(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 296 798**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01968511 .4**
(86) Fecha de presentación : **06.09.2001**
(87) Número de publicación de la solicitud: **1317839**
(87) Fecha de publicación de la solicitud: **11.06.2003**

(54) Título: **Aparato y procedimiento para encriptar selectivamente la parte de carga útil de datos multimedia enviados a través de una red.**

(30) Prioridad: **06.09.2000 US 656166**

(45) Fecha de publicación de la mención BOPI:
01.05.2008

(45) Fecha de la publicación del folleto de la patente:
01.05.2008

(73) Titular/es: **Widevine Technologies, Inc.**
900 Fourth Avenue, Suite 3400
Seattle, Washington 98164, US

(72) Inventor/es: **Kollmyer, Brad;**
Baker, Brian;
Shapiro, Eric;
Kollmyer, Aric;
Rutman, Mike;
MacLean, Duncan;
Robertson, Dan;
Taylor, Neal;
Hunsche, Dick y
Walker, Amanda

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Aparato y procedimiento para encriptar selectivamente la parte de carga útil de datos multimedia enviados a través de una red.

Antecedentes de la invención

1. **Campo de la invención**

La presente invención se refiere en general a la transmisión de datos a través de una red y, más específicamente, a un aparato, sistema y procedimiento para encriptar y desencriptar selectivamente diferentes partes de datos enviados a través de una red.

2. **Descripción de la técnica relacionada**

La conexión en red, ejemplificada actualmente por Internet, comenzó como una manera de que los usuarios compartieran archivos e información basada en texto. Sin embargo, la tecnología ha avanzado mucho más allá del texto. Internet puede utilizarse para llevar a cabo videoconferencias en las que los participantes en la conferencia pueden verse unos a otros en tiempo real en sus pantallas de ordenador o dispositivos de conferencia conectados en red. Los usuarios de Internet pueden ver secuencias de vídeo en vivo de eventos a medida que éstos se producen, o ver programación grabada previamente "bajo demanda", es decir, siempre que elijan en lugar de una planificación de emisión.

Para entender cómo se transmite vídeo y contenido multimedia a través de Internet, primero es necesario entender el concepto de flujo continuo. El flujo continuo resuelve un problema de hace tiempo inherente al transmitir información de medios a través de Internet: los archivos multimedia son bastante grandes, y la mayoría de los usuarios tienen conexiones de red de un ancho de banda relativamente bajo. Enviar vídeos con calidad de emisión o audio con calidad de CD a través de Internet nunca ha sido fácil o práctico. Llevaría horas enviar un único archivo de audio o vídeo a través de Internet al ordenador de alguien. La persona en el otro extremo tendría que esperar hasta que se hubiera descargado todo el archivo antes de que pudiera comenzar la reproducción. La reproducción podría durar sólo algunos minutos.

Desde hace tiempo ha sido posible reducir la cantidad de datos requerida para transmitir material multimedia. Una manera es reducir la resolución, la frecuencia de imagen o la frecuencia de muestreo de los datos transmitidos, lo que tiene el efecto secundario de reducir la calidad percibida del contenido de audio o vídeo. Otro procedimiento comúnmente utilizado es aplicar compresión de datos para eliminar redundancias y conservar sólo los datos más esenciales de un archivo multimedia. Combinando estas dos técnicas, es posible producir archivos multimedia de calidad razonable que puedan transmitirse a través de conexiones de Internet típicas en tramas de tiempo similares al tiempo de ejecución del propio contenido de medios, es decir, minutos en lugar de horas. La calidad real de material multimedia descargado varía dependiendo del ancho de banda de red disponible y la buena disposición del usuario para esperar a que llegue; es posible establecer un equilibrio entre calidad y tamaño de archivo y preparar versiones de calidad superior del contenido para usuarios con más ancho de banda.

Cuando la cantidad de datos por segundo de contenido multimedia es igual o inferior a la cantidad de ancho de banda disponible para un usuario de red, puede producirse flujo continuo. El flujo continuo es esencialmente una entrega "justo a tiempo" de datos multimedia. El usuario no necesita esperar a que llegue todo el archivo antes de poder empezar a verlo, ni necesita dedicar una gran parte de almacenamiento de su ordenador para los datos recibidos. A medida que llegan al ordenador cliente, los datos multimedia se almacenan normalmente en una memoria intermedia que puede guardar varios segundos de datos, con el fin de evitar interrupciones en la reproducción provocadas por conexiones de red inestables. Cuando la memoria intermedia se llena inicialmente, lo que sucede en segundos en lugar de en minutos u horas, comienza la reproducción, y las tramas individuales de segmentos de vídeo y/o audio se recuperan de la memoria intermedia, se descodifican y se visualizan en el monitor de vídeo del cliente, se reproducen mediante el sistema de sonido del cliente, o se reproducen de otra manera a través del dispositivo conectado a la red del cliente. Después de que se han reproducido los datos, en muchos casos se desechan y deben transmitirse de nuevo si el usuario desea volver a ver una parte previa del programa.

La World Wide Web funciona con un modelo cliente/servidor; es decir, un usuario (es decir, un cliente) ejecuta un software en su ordenador personal u otro dispositivo de red (tal como un aparato de red o teléfono inalámbrico que puede acceder a Internet) que pueda acceder a los recursos de un servidor de red. El servidor puede permitir a muchos usuarios diferentes acceder a sus recursos al mismo tiempo y no necesita dedicarse a proporcionar recursos a un único usuario. En este modelo, el software cliente, es decir, un navegador o un reproductor, se ejecuta en el ordenador del usuario. Cuando un usuario solicita un vídeo u otro contenido multimedia que está en la web, su software cliente contacta con el servidor web que contiene la información o recursos deseados y envía un mensaje de solicitud. El servidor web localiza y envía la información solicitada al navegador o reproductor, que visualiza los resultados interpretando los datos recibidos según sea apropiado, por ejemplo visualizándolos como vídeo en la pantalla del ordenador.

La información de la web se direcciona por medio de Localizadores Uniformes de Recursos los (URL). Un URL especifica el protocolo que va a utilizarse para acceder a la información requerida (comúnmente HTTP, protocolo de

transferencia de hipertexto), la dirección o nombre de Internet del ordenador central que contiene la información, cualquier información de autenticación requerida para conseguir el acceso a la información (tal como un ID de usuario y contraseña), un número de puerto TCP/IP opcional si el recurso no está disponible en el puerto estándar para el protocolo especificado y una trayectoria para la información deseada en una jerarquía virtual designada por los operadores del servidor. Adicionalmente, el URL puede contener información introducida por el usuario tal como texto de consulta para una búsqueda en una base de datos. Los URL pueden especificarse de muchas maneras, incluyendo pero no limitándose a escribirse en un cliente web, pulsando sobre un "hiperenlace" en algún otro documento web, eligiendo un "marcador" en un navegador web para volver a una página visitada previamente o rellenando un formulario web y mandándolo al servidor.

Cuando se realiza una solicitud para un URL particular, la solicitud se envía al servidor apropiado utilizando el protocolo indicado en el URL, tal como HTTP, y los datos solicitados (o un mensaje de error si no puede satisfacerse la solicitud) se devuelven mediante el mismo procedimiento. Sin embargo, HTTP y otros protocolos web se añaden a los protocolos de Internet fundamentales, tales como TCP (protocolo de control de transmisión) o UDP (protocolo de datagramas de usuario). Los protocolos utilizados para medios de flujo continuo se añaden a estos protocolos fundamentales de la misma manera que lo hacen otros protocolos de alto nivel, tales como HTTP. Es esencial darse cuenta de que todo el tráfico de Internet se lleva mediante un número relativamente pequeño de protocolos fundamentales de bajo nivel tales como TCP y UDP, que se utilizan para establecer la conexión entre ordenadores que soporta el protocolo de nivel superior. Cuando el contenido multimedia se envía mediante flujo continuo, entonces, el servidor puede utilizar o bien TCP o bien UDP.

El RTP (protocolo de tiempo real), el RTSP (protocolo de flujo continuo de tiempo real) y el RTCP (protocolo de control de tiempo real) son tres de los muchos posibles protocolos de medios de flujo continuo que pueden añadirse a los protocolos de bajo nivel de Internet. De hecho, RTP, RTSP y RTCP sirven funciones complementarias y se utilizan más a menudo juntos como parte de algunas de las implementaciones de flujo continuo más comunes. RTSP se utiliza para configurar y gestionar una conexión de flujo continuo entre un servidor y un cliente, RTP se utiliza para entregar los datos multimedia reales, y RTCP proporciona sincronismo y otras señales de control entre el cliente y el servidor de flujo continuo. A menudo, RTP se envía sobre UDP, un protocolo de baja sobrecarga que entrega los datos tan rápidamente como sea posible, pero no garantiza que cualquier pieza particular de datos (un "paquete" en terminología de red) llegará realmente a su destino. Los paquetes RTCP se envían intercalados con los datos o en paralelo con el canal de medios RTP a través de TCP.

Un serio inconveniente al utilizar Internet para la distribución de medios mediante flujo continuo es que los datos primordiales pasan a menudo a través de redes y sistemas en su ruta hasta el cliente que el emisor de datos no controla. Una vez que los datos abandonan la red protegida del emisor, son vulnerables de interceptarse. Esto es particularmente preocupante cuando se transmiten a través de la red datos propietarios tales como una película, ya sea Internet pública o una red privada de terceras partes. Los datos pueden interceptarse y copiarse potencialmente en cualquier punto a medida que se transmiten a través de estas redes. Sin alguna manera de proteger los datos de la interceptación y de duplicación no autorizada, Internet nunca proporcionará la seguridad necesaria para permitir que los propietarios de derechos de autor distribuyan de manera segura sus trabajos a través de la red.

La encriptación es una manera de tratar esta cuestión. La encriptación proporciona una manera de codificar información de manera que sólo el destinatario previsto pueda verla. Aunque cualquiera puede interceptar los datos, sólo el destinatario legítimo podrá desencriptarlos, recuperar el mensaje original o contenido de medios y visualizarlos. Se han creado muchas soluciones de encriptación para proporcionar este tipo de seguridad. Por ejemplo, el software denominado VPN (red privada virtual) permite a un grupo de ordenadores conectados a Internet comportarse como si estuvieran conectados a una red local físicamente segura, utilizando encriptación para garantizar que sólo los ordenadores en la VPN pueden acceder a los recursos de la red privada. Otras aplicaciones de encriptación para permitir comunicaciones privadas a través de Internet incluyen pero no están limitadas a PGP (privacidad bastante buena), IPSec (Seguridad IP) y SSL (capa de conexiones seguras).

Las organizaciones, a menudo empresas pero no limitadas a las mismas, también protegen sus datos propietarios mediante la utilización de cortafuegos. Cada vez que una empresa se conecta su red informática interna o red de área local (LAN) a Internet, se enfrenta a un problema similar de que los datos privados sean interceptados. Puesto que la encriptación se utiliza para garantizar que los datos enviados a través de Internet pública sólo pueden utilizarse por destinatarios previstos, los cortafuegos tienen como objetivo mantener la información propietaria segura en una LAN que está conectada a Internet impidiendo que usuarios no autorizados accedan a la información almacenada en la red interna a través de Internet pública. Debido a la naturaleza pública de Internet, cada LAN conectada a ésta es vulnerable de ser atacada desde el exterior. Los cortafuegos permiten a cualquiera en la LAN protegida acceder a Internet de maneras permitidas mediante la configuración del cortafuegos, mientras que impiden que los piratas informáticos de Internet consigan acceso a la LAN y roben información y/o borren o estropeen de otro modo datos valiosos.

Los cortafuegos son dispositivos de propósito especial añadidos a encaminadores, servidores, y software especializado. Una de las clases más simples de cortafuegos utiliza filtrado de paquetes. En el filtrado de paquetes, un encaminador comprueba cada paquete de datos que se desplaza entre Internet y la LAN examinando su cabecera. Cada paquete TCP/IP presenta una cabecera que contiene la dirección IP del emisor y el receptor así como el número de puerto de la conexión y otra información. Examinando la cabecera, y en particular en número de puerto, el encamina-

dor puede determinar con bastante precisión el tipo de servicio de Internet para el que está utilizándose cada paquete. Cada servicio de Internet, incluyendo HTTP (la web), FTP (protocolo de transferencia de archivos), Telnet, rlogin y muchos otros, presentan un número de puerto estándar que se utiliza por convenio para la mayor parte de los accesos al servicio. Aunque puede utilizarse cualquier número de puerto para cualquier servicio, es mucho más conveniente para los usuarios utilizar los números de puerto estándar, y prácticamente todos los servicios de Internet previstos para su acceso por el público lo hacen. Una vez que el encaminador conoce para qué cliente y para qué servicio está destinado un paquete, puede simplemente bloquear el acceso externo a ordenadores centrales y servicios que los usuarios de Internet pública no deberían poder utilizar. Los administradores del sistema establecen las reglas para determinar qué paquetes deberían permitirse en la red y cuáles deberían bloquearse.

Los servidores proxy se utilizan comúnmente en conjunción con los cortafuegos. Un servidor proxy es una pasarela de software que se ejecuta en un ordenador que es accesible tanto por la LAN protegida como por Internet. Todos los accesos a Internet desde la LAN deben ir a través del servidor proxy, como deben hacerlo todos los accesos a la LAN desde Internet pública. Cuando un ordenador en la LAN solicita un recurso de Internet tal como una página web, esa solicitud se envía al servidor proxy. A continuación, el servidor proxy realiza la solicitud al recurso de Internet y reenvía de nuevo cualquier dato devuelto al solicitante original en la LAN. Puesto que Internet y la LAN se tocan sólo en el punto único del servidor proxy, que actúa como un intermediario, la protección de la red implica proteger sólo un ordenador, en vez de docenas o cientos. Los empresarios utilizan frecuentemente los servidores proxy para controlar y supervisar cómo sus empleados utilizan Internet, así como para impedir los intentos de intrusión desde Internet.

Una NAT, el término utilizado para redes que utilizan traducción de direcciones de red, complica también la entrega de datos de Internet. En una NAT, una red direccionada de manera privada se establece separada de Internet mediante un encaminador NAT. Este encaminador a su vez presenta una dirección de Internet pública. Traduciendo las direcciones de la red privada a direcciones reconocibles en Internet pública y viceversa, el encaminador NAT facilita la conectividad a Internet para las máquinas conectadas en red de manera privada. Las NAT se utilizan a menudo si hay disponibles números limitados de direcciones públicas en comparación con el número de usuarios (un usuario podría utilizar una NAT para múltiples máquinas compartiendo una conexión de módem de cable) o en conjunción con cortafuegos y/o proxys para proporcionar una capa adicional de seguridad a la red privada.

Los paquetes de datos pueden dividirse normalmente en dos partes, las partes de cabecera y de carga útil. La cabecera es la parte del paquete que incluye los encaminamientos u otra información de configuración. La carga útil es la parte del paquete de datos que es justo los datos de interés, como por ejemplo: contenido multimedia. Por ejemplo, en un paquete de red, la cabecera contiene datos para su utilización por encaminadores de red al entregar el paquete a su destino final, así como otros datos acerca del paquete tales como tamaño e información de formateado. En un paquete RTP a título de ejemplo, la cabecera contiene información de canales así como otra información necesaria para el reproductor para dirigir la carga útil (contenido de medios) RTP. Algunos paquetes complejos pueden contener múltiples cabeceras y diversa información de carga no útil y se hará referencia a los mismos en la presente memoria como la parte de carga no útil.

Muchas soluciones de encriptación actuales, tales como IPsec, encriptan datos de una manera demasiado indiscriminada, encriptando no sólo la carga útil sino también partes de la cabecera o parte de carga no útil. Sólo la información de encaminamiento permanece sin encriptar, prestando de ese modo información necesaria a los cortafuegos, los proxys y/o las NAT para retransmitir apropiadamente los paquetes cifrados que detendrán al paquete antes de que pueda transitar en una red privada o protegida. Otras soluciones proporcionan encriptación inadecuada para garantizar la integridad de los datos a través de la red pública. Algunas soluciones de encriptación de medios de flujo continuo tratan el problema colocando el sistema de encriptación en la máquina servidor en forma de software especial que encripta los medios de flujo continuo antes de que se conviertan en paquetes para su transmisión en la red. Aunque esto da como resultado paquetes que pueden pasar a menudo satisfactoriamente a través de servidores proxy y cortafuegos, esta estrategia es limitante. Esto se debe a que esta solución requiere la modificación del servidor de flujo continuo y requiere a menudo la adición de servidores de flujo continuo adicionales o de capacidad de procesamiento para manejar la carga de trabajo aumentada que añade la encriptación. Además, la solución debe rediseñarse para cada plataforma de servidor de flujo continuo soportada.

La patente US nº 5.640.456 da a conocer un dispositivo de encriptación/desencriptación de red informática que encripta o desencripta selectivamente sólo la parte de datos de un paquete de datos según información extraída de la cabecera del paquete de datos.

Breve sumario de la invención

La presente invención tiene como objetivo proporcionar un aparato y procedimiento que examina, analiza sintácticamente y encripta selectivamente sólo una parte de carga útil (por ejemplo, contenido de medios) de datos, dejando una parte de carga no útil intacta de manera que los datos puedan cruzar cortafuegos, proxys y NAT sin que los cortafuegos, proxys o NAT tengan que modificarse para alojar los datos encriptados. La invención puede garantizar que la parte del flujo de datos que los cortafuegos, proxys y NAT requieren para entregar apropiadamente los datos a los destinatarios previstos (por ejemplo, ordenador cliente) no está encriptada.

Según la presente invención, se proporciona un aparato para encriptar selectivamente datos para su transmisión a través de una red entre un servidor y un cliente, comprendiendo el aparato: unos medios para analizar sintácticamente

datos en una parte de carga útil y una parte de carga no útil; unos medios para encriptar la carga útil de los datos; y unos medios para combinar la parte de carga útil de los datos con la parte de carga no útil de los datos, en el que los medios para la encriptación están dispuestos para reconocer un tipo de datos predefinido en la parte de carga útil con el fin de determinar si la parte de carga útil ha de encriptarse, y la parte de carga no útil de los datos incluye más que información de encaminamiento. También se dan a conocer procedimientos correspondientes para encriptar y desencriptar datos selectivamente.

Por tanto, si los medios para la encriptación no ven un tipo de datos que reconocen específicamente, entonces lo ignoran, pero si los medios para la encriptación ven un tipo de datos que reconocen (por ejemplo, contenido multimedia), entonces encriptan selectivamente sólo la parte del flujo de datos reconocida.

Breve descripción de las diversas vistas del dibujo

Los dibujos adjuntos, que se incorporan y que constituyen una parte de la presente memoria, ilustran por lo menos una forma de realización a título de ejemplo de la invención y, junto con la descripción, explican las diversas ventajas y principios de la invención. En los dibujos:

La figura 1 es una ilustración de un sistema informático a título de ejemplo sobre el que puede implementarse un puente de encriptación.

La figura 2 es un diagrama de flujo de un proceso de encriptación a título de ejemplo.

La figura 3 es un diagrama de flujo de un proceso de desencriptación a título de ejemplo.

La figura 4 es un diagrama a título de ejemplo de una corrección de compatibilidad utilizada en una arquitectura de red de conexiones Windows™.

La figura 5 es un diagrama a título de ejemplo de una corrección de compatibilidad utilizada en una arquitectura de red basada en flujos.

Descripción detallada de la invención

La siguiente descripción detallada se refiere al dibujo adjunto, que ilustra la forma de realización a título de ejemplo de la presente invención. Otras formas de realización son posibles y pueden realizarse modificaciones en las formas de realización a título de ejemplo sin apartarse del espíritu y alcance de la invención. Por lo tanto, la siguiente descripción detallada no tiene la intención de limitar la invención. En su lugar, el alcance de la invención se define mediante las reivindicaciones adjuntas.

La figura 1 ilustra un sistema 100 informático a título de ejemplo que incluye un puente 110 de encriptación (al que también se hace referencia como "EB") de la invención interpuesto entre los servidores 120 de flujo continuo, que proporciona flujos 170 de medios (datos de carga útil), y una red externa tal como Internet 130 y un ordenador 140 de usuario o cliente. El EB 110 funciona de tal manera que como los datos se envían a través del EB 110, estando encriptada sólo la parte de los datos seleccionada (por ejemplo, datos multimedia). El EB 110 puede configurarse de tal manera que encripte también otros datos. Por ejemplo, el EB 110 puede configurarse para encriptar/proteger datos que podrían incluir, pero que no se limitan a, libros electrónicos, grabaciones o imágenes médicas, datos financieros o cualquier otros datos que requieran transmisión segura a través de una red.

El EB 110, que puede representar una única máquina o un grupo de máquinas, está interpuesto entre los servidores 120 e Internet 130. Todos los datos pertinentes que se mueven desde los servidores 120 e Internet 130 a través del EB 110 necesitan hacerse seguros mediante la encriptación; sin embargo, el tráfico entre el EB 110 y los servidores 120 no tiene que encriptarse puesto que está en una "zona segura" en virtud de no estar expuesto a la red externa. Los canales 150 de datos pueden representar datos de control tales como pausa, reproducción y rebobinado o datos de modulación de velocidad para los servidores 120 de flujo continuo o pueden utilizarse para formas de datos más complejas y supervisión. Adicionalmente, los canales 150 de datos pueden utilizarse para ceder estos datos de supervisión a otras máquinas tales como servidores de comercio electrónico o supervisión de calidad para servicios no relacionados directamente con el proceso de encriptación de flujo.

El EB 110 pasa datos a clientes 140 de red y garantiza a los propietarios de los datos o proveedores de contenido (por ejemplo, Yahoo, Inc. AOL, Inc., etc.) que los datos de sus servidores 120 de flujo continuo se encriptarán de manera segura mientras atraviesan Internet 130 y que una vez en la máquina cliente 140 los datos serán difíciles de copiar. La seguridad en la máquina 140 cliente puede llevarse a cabo mediante diversas técnicas, incluyendo, pero no limitadas, a comprobar e impedir las técnicas de piratería conocidas y supervisar que la máquina 140 cliente no sufre un comportamiento sospechoso. Los servidores 120 de flujo continuo y los clientes 140 son las fuentes y destinatarios finales, respectivamente, de los flujos 170 de datos (por ejemplo, contenido multimedia) y canales 150 de datos (por ejemplo, datos de control) transportados a través del EB 110. Un manejador 160 de datos adicional (por ejemplo, un sistema de comercio electrónico, un sistema de supervisión de calidad, etc.) también puede conectarse al EB 110, lo que se describe adicionalmente posteriormente.

Los operadores de servidor 120 de flujo continuo (por ejemplo propietarios de contenido o proveedores de servicio para propietarios de contenido) son los clientes primarios del sistema, que proporcionan el contenido a las transmisiones solicitadas por un cliente 140 a través de una red tal como Internet 130. El cliente 140, con el fin de este ejemplo, está equipado con software de reproducción de medios. Para este ejemplo, el software de reproducción de medios podría ser el reproductor Apple Computer Quicktime™ Player, Real Player™, el Windows Media Player™ o cualquier otro software que pueda reproducir flujos multimedia. Internet 130 es una red pública. El manejador 160 de datos es, por ejemplo, un sistema de comercio electrónico u otro sistema de datos o supervisión externo que un cliente puede elegir para utilizar en conjunción con una solución de seguridad de flujo continuo.

La figura 2 es un diagrama de flujo de un proceso de encriptación a título de ejemplo de la invención para analizar sintácticamente y encriptar selectivamente datos que se envían a través de una red pública entre un servidor y un cliente. Este proceso comprende reconocer un nuevo flujo de datos que llega al EB 210; determinar si los datos han de encriptarse 220; ignorar y pasar el flujo de datos si no ha de encriptarse 222; determinar si está presente una corrección de compatibilidad en el cliente/objetivo 230; utilizar la corrección de compatibilidad si ya no está presente 232; determinar si una clave de encriptación está vigente 240; intercambiar clave(s) de encriptación con la corrección de compatibilidad en el lado del cliente si la clave no estuviese vigente 242; analizar sintácticamente datos en partes de carga útil y de carga no útil 250; encriptar la parte de carga útil utilizando la clave intercambiada 260; pasar los datos que están constituidos por partes de carga útil y de carga no útil a través de la red 270; determinar si los datos procesados son los últimos del flujo 280; recibir retroalimentación desde la corrección de compatibilidad si los datos no eran la parte final del flujo 282; determinar si el cliente está en situación comprometida 284 (por ejemplo, está pirateado o los datos que necesitan seguridad están de otro modo en peligro); cortar el flujo de datos si el cliente está en situación comprometida 286; reanudar el análisis sintáctico del flujo establecido si el cliente no está en situación comprometida 288; y finalizar la sesión de flujo continuo si los datos fueron los últimos del flujo 290.

Los beneficios del sistema EB incluyen: el EB se coloca junto al sistema servidor de flujo continuo del cliente con mínimos costes de integración; no hay necesidad de modificar el sistema servidor para que funcione el EB; el EB es transparente tanto al software en el lado del cliente como al sistema servidor de flujo continuo con un software cliente que parece comunicarse con los servidores sin un intermediario inesperado y con servidores que entregan datos a clientes sin detectar el proceso de encriptación en curso.

Además, el sistema de EB proporciona análisis sintáctico y encriptación para una variedad de flujos y tipos de datos incluyendo pero no limitados al formato de Windows Media™ y RTP/TRSP utilizando entrega TCP, o TCP/UDP o http. Todos los datos de carga útil enviados a través de estos formatos se encriptan a medida que los datos se desplazan desde el servidor a través del EB al cliente.

La encriptación se lleva a cabo a través de un algoritmo de encriptación tal como DES-X, una técnica ampliamente conocida en la técnica, y otros algoritmos pueden sustituirse dependiendo del cliente y otras necesidades. El análisis sintáctico y la encriptación de los flujos de datos no interfieren con la capacidad del flujo para pasar a través del servidor proxy, cortafuegos o NAT que analizan sintácticamente paquetes para facilitar la entrega de datos a una LAN protegida. Esta es una característica importante de la invención puesto que los solicitantes no conocen ningún software que analice sintácticamente el contenido de manera selectiva y actúe posteriormente sólo sobre la parte de carga útil de los datos como la presente invención. Además, no se requiere autenticación externa puesto que el EB maneja el intercambio de claves de encriptación directamente con el cliente.

Además, el EB es dimensionable para permitir la adición de más máquinas de encriptación a medida que aumenta al ancho de banda. Las máquinas de encriptación son dimensionables para permitir la adición de tarjetas de red y procesadores adicionales para manejar el ancho de banda aumentado. Esto permite al sistema un máximo crecimiento con un mínimo aumento en el tamaño físico del EB.

A medida que se añaden más máquinas de encriptación al EB, la encriptación se extiende entre esas máquinas de encriptación disponibles para maximizar el rendimiento global. El EB puede configurarse mientras está en línea para: añadir o eliminar máquinas de encriptación; desconectar el EB; impedir que el sistema acepte nuevos flujos y permitir que acaben flujos existentes; leer el estado para saber si una máquina de encriptación dada ya no suministra flujos y puede eliminarse de manera segura del sistema; y reunir datos sobre la capacidad del flujo de datos, utilización y calidad de datos transferidos a través del EB.

Además, la arquitectura de EB y de corrección de compatibilidad proporciona núcleos conectables para cambiar y mantener características tales como el algoritmo de encriptación y monitores de seguridad en el lado del cliente. Un núcleo conectable es un código modular que permite que partes del programa global se sustituyan fácilmente sin perturbar la funcionalidad restante. Por ejemplo, la invención permite al EB encriptar con una variedad de algoritmos de tal manera que cuando se establece un nuevo flujo de datos a través del EB, podría enviarse un nuevo núcleo de encriptación al cliente para permitir que la parte de carga útil se encripte con un algoritmo diferente (por ejemplo Blowfish o RSA™ en vez de DES-X). Expresado de otra manera, el algoritmo de encriptación puede cambiarse en cualquier momento puesto que la arquitectura software es completamente conectable/intercambiable. En cuanto al sistema de intercambio de claves, aunque actualmente se utilizan protocolos estándar, pueden cambiarse en cualquier momento puesto que esta arquitectura también es conectable/intercambiable. En cuanto al sistema de seguridad en el lado del cliente (es decir, detección de piratas informáticos), esto también puede modificarse en cualquier momento puesto que

la arquitectura es conectable/intercambiable. Toda la funcionalidad de núcleo de la corrección de compatibilidad en el lado del cliente está implementada a través de esta arquitectura conectable/intercambiable.

Otro aspecto nuevo de la invención es la encriptación "sobre la marcha", que hace inútiles los paquetes de datos que se transmiten a través de la red para cualquier ordenador distinto a la máquina prevista. Esto se realiza de manera transparente con respecto al mecanismo de reproducción de medios cliente (por ejemplo, software reproductor de medios) y al servidor y en tiempo real. La implementación inicial de la invención utiliza DES-X, un algoritmo optimizado en velocidad ampliamente conocido en la técnica, aunque a través de la arquitectura de núcleos conectables comentada anteriormente este podría cambiarse por otros algoritmos que pueden incluir, pero no limitados a, algoritmos RSA™ o los algoritmos Blowfihs y Two-Fish ampliamente conocidos.

Por tanto, la invención proporcionar un puente de software que examina los datos de red que pasan a través de la misma, analiza sintácticamente los datos de red y sólo encripta la parte de carga útil relevante, dejando intacta en su totalidad la parte de carga no útil que puede incluir datos tales como encaminamiento, tamaño y otros datos de cabecera que rodean la parte de carga útil. Dicho de otro modo, ciertas partes de los datos están encriptadas y otras partes de los datos no están encriptadas o no necesitan encriptarse. Lo que hacen los sistemas y procedimientos de la invención es analizar sintácticamente la red y examinar realmente el formato de datos, encriptando sólo la parte de los datos que contiene, en el caso a título de ejemplo, contenido multimedia. La selectividad de los datos que van a encriptarse se basa en el formato de los datos enviados, que el EB reconoce y al que responde apropiadamente. El EB de la invención se sitúa entre los servidores y clientes y encripta los datos. La desencriptación tiene lugar en el cliente utilizando la corrección de compatibilidad y núcleos conectables tal como se comentó anteriormente. De esta manera, los datos, si se interceptan en la red, están encriptados y son inútiles para el interceptor. Los datos no pueden interceptarse antes de la encriptación puesto que el EB y los servidores están conectados a través de una conexión de red segura.

Tal como se expuso anteriormente, el flujo de datos encriptados de la invención puede pasar a través de un servidor proxy, cortafuegos o NAT sin que esos mecanismos necesiten modificarse para alojar el flujo de datos. Un beneficio de la invención sobre soluciones de encriptación actuales es la capacidad para producir flujos de datos encriptados que pueden atravesar servidores proxy, cortafuegos y NAT. Esta capacidad para producir datos que cruzan servidores proxy, cortafuegos y NAT no modificados se produce como resultado de la capacidad de la invención de analizar sintácticamente datos de manera selectiva en partes de carga útil y de carga no útil y encriptar sólo la parte de carga útil, un nivel de selectividad que no proporcionan las soluciones de encriptación actuales.

Para los operadores de servidores de flujo continuo esto se vuelve muy importante puesto que muchas redes domésticas, de oficinas y de otro tipo están protegidas o aisladas de Internet pública mediante cortafuegos, servidores proxy y/o NAT. Con las soluciones de encriptación actuales que encriptan datos de manera menos discriminada, los datos no pueden entregarse a través de cortafuegos, servidores proxy y NAT no modificados.

Por ejemplo, cuando un usuario solicita datos desde un servidor de flujo continuo, el flujo de datos se organiza en paquetes que presentan datos específicos para identificar el usuario objetivo. Sin analizar sintácticamente los datos con precisión en partes de carga útil y de carga no útil, los datos específicos de usuario se dañan o mezclan fácilmente durante el proceso de encriptación, haciendo imposible que el cortafuegos, servidor proxy o NAT entregue los datos al usuario solicitante. Por el contrario, la presente invención separa con precisión las partes de carga útil y de carga no útil, encriptando sólo la parte de carga útil de tal modo que los datos parecen no cambiados para el cortafuegos, servidor proxy o NAT que sólo requiere la parte de carga no útil para efectuar la entrega al usuario que solicita el flujo de datos.

Un cortafuegos, por ejemplo, no reconoce o intenta bloquear el flujo de datos encriptados porque los protocolos de transporte no definen la aparición de la parte de carga útil, sólo la aparición de la parte de carga no útil. El cortafuegos examina la parte de carga no útil que incluye, pero que no se limita a, datos de cabecera, tamaño y encaminamiento. Si los datos de la parte de carga no útil identifica el flujo de datos como una respuesta a una solicitud de usuario, entonces el cortafuegos determina que el flujo de datos no es malicioso en origen y no impedirá su transmisión. Sin embargo, si el cortafuegos no puede analizar sintácticamente la parte de carga no útil o no reconoce la parte de carga no útil, entonces se bloqueará la transmisión de los datos.

En soluciones de encriptación existentes en las que se encripta toda la parte de datos de paquetes, son necesarias modificaciones especiales en cada cortafuegos, servidor proxy o NAT por los que pasa el flujo de datos. Es decir, los cortafuegos, servidores proxy y NAT tendrían que actualizarse para identificar los datos encriptados. La presente invención no requiere modificaciones de los cortafuegos, servidores proxy o NAT ya utilizados porque encripta selectivamente los paquetes de datos dejando las partes importantes al cortafuegos, servidores proxy y NAT no modificados de tal manera que el cortafuegos, servidor proxy y NAT pueden hacer pasar el flujo de datos hacia el objetivo previsto.

Existen algunas soluciones de encriptación existentes que encriptan sólo la parte de medios de un flujo de datos colocando el software de encriptación en el servidor de flujo continuo como una conexión al software de servidor de flujo continuo, colocando una fuerte carga de procesamiento en el servidor de flujo continuo. Esto se opone a un beneficio de la invención porque la invención puede utilizarse con una pluralidad de servidores de flujo continuo sin que se requiera modificación de los servidores de flujo continuo y proporcionando encriptación sin afectar el rendimiento de procesamiento de los servidores de flujo continuo.

Otra característica de la invención es que proporciona un sistema que es independiente en cuanto al formato de medios utilizado. Es decir, la invención funciona basándose en el protocolo de datos en lugar de en el formato del archivo. El flujo continuo multimedia a través de redes se lleva a cabo a través de varios protocolos. La invención reconoce el protocolo de flujo continuo y actúa sobre los datos en lugar de requerir información específica del formato de archivo que está transmitiéndose. La invención también es independiente en cuanto a los sistemas operativos de las máquinas de servidor puesto que la invención no requiere acceso directo a las máquinas de servidor, la invención simplemente requiere que los flujos de datos del servidor de flujo continuo pasen a través del EB.

La invención proporciona asimismo un sistema cliente, al que también se hace referencia como una corrección de compatibilidad de desencriptación o simplemente una corrección de compatibilidad, que es un software transparente que se descarga o se instala previamente en la máquina cliente (por ejemplo, ordenador personal, aparato de red u otro dispositivo de red) y se utiliza para desencriptar flujos de datos entrantes desde el EB en su camino al software reproductor de medios. La figura 3 es un diagrama de flujo de un proceso de desencriptación a título de ejemplo del software de corrección de compatibilidad de desencriptación realizado en la máquina cliente. El proceso comprende flujos de datos según se inician 310; determinar si los datos son un flujo encriptado 320; ignorar el flujo si no son datos encriptados 322; determinar si la clave de encriptación está vigente 330; negociar una clave con el puente/fuente de encriptación si la clave no está vigente 340; analizar sintácticamente los datos en partes de carga útil y de carga no útil 350; desencriptar sólo la parte de carga útil 360; pasar los datos a operaciones de nivel superior (por ejemplo, el reproductor de medios) 370; determinar si los datos son la última parte de un flujo 380; examinar el entorno de funcionamiento para seguridad 382; determinar si el entorno del cliente está en situación comprometida (pirateado, etc.) 384; cortar el flujo de datos si el cliente está en situación comprometida 385; comunicarse con el puente/fuente de encriptación 386; reanudar el análisis sintáctico de los datos 388; y finalizar el flujo si los datos fueron la última parte del flujo 390.

La desencriptación se lleva a cabo añadiendo una corrección de compatibilidad de desencriptación 420 en un proveedor 410 de servicio por capas en una arquitectura de red de conexiones Windows™ tal como se muestra en la figura 4 o una conexión 510 de flujos en una arquitectura de red basada en flujos tal como se muestra en la figura 5. La figura 4 es un diagrama a título de ejemplo de una arquitectura de red de conexiones Windows™. En la arquitectura de conexión en red Windows™, la corrección de compatibilidad de desencriptación 420 es el proveedor de servicio por capas (LSP) más alto de modo que un LSP adicional no puede simplemente almacenar datos desencriptados en un entorno inseguro. Esto puede extrapolarse también a otros protocolos de conexión en red basados en conexiones. La figura 5 es un diagrama de modo de ejemplo de una arquitectura de red basada en flujos. El diagrama representa la colocación de la corrección de compatibilidad de la invención 520 dentro de una arquitectura 510 basada en flujos tal como la empleada por versiones actuales de MAC OS™ y algunas versiones de Unix.

Cuando un usuario solicita datos que están encriptados por el EB de la invención, el software transparente se instala a través de un control Active-X™, un medio ampliamente documentado para entregar programas ejecutables a un ordenador Windows™. La instalación de la corrección de compatibilidad de desencriptación es transparente al usuario y no provoca un rearranque, reinicio del navegador del usuario ni requiere interacción del usuario. Hay algunas excepciones tales como el Mac OS™ y Windows NT™ o Windows 2000™ en entornos seguros o máquinas cliente basadas en Linux o Unix porque la instalación transparente requiere privilegios administrativos de usuario en la máquina cliente y la capacidad de la máquina cliente para recibir programas a través del mecanismo Active-X™.

Después de que ha finalizado el último flujo, la corrección de compatibilidad de desencriptación se desinstala tanto como sea posible, dejando sólo una capa pequeña de modo que no se requieren privilegios administrativos de usuario para futuras desencriptaciones. La corrección de compatibilidad de desencriptación se instala en memoria volátil para reducir los cambios de utilización indebida por una tercera parte.

Después de la instalación, la corrección de compatibilidad de desencriptación desencripta sólo los datos que provienen del EB de la invención que van a reproductores objetivo tales como Windows Media™ Player, QuickTime™ Movie Player, Real Player™, etc. La desencriptación no afecta a datos dirigidos a otras aplicaciones o flujos de medios que no están encriptados por el EB de la invención.

La corrección de compatibilidad de desencriptación se ejecuta en, por ejemplo, sistemas operativos tales como Windows 95™, Windows 98™, Windows ME™, Windows NT™, Windows 2000™ así como Mac OS™ y numerosas distribuciones de Linux y Unix. Donde sea posible la instalación basada en Active-X™ la instalación de la corrección de compatibilidad de desencriptación puede llevarse a cabo con la mayoría de navegadores tales como Internet Explorer™ o Netscape™.

En suma, el EB de la invención se sitúa entre el servidor y el cliente y analiza sintácticamente y encripta una parte seleccionada de los datos de flujo continuo tales como la parte de medios. Cuando se inicia el flujo, el núcleo de desencriptación se envía como parte del flujo al lado del cliente. A continuación, el cliente puede desencriptar los datos entrantes durante la duración del flujo. Si se inicia otro flujo, se produce desencriptación de la misma manera. Para cada flujo, las claves de encriptación pueden establecerse para la duración del flujo o cambiarse durante la duración del flujo para aumentar la seguridad.

Como un ejemplo, un cliente puede solicitar privilegios para conseguir datos de flujo continuo desde un sistema de comercio electrónico del proveedor de servicio. La parte de servidor del proveedor de servicio (infraestructura de

servidor) autorizará al servidor de flujo continuo iniciar un flujo. Ese flujo se inicia a través del EB. Una vez iniciado, el flujo se analiza sintácticamente y se encripta selectivamente mediante el EB antes de que se pase a través de la red. Las claves de encriptación se intercambian, por ejemplo, mediante el mecanismo Diffy-Helman que se conoce en el campo. Características únicas de la invención incluyen el análisis sintáctico y la encriptación selectiva de sólo la parte de carga útil del flujo de datos y la capacidad para enchufar otros mecanismos de intercambios de claves y algoritmos de encriptación según dicten las necesidades de seguridad o del cliente.

Resultará evidente para un experto ordinario en la materia que las formas de realización descritas anteriormente pueden ponerse en práctica en muchas formas de realización diferentes de software, firmware y hardware en las entidades ilustradas en las figuras. El código de software real o hardware de control especializado utilizados para poner en práctica la presente invención no es limitante de la presente invención. Por tanto, el funcionamiento y comportamiento de las formas de realización se describieron sin referencia específica al código de software específico o componentes de hardware especializados, entendiéndose que un experto ordinario en la materia podría diseñar software y hardware de control para poner en práctica las formas de realización basándose en la descripción de la presente memoria.

REIVINDICACIONES

1. Aparato (110) para encriptar selectivamente datos para su transmisión a través de una red (130) entre un servidor (120) y un cliente (140), comprendiendo el aparato:

unos medios para analizar sintácticamente datos en una parte de carga útil y una parte de carga no útil;

unos medios para encriptar la carga útil de los datos; y

unos medios para combinar la parte de carga útil de los datos con la parte de carga no útil de los datos,

caracterizado porque:

los medios para la encriptación están dispuestos para reconocer un tipo de datos predefinido en la parte de carga útil con el fin de determinar si la parte de carga útil ha de encriptarse, y

la parte de carga no útil de los datos incluye más que información de encaminamiento.

2. Aparato según la reivindicación 1, en el que los datos incluyen datos de flujo continuo, tales como datos multimedia.

3. Aparato según la reivindicación 1 ó 2, en el que la parte de carga no útil de los datos incluye por lo menos uno de entre una cabecera y datos de control.

4. Aparato según cualquiera de las reivindicaciones anteriores, que comprende asimismo unos medios para enviar las partes de carga útil y de carga no útil combinadas de los datos a través de la red (130) al cliente (140).

5. Aparato según cualquiera de las reivindicaciones anteriores, que comprende asimismo unos medios para recibir los datos desde el servidor (120) antes de que los datos se envíen a través de la red (130) al cliente (140).

6. Aparato según cualquiera de las reivindicaciones anteriores, que comprende asimismo unos medios para establecer un flujo de datos entre el servidor (120) y el cliente (140).

7. Aparato según cualquiera de las reivindicaciones anteriores, que comprende asimismo unos medios para negociar una clave de encriptación con el cliente (140).

8. Aparato según la reivindicación 7, en el que la negociación de claves y el intercambio de claves se producen durante la transmisión de un flujo.

9. Aparato según la reivindicación 8, en el que la encriptación mediante los medios de encriptación es transparente para el servidor (120).

10. Aparato según la reivindicación 7, en el que los medios para negociar una clave de encriptación están dispuestos para determinar si una clave de encriptación existente está vigente.

11. Aparato según cualquiera de las reivindicaciones anteriores, que comprende asimismo unos medios para desencriptar la parte de carga útil de los datos.

12. Aparato según cualquiera de las reivindicaciones anteriores, en el que los medios de análisis sintáctico están dispuestos para analizar sintácticamente los datos en diferentes partes basándose en un formato de medios.

13. Aparato según cualquiera de las reivindicaciones 1 a 11, en el que los medios de análisis sintáctico están dispuestos para analizar sintácticamente los datos en diferentes partes basándose en un protocolo de datos utilizado para transmitir un flujo de datos.

14. Aparato según cualquiera de las reivindicaciones anteriores, en el que los medios de encriptación están dispuestos para encriptar la parte de carga útil si el tipo de datos predefinido reconocido presenta un formato de medios.

15. Aparato según cualquiera de las reivindicaciones anteriores, en el que el aparato comprende una aplicación que incluye un núcleo conectable que codifica un algoritmo de encriptación para encriptar la parte de carga útil de los datos, en el que el núcleo conectable permite que el algoritmo de encriptación se cambie fácilmente.

16. Aparato según cualquiera de las reivindicaciones 1 a 14, en el que el aparato está implementado sobre un puente de encriptación.

17. Procedimiento para encriptar selectivamente datos recibidos desde una fuente de datos, incluyendo los datos unas partes de carga útil y de carga no útil que se diferencian entre sí en por lo menos una característica, debiendo enviarse posteriormente los datos recibidos a través de una red a un cliente, comprendiendo el procedimiento:

analizar sintácticamente los datos recibidos en partes que incluyen las partes de carga útil y de carga no útil;

reconocer un tipo de datos predefinido en la parte de carga útil para determinar si la parte de carga útil ha de encriptarse y, si ha de encriptarse, encriptar la parte de carga útil de los datos recibidos; y

enviar los datos recibidos incluyendo la parte de carga útil y la parte de carga no útil de los datos recibidos a través de la red al cliente.

18. Procedimiento según la reivindicación 17, en el que la fuente de datos es un servidor.

19. Procedimiento según la reivindicación 17 ó 18, que comprende asimismo determinar si se establece un flujo entre un servidor y el cliente.

20. Procedimiento según cualquiera de las reivindicaciones 17 a 19, que comprende asimismo negociar una clave de encriptación con el cliente.

21. Procedimiento según la reivindicación 20, en el que los datos recibidos desde la fuente de datos son datos de flujo continuo enviados durante una sesión de flujo continuo y la negociación de la clave de encriptación se lleva a cabo durante la sesión de flujo continuo.

22. Procedimiento según la reivindicación 20, en el que los datos recibidos desde la fuente de datos son datos de flujo continuo enviados durante una sesión de flujo continuo, y el procedimiento comprende asimismo examinar al cliente durante la sesión de flujo continuo y finalizar la sesión de flujo continuo si la clave de encriptación en el cliente no es válida.

23. Procedimiento según la reivindicación 20, en el que la clave de encriptación se negocia con una corrección de compatibilidad de desencriptación en el cliente.

24. Procedimiento según cualquiera de las reivindicaciones 17 a 23, que comprende además determinar si los datos recibidos son datos de flujo continuo.

25. Procedimiento según la reivindicación 24, que comprende analizar sintácticamente, encriptar y enviar los datos si los datos son datos de flujo continuo y enviar los datos si los datos no son datos de flujo continuo.

26. Procedimiento según cualquiera de las reivindicaciones 17 a 25, que comprende asimismo determinar si está presente una corrección de compatibilidad en el cliente.

27. Procedimiento según la reivindicación 26, que comprende asimismo enviar una corrección de compatibilidad al cliente si se determina que la corrección de compatibilidad no está presente en el cliente.

28. Procedimiento según cualquiera de las reivindicaciones 17 a 27, que comprende asimismo determinar si está vigente una clave de encriptación en el cliente.

29. Procedimiento según cualquiera de las reivindicaciones 17 a 28, en el que la parte de los datos de carga no útil incluye por lo menos uno de entre una cabecera, datos de control y datos de encaminamiento.

30. Procedimiento según cualquiera de las reivindicaciones 17 a 29, en el que los datos recibidos desde la fuente de datos para enviar al cliente son un flujo de paquetes, comprendiendo asimismo el procedimiento determinar si un paquete es el último paquete en un flujo de datos.

31. Procedimiento según la reivindicación 30, que comprende asimismo recibir retroalimentación de una corrección de compatibilidad de desencriptación en el cliente si se determina que el paquete no es el último paquete en el flujo de datos.

32. Procedimiento según cualquiera de las reivindicaciones 17 a 31, que comprende asimismo determinar si el cliente está en situación comprometida.

33. Procedimiento según la reivindicación 32, que comprende asimismo continuar el análisis sintáctico, la encriptación y el envío de los datos tal como se mencionó anteriormente si se determina que el cliente no está en situación comprometida.

34. Procedimiento según la reivindicación 32 ó 33, que comprende asimismo finalizar el envío al cliente si se determina que el cliente está en situación comprometida.

35. Procedimiento para desencriptar selectivamente datos de flujo continuo en un cliente, incluyendo los datos de flujo continuo partes de carga útil y de carga no útil que se diferencian entre sí en por lo menos una característica, habiéndose enviado los datos a través de una red al cliente desde una fuente de encriptación, comprendiendo el procedimiento:

recibir los datos enviados a través de la red;

analizar sintácticamente los datos en partes que incluyen las partes de carga útil y de carga no útil;

si la parte de carga útil de los datos está encriptada como resultado de reconocer un tipo de datos predefinido en la parte de carga útil, desencriptar la parte de carga útil de los datos; y

pasar la parte de carga útil desencriptada de los datos a un nivel superior de operaciones para su reproducción en el cliente.

36. Procedimiento según la reivindicación 35, que comprende asimismo determinar si los datos son un flujo no encriptado antes de analizar sintácticamente los datos de las partes de carga útil y de carga no útil.

37. Procedimiento según la reivindicación 36, que comprende asimismo pasar los datos a dicho nivel superior de operaciones sin análisis sintáctico y desencriptación cuando se determina que los datos son un flujo no encriptado.

38. Procedimiento según la reivindicación 35, que comprende asimismo negociar una clave de desencriptación con la fuente de encriptación.

39. Procedimiento según la reivindicación 38, en el que los datos de flujo continuo se envían desde la fuente de encriptación durante una sesión de flujo continuo y la negociación de la clave de desencriptación se lleva a cabo durante la sesión de flujo continuo.

40. Procedimiento según la reivindicación 38, que comprende asimismo finalizar un flujo si la clave de desencriptación no es válida.

41. Procedimiento según cualquiera de las reivindicaciones 35 a 40, en el que los datos se envían desde la fuente de encriptación a través de la red como un flujo de paquetes de datos, comprendiendo asimismo el procedimiento determinar si un paquete recibido por el cliente es un último paquete en un flujo de datos.

42. Procedimiento según la reivindicación 41, que comprende asimismo enviar retroalimentación a la fuente de encriptación si se determina que el paquete no es el último paquete en el flujo de datos.

43. Procedimiento según cualquiera de las reivindicaciones 35 a 42, que comprende asimismo determinar si el cliente está en situación comprometida.

44. Procedimiento según la reivindicación 43, que comprende asimismo continuar el análisis sintáctico, la desencriptación y el paso de los datos tal como se mencionó anteriormente si se determina que el cliente no está en situación comprometida.

45. Procedimiento según la reivindicación 43 ó 44, que comprende asimismo finalizar una sesión de flujo continuo si se determina que el cliente está en situación comprometida.

46. Procedimiento según la reivindicación 45, en el que la finalización de la sesión de flujo continuo incluye detener el envío de datos a través de la red.

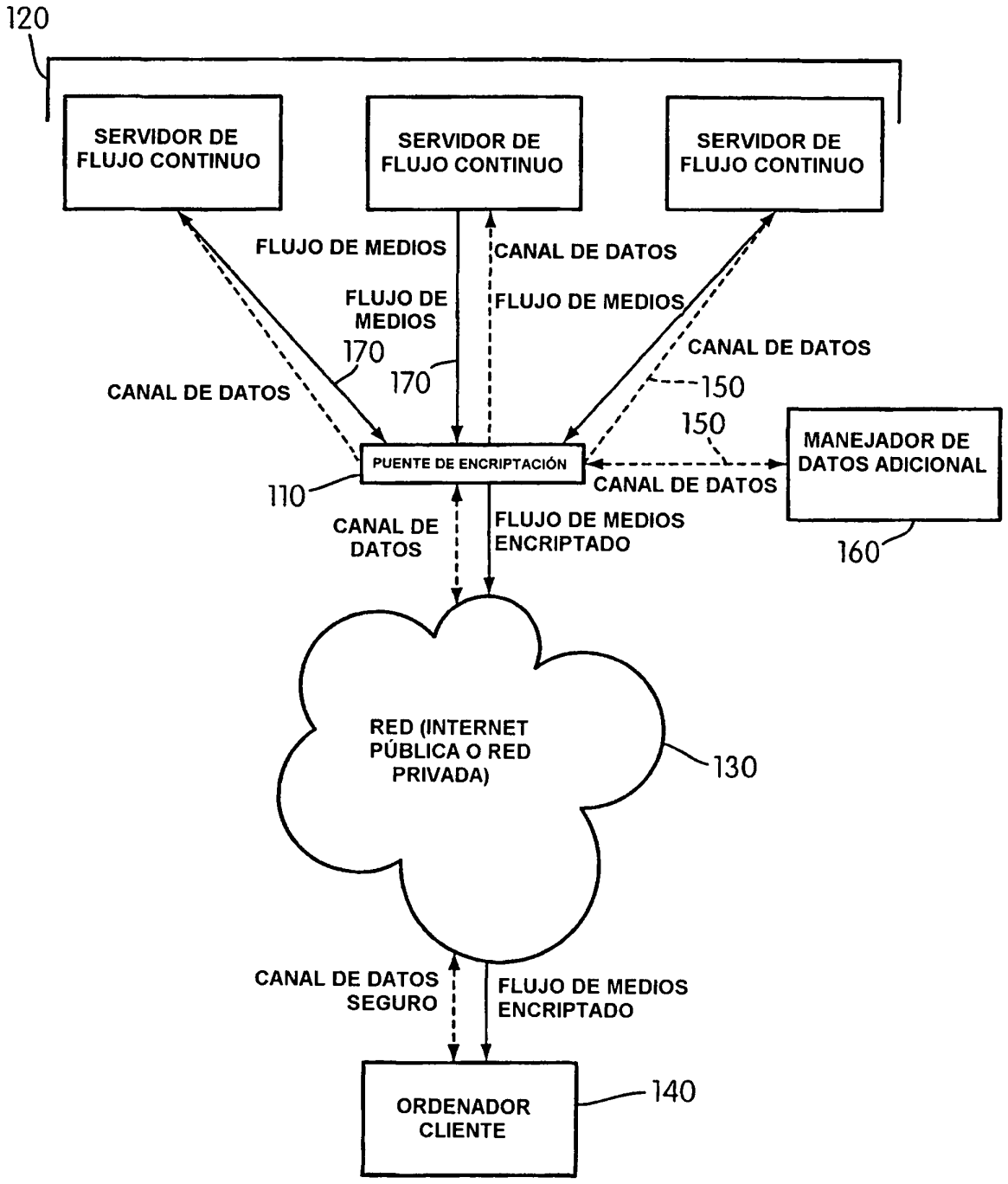
120
SERVIDOR DE FLUJO CONTINUO
SERVIDOR DE FLUJO CONTINUO
SERVIDOR DE FLUJO CONTINUO
FLUJO DE MEDIOS
CANAL DE DATOS
FLUJO DE MEDIOS
FLUJO DE MEDIOS
170
170
CANAL DE DATOS
CANAL DE DATOS
150
150
MANEJADOR DE DATOS ADICIONAL
PUENTE DE ENCRIPTACIÓN
110
CANAL DE DATOS
CANAL DE DATOS
FLUJO DE MEDIOS ENCRIPTADO
160
RED (INTERNET PÚBLICA O RED PRIVADA)
130
CANAL DE DATOS SEGURO
FLUJO DE MEDIOS ENCRIPTADO
ORDENADOR CLIENTE
140

FIG. 1

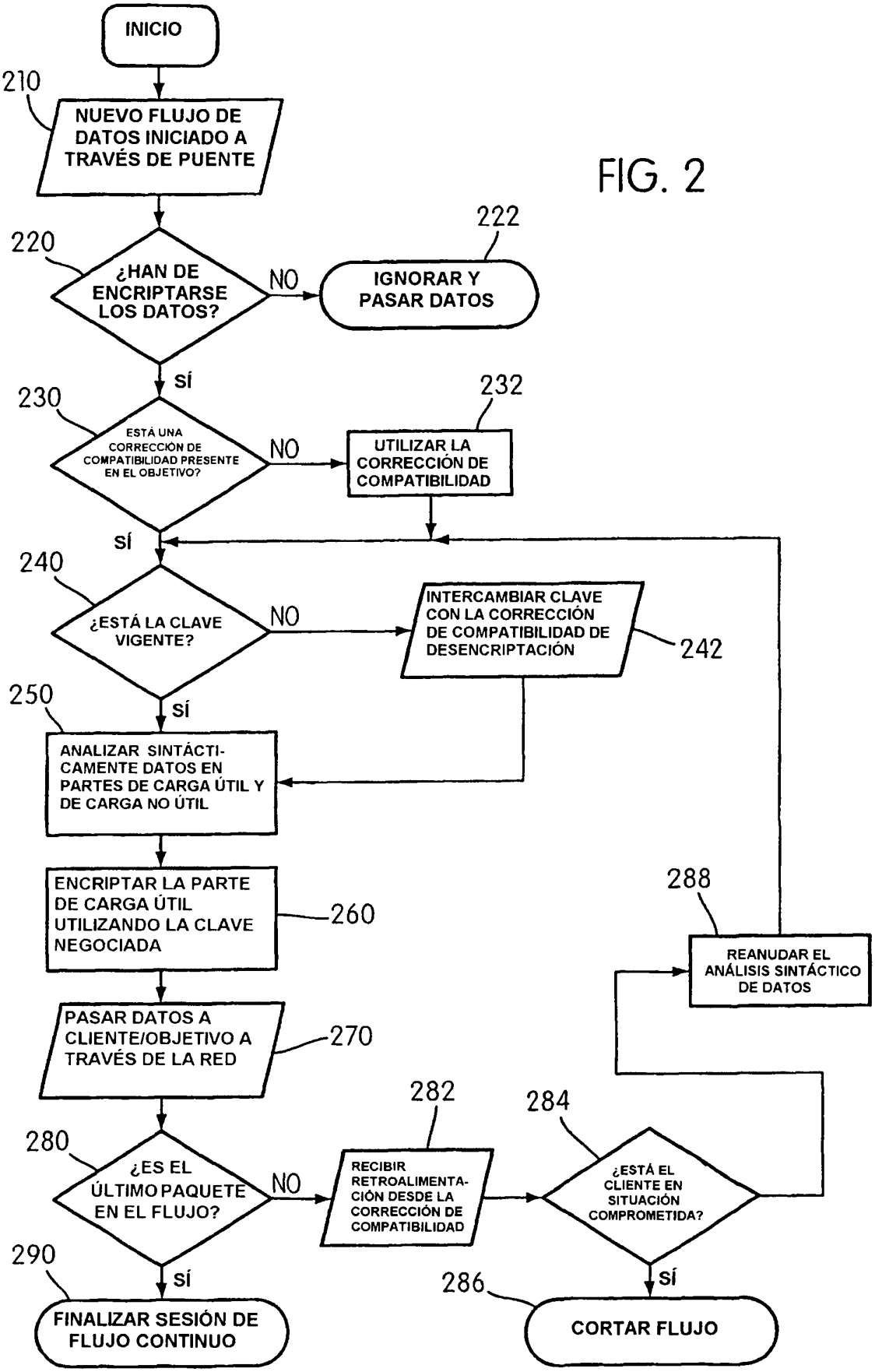
INICIO
210
NUEVO FLUJO DE DATOS INICIADO A TRAVÉS DE PUENTE
220
¿HAN DE ENCRIPTARSE LOS DATOS?
NO
222
IGNORAR Y PASAR DATOS
SÍ
230
ESTÁ UNA CORRECCIÓN DE COMPATIBILIDAD PRESENTE EN EL OBJETIVO?
NO
232
UTILIZAR LA CORRECCIÓN DE COMPATIBILIDAD
SÍ
240
¿ESTÁ LA CLAVE VIGENTE?
NO
INTERCAMBIAR CLAVE CON LA CORRECCIÓN DE COMPATIBILIDAD DE DESENCRIPTACIÓN
242
SÍ
250
ANALIZAR SINTÁCTICAMENTE DATOS EN PARTES DE CARGA ÚTIL Y DE CARGA NO ÚTIL
ENCRIPTAR LA PARTE DE CARGA ÚTIL UTILIZANDO LA CLAVE NEGOCIADA
260
PASAR DATOS A CLIENTE/OBJETIVO A TRAVÉS DE LA RED
270
280
¿ES EL ÚLTIMO PAQUETE EN EL FLUJO?
NO
282
RECIBIR RETROALIMENTACIÓN DESDE LA CORRECCIÓN DE COMPATIBILIDAD
284
¿ESTÁ EL CLIENTE EN SITUACIÓN COMPROMETIDA?
SÍ
286
CORTAR FLUJO
288
REANUDAR EL ANÁLISIS SINTÁCTICO DE DATOS
290
SÍ
FINALIZAR SESIÓN DE FLUJO CONTINUO

FIG. 2

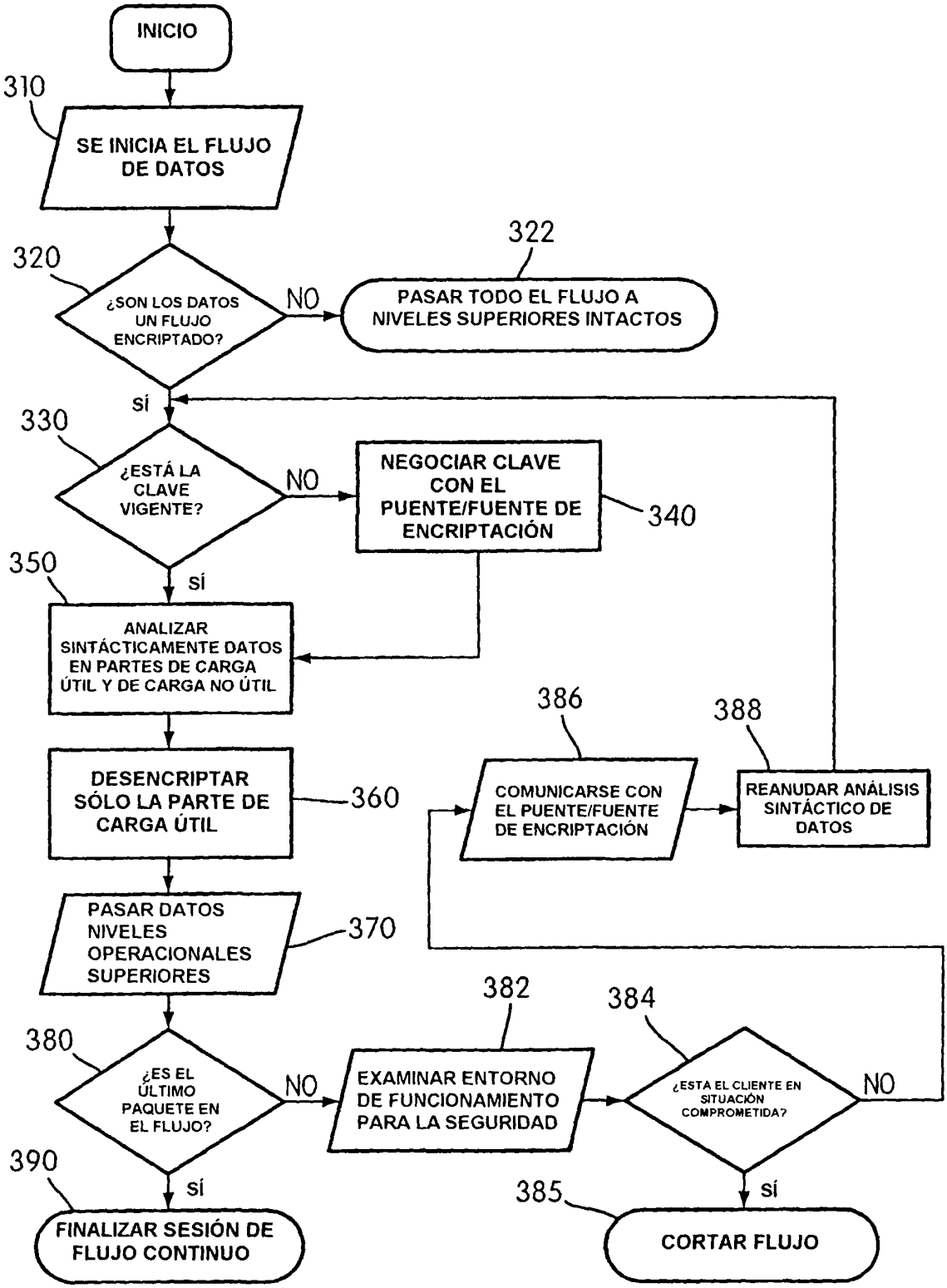
INICIO
310
SE INICIA EL FLUJO DE DATOS
320
¿SON LOS DATOS UN FLUJO ENCRIPTADO?
NO
322
PASAR TODO EL FLUJO A NIVELES SUPERIORES INTACTOS
SÍ
330
¿ESTÁ LA CLAVE VIGENTE?
NO
NEGOCIAR CLAVE CON EL PUENTE/FUENTE DE ENCRIPTACIÓN
340
SÍ
350
ANALIZAR SINTÁCTICAMENTE DATOS EN PARTES DE CARGA ÚTIL Y DE CARGA NO ÚTIL
386
388
DESENCRIPTAR SÓLO LA PARTE DE CARGA ÚTIL
360
COMUNICARSE CON EL PUENTE/FUENTE DE ENCRIPTACIÓN
REANUDAR ANÁLISIS SINTÁCTICO DE DATOS
PASAR DATOS NIVELES OPERACIONALES SUPERIORES
370
382
384
380
¿ES EL ÚLTIMO PAQUETE EN EL FLUJO?
NO
EXAMINAR ENTORNO DE FUNCIONAMIENTO PARA LA SEGURIDAD
¿ESTA EL CLIENTE EN SITUACIÓN COMPROMETIDA?
NO
390
SÍ
385
SÍ
FINALIZAR SESIÓN DE FLUJO CONTINUO
CORTAR FLUJO

FIG. 3

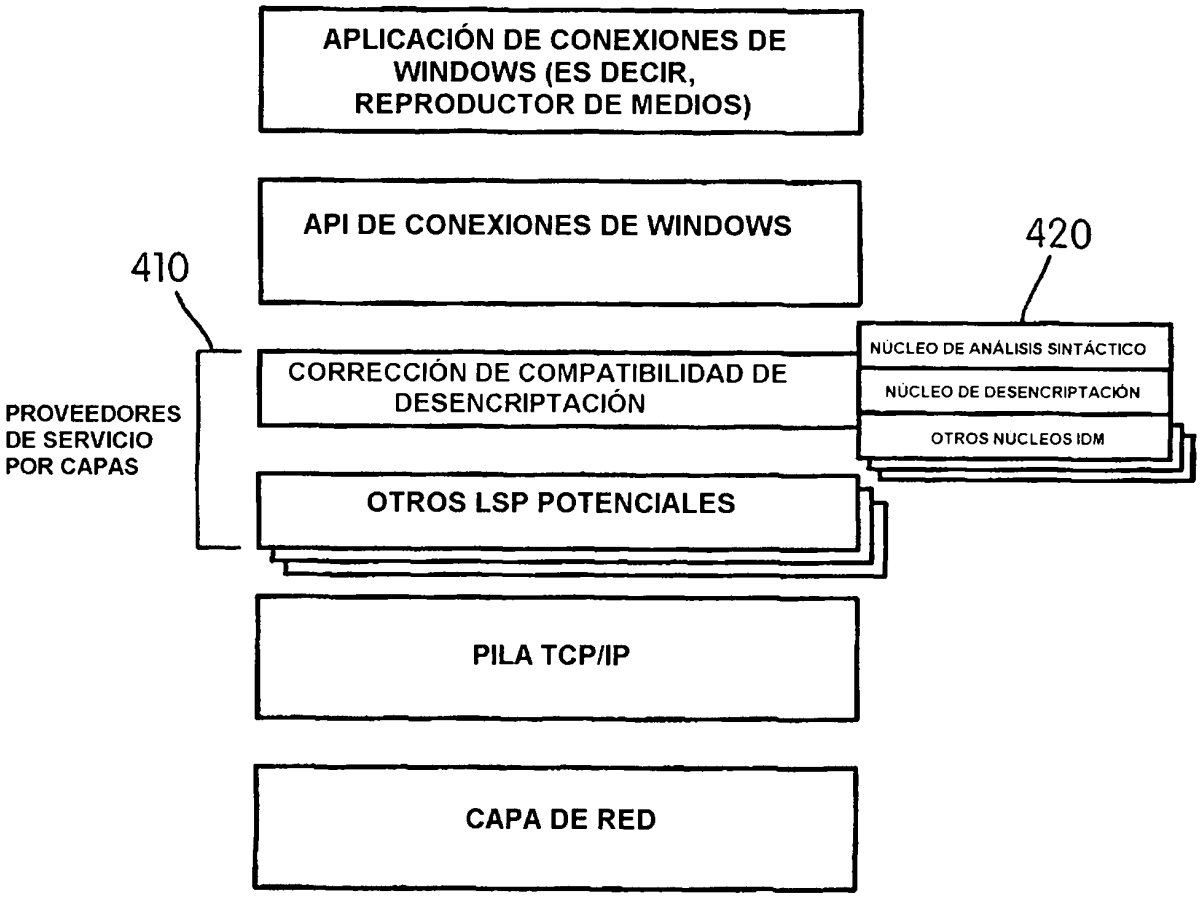
APLICACIÓN DE CONEXIONES DE WINDOWS (ES DECIR, REPRODUCTOR DE MEDIOS)
API DE CONEXIONES DE WINDOWS
410
420
PROVEEDORES DE SERVICIO POR CAPAS
CORRECCIÓN DE COMPATIBILIDAD DE DESENCRIPTACIÓN
NÚCLEO DE ANÁLISIS SINTÁCTICO
NÚCLEO DE DESENCRIPTACIÓN
OTROS NUCLEOS IDM
OTROS LSP POTENCIALES
PILA TCP/IP
CAPA DE RED

FIG. 4

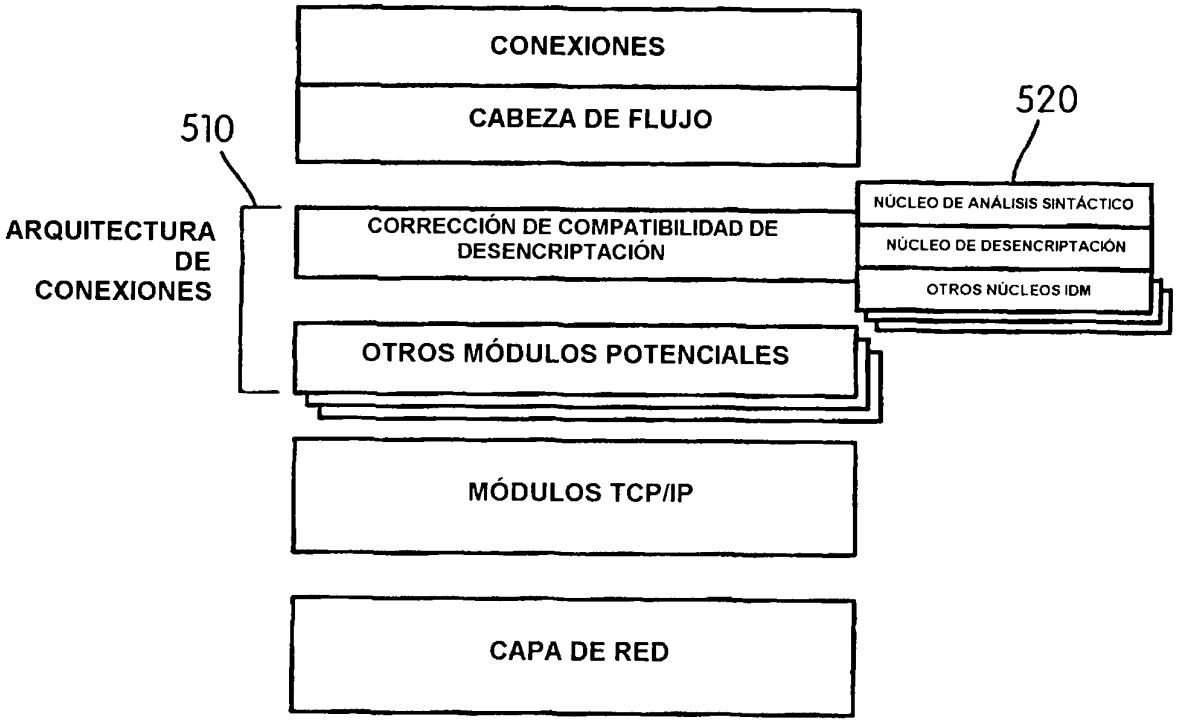
CONEXIONES
CABEZA DE FLUJO
510
520
ARQUITECTURA DE CONEXIONES
CORRECCIÓN DE COMPATIBILIDAD DE DESENCRIPTACIÓN
NÚCLEO DE ANÁLISIS SINTÁCTICO
NÚCLEO DE DESENCRIPTACIÓN
OTROS NÚCLEOS IDM
OTROS MÓDULOS POTENCIALES
MÓDULOS TCP/IP
CAPA DE RED

FIG. 5