produciendo un ataque. Este procedimiento es una

mejora en relación con los sistemas pasivos, que no se comprueban a sí mismos y, por tanto, no pueden informar adecuadamente sobre su propio estado cuando han sido desactivados.

Un defecto muy importante de este enfoque es que estos sistemas de seguridad residen en las mismas redes que tratan de proteger y son igualmente vulnerables a un ataque una vez que el intruso se ha asegurado una posición en la red. En otras palabras, ellos mismos no son inmunes a los ataques de los intrusos. Como resultado, cada avance en la técnica anterior es sólo un nuevo obstáculo de seguridad a salvar en la red. A la luz de esto, el enfoque de exploración activa descrito en Kurtzberg no es fundamentalmente diferente de cualquier otra medida de seguridad (tal como un cortafuegos), ya que es no jerárquico y depende completamente de la vigilancia de un administrador de red humano.

Por tanto, existe la necesidad de un sistema de seguridad de red que se autodiagnostique, que pueda proteger una red objetivo frente a intrusos tanto internos como externos y que sea resistente a los ataques perpetrados en el sistema que está destinado a proteger. Además, existe la necesidad de un sistema de seguridad activo que tome medidas moderadas contra amenazas a la seguridad percibidas, incluso en ausencia de un administrador de red humano.

SUMARIO DE LA INVENCIÓN

Así, un objetivo de la presente invención es proporcionar un sistema de seguridad de red para una red de ordenadores que sea capaz de solucionar los problemas de la técnica anterior arriba mencionados.

Otro objetivo de la presente invención es proporcionar un sistema de seguridad de red que tenga un componente que pueda vigilar directamente en una red múltiples dispositivos de seguridad de red en cuanto a firmas de ataque y otras actividades de red sospechosas que sugieran un intento de comprometer la seguridad de dicha red.

Otro objetivo de la presente invención es proporcionar un sistema de seguridad de red que pueda detectar dinámicamente nuevos patrones o tendencias en la actividad de red que sugieran un intento de comprometer la seguridad de una red o de una pluralidad de redes no relacionadas de otro modo.

Otro objetivo de la presente invención es proporcionar un sistema de seguridad de red que pueda resistir a la intrusión durante un ataque a la red.

Otro objetivo de la presente invención es proporcionar un sistema de seguridad que proporcione una verificación de integridad de los dispositivos de seguridad en una red y pueda también verificar de forma fiable su propia integridad.

Otro objetivo de la presente invención es proporcionar un sistema de seguridad para una red informática que pueda tomar medidas correctivas después de haberse detectado un ataque con el fin de impedir que un intruso siga teniendo acceso a la red.

Otro objetivo de la presente invención es proporcionar un sistema de seguridad que satisfaga los objetivos anteriores para ordenadores individuales conectados a una red abierta.

De acuerdo con la presente invención, se proporciona un sistema de seguridad para una red informática que tiene las características distintivas de la reivindicación 1.

Según un ejemplo de la presente invención, se proporciona un sistema de seguridad de red para impedir la intrusión en una red objetivo que tiene al menos un subsistema de seguridad local con respecto a la red objetivo previsto para vigilar el tráfico de red y para detectar ataques al sistema por parte de un intruso. El subsistema está conectado a través de un enlace seguro a un sistema maestro, que no está conectado de otra manera al sistema objetivo. El sistema maestro vigila el subsistema a través del enlace seguro y registra información relacionada con el estado del subsistema. Si el subsistema detecta un ataque a la red objetivo o no responde al sistema maestro, el sistema maestro tomará una medida adecuada, que va desde registrar el incidente o comunicarlo a un administrador de red a intentar apagar la red. Por consiguiente, ni siquiera los ataques que desactiven por completo el subsistema impedirán que el sistema maestro responda siempre que el enlace siga siendo seguro.

Según otro ejemplo de la presente invención, se implementa una jerarquía multinivel que subordina al subsistema al sistema maestro. En esta configuración, sólo pueden pasarse comandos del sistema maestro al subsistema, lo que asegura que no sea posible socavar la integridad del sistema maestro, ni siquiera en caso de ataques con éxito a la red objetivo o al subsistema mismo. Por tanto, ni siquiera una subversión del subsistema y un enlace comprometido entre éste y el sistema maestro son suficientes para desactivar el sistema maestro.

Según otro ejemplo de la presente invención, está previsto un generador de seudoataques asociado al sistema maestro que simula ataques a la red objetivo

que debería estar dirigida por el subsistema. Comparando los seudoataques realizados a la red objetivo con los ataques realmente detectados por el subsistema, el sistema maestro puede determinar si la integridad del subsistema se ha visto comprometida. Igualmente, el subsistema puede generar sus propios seudoataques a otros componentes de seguridad de la red para establecer también su integridad. Por tanto, es posible comprobar exhaustivamente todo dispositivo conectado a la red objetivo relacionado con la seguridad.

En otro ejemplo de la presente invención, el subsistema y el sistema maestro actuando a través del subsistema pueden aplicar medidas correctivas para mitigar o frustrar un ataque intruso a la red objetivo.

BREVE DESCRIPCIÓN DE LAS FIGURAS

Fig. 1: diagrama de bloques que muestra la estructura general de un ejemplo de un sistema de red según la técnica anterior.

Fig. 2: diagrama de bloques que muestra un ejemplo de una red que incorpora el sistema de la presente invención.

DESCRIPCIÓN DE REALIZACIONES PREFERENTES

A continuación se describen realizaciones preferentes de un sistema de seguridad de red según la presente invención en referencia a las figuras adjuntas.

En referencia a la Fig. 2, se muestra una primera realización de la presente invención. Se muestra una red objetivo 100 que tiene los mismos componentes básicos que la red de la técnica anterior mostrada en la Fig. 1, con la adición del subsistema 50 de seguridad, pero debería señalarse que la configuración real de la red objetivo no es crítica, con la excepción de al menos un subsistema 50 de seguridad. El subsistema 50 de seguridad, los servidores 14, las estaciones 16 de trabajo, el IDS 18, el servidor 20 de acceso remoto, el servidor web 22, el cortafuegos 24 y el enrutador 26 están todos ellos conectados entre sí a través de una red troncal 12. Cada uno de los dispositivos realiza una comunicación a través de la red troncal según un protocolo de comunicación predeterminado, tal como el protocolo de control de transmisión/protocolo de Internet (TCP/IP, por sus siglas en inglés).

La red objetivo 100 está conectada a través del cortafuegos 24 y el enrutador 26 a Internet 30, así como a través del servidor 20 de acceso remoto, que también puede ser conectado de forma selectiva a Internet 30 a través del usuario remoto 21. Estos

dos puntos potenciales de contacto con una red abierta, en este caso Internet, exponen a la red objetivo 100 a la amenaza de una intrusión desde cualquier anfitrión con acceso a Internet, tal como el usuario 31 de Internet. Además de las amenazas desde el exterior, las que tienen acceso directo a los recursos de la red objetivo 100, tales como aquellas que están utilizando una de las estaciones 16 de trabajo, también representan amenazas de intrusión. Si un intruso consiguiese acceso a uno de los dispositivos críticos relacionados con la seguridad, como el IDS 18 o el cortafuegos 24 o cualquier ordenador de confianza de dentro o fuera de la red objetivo 100, la seguridad de la red podría verse comprometida.

En la presente invención, el subsistema 50 de seguridad está conectado a la red troncal 12 y enlazado a cada uno de los dispositivos de red mediante un enlace seguro 52. Tal enlace seguro puede establecerse a través de un protocolo de comunicación encriptado, tal como la capa de conexión segura (SSL, por sus siglas en inglés). Esto asegura que la comunicación entre el subsistema 50 de seguridad y los demás componentes de la red objetivo no pueda ser interceptada por un intruso. Un enlace seguro 54 similar puede estar establecido como un túnel de red privada virtual (VPN, por sus siglas en inglés) entre el subsistema 50 de seguridad y un sistema maestro 60 conectado a una red remota 110. Aunque la red remota se muestra como provista de sus propios cortafuegos 62, servidores 66 y enrutador 68, la configuración final de la red remota 110 no es crítica, aparte del enlace seguro 54 que conecta el subsistema 50 de seguridad y el sistema maestro 60. Sin embargo, pueden establecerse enlaces seguros 55 entre un dispositivo, tal como un escáner 63 de red, y un enrutador 26 o un usuario remoto 21 de la red 100. El enlace seguro 54 asegura que la comunicación entre las dos redes no pueda ser interceptada por un intruso. Por tanto, no debería haber ninguna conexión directa entre la red objetivo 100 y la red remota 110 que no sea a través de un enlace seguro.

Preferentemente, el sistema de seguridad aquí definido está integrado como un paquete software e implementado en ordenadores que comprenden al menos un sistema maestro y el subsistema de seguridad.

Durante el funcionamiento, el subsistema 50 de seguridad vigila las actividades de los dispositivos de la red objetivo 100. En particular, se comprueban las funciones críticas del IDS 18 y del cortafuegos 24 relacionadas con la seguridad. El procedimiento concreto empleado por el subsistema 50 de seguridad para

comprobar estos dispositivos no es crítico, pero sería adecuado el enfoque arriba mencionado en el que se emplean ataques simulados a los componentes.

Al comprobar los dispositivos, si no puede verificarse la integridad de un dispositivo de la red objetivo 100, el subsistema 50 de seguridad reacciona. Por ejemplo, si el subsistema ha detectado que el IDS 18 no reacciona adecuadamente a ataques contra el mismo procedentes de Internet, las contramedidas adecuadas podrían incluir cortar o restringir el acceso a la red en el cortafuegos 24 o una parada en el nivel de aplicaciones. Si, en su lugar, se determina que el cortafuegos no está funcionando, las medidas adecuadas podrían incluir desactivar el acceso a cualesquiera servidores 14 que guarden datos sensibles. En una posible configuración de la presente invención, el subsistema 50 de seguridad comunica el estado del dispositivo de red al sistema maestro 60, que procesa la información y toma una decisión sobre posteriores acciones. En una configuración alternativa, el subsistema 50 de seguridad es responsable de implementar contramedidas directamente. Sin embargo, en ambos casos, los resultados de cada comprobación pasan al sistema maestro 60, donde son almacenados para su análisis.

El sistema de la presente invención puede ayudar también a frustrar ataques en curso y es excepcionalmente adecuado para ello. En otra realización preferente de la presente invención, el sistema maestro 60 sustituye jerárquicamente al subsistema 50 de seguridad. Como tal, las actividades del subsistema 50 de seguridad se definen como procesos “hijos” del sistema maestro 60 y están subordinadas al mismo. Aunque la información fluye preferiblemente en ambos sentidos entre el sistema maestro 60 y el subsistema 50 de seguridad en esta realización, el sistema maestro de esta realización no acepta instrucciones del subsistema.

Como se ha señalado en la descripción de la técnica anterior, los sistemas de seguridad no jerárquicos están conectados directamente a una red objetivo y son intrínsecamente susceptibles de ataques a esa red. Esto contrasta con la presente realización, donde, aunque fuese completamente subvertido durante un ataque al sistema objetivo 100, el subsistema 50 de seguridad no tendría como resultado una toma del sistema maestro 60. El beneficio de esta configuración es que el sistema maestro aún sería capaz de llevar a cabo su función. Por ejemplo, si el sistema maestro 60 está configurado para activar una alarma cuando el subsistema 50 de seguridad ya no responde, en esta realización no habría manera de que los intrusos en la red objetivo 100 apagaran de forma remota el sistema maestro 60, ya que el

sistema maestro no responderá a ninguna instrucción emitida desde un sistema subordinado. Aunque el sistema maestro 60 pueda perder el control de la red objetivo, no está en peligro de ser tomado a través de la misma. Adicionalmente, si el enlace 54 entre el sistema maestro 60 y el subsistema 50 de seguridad se corta o se ve comprometido, las instrucciones pueden enrutarse en su lugar a través de los enlaces seguros 55.

En otra realización más de la presente invención, la red remota 110 está conectada a través de un enrutador 70 a una red abierta, tal como Internet. Esto permite al sistema maestro 60 enviar seudoataques aleatorios a la red objetivo 100. Los seudoataques pueden imitar cualquiera de las firmas de ataque reales conocidas por el sistema maestro que puedan ser detectadas por la red objetivo. Si el sistema maestro no recibe la respuesta esperada, es una indicación temprana del ataque de un intruso a la red objetivo.

Como se ha explicado más arriba, según la presente invención es posible proporcionar un procedimiento y un aparato para verificar la integridad de ordenadores y redes informáticas que es independiente de la red o del ordenador que se esté comprobando. Además, detectando señales tempranas de actividad de intrusos en una red, la presente invención aumenta la probabilidad de que los ataques de los intrusos puedan frustrarse antes de que tengan éxito.

Cuando se implementa en un ordenador individual, tal como una sola estación 16 de trabajo conectada a una red abierta tal como Internet 30, la presente invención funciona de manera similar para impedir ataques a ese ordenador procedentes de la red abierta. En ausencia de una red troncal 12, las funciones del subsistema 50 de seguridad pueden estar directamente incorporadas en un ordenador individual, por ejemplo mediante software o hardware periférico.

Cuando se implementa en una pluralidad de redes objetivo no relacionadas de otro modo, la presente invención funciona para impedir ataques según los procedimientos aquí descritos en cada red objetivo individualmente. La ventaja de esta configuración es que es posible coordinar informaciones de seguridad entre varias redes sin conectar las redes entre sí.

Pueden contemplarse muchas realizaciones de la presente invención diferentes sin apartarse del alcance de la invención. Debe entenderse que la presente invención no está limitada a las realizaciones específicas descritas en esta especificación.

Por el contrario, se tiene la intención de que la presente invención cubra diversas modificaciones y disposiciones equivalentes incluidas en las reivindicaciones.

Reivindicaciones

1. Sistema de seguridad para una red informática, teniendo la red una pluralidad de dispositivos conectados a la misma, teniendo al menos algunos de los dispositivos funciones relacionadas con la seguridad, comprendiendo el sistema de seguridad: (a) un subsistema de seguridad (50) asociado con al menos algunos de los dispositivos de la red, estando dicho subsistema de seguridad (50) adaptado para comprobar la integridad de las funciones relacionadas con la seguridad, estando dicho subsistema de seguridad (50) configurado para detectar ataques a dicha red; (b) un sistema maestro (60) que está adaptado para vigilar la integridad del subsistema de seguridad (50), registrar información relacionada con los ataques detectados por dicho subsistema de seguridad (50) y recibir y almacenar resultados de la comprobación de integridad de los dispositivos que tienen funciones relacionadas con la seguridad; y (c) un primer enlace seguro (54) conectado entre el subsistema de seguridad (50) y el sistema maestro (60), estando el sistema maestro (60) adaptado para vigilar la integridad del subsistema de seguridad (50) y para recibir los resultados de la comprobación de integridad de los dispositivos que tienen funciones relacionadas con la seguridad a través del primer enlace seguro (54), donde el sistema maestro (60) o el subsistema de seguridad (50) está adaptado además para vigilar si un dispositivo que tiene funciones relacionadas con la seguridad responde al subsistema (50) de seguridad en respuesta a la comprobación de integridad y donde el subsistema de seguridad (50) o el sistema maestro (60) está adaptado para tomar contramedidas de seguridad cuando no se detecta ninguna respuesta.

2. Sistema según la reivindicación 1, donde el subsistema de seguridad (50) comprueba la integridad de las funciones relacionadas con la seguridad generando seudoataques a los dispositivos que tienen funciones relacionadas con la seguridad.

3. Sistema según la reivindicación 1 o 2, donde dichas contramedidas de seguridad incluyen restringir o desactivar el acceso a la red o a un dispositivo de la red.

4. Sistema según las reivindicaciones 1, 2 o 3, donde el sistema maestro (60) comprende además un generador de seudoataques que genera ataques a la red, detectando el subsistema de seguridad (50) tales ataques cuando funciona correctamente, comparando el sistema maestro (60) los seudoataques

realizados a la red con los ataques realmente detectados por el subsistema (50), determinando así el sistema maestro (60) si la integridad del subsistema (50) se ha visto comprometida.

5. Sistema según cualquiera de las reivindicaciones anteriores, donde el primer enlace seguro (54) está definido por un túnel de red privada virtual (VPN).

6. Sistema según cualquiera de las reivindicaciones anteriores, donde al menos uno de los dispositivos que tienen funciones relacionadas con la seguridad es un cortafuegos (24).

7. Sistema según cualquiera de las reivindicaciones anteriores, donde al menos uno de los dispositivos que tienen funciones relacionadas con la seguridad es un sistema de detección de intrusiones de red.

8. Sistema según cualquiera de las reivindicaciones, donde el sistema maestro (60) no acepta instrucciones del subsistema (50) de seguridad.

9. Sistema según cualquiera de las reivindicaciones anteriores que además comprende un segundo enlace seguro (55) conectado entre el sistema maestro (60) y la red que permite una comunicación de datos desde el sistema maestro (60) a la red para emitir instrucciones a los dispositivos de red.

10. Sistema según la reivindicación 9, donde las instrucciones se emiten si el primer enlace seguro (54) se corta o se ve comprometido.

11. Sistema según cualquiera de las reivindicaciones anteriores, donde el sistema maestro (60) reemplaza jerárquicamente al subsistema de seguridad (50).

12. Sistema según cualquiera de las reivindicaciones anteriores, donde el subsistema de seguridad (50) está jerárquicamente subordinado al sistema maestro (60).

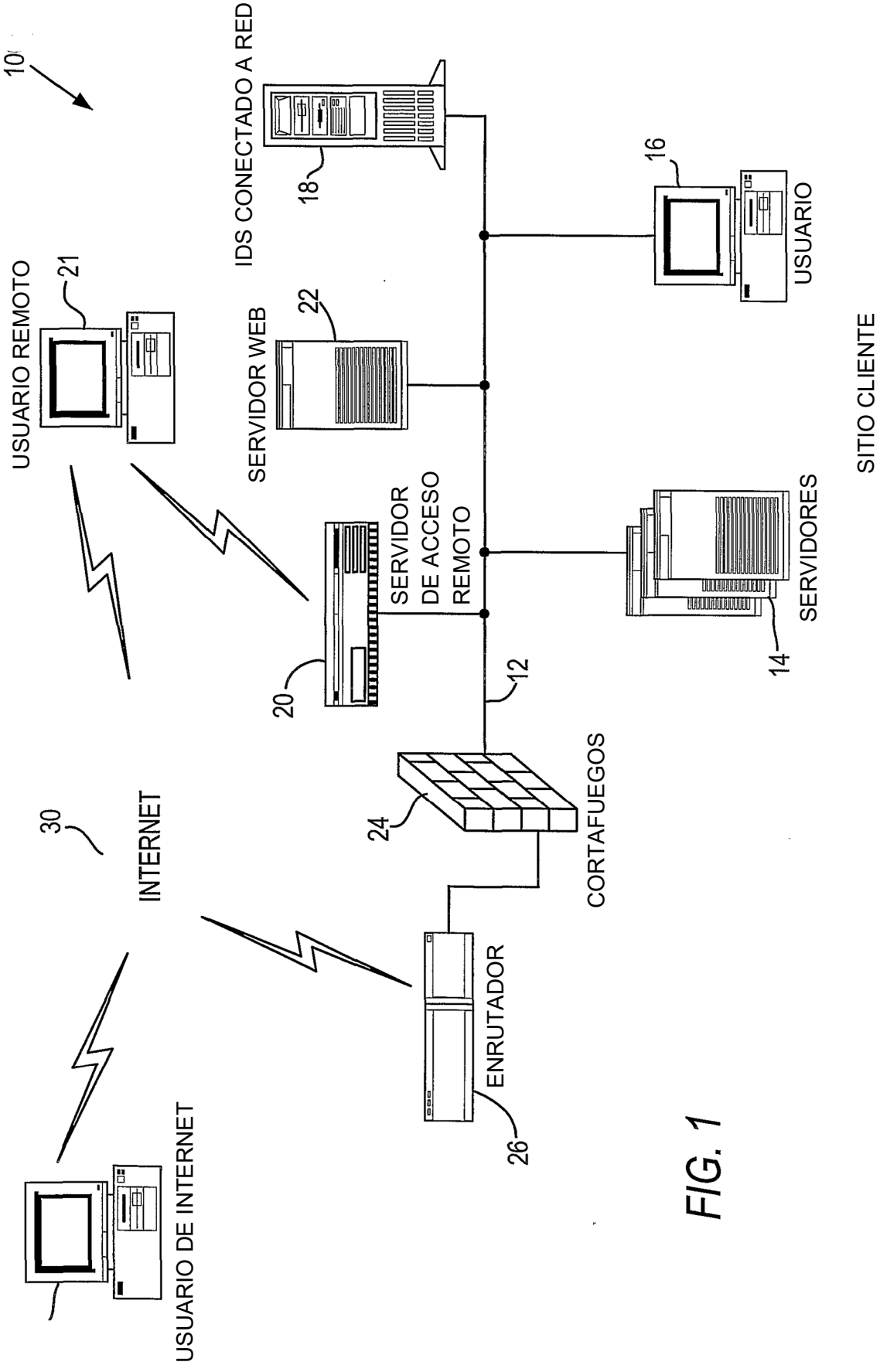
10
IDS CONECTADO A RED
18
16
USUARIO
USUARIO REMOTO
21
SERVIDOR WEB
22
SERVIDOR DE ACCESO REMOTO
20
SERVIDORES
14
SITIO CLIENTE
12
30
INTERNET
24
CORTAFUEGOS
ENRUTADOR
26
USUARIO DE INTERNET

FIG. 1

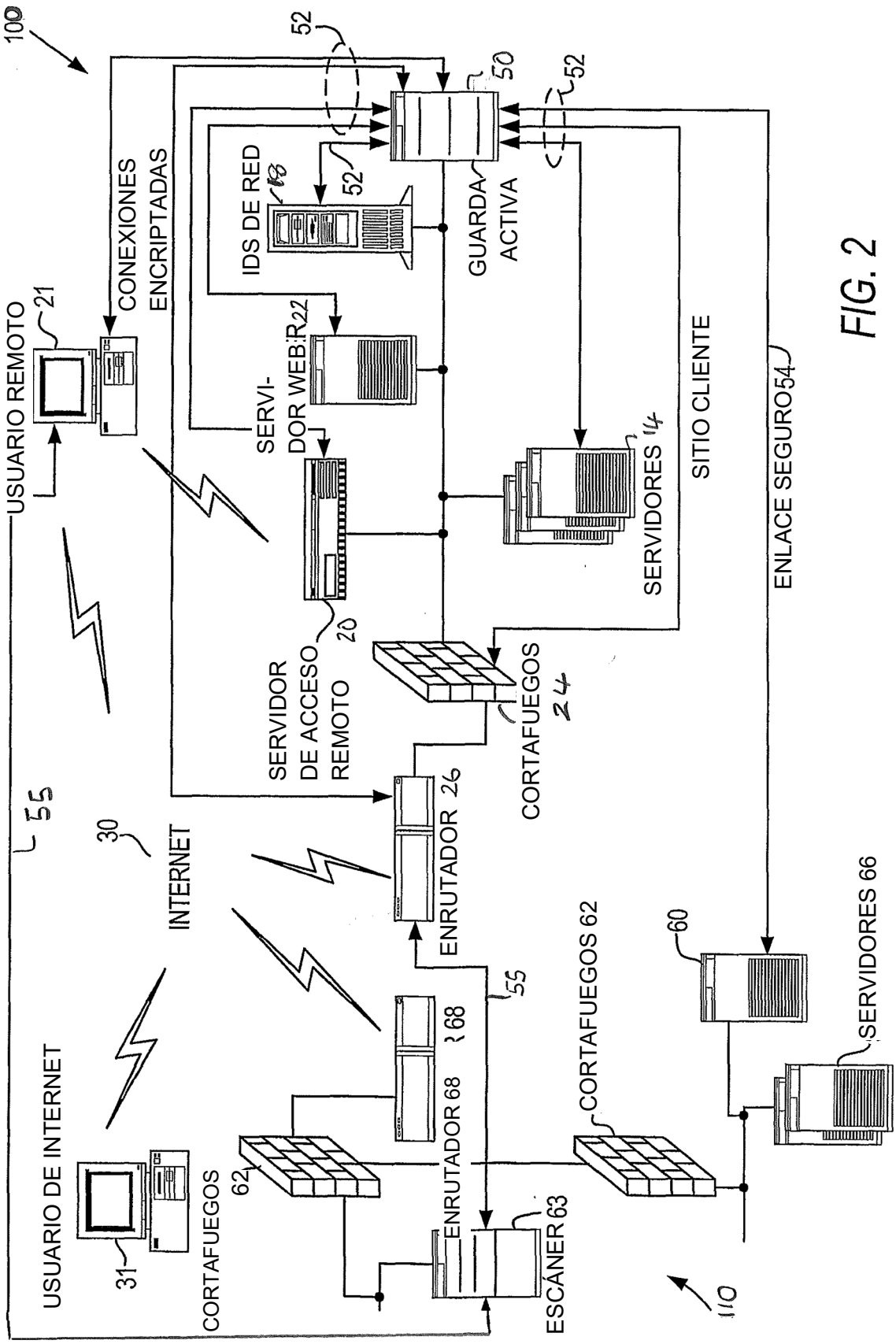
100
52
50
52
CONEXIONES ENCRIPTADAS
IDS DE RED 18
52
GUARDA ACTIVA
USUARIO REMOTO 21
SERVI-DOR WEB 22
SITIO CLIENTE
SERVIDORES 14
ENLACE SEGURO 54
SERVIDOR DE ACCESO REMOTO 20
CORTAFUEGOS 24
55
30
INTERNET
ENRUTADOR 26
CORTAFUEGOS 62
60
SERVIDORES 66
ENRUTADOR 68
55
USUARIO DE INTERNET
31
CORTAFUEGOS 62
ESCÁNER 63
110

FIG. 2