(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 312 573**

(51) Int. Cl.:
G06F 17/30 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02730949 .1**
(96) Fecha de presentación : **21.05.2002**
(97) Número de publicación de la solicitud: **1479191**
(97) Fecha de publicación de la solicitud: **24.11.2004**

(54) Título: **Sistema y procedimiento para interceptar un acceso de red.**

(30) Prioridad: **26.02.2002 KR 10-2002-0010156**

(45) Fecha de publicación de la mención BOPI:
01.03.2009

(45) Fecha de la publicación del folleto de la patente:
01.03.2009

(73) Titular/es: **Netpia.Com, Inc.**
35-1, 8-GA, Youngdeungpo-dong,
Youngdeungpo-gu
Seoul 150-038, KR

(72) Inventor/es: **Lee, Pan-Jung;**
Bae, Jeen-Hyun y
Cho, Byung-Chul

(74) Agente: **Ponti Sales, Adelaida**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Sistema y procedimiento para interceptar un acceso de red.

Antecedentes de la invención

Campo de la invención

La presente invención se refiere a un sistema y procedimiento para interceptar el acceso a una red. Más específicamente, la presente invención se refiere a un sistema y procedimiento para interceptar selectivamente el acceso a un sitio predeterminado en una red que comprende Internet.

Descripción de la técnica relacionada

A través de Internet, una red inmensa, se han llegado a compartir diferentes tipos de información generada globalmente, según técnicas recientes de desarrollo de la red, y por consiguiente han aumentado también los sitios que proporcionan diferentes servicios a través de Internet.

En esta progresión se han activado también sitios dañinos que proporcionan información mala. Con relación a esto, algunas personas han expresado su opinión respecto a la protección de los menores y, consiguientemente, se han desarrollado soluciones para evitar su acceso a los sitios dañinos.

Los procedimientos para interceptar el acceso a sitios predeterminados como los sitios dañinos se clasifican como procedimientos centrados en el cliente y procedimientos centrados en el servidor.

El procedimiento centrado en el cliente es un procedimiento que consiste en instalar programas de interceptación de pornografía en cada ordenador personal, e interceptar una solicitud de acceso cuando se produce una solicitud de acceso a un sitio predeterminado registrado previamente en una base de datos. Dicho procedimiento se ha utilizado en el pasado.

Sin embargo, el procedimiento arriba descrito no distribuye los programas de una forma fluida, y es molesto tener que volver a instalar los programas correspondientes cada vez que se instala el O/S (sistema operativo).

En el procedimiento centrado en el servidor, al cual se refiere también como un procedimiento de servidor delegado (proxy), el servidor delegado intercepta el acceso a un sitio predeterminado cuando se produce una solicitud de acceso al sitio predeterminado registrado con anterioridad. En este procedimiento, no existe la necesidad de instalar programas en el ordenador cliente, pero se requiere reconfigurar una red de forma que todos los usuarios de la red deban utilizar el servidor delegado correspondiente, y además se requiere configurar una red diferente para cada grupo de usuarios para proporcionar un grado de protección diferente a cada grupo.

WO 01/98934 describe un programa de filtrado de contenido de Internet que comprende dos componentes. Un componente se ejecuta en un servidor de Internet y el otro se ejecuta localmente en un ordenador de usuario. Los dos componentes cooperan mútuamente para filtrar el contenido de Internet, donde cada componente realiza tareas separadas. El componente del servidor de Internet almacena perfiles de usuario, una lista y/o tabla de URL prohibidos y permitidos, y recibe solicitudes de URL redireccionadas. Las solicitudes de URL redireccionadas se utilizan, junto con un perfil de usuario, para determinar si se permite o niega el acceso al contenido asociado con el URL. El componente que se ejecuta localmente sobre un sistema de ordenador de usuario actúa como un cliente del componente del servidor de Internet, realizando funciones de identificación y conexión para un usuario, exploración de contenidos de Internet asociados con URL permitidos, y actualización del componente del servidor de Internet con un URL, que indica que el URL se prohibe si se localiza una palabra o frase predeterminada dentro del contenido de Internet asociado con el URL.

WO 01/55873 describe un procedimiento y sistema para proporcionar acceso flexible a sitios de Internet. El sistema comprende una base de datos de sitios de Internet que se han clasificado en categorías de forma que el sistema determina la categoría de la información a la que accede un usuario en Internet. El sistema se programa también de forma que se permite a los usuarios acceder solamente un número limitado de veces a los sitios de una categoría concreta. Además, los usuarios pueden solicitar un acceso diferido, donde el sitio que se solicita se almacena en un servidor y se encuentra disponible para el usuario en un momento posterior. Además si un usuario elige acceder a un sitio que se encuentra comprendido dentro de ciertas categorías predefinidas, se presenta al usuario la posibilidad de acceder a la página pero advirtiéndole de que su acceso quedará registrado en un fichero.

US 6.065.056 describe un sistema para bloquear actividades no deseadas en la utilización del ordenador. Una aplicación de monitorización que se titula “X-Stop” se ejecuta en segundo plano en un ordenador que tiene acceso a Internet. La aplicación X-Stop contiene un módulo de teclado, un módulo de ratón, un módulo de portapapeles y un módulo de conexión a Internet en Windows (winsock). Cada módulo monitoriza los datos que entran o salen de la aplicación principal del ordenador y compara los datos con los almacenados en librerías almacenadas en memoria. Si se encuentra una correspondencia en una librería, se inicia una rutina de bloqueo y se muestra una ventana de texto para introducir una contraseña de desbloqueo por parte de un supervisor.

Pensando en la finalidad anterior, la presente invención es un sistema para el control de la interceptación del acceso entre una pluralidad de anfitriones primeros y de anfitriones segundos a través de una red según la reivindicación 1, y un procedimiento para el control de la interceptación del acceso entre una pluralidad de anfitriones primeros y de anfitriones segundos a través de una red en un sistema según la reivindicación 7.

Otras características de la invención se encuentran en las reivindicaciones dependientes.

Resumen de la invención

Una ventaja de la presente invención es proporcionar un servicio de interceptación de acceso a sitios predeterminados a usuarios que desean la interceptación del acceso.

En concreto, una ventaja de la presente invención es interceptar el acceso a sitios predeterminados sin la instalación de programas adicionales para la interceptación de acceso a sitios, y sin reconfiguración de la red.

En un aspecto de la presente invención, un sistema de interceptación de acceso conectado a una pluralidad de anfitriones primeros y de anfitriones segundos a través de una red comprende:

una base de datos de información de interceptación para almacenar información sobre los anfitriones segundos que son objetivos de la interceptación de acceso, e información sobre la configuración de la interceptación; un monitor de red para monitorizar un estado de generación de paquetes de transmisión procedentes del anfitrión primero de la red, y recibir los paquetes de transmisión generados; un procesador de acceso para determinar si un destino incluido dentro de los paquetes de transmisión recibidos es un objetivo de la interceptación de acceso sobre la base de la información almacenada dentro de la base de datos de información de interceptación; y un generador de paquetes para generar un paquete de interceptación de acceso, y transmitirlo al anfitrión primero de forma que el anfitrión primero pueda detener el intento de acceso a la red, cuando el destino de los paquetes de transmisión es un objetivo de la interceptación de acceso según el resultado de la determinación.

El paquete de interceptación de acceso comprende un formato de mensaje IC-MP (protocolo de mensaje de control de Internet) con un código de “red inaccesible”, y el anfitrión primero determina que la red es inaccesible y detiene el intento de acceso al anfitrión segundo cuando se recibe el paquete de interceptación de acceso.

El sistema de interceptación de acceso recibe direcciones IP de los anfitriones primeros que han solicitado interceptación de acceso a un ISP (proveedor de acceso a Internet), y el procesador de acceso determina si el destino de los paquetes de transmisión es un objetivo de interceptación de acceso y realiza selectivamente el proceso de la interceptación de acceso cuando la dirección IP del anfitrión primero que ha generado los paquetes de transmisión se corresponde con la dirección IP proporcionada por el ISP.

La información de configuración de interceptación almacenada en la base de datos de información de interceptación comprende una fecha u hora para la interceptación del anfitrión segundo que es un objetivo de la interceptación de acceso, y el procesador de acceso controla al generador de paquete para realizar el proceso de la interceptación de acceso cuando se establece que el objetivo de interceptación de acceso debe ser interceptado en la fecha u hora actuales en el caso de que el destino del paquete de transmisión sea un objetivo de la interceptación de acceso.

La información de configuración de interceptación comprende la autenticación del usuario que ha solicitado la interceptación de acceso, y el procesador de acceso realiza la modificación de la fecha o la hora y la cancelación de la interceptación según una solicitud por parte del usuario autenticado.

Los anfitriones primeros se conectan a un concentrador conmutador, y el sistema de interceptación de acceso monitoriza los paquetes generados por los anfitriones primeros y transmite/recibe los paquetes a través de un concentrador virtual conectado al concentrador conmutador.

En otro aspecto de la presente invención, un procedimiento para controlar la interceptación del acceso entre una pluralidad de anfitriones primeros y de anfitriones segundos a través de una red comprende: (a) monitorizar un estado de generación de paquetes de transmisión procedentes del anfitrión primero de la red; (b) recibir los paquetes de transmisión generados por el anfitrión primero de la red; (c) determinar si el anfitrión segundo que es un destino comprendido dentro de los paquetes de transmisión recibidos es un objetivo de la interceptación de acceso; y (d) generar un paquete de interceptación de acceso cuando el anfitrión segundo que es el destino de los paquetes de transmisión es un objetivo de la interceptación de acceso según el resultado determinado, y transmitir el paquete de interceptación de acceso al anfitrión primero de forma que el anfitrión primero puede detener el intento de acceso a red.

La etapa (a) comprende: recibir direcciones IP de los anfitriones primeros que han solicitado interceptación de acceso por parte de un ISP; determinar si la dirección IP del anfitrión primero que ha generado el paquete de transmisión se corresponde con la dirección IP proporcionada por el ISP; y determinar si el anfitrión segundo que es un destino del paquete de transmisión es un objetivo de la interceptación de acceso cuando la dirección IP del anfitrión primero que ha generado el paquete de transmisión se corresponde con la dirección IP proporcionada por el ISP según el resultado determinado.

El procedimiento comprende además: recibir del usuario del anfitrión primero una fecha u hora deseada de cancelación del anfitrión segundo que es un objetivo de la interceptación de acceso, y establecer la fecha y hora; y modificar la fecha u hora y realizar la cancelación de la interceptación de acceso para un usuario autenticado, y la etapa (d) comprende además generar un paquete de interceptación de acceso y transmitir el paquete de interceptación de acceso al anfitrión primero cuando el anfitrión segundo que es un destino del paquete de transmisión es un objetivo de la interceptación de acceso y el anfitrión segundo se establece para tener el acceso interceptado en la fecha u hora actuales.

Breve descripción de las figuras

Las figuras adjuntas, que se incorporan y constituyen una parte de la especificación, ilustran una realización de la presente invención y, junto con la descripción, sirven para explicar los principios de la presente invención:

la figura 1 muestra una arquitectura general de capa TCP-IP;

la figura 2 muestra una configuración de un sistema de interceptación de acceso a red según una realización preferida de la presente invención;

la figura 3 muestra un diagrama de configuración de un paquete de interceptación de acceso según una realización preferida de la presente invención; y

la figura 4 muestra un diagrama de flujo de un procedimiento de interceptación de acceso a red según una realización preferida de la presente invención.

Descripción detallada de las realizaciones preferidas

En la siguiente descripción detallada, solamente se muestra y describe la realización preferida de la presente invención, simplemente a modo de ilustración del mejor modo de realizar la invención contemplado por los inventores. Como se hará presente, la presente invención se puede modificar en diferentes aspectos obvios, sin salir de la invención. Por consiguiente, las figuras y la descripción se deben contemplar como de naturaleza ilustrativa, y no restrictiva.

En el pasado algunos usuarios crearon redes independientes y, por consiguiente, los usuarios debían establecer entornos de hardware de comunicación según sus propias especificaciones de red. Pero puesto que no existía ninguna red que soportara todos los tipos de especificaciones de red, era imposible construir una red amplia utilizando una única especificación de hardware.

Para solucionar este problema, se desarrolló el TCP/IP (protocolo de transmisión/protocolo de Internet) para la comunicación entre diferentes dispositivos, y se convirtió en la base de la red de conmutación de paquetes, la ARPANET (red de la agencia de proyectos de investigación avanzados). La técnica TCP/IP ha formado un fundamento para construir la Internet mundial a la cual se conectan actualmente hogares, campus, escuelas, empresas comerciales y centros de investigación gubernamentales.

La figura 1 muestra una arquitectura general de capa TCP/IP. Como se muestra, TCP/IP comprende una capa de aplicación, una capa de transporte de anfitrión a anfitrión, una capa de Internet, y una capa de interficie de red.

La capa de Internet se utiliza para establecer la ruta de los datos desde un anfitrión de transmisión hasta un anfitrión receptor que es un destino, y comprende un IP (protocolo de Internet), un ICMP (protocolo de mensaje de control de Internet), un IGMP (protocolo de gestión de grupo de Internet) y un ARP (protocolo de resolución de dirección).

IP es un protocolo para controlar la transmisión y recepción de paquetes de datos (datagramas) en una red y entre redes, y se encuentra acoplado con una capa de red en el modelo OSI. El ICMP es un protocolo para controlar los mensajes entre un servidor anfitrión y una pasarela de Internet, y para notificar errores. Los mensajes de control del ICMP se cargan en una unidad de datos de un datagrama IP, y a continuación se transmiten, y tienen funciones de control de errores de transmisión, comprobar si se alcanza el destino final, informar al anfitrión original, controlar las velocidades de transmisión cuando las velocidades de transmisión no pueden ser controladas por un anfitrión o una pasarela, y solicitar la modificación de una ruta de comunicación desde una pasarela.

En la realización preferida de la presente invención, el ICMP con las funciones arriba mencionadas se utiliza para detectar si el estado de la conexión de red se encuentra mal físicamente, y rechazar la recepción de paquetes transmitidos desde un anfitrión predeterminado.

La figura 2 muestra un sistema de interceptación de acceso según una realización preferida de la presente invención.

El sistema de interceptación de acceso 10 se conecta a los anfitriones primeros 31 a 3n y a los anfitriones segundos 41 a 4m a través de Internet 20. En detalle, el sistema de interceptación de acceso 10 se conecta a un concentrador virtual 60 conectado a un concentrador conmutador 50 para conectarse a los anfitriones primeros 31 a 3n; y el concentrador virtual 60 se conecta a Internet a través de un encaminador 70, y los anfitriones segundos 41 a 4m se conectan a internet 20. Por tanto, el sistema de interceptación de acceso 10 transmite y recibe paquetes a/desde los anfitriones

primeros 31 a 3n a través del concentrador virtual 60 y del concentrador conmutador 50, y también transmite y recibe paquetes a/desde los anfitriones segundos 41 a 4m a través del concentrador virtual 60, el encaminador 70 e Internet 20.

En este caso, para facilitar la descripción sin restringirse a la misma, un anfitrión que intenta el acceso, es decir un ordenador que permite la comunicación bidireccional con otros ordenadores a través de Internet, es referido como "anfitrión primero", y un anfitrión al que se accede, como un sitio, es referido como "anfitrión segundo".

Puesto que los anfitriones primeros 31 a 3n se conectan a una pluralidad de puertos del concentrador conmutador 50, los datos generados por los anfitriones primeros 31 a 3n conectados a los puertos respectivos se introducen en el concentrador conmutador 50 y a continuación se transmiten, y el concentrador conmutador 50 analiza los datos, selecciona el destino, y envía los datos al destino o, cuando no se han establecido puertos en espejo, los transmite el concentrador conmutador 50. Aquí, el concentrador conmutador se utiliza para mejorar las velocidades de la red y, además, se puede utilizar también un concentrador general.

Puesto que el concentrador virtual 60 funciona solamente en el procedimiento de transmisión, el concentrador virtual 60 conecta al concentrador conmutador 50 con el sistema de interceptación de acceso cuando el concentrador conmutador 50 no soporta puertos en espejo.

El encaminador 70 es un dispositivo para conectar redes separadas utilizando el mismo protocolo de transmisión, y conecta las capas de red para transmitir datos. Esto es, el encaminador 70 determina un nodo de otra red o una red del encaminador 70 según una tabla de asignación de ruta, y también selecciona la ruta más efectiva entre muchas rutas y transmite los datos.

El sistema de interceptación de acceso 10 conectado al concentrador virtual 60, para interceptar el acceso a sitios predeterminados, comprende una base de datos de información de interceptación 11, un monitor de red 12, un procesador de acceso 13, y un generador de paquete 14.

La base de datos de información de interceptación 11 almacena información sobre los anfitriones segundos que son objetivos de la interceptación de acceso, e información sobre la configuración de interceptación (es decir, una fecha, un periodo, una hora para interceptar, e información de autenticación de un solicitante de interceptación), por ejemplo información que comprende direcciones IP de los anfitriones segundos que corresponden a sitios de pornografía, y URL (localizadores uniformes de recursos). Además, puede almacenar también información sobre solicitantes de interceptación de acceso (por ejemplo direcciones IP) proporcionada por los ISP (proveedores de servicios de Internet) para interceptar el acceso de los anfitriones primeros que han solicitado la interceptación del acceso.

El monitor de red 12 monitoriza los estados de la transmisión de paquetes en la red a través del concentrador virtual 60 para recibir paquetes transmitidos.

El procesador de acceso 13 determina si se accede al destino correspondiente según si la base de datos de interceptación 11 almacena una dirección de destino a la cual se transmiten los paquetes recibidos por el monitor de red 12.

El generador de paquetes 14 genera paquetes de interceptación de acceso, y los transmite al anfitrión primero que ha transmitido los paquetes correspondientes (que se referirán de aquí en adelante como paquetes de transmisión) de forma que el anfitrión primero puede detectar que la red actual es inaccesible, cuando el destino al que se van a transmitir los paquetes de transmisión corresponde a un anfitrión objetivo de la interceptación de acceso según el resultado determinado procedente del procesador de acceso 13.

Los paquetes de interceptación de acceso se generan en el formato de mensajes ICMP. La figura 3 muestra una configuración resumida del mensaje ICMP.

El paquete de interceptación de acceso es un mensaje ICMP con una cabecera de 64 bits y, como se muestra en la figura 3, puede ser uno de una pluralidad de tipos cada uno de los cuales presenta una pluralidad de códigos. También comprende una suma de control que representa un número de bits en una unidad de transmisión de forma que una parte receptora pueda comprobar si ha llegado la misma cantidad de bits, detectando de esta forma errores de transmisión.

En este caso un código de "red inaccesible" se registra en los códigos y se transmite de forma que el anfitrión primero detecte que la red es inaccesible. Por tanto, el anfitrión primero detiene el intento de acceso según el estado inaccesible de la red, y cuando se envía un paquete de respuesta desde el anfitrión segundo que es el destino del paquete, el anfitrión primero no lo recibe.

A continuación, se describirá un procedimiento para la interceptación del acceso a un anfitrión predeterminado sobre la base del sistema de interceptación de acceso anteriormente configurado.

La figura 4 muestra un diagrama de flujo para un procedimiento de interceptación de acceso según una realización preferida de la presente invención.

El sistema de interceptación de acceso 10 funciona en el modo de monitorización de los estados de generación de paquetes sobre la red, como en un modo promiscuo.

En este estado, como se muestra en la figura 4, el anfitrión primero 31 que intenta acceder al anfitrión segundo que es un sitio predeterminado conectado a Internet 20 genera paquetes de transmisión que comprenden una dirección del anfitrión segundo al que desea acceder el destino en la etapa S100.

Como se ha descrito, los paquetes de transmisión generados por los anfitriones primeros respectivos se transmiten al concentrador conmutador 50 a través de los puertos correspondientes, y el concentrador conmutador 50 emite los paquetes de transmisión en la etapa S110. Por tanto, los paquetes de transmisión se transmiten a otro anfitrión primero conectado a una LAN 80, y también al sistema de interceptación de acceso 10 conectado al servidor virtual 60. Además se transmiten al anfitrión segundo 41, que es el destino correspondiente, a través del encaminador 70.

El monitor de red 12 del sistema de interceptación de acceso 10 funciona en modo promiscuo y utiliza la función de espejo de puerto para monitorizar la red en la etapa S120, y cuando se transmiten los paquetes de transmisión desde el anfitrión primero, el monitor de red 12 recibe los paquetes de transmisión emitidos y los proporciona al procesador de acceso 13 en la etapa S130.

En primer lugar, el procesador de acceso 13 determina si el anfitrión primero que ha transmitido los paquetes de transmisión es un usuario que ha solicitado un servicio de interceptación de acceso en las etapas S140 y S150.

En la realización preferida de la presente invención, para interceptar a los usuarios que han solicitado del ISP el servicio de interceptación sin interceptar a todos los subscriptores del ISP, cuando un subscriptor de ISP solicita acceso a un sitio predeterminado (un anfitrión segundo), el ISP registra al subscriptor correspondiente como solicitante de interceptación de acceso, y proporciona la información correspondiente al sistema de interceptación de acceso.

En este caso, la base de datos de información de interceptación 11 almacena información sobre el solicitante de interceptación de acceso (por ejemplo, una dirección IP), el procesador de acceso 13 determina si la dirección IP del anfitrión primero 31 que ha generado los paquetes de transmisión se corresponde con el solicitante de interceptación de acceso proporcionado desde el ISP sobre la base de la información almacenada en la base de datos de información de interceptación 11, y cuando la dirección IP corresponde al solicitante de interceptación de acceso, se utiliza la información de la base de datos de interceptación para determinar si el destino de los paquetes de transmisión correspondientes es un objetivo de la interceptación.

Esto es, el procesador de acceso 13 analiza los paquetes de transmisión proporcionados desde el monitor de red 12 para encontrar una dirección de destino a la cual se transmitirán los paquetes de transmisión, y determina si la dirección de destino se encuentra almacenada en la base de datos de información de interceptación 11 en la etapa S160.

Cuando la dirección de destino de los paquetes de transmisión se encuentra almacenada en la base de datos de información de interceptación 11, el procesador de acceso 13 determina que el destino de los paquetes de transmisión es un objetivo de la interceptación de acceso como un sitio de pornografía, por tanto controla al generador de paquetes 14 para generar un paquete de interceptación de acceso que tiene al anfitrión primero que requiere el acceso como destino con el formato del mensaje ICMP conteniendo un código de “red inaccesible”, de forma que no se pueda transmitir ni recibir ningún paquete entre el anfitrión primero que había solicitado el acceso y el anfitrión segundo que es un objetivo del acceso en las etapas S170 y S180.

El paquete de interceptación de acceso generado por el generador de paquetes 14 se transmite al concentrador conmutador 50 a través del concentrador virtual 60, y el concentrador conmutador 50 transmite el paquete de interceptación de acceso al anfitrión primero correspondiente 31 según la dirección de destino del paquete de interceptación de mensaje en la etapa S190.

Cuando se transmite el paquete de interceptación de acceso después de la solicitud de acceso, y el código del paquete de interceptación de acceso es un código de “red inaccesible”, el anfitrión primero 31 determina que el acceso al anfitrión segundo es imposible, y detiene el intento de acceso en las etapas S200 y S210. Esto es lo mismo que en el caso en el que el acceso a un sitio correspondiente es imposible porque un cable de LAN se encuentra desconectado o un encaminador presenta algún problema de funcionamiento.

Por tanto, cuando el anfitrión segundo (por ejemplo un sitio de pornografía) que ha recibido los paquetes de transmisión a través del encaminador 70 genera un paquete de respuesta en el cual se registra el anfitrión primero que ha transmitido los paquetes de transmisión al destino, y transmite el paquete de respuesta al anfitrión primero, el anfitrión primero no recibe el paquete de respuesta puesto que el anfitrión primero ya ha detenido el intento de acceso según el estado de red inaccesible.

Como resultado, cuando no se encuentra instalado en cada anfitrión primero un programa de interceptación de acceso, y la red no se encuentra configurada de forma que todos los anfitriones primeros deban utilizar un servidor delegado predeterminado, se consigue de forma sencilla la interceptación del acceso a sitios predeterminados.

Cuando la dirección de destino de los paquetes de transmisión no se encuentra almacenada en la base de datos de información de interceptación 11, se determina que el destino de los paquetes de transmisión no es un objetivo de la interceptación de acceso, y no se realiza la interceptación del acceso. Por tanto, en este caso, cuando los paquetes de transmisión enviados sobre la red se transmiten al anfitrión segundo 41 que es el destino correspondiente a través del encaminador 70, el anfitrión segundo 41 genera un paquete de respuesta acoplado con el paquete de transmisión, y transmite el mismo al anfitrión primero 31. Por consiguiente, los paquetes se transmiten y reciben entre el anfitrión primero 31 y el anfitrión segundo 41, y el anfitrión primero 31 obtiene la información deseada del anfitrión segundo 41 en la etapa S220.

La interceptación de acceso arriba mencionada se puede aplicar en redes de tamaño ISP y en redes pequeñas como una LAN.

Se pueden omitir las etapas S140 y S150 para determinar si el anfitrión primero es un usuario que solicitó la interceptación de acceso. Esto es, solamente por medio de comprobar si el destino del paquete de transmisión corresponde a un objetivo de la interceptación de acceso sin comprobar si el anfitrión primero que ha generado el paquete de transmisión es un usuario que ha solicitado la interceptación de acceso, se puede interceptar el acceso a un anfitrión predeterminado como se ha descrito anteriormente.

También, por medio de establecer los anfitriones segundos para realizar la interceptación de acceso para cada anfitrión primero, se puede interceptar el acceso a un anfitrión predeterminado para cada anfitrión primero.

Además, la interceptación de acceso se puede ejecutar solamente para el solicitante de interceptación de acceso por separación de mes, fecha y año. Esto es, el solicitante de interceptación de acceso puede solicitar la interceptación de acceso de una dirección predeterminada en una fecha u hora específicas y, por consiguiente, la interceptación de acceso arriba mencionada se puede realizar cuando la dirección de destino a la que se van a transmitir los paquetes de transmisión es un objetivo de interceptación de acceso y la interceptación de acceso se establece en la fecha y hora actuales. En este caso, se requiere el almacenamiento de información de autenticación del solicitante en la base de datos de información de interceptación de forma que solamente el solicitante correspondiente pueda establecer la interceptación de acceso o la cancelación, y el sistema de interceptación de acceso autentica al solicitante sobre la base de la información de autenticación, y ejecuta la interceptación de acceso o la cancelación. En este caso, la información de establecimiento de interceptación almacenada en la base de datos de información de interceptación comprende una fecha, un periodo, hora, y la información de autenticación del solicitante para la interceptación de un anfitrión segundo específico para cada anfitrión primero.

Como anteriormente se ha descrito, cuando no se encuentra instalado un programa de interceptación de acceso en todos los clientes, y la red no se encuentra configurada de forma que todos los clientes deban utilizar un servidor delegado específico, se logra fácilmente la interceptación del acceso a un sitio específico.

También, el acceso a sitios predeterminados se puede interceptar de forma sencilla sin modificar las configuraciones de red convencionales.

Además, la interceptación de acceso se puede realizar para direcciones IP específicas.

Por tanto, se pueden reducir las sobrecargas de ancho de banda por medio de interceptar en la red solicitudes de acceso no necesarias.

Mientras que la presente invención se ha descrito en conexión con lo que se considera actualmente como la realización más práctica y preferida, debe entenderse que la presente invención no se encuentra limitada a las realizaciones descritas sino que, por el contrario, pretende cubrir varias modificaciones y disposiciones equivalentes comprendidas dentro del ámbito de las reivindicaciones adjuntas.

Referencias citadas en la presente descripción

Esta lista de referencias citadas por el solicitante está prevista únicamente para ayudar al lector y no forma parte del documento de patente europea. Aunque se ha puesto el máximo cuidado en su realización, no se pueden excluir errores u omisiones y la OEP declina cualquier responsabilidad en este respecto.

Documentos de patente citados en la presente descripción

- WO 0198934 A [0008]
- WO 0155873 A [0009]
- US 6065056 A [0010]

REIVINDICACIONES

1. Sistema (10) para controlar la interceptación del acceso entre una pluralidad de anfitriones primeros (3n) y de anfitriones segundos (4m) a través de una red, que comprende:

una base de datos de información de interceptación (11) para almacenar información sobre los anfitriones segundos que son objetivos de la interceptación de acceso, e información sobre la configuración de la interceptación;

un monitor de red (12) para monitorizar un estado de generación de paquetes de transmisión del anfitrión primero sobre la red, y recibir los paquetes de transmisión generados;

un procesador de acceso (13) para determinar si un destino comprendido en los paquetes de transmisión recibidos es un objetivo de la interceptación de acceso sobre la base de la información almacenada en la base de datos de información de interceptación; y

un generador de paquetes (14) para generar un paquete de interceptación de acceso que comprende un código de red inaccesible, y transmitir el mismo al anfitrión primero de forma que el anfitrión primero puede detener el intento de acceso a red, cuando el destino de los paquetes de transmisión es un objetivo de la interceptación de acceso según el resultado determinado,

donde el sistema se conecta a un concentrador (50) que se sitúa en una posición que atraviesan los datos entre el anfitrión primero (3n) y el anfitrión segundo (4m), y se encuentra adaptado para transmitir el paquete de transmisión generado por el anfitrión primero al anfitrión segundo, y el monitor de red (12) se encuentra adaptado para monitorizar los paquetes de transmisión generados por los anfitriones primeros utilizando una función de espejo de puerto.

2. Sistema de la reivindicación 1, en el que el paquete de interceptación de acceso comprende un formato de mensaje ICMP (protocolo de mensaje de control de Internet) con un código de "red inaccesible", y el anfitrión primero se encuentra adaptado para determinar que la red es inaccesible y detener el intento de acceso al anfitrión segundo cuando recibe el paquete de interceptación de acceso.

3. Sistema de la reivindicación 1, en el que el sistema de interceptación de acceso se adapta para recibir direcciones IP de los anfitriones primeros que han solicitado interceptación de acceso a un ISP (proveedor de servicio de Internet), y el procesador de acceso se encuentra adaptado para determinar si el destino de los paquetes de transmisión es un objetivo de la interceptación de acceso y realizar selectivamente el proceso de interceptación de acceso, cuando la dirección IP del anfitrión primero que ha generado los paquetes de transmisión se corresponde con la dirección IP proporcionada por el ISP.

4. Sistema de la reivindicación 1, en el que la información de configuración de interceptación almacenada en la base de datos de información de interceptación comprende una fecha y hora para la interceptación del anfitrión segundo que es un objetivo de la interceptación de acceso, y el procesador se encuentra adaptado para controlar al generador de paquetes para realizar el proceso de interceptación de acceso cuando se establece que el objetivo de interceptación de acceso va a ser interceptado en la fecha u hora actual en el caso de que el destino de los paquetes de transmisión es un objetivo de la interceptación de acceso.

5. Sistema de la reivindicación 1, en el que la información de configuración de interceptación comprende la autenticación del usuario que ha solicitado la interceptación de acceso, y el procesador de interceptación se encuentra adaptado para realizar la modificación de la fecha u hora y la cancelación de la interceptación según una solicitud por parte del usuario autenticado.

6. Sistema de la reivindicación 1, en el que los anfitriones primeros se conectan a un concentrador conmutador, y el sistema de interceptación de acceso se adapta para monitorizar los paquetes generados por los anfitriones primeros y para transmitir/recibir los paquetes a través de un concentrador virtual conectado al concentrador conmutador.

7. Procedimiento para controlar la interceptación de acceso entre una pluralidad de anfitriones primeros (3n) y de anfitriones segundos (4m) a través de una red en un sistema (10), que comprende:

(a) monitorizar, por parte del sistema (10) un estado de generación de paquetes de transmisión del anfitrión primero en la red;

(b) recibir, por parte del sistema (10), los paquetes de transmisión generados por el anfitrión primero en la red;

(c) determinar, por parte del sistema (10), si el anfitrión segundo, que es un destino comprendido en los paquetes de transmisión recibidos, es un objetivo de la interceptación de acceso; y

(d) generar, por parte del sistema (10), un paquete de interceptación de acceso con un código de red inaccesible cuando el anfitrión segundo que es el destino de los paquetes de transmisión es un objetivo de la interceptación de

acceso según el resultado determinado, y transmitir el paquete de interceptación de acceso al anfitrión primero de forma que el anfitrión primero puede detener el intento de acceso a la red,

donde el sistema (10) se encuentra conectado a un concentrador (50) que se encuentra situado en una posición que atraviesan los datos entre el anfitrión primero (3n) y el anfitrión segundo (4m), y el paquete de transmisión generado por el anfitrión primero se transmite al anfitrión segundo, y un monitor de red (12), comprendido en el sistema (10), monitoriza los paquetes de transmisión generados por el anfitrión primero utilizando una función de espejo de puerto.

8. Procedimiento de la reivindicación 7, en el que (a) comprende:

recibir desde un ISP (proveedor de servicio de Internet) direcciones IP de los anfitriones primeros que han solicitado la interceptación de acceso;

determinar si la dirección IP del anfitrión primero que ha generado el paquete de transmisión se corresponde con la dirección IP proporcionada por el ISP; y

determinar si el anfitrión segundo que es el destino del paquete de transmisión es un objetivo de la interceptación de acceso cuando la dirección IP del anfitrión primero que ha generado el paquete de transmisión se corresponde con la dirección IP proporcionada por el ISP según el resultado determinado.

9. Procedimiento de la reivindicación 7, que comprende además:

recibir la fecha u hora de interceptación deseada del anfitrión segundo que es un objetivo de la interceptación de acceso desde el usuario del anfitrión primero, y establecer la fecha y hora; y

modificar la fecha u hora y realizar la cancelación de acceso para un usuario autenticado, y (d) comprende además generar un paquete de interceptación de acceso y transmitir el paquete de interceptación de acceso al anfitrión primero cuando el anfitrión segundo que es un destino del paquete de transmisión es un objetivo de interceptación de acceso y el anfitrión segundo se establece para tener el acceso interceptado en la fecha u hora actual.

FIG.1

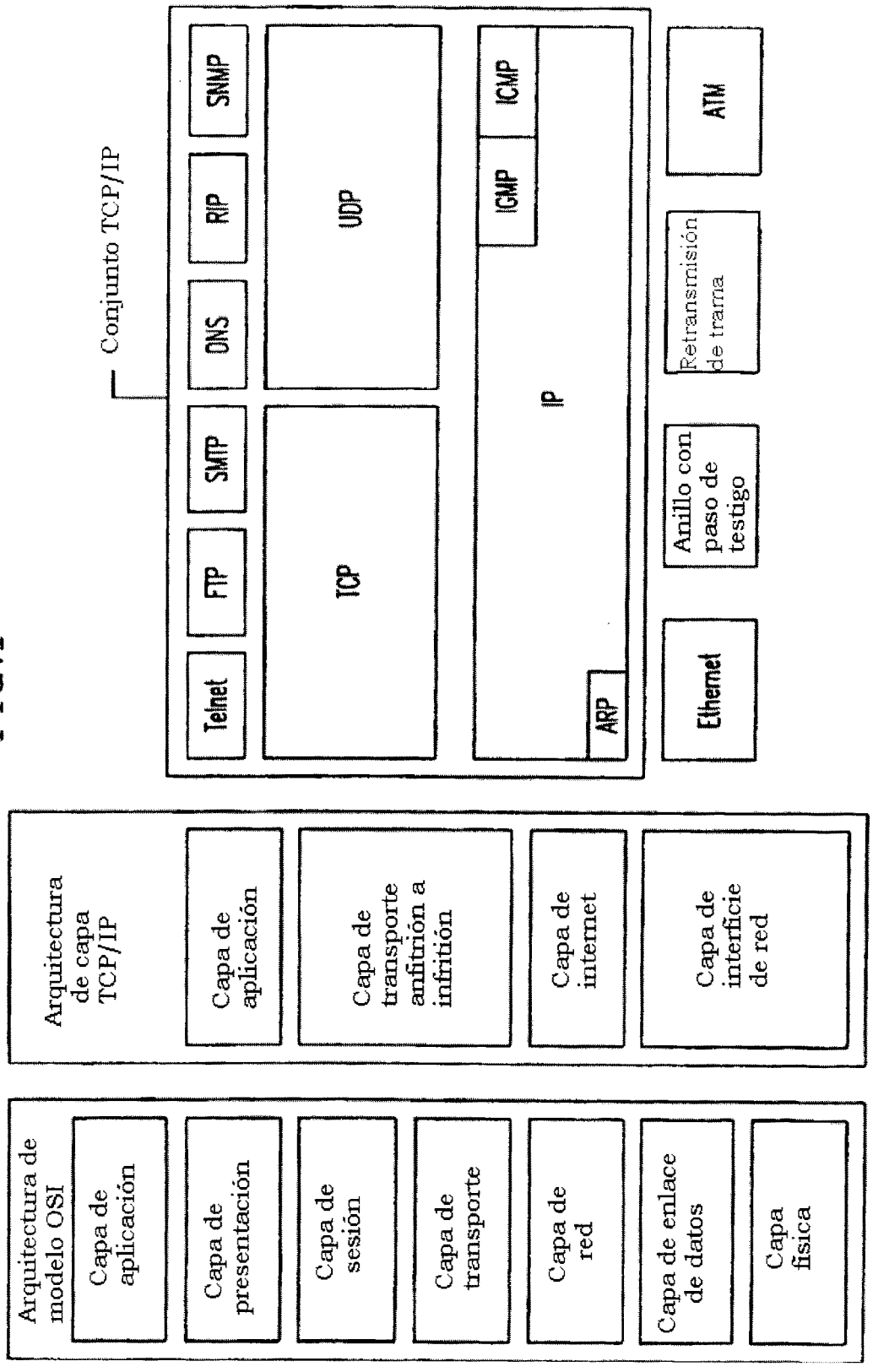

Arquitectura de modelo OSI
Capa de aplicación
Capa de presentación
Capa de sesión
Capa de transporte
Capa de red
Capa de enlace de datos
Capa física
Arquitectura de capa TCP/IP
Capa de aplicación
Capa de transporte anfitrión a infritión
Capa de internet
Capa de interficie de red
Conjunto TCP/IP
Telnet
FTP
SMTP
TCP
DNS
RIP
SNMP
UDP
IGMP
ICMP
IP
ARP
Ethernet
Anillo con paso de testigo
Retransmisión de trama
ATM

FIG.2

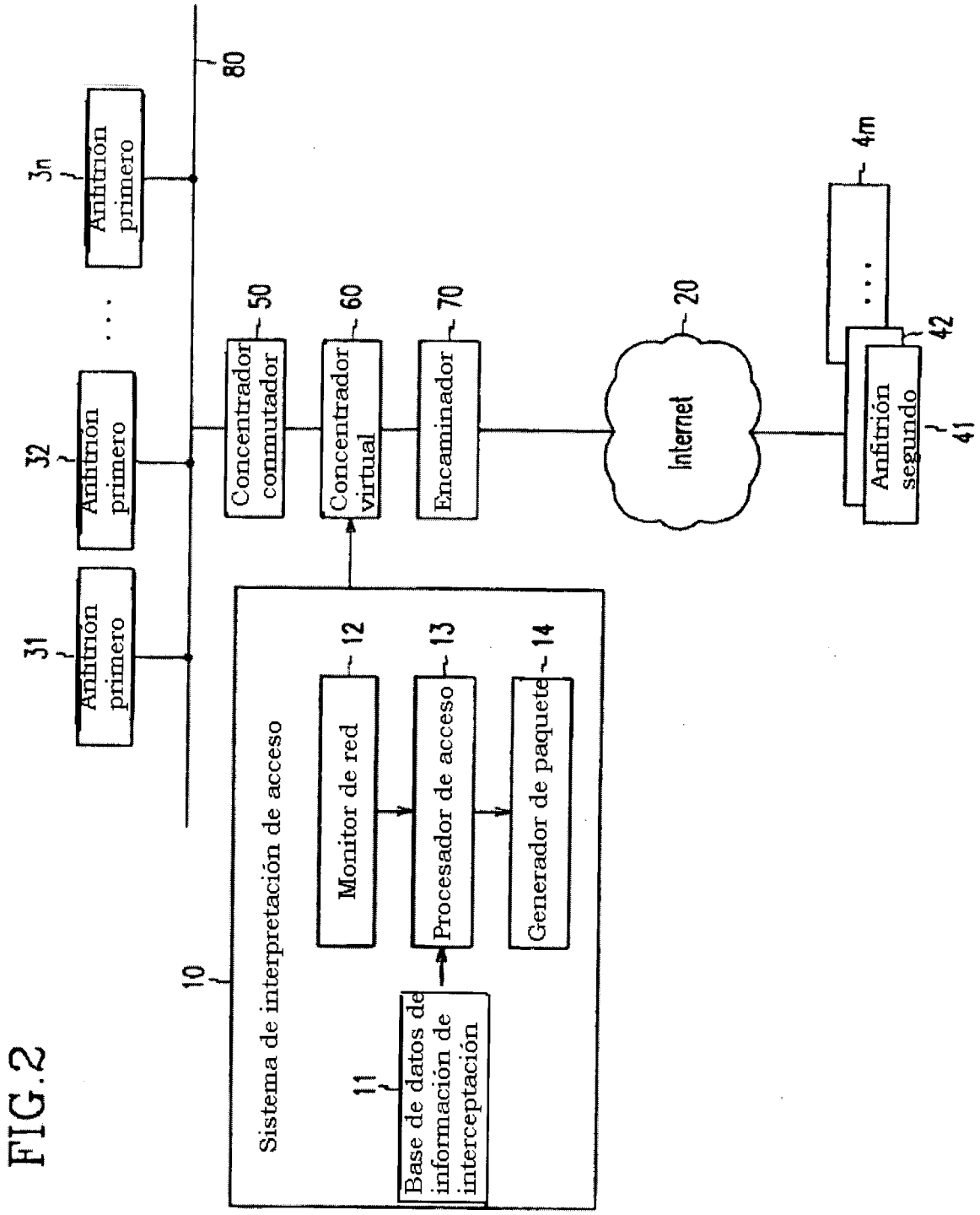

Anfitrión primero
31
Anfitrión primero
32
Anfitrión primero
3n
80
Concentrador conmutador
50
Concentrador virtual
60
Encaminador
70
Internet
20
Anfitrión segundo
41
42
4m
Sistema de interpretación de acceso
10
Monitor de red
12
Procesador de acceso
13
Generador de paquete
14
Base de datos de información de interceptación
11

FIG.3

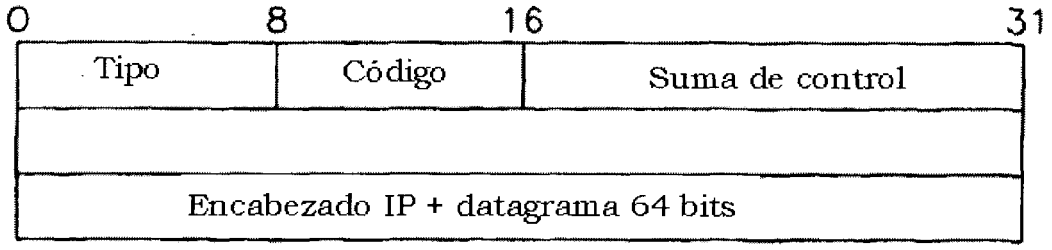
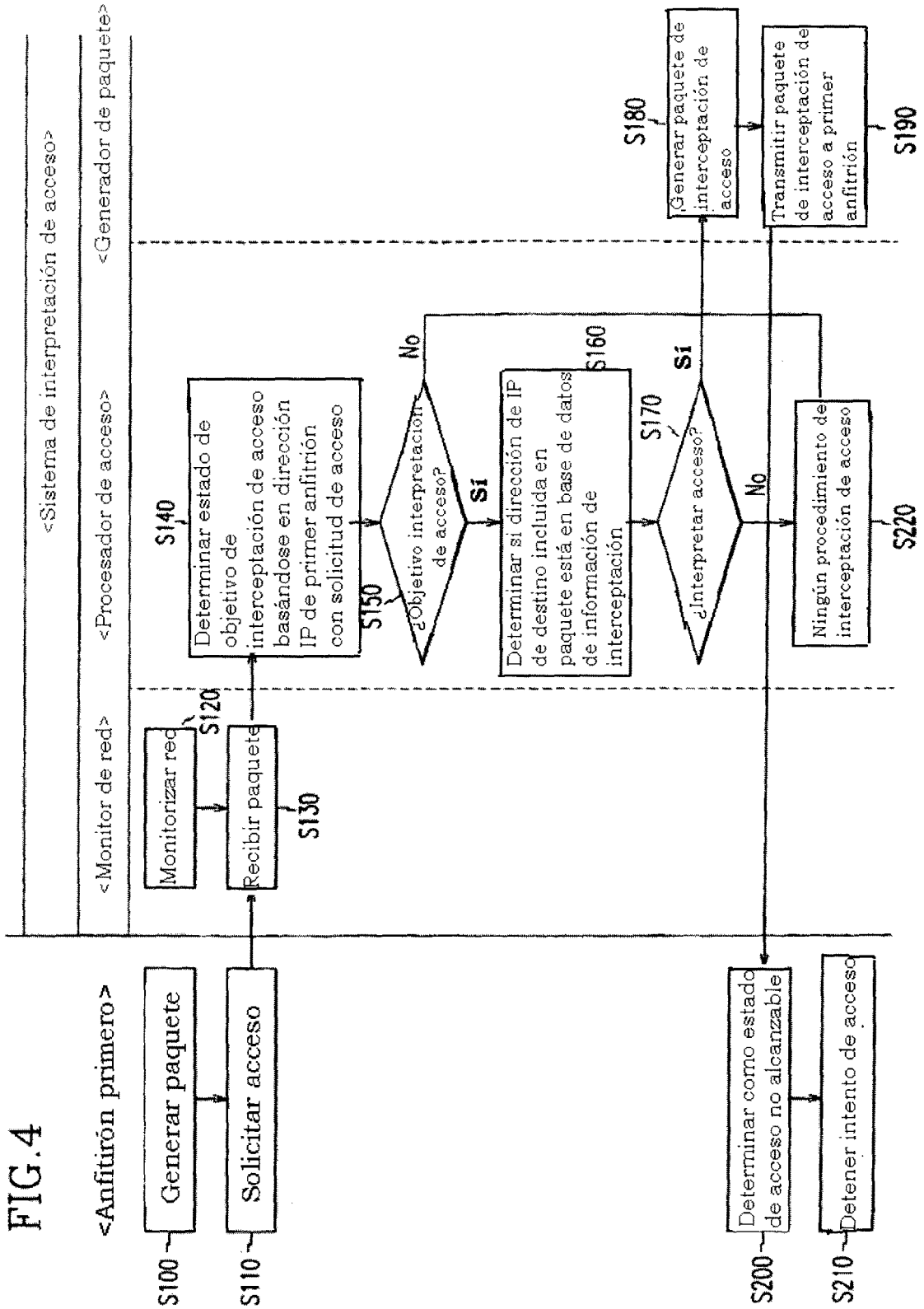

0
8
16
31
Tipo
Código
Suma de control
Encabezado IP + datagrama 64 bits

FIG.4


<Sistema de interpretación de acceso>
<Monitor de red>
<Procesador de acceso>
<Generador de paquete>
<Anfitrión primero>
Generar paquete
Solicitar acceso
Monitorizar red
Recibir paquete
Determinar estado de objetivo de interceptación de acceso basándose en dirección IP de primer anfitrión con solicitud de acceso
¿Objetivo interpretación de acceso?
Determinar si dirección de IP de destino incluida en paquete está en base de datos de información de interceptación
¿Interpretar acceso?
Generar paquete de interceptación de acceso
Transmitir paquete de interceptación de acceso a primer anfitrión
Ningún procedimiento de interceptación de acceso
Determinar como estado de acceso no alcanzable
Detener intento de acceso
S100
S110
S120
S130
S140
S150
S160
S170
S180
S190
S200
S210
S220
Sí
No