(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 270 902**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **00992491 .1**
(86) Fecha de presentación : **09.11.2000**
(87) Número de publicación de la solicitud: **1340338**
(87) Fecha de publicación de la solicitud: **03.09.2003**

(54) Título: **Sistema de seguridad electrónico y esquema para una red de comunicaciones.**

(45) Fecha de publicación de la mención BOPI:
16.04.2007

(45) Fecha de la publicación del folleto de la patente:
16.04.2007

(73) Titular/es: **Accenture LLP**
1661 Page Mill Road
Palo Alto, California 94304, US

(72) Inventor/es: **Cornelius, Shawn, S.;**
Donoughe, Clifford;
Huffman, Arnold, Z.;
Klug, Matthew, C.;
Krahn, Richard, R.;
Kurup, Mohan;
Madden, Edward;
Sabaka, David, E.;
Su, Eric, C. y
Sweeney, Michael, S.

(74) Agente: **Elzaburu Márquez, Alberto**

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

DESCRIPCIÓN

Sistema de seguridad electrónico y esquema para una red de comunicaciones.

Campo de la invención

Esta invención se refiere a un sistema de seguridad electrónico y a un esquema de seguridad para una red de comunicaciones.

Antecedentes

Un sistema de seguridad electrónico puede utilizar protección de palabra de paso, un cortafuego o ambos para impedir que un usuario no autorizado comprometa la integridad de una transacción de empresa a empresa o un recurso interno de procesamiento de datos de una entidad comercial. Un recurso interno de procesamiento de datos puede incluir un servidor de empresa a empresa, un sistema de planificación de los recursos de una compañía, un sistema de procesamiento o tratamiento de datos o cualquier combinación de los elementos anteriores. Debido a los deficientes sistemas de seguridad electrónicos que se han venido utilizando en la técnica anterior, una entidad comercial puede verse impedida de encontrar socios comerciales que deseen poner en riesgo sus recursos internos de procesamiento de datos al participar en transacciones electrónicas a través de una red de comunicaciones externa, tal como la Internet. Los riesgos en cuanto a seguridad asociados a sistemas de seguridad inadecuados incluyen la apropiación indebida de información confidencial, de secretos comerciales y de información privada del cliente. Por otra parte, un usuario no autorizado puede adulterar o utilizar indebidamente software o programación que interrumpa las operaciones comerciales de una entidad.

Un recurso interno de tratamiento de datos puede incluir un sistema de autentificación de palabra de paso que proporcione un registro de identificación de entrada y una palabra de paso asociada con el fin de restringir el acceso al tráfico no autorizado. En consecuencia, el sistema de autentificación puede proteger los recursos internos de tratamiento de datos de la entidad de alguna exposición a tráfico externo no autorizado a través de una red de comunicaciones externa (por ejemplo, la Internet). Sin embargo, el esquema de protección de palabra de paso se ve limitado en su efectividad debido a que un usuario no autorizado puede descubrir una combinación de identificador de registro de entrada y palabra de paso autorizada, al probar numerosas combinaciones e iteraciones de posibles identificadores de registro de entrada y palabra de paso, por ejemplo.

El esquema de protección de palabra de paso se complementa, típicamente, con un esquema de protección de cortafuego. Un cortafuego hace referencia a instrucciones de software o programación, de hardware o dispositivos físicos, o de ambos, que filtran el tráfico para permitir el paso a través del cortafuego electrónico tan solo del tráfico procedente de una fuente aprobada o que tenga un identificador de puerta aprobado. El cortafuego puede bloquear el paso de tráfico no autorizado impidiendo que alcance el sistema de comunicación de datos desde la red de comunicaciones externa. El cortafuego puede evitar que personas ajenas y no autorizadas logren acceder a los recursos internos de tratamiento de datos de una entidad.

La eficacia de la solución del cortafuego se deteriora cuando se interpone un servidor de web en un recorrido o camino de comunicaciones entre el cortafuego y la red de comunicaciones externa. El servidor de web arrastra o capta intrínsecamente usuarios desconocidos desde la red de comunicaciones externa (por ejemplo, la Internet). Por otra parte, las medidas de seguridad para el servidor de web tienden a ser mínimas en comparación con las de los recursos internos de tratamiento de datos, con el fin de mantener el servidor de web abierto y accesible a posibles clientes y otra actividad económica. Debido a la presente proliferación en el número de usuarios que el cortafuego ha de proteger de la presencia del servidor de web, los recursos internos del sistema de comunicación de datos y las transacciones electrónicas son más vulnerables ante los ataques.

La tarea de proporcionar la suficiente seguridad a un sistema interno de tratamiento de datos (por ejemplo, un sistema de planificación de los recursos de una empresa) se ve complicada adicionalmente por el requisito de proporcionar el acceso de los recursos internos de tratamiento de datos a la red de comunicación externa con el fin de legitimar tratos comerciales y transacciones electrónicas con socios comerciales u otros usuarios. Así pues, existe la necesidad de una configuración de seguridad que proteja adecuadamente los recursos internos de tratamiento de datos de un sistema interno de la entidad, del acceso por parte de un usuario no autorizado, al tiempo que proporciona un fácil acceso de comunicaciones entre socios comerciales.

El documento WO-A-99/15950 describe una arquitectura de sistema de red dividida en tres divisiones arquitectónicas o estructurales principales: una estación de trabajo de cliente, un área de red segura, y los servidores de aplicación y la Intranet del propietario del sistema. Un doble sistema de cortafuegos crea el área de red segura entre dos cortafuegos. Uno de los cortafuegos incluye dispositivos de encaminamiento de filtrado específico de puerta que pueden conectarse únicamente con una puerta designada de un servidor de despacho situado dentro del área de red segura. El servidor de despacho se conecta a través de un cortafuego subordinado o delegado a los servidores de aplicación. Esto garantiza que un impostor o falsificador no puede conectarse directamente a ningún servidor de aplicación situado dentro de la Intranet del propietario, lo que garantiza la seguridad y la integridad internas del sistema.

Sumario de la invención

La presente invención proporciona un sistema y un método para proporcionar seguridad electrónica de acuerdo con las reivindicaciones 1 y 14, respectivamente.

De acuerdo con las realizaciones de la invención, un esquema de seguridad y un sistema de seguridad electrónicos para una red de comunicaciones impide o inhibe el acceso no autorizado a un recurso interno de un sistema informático interno de una entidad. Un servidor incluye un primer conjunto de puertas o accesos para la comunicación entre una red de comunicaciones externa y el servidor. El servidor tiene un segundo conjunto de puertas para las comunicaciones entre una red de comunicaciones interna y el servidor. Se ha interpuesto un primer cortafuego en un recorrido o camino de comunicación entre el servidor y la red de comunicaciones externa. El primer cortafuego está en comunicación con el primer conjunto de puertas con el fin de proporcionar al menos una inter-

conexión entre el primer conjunto de puertas y la red de comunicaciones externa. Se ha interpuesto un segundo cortafuego en un camino de comunicación entre el servidor y la red de comunicaciones interna. El segundo cortafuego está en comunicación con el segundo conjunto de puertas con el fin de proporcionar un número entero no negativo de intercomunicaciones entre el segundo conjunto de puertas y la red de comunicaciones interna.

Preferiblemente, una interconexión del primer cortafuego está asociada con un primer identificador de puerta y una interconexión del segundo cortafuego está asociada con un segundo identificador de puerta. Una interconexión se refiere a un camino de comunicaciones entre una puerta de entrada y una puerta de salida de un cortafuego. Además, el primer identificador de puerta es diferente del segundo identificador de puerta para cada interconexión activa, de tal manera que la penetración externa del primer cortafuego por un mensaje no autorizado es bloqueada por el segundo cortafuego.

Otras medidas de seguridad pueden complementar la asignación de diferentes identificadores de puerta al primer cortafuego y al segundo cortafuego para mejorar adicionalmente la integridad de la protección de seguridad de un recurso interno.

Breve descripción de las diversas vistas de los dibujos

La Figura 1 es un diagrama de bloques de un sistema para proporcionar seguridad electrónica para un entorno de red de comunicaciones de acuerdo con las realizaciones de la invención.

La Figura 2 es un diagrama de flujo de una realización de un método para proporcionar seguridad electrónica para una red de comunicaciones.

La Figura 3 es un diagrama de flujo de otra realización de un método para proporcionar seguridad electrónica para una red de comunicaciones.

Las Figuras 4 a 7 muestran diversas aplicaciones ilustrativas de disposiciones de seguridad de doble pared de acuerdo con las realizaciones de la invención.

Descripción detallada

De acuerdo con la invención, la Figura 1 muestra un primer sistema de comunicaciones 40 de una primera entidad, conectado a una red de comunicaciones externa 22, tal como la Internet. A su vez, la red de comunicaciones externa 22 está acoplada a un segundo sistema de comunicaciones 140 de una segunda entidad. La primera entidad y la segunda entidad pueden ser socios comerciales que intercambian datos transaccionales en forma de mensajes de datos a través de la red de comunicaciones externa 22. La red de comunicaciones externa 22 proporciona soporte a las comunicaciones entre un terminal externo autorizado 26 y uno de los sistemas de comunicación 40, 140. La red de comunicaciones externa 22 puede proporcionar también soporte a las comunicaciones entre un terminal de usuario no autorizado 24 y uno de los sistemas de comunicación 40, 140.

El primer sistema de comunicaciones 40 incluye una disposición de seguridad 34 que puede estar acoplada a la red de comunicaciones externa 22 y a una red de comunicaciones interna 14. La red de comunicaciones interna 14 puede estar acoplada a uno o más de los siguientes recursos internos: un primer sistema 12 de tratamiento de datos, un sistema 13 de gestión de base de datos y uno o más terminales internos 10.

El segundo sistema de comunicaciones 140 incluye una disposición de seguridad 34 que puede estar acoplada a la red de comunicaciones externa 22 y acoplada a una red de comunicaciones interna 14. La red de comunicaciones interna 14 puede estar acoplada a uno o más de los siguientes recursos internos: un segundo sistema 112 de tratamiento de datos, un sistema 13 de gestión de base de datos y uno o más terminales internos 10.

En general, un recurso interno 27 se refiere a cualquier sistema de procesamiento de datos que dé soporte a una actividad operacional o aplicación de negocios de una entidad o una persona afiliada a la entidad. Un recurso interno 27 incluye cualquiera de los siguientes: un servidor 29, un primer sistema 12 de procesamiento de datos (por ejemplo, un sistema de planificación de recursos de empresa (ERP -"enterprise resource planning"), un sistema 13 de gestión de base de datos, una base de datos y uno o más terminales internos 10.

Un primer sistema 12 de tratamiento de datos o un segundo sistema 112 de tratamiento de datos hace referencia a un sistema informático que lleva a cabo una función comercial o una función operacional para un usuario. Un sistema de planificación de recursos de empresa es un ejemplo de un primer sistema 12 de tratamiento de datos o de un segundo sistema 112 de tratamiento de datos. Un sistema de planificación de recursos de empresa da soporte al compartimiento de información entre diferentes secciones organizativas o diferentes sistemas informáticos de una entidad comercial. Por ejemplo, en el contexto de una corporación de fabricación, un sistema de planificación de recursos de empresa puede integrar ingeniería, ventas, gestión de materiales, compras, planificación de la producción y funciones de contabilidad de la corporación de fabricación. Un sistema 13 de base de datos de gestión incluye instrucciones de software o programación y dispositivos físicos o hardware para el almacenamiento y la recuperación de datos (por ejemplo, procedimientos de consulta) de una o más bases de datos.

Un terminal interno 10 puede comprender una computadora de cliente, una estación de trabajo u otro sistema de procesamiento de datos que esté dispuesto para comunicarse a través de la red de comunicaciones interna 14. En una de las realizaciones, los terminales internos 10 incluyen desde un primer cliente hasta un cliente enésimo. Un cliente puede comunicarse con otro cliente a través de la red de comunicaciones interna 14.

En una realización, la disposición de seguridad 34 se encuentra situada en un recorrido o camino de comunicaciones entre una red de comunicaciones interna 14 y una red de comunicaciones externa 22. La disposición de seguridad 34 puede controlar el acceso a los recursos internos 27 a través de una red de comunicaciones interna 14 ó de otra manera. Una red de comunicaciones interna 14 puede consistir en una red privada o una Intranet. Si bien los recursos internos 27 están conectados con la red de comunicaciones interna 14 como se muestra en la Figura 1, en una realización alternativa, cualquiera de los recursos internos 27 puede estar conectado directamente con la disposición de seguridad 34 de la invención.

Un servidor 29 da soporte a una transacción o intercambio de información entre diferentes entidades por medio de la red de comunicaciones externa 22. El servidor 29 puede actuar como un intermediario o una

interfaz entre diferentes entidades comerciales con el fin de garantizar el intercambio adecuado de los datos.

En una realización, una disposición de seguridad 34 comprende un servidor 29 emparedado o intercalado entre un primer cortafuego 30 y un segundo cortafuego 32. Un primer cortafuego 30 puede consistir en software, hardware o ambos. De forma similar, el segundo cortafuego 32 puede consistir en software, hardware o ambos. Como se muestra en la Figura 1, el primer cortafuego 30 representa un cortafuego exterior, en tanto que el segundo cortafuego 32 representa un cortafuego interior. Un cortafuego exterior se refiere a un cortafuego que está interpuesto en un camino de comunicaciones potencial o real, entre la red de comunicaciones externa 22 y el servidor 29. El cortafuego interior se refiere a un cortafuego que se encuentra interpuesto en un camino de comunicaciones potencial o real, entre el servidor 29 y la red de comunicaciones interna 14 ó un recurso interno 27.

El primer cortafuego 30 ó el segundo cortafuego 32 quiere decir un sistema que impide el acceso no autorizado a o desde un recurso interno 27. El primer cortafuego 30, el segundo cortafuego 32, ó ambos, pueden evitar el acceso por parte de un usuario no autorizado a la red de comunicaciones interna 14 ó a un recurso interno 27 desde la red de comunicaciones externa 22. El primer cortafuego 30 y el segundo cortafuego 32 pueden incluir hardware tal como un servidor subordinado o delegado, un dispositivo de encaminamiento de filtrado por paquetes, una computadora principal desprotegida o expuesta a los ataques, u otro sistema de tratamiento de datos destinado a proporcionar seguridad electrónica a un recurso interno 27.

Si bien son posibles una variedad de configuraciones de cortafuego y caen dentro del ámbito de la invención, en una realización preferida, el primer cortafuego 30 y el segundo cortafuego 32 se implementan por medio de dispositivos de encaminamiento de filtrado por paquetes. En una realización alternativa, la disposición de seguridad 34 puede realizarse en la práctica en una única computadora, de tal manera que el primer cortafuego 30, el servidor 29 y el segundo cortafuego 32 representan la organización lógica de las instrucciones de software dentro de la computadora. Para la configuración del dispositivo de encaminamiento de filtrado por paquetes, el primer cortafuego 30 y el segundo cortafuego 32 hacen un muestreo de los mensajes o paquetes de datos procedentes de al menos la red de comunicaciones externa 22. El primer cortafuego 30, el segundo cortafuego 32, ó ambos, tienen, preferiblemente, un criterio que bloquea el paso de los mensajes de datos y los paquetes de datos que no satisfacen una métrica de seguridad definida. La métrica de seguridad definida puede expresarse como una regla de filtrado. El dispositivo de encaminamiento de filtrado por paquetes puede contener reglas de filtrado que determinan qué paquetes que se dejan pasar a través del primer cortafuego 30 ó del segundo cortafuego 32, y a qué paquetes se les impide el paso por parte del primer cortafuego 30 ó del segundo cortafuego 32. Las reglas de filtrado del primer cortafuego 30 pueden ser diferentes de las reglas de filtrado del segundo cortafuego 32.

Un paquete de datos enviado desde un terminal externo autorizado 26, un terminal de usuario no autorizado 24 ó un segundo sistema 112 de tratamiento de datos, a través de la red de comunicaciones externa 22, tiene, típicamente, un encabezamiento de paquete. Aunque el encabezamiento de paquete puede diferir en el formato de los datos dependiendo del protocolo de comunicación aplicable, en una realización se utilizan paquetes de datos de protocolo de Internet (IP -"Internet Protocol"). El paquete de datos de un encabezamiento de paquete de protocolo de Internet incluye una dirección de suministro de IP, una dirección de destino de IP, un protocolo encapsulado, un acceso o puerta de fuente, una puerta de destino, un tipo de mensaje, la interfaz entrante del paquete de datos, así como la interfaz saliente del paquete de datos.

Un protocolo encapsulado define el formato y el procedimiento para transmitir datos entre dispositivos de comunicaciones entrantes. El protocolo encapsulado puede consistir en Protocolo de Control de Transmisión (TCP -"Transmission Control Protocol"), Protocolo de Diagrama de Datos de Usuario (UDP -"User Datagram Protocol"), Protocolo de Mensajes de Control de Internet (ICMP -"Internet Control Message Protocol"), Protocolo de Internet (IP), o en alguna combinación funcional de los anteriores protocolos. Los TCP e IP son protocolos que facilitan las comunicaciones entre computadoras centrales o principales y una red de comunicaciones, tal como la Internet. El UDP es un protocolo sin conexiones para la transferencia de diagramas de datos (es decir, de paquetes de datos) a través de una red que da soporte al IP. El ICMP hace referencia a una mejora del Protocolo de Internet que proporciona soporte a paquetes de datos que contienen mensajes de error, de control y de datos. La puerta de fuente y la puerta de destino pueden haberse asignado a puertas de TCP o de UDP, por ejemplo, en los cortafuegos.

Las reglas de filtrado analizan generalmente el contenido del encabezamiento del paquete para determinar si admitir el paquete de IP para su paso a través de al menos uno de los cortafuegos (por ejemplo, el 30 ó el 32) asociados con el encabezamiento de IP, o bien bloquear el paso del encabezamiento de IP asociado al paquete de IP a través de al menos uno de los cortafuegos. Una interconexión de un cortafuego consiste en un camino de comunicación entre una puerta de entrada y una puerta de salida de un cortafuego. Una puerta de entrada y una puerta de salida de un mensaje de datos entrante pueden diferir de una puerta de entrada y una puerta de salida de un mensaje de datos saliente. Por ejemplo, una puerta de entrada de un cortafuego (30, 32) para un mensaje de datos entrante procedente de la red de comunicaciones externa 22, puede convertirse en una puerta de salida para un mensaje de datos saliente a través de la red de comunicaciones externa 22. De la misma manera, una puerta de entrada de un cortafuego (30, 32) para un mensaje de datos saliente puede convertirse en una puerta de salida para un mensaje de datos entrante.

Una interconexión o abertura se refiere a un camino de comunicaciones entre una puerta de entrada y una puerta de salida de un cortafuego (30, 32). Una puerta de entrada puede ser una puerta física o una puerta virtual (por ejemplo, una emulación ideada con software) situada dentro de una computadora. Similarmente, una puerta de salida puede ser una puerta física o una puerta virtual situada dentro de una computadora. Una interconexión puede representar la conexión eléctrica real entre una puerta de entrada y una puerta de salida de un cortafuego (30, 32), si bien, en la práctica, un cortafuego incluye típicamente va-

rias capas de software o programación que actúan como interfaz con la capa física, a fin de introducir un procesamiento de datos entre la puerta de entrada y la puerta de salida del cortafuego. La ausencia de toda interconexión representa un estado bloqueado en el que se bloquea el progreso de las comunicaciones a través de cualquier camino de comunicaciones entre una puerta de entrada y una puerta de salida del cortafuego (30, 32). Los paquetes de datos o mensajes bloqueados pueden ser borrados, devueltos al emisor o procesados de otro modo.

El primer cortafuego 30 proporciona al menos un camino de comunicaciones o interconexión entre el servidor 29 y la red de comunicaciones externa 22. El segundo cortafuego 32 puede proporcionar un número entero no negativo de interconexiones. El número de interconexiones del segundo cortafuego 32 puede depender de un modo de seguridad. Durante un modo de seguridad normal, el número de primeras interconexiones del primer cortafuego 30 es menor o igual que el número de segundas interconexiones del segundo cortafuego 32. De acuerdo con ello, el segundo cortafuego 32 es capaz de proporcionar soporte a múltiples terminales internos utilizando los recursos computacionales del servidor 29 ó accediendo a la red de comunicaciones externa 22. En el curso de un modo de alta seguridad, el segundo cortafuego 32 puede proporcionar una interconexión selectivamente activa entre el servidor 29 y la red de comunicaciones interna 14 con el fin de facilitar la interacción del servidor 29 con otra entidad comercial. Por ejemplo, puede hacerse disponible una interconexión selectivamente activa del segundo cortafuego 32 en instantes fijados, al ocurrir un suceso, o conforme a un criterio según se necesite a lo largo de una duración limitada, para el funcionamiento adecuado o completo del servidor 29.

El primer cortafuego 30 tiene puertas exteriores 15 y puertas interiores 17. Las puertas exteriores 15 están dispuestas en un lado exterior de la disposición de seguridad 34, hacia la red de comunicaciones externa 22. Las puertas interiores 17 están dispuestas en un lado interior de la disposición de seguridad 34, en alejamiento de la red de comunicaciones externa 22. Una combinación de una puerta interior 17 y de una puerta exterior 18 tiene un identificador de puerta. Las puertas interiores 17 pueden ser puertas virtuales situadas dentro de una computadora o puertas físicas. El primer cortafuego 30 puede establecer una o más interconexiones o caminos de datos entre pares de puertas exteriores 15 y puertas interiores 17. Las interconexiones del primer cortafuego 30 (o del segundo cortafuego 32) se refieren a caminos de datos, con independencia de si está presente cualquier camino de circuitos eléctricos directo entre las puertas exteriores 15 y las puertas interiores 17.

El segundo cortafuego 32 tiene puertas exteriores 15 y puertas interiores 17. Las puertas exteriores 15 están dispuestas en uno de los lados de la disposición de seguridad 34, hacia la red de comunicaciones interna 14. Las puertas interiores 17 están dispuestas en un lado opuesto del segundo cortafuego 32, en alejamiento de la red de comunicaciones interna 14. Una combinación de puertas interiores 17 y puertas exteriores 15 tiene un identificador de puerta. El segundo cortafuego 32 puede establecer cero o más interconexiones o caminos de datos entre las puertas exteriores 15 y las puertas interiores 17.

El primer cortafuego 30 y el segundo cortafuego 32 facilitan una seguridad mejorada empleando una de las siguientes técnicas: (1) asignar un número menor (o un número igual) de interconexiones para el primer cortafuego 30 que para el segundo cortafuego 32, con el fin de restringir el acceso a los recursos internos 27 de la entidad; (2) asignar diferentes identificadores de puerta para las puertas abiertas del segundo cortafuego 32 y del primer cortafuego 30, a fin de impedir una penetración no autorizada tanto del primer cortafuego 30 como del segundo cortafuego 32 desde un terminal de usuario no autorizado 24, a través de la red de comunicaciones externa 22; (3) asignar o dedicar funciones particulares a interconexiones o identificadores de puerta del primer cortafuego 30, del segundo cortafuego 32 ó de ambos; (4) asignar una clave de filtrado de paquetes basándose en una dirección de fuente de un segundo sistema 112 de tratamiento de datos o de un primer sistema 12 de tratamiento de datos, de tal manera que la clave de filtrado de paquetes es asignada a un identificador de puerta o un grupo de identificadores de puerta concretos del primer cortafuego 30 y del segundo cortafuego 32.

De acuerdo con una primera técnica, la disposición del primer cortafuego 30 y del segundo cortafuego 32 restringe el acceso no deseado por parte de un terminal de usuario no autorizado 24 a los recursos internos 27 del primer sistema de comunicaciones 40, al asignar un número menor (o un número igual) de interconexiones para el primer cortafuego 30 que para el segundo cortafuego 32. En consecuencia, el servidor 29 asigna un número menor en el primer conjunto 36 de puertas con respecto al segundo conjunto 38 de puertas.

El número mayor (o igual) de interconexiones asociadas con el segundo cortafuego 32 permite al servidor 29 soportar totalmente las transacciones comerciales que son conducidas hasta el segundo sistema de comunicaciones 112, por ejemplo. El mayor número de interconexiones del segundo cortafuego 32 puede servir a los requerimientos de las fuentes internas 29 para acceder a los recursos externos disponibles a través de la red de comunicaciones externa 22. Por ejemplo, el usuario de un terminal interno 10 puede acceder a un recurso de comunicaciones público (por ejemplo, una página web) a través de la red de comunicaciones externa 22.

Si bien se muestran en la Figura 1 cuatro interconexiones posibles, en una realización, tan poco como una de las interconexiones del primer cortafuego 30 puede soportar una transacción de empresa a empresa entre el primer sistema 12 de tratamiento de datos y el segundo sistema 112 de tratamiento de datos. Esto es, tres de las cuatro interconexiones pueden permanecer cerradas al tiempo que se proporciona soporte a una transacción comercial entre las primera y segunda entidades. La interconexión abierta puede dar soporte a una transacción de empresa a empresa. La puerta de la que se trate puede comprender una puerta que está dedicada al HTTP (protocolo de transferencia de hipertexto -"hypertext transfer protocol") o al HTTPS (protocolo de transferencia de hipertexto segura -"hypertext transfer protocol, secure"). Tanto el HTTP como el HTTPS proporcionan soporte a la transferencia de documentos en lenguaje de adición de hipertexto (HTML -"hypertext mark-up language") o en lenguaje de adición extensible (XML -"extensible mark-up language").

De acuerdo con una segunda técnica para un men-

saje de datos o un paquete de datos dado, una interconexión del primer cortafuego 30 (por ejemplo, el cortafuego exterior) está asociada con un primer identificador de puerta para la puerta exterior 15 y, una interconexión del segundo cortafuego 32 (por ejemplo, cortafuego interior) está asociada con un segundo identificador de puerta para la puerta interior 17. Por otra parte, el primer identificador de puerta es diferente del segundo identificador de puerta para cada interconexión activa del primer cortafuego 30 y del segundo cortafuego 32, de tal modo que se bloquea la penetración externa de un mensaje de datos a través del primer cortafuego 30 por parte del segundo cortafuego 32.

Los identificadores de puerta de las puertas exteriores 15 del primer cortafuego 30 difieren de los identificadores de puerta de las puertas interiores 17 del segundo cortafuego 32, de tal manera que, si un mensaje o paquete de datos no autorizado es capaz de transgredir el primer cortafuego 30 mediante la determinación de la identidad de un identificador de puerta de las puertas exteriores 15 del primer cortafuego 30, se bloquea o deniega la entrada del mensaje o paquete de datos no autorizado al segundo cortafuego 32 por las puertas interiores 17 del segundo cortafuego 32. Por ejemplo, si el segundo cortafuego 32 se materializa como un dispositivo de encaminamiento de filtrado por paquetes, el segundo cortafuego rechaza la entrada o paso de un paquete de datos o mensaje de datos a través del segundo cortafuego 32 basándose en el identificador de puerta de destino contenido en el paquete de datos.

El identificador de puerta de destino contenido en el paquete de datos se compara con el primer identificador de puerta de una puerta exterior 15 del primer cortafuego 30. Si el identificador de puerta de destino coincide con el primer identificador de puerta, el primer cortafuego 30 permite al mensaje de datos pasar a través de una interconexión del primer cortafuego 30. De forma similar, si el identificador de puerta de destino contenido en el paquete de datos coincide con un identificador de puerta de una puerta interna 17 del segundo cortafuegos 32, el mensaje de datos pasa a través del segundo cortafuego 32 a través de una interconexión. El paso a través del segundo cortafuego 32 puede llevarse a cabo de acuerdo con al menos dos procedimientos alternativos. Bajo un primer procedimiento, una fuente (por ejemplo, un segundo sistema de comunicaciones 112) organiza un paquete de datos o un mensaje entrante en un formato de datos que proporciona soporte a múltiples indicadores de puerta de destino. Bajo un segundo procedimiento, el primer cortafuego 30 incluye un traductor de identificador de puerta destinado a traducir un identificador de puerta de destino recibido a un identificador de puerta de destino revisado, con la primera autentificación de cortafuego de un mensaje de datos o de un paquete de datos. Dicho procedimiento de autentificación puede requerir la validación de que la dirección de fuente coincide con una lista de direcciones de fuente definidas, asociadas con socios comerciales autorizados, la cual puede incluir la primera entidad y la segunda entidad.

El servidor 29 puede ser responsable de asignar el identificador de puerta adecuado que se necesite para penetrar en el segundo cortafuego 32. De esta forma, el servidor 29 puede tener medidas de seguridad adicionales tales como un programa de aplicación cifrado y procedimientos de autentificación. El mensaje de datos se autentifica antes de la asignación de empresa a empresa el identificador de puerta apropiado para la penetración del segundo cortafuegos 32.

De acuerdo con una tercera técnica de mejora de la seguridad, las puertas individuales del primer cortafuego 30, del segundo cortafuego 32 ó del servidor 29 pueden ser asignadas o dedicadas a usos, aplicaciones o funciones particulares con el fin de proporcionar una medida adicional de seguridad. Por ejemplo, el primer conjunto 36 de puertas del servidor puede ser asignado o dedicado a usos, aplicaciones o funciones particulares. Si una puerta particular no proporciona soporte a ningún uso, aplicación o función, no se redirige ningún mensaje de datos ni paquete de datos a una puerta de soporte apropiada, pero puede ser registrado en una base de datos (por ejemplo, un registro de actividades sospechosas) para perseguir la actividad fraudulenta. Como resultado de ello, el emisor autorizado de un mensaje de datos entrante, de un mensaje de datos saliente o de ambos necesitará solicitar el identificador de puerta de entrada correcto que proporcione soporte a una función deseada correspondiente dentro de un cuerpo del mensaje o paquete de datos, a fin de facilitar la transmisión a través de la disposición de seguridad 34 para obtener el acceso a los recursos internos 27.

De acuerdo con una cuarta técnica, el primer cortafuego 30 ó el segundo cortafuego 32 puede utilizar un filtrado por paquetes para bloquear el paso de todos los mensajes o paquetes de datos a través del primer cortafuego 30 ó del segundo cortafuego 32, respectivamente, siempre y cuando el mensaje o paquete no tenga una dirección de fuente autorizada (por ejemplo, establecida en el encabezamiento de un paquete de datos correspondiente) o alguna otra clave de filtrado por paquetes. Existe una dirección de fuente autorizada que está afiliada con un sistema de procesamiento de datos o un servidor de un socio comercial, tal como la primera entidad o la segunda entidad.

Si bien la Figura 1 muestra cuatro líneas de comunicación entre el primer cortafuego 30 y el servidor 29, así como una única línea de comunicación entre el segundo cortafuego 32 y el servidor 29, son posibles otras configuraciones de líneas de comunicación y caen dentro del ámbito de la invención. Como se muestra en la Figura 1, el primer cortafuego 30 da soporte a cuatro interconexiones, designadas como una interconexión primaria 61, una interconexión secundaria 62, una interconexión terciaria 63 y una interconexión cuaternaria 64. Pueden utilizarse tan pocas como una de las interconexiones (por ejemplo, la interconexión primaria 61 ó la interconexión secundaria 62) para proporcionar soporte a la capacidad funcional completa de las transacciones de empresa a empresa entre el primer sistema 12 de tratamiento de datos y el segundo sistema 112 de tratamiento de datos. Cada una de las interconexiones tiene su propia protección de seguridad contra el tráfico no autorizado, en virtud de la capacidad funcional restringida de la interconexión y de las puertas interiores 17 y las puertas exteriores 15 asociadas. De acuerdo con ello, en el caso de que se utilice tan solo una interconexión, la interconexión puede consistir en una interconexión de propósito general para transportar una mezcla de diferentes tipos de tráfico.

La interconexión primaria 61 proporciona soporte

a tráfico de Protocolo de Transferencia de Hipertexto (HTTP -"HyperText Transfer Protocol") normal, pero bloquea otros tipos de tráfico. El Protocolo de Transferencia de Hipertexto (HTTP) se refiere a un protocolo que define el modo como los mensajes de datos son formateados, transmitidos y procesados para servidores y ojeadores de Web. El tráfico de HTTP incluye documentos en HTML y documentos en XML. El tráfico de HTTP proporciona soporte a peticiones de transferencia de páginas web ordinarias y sus respuestas. Por otra parte, en una realización, la interconexión primaria 61 tan solo permite que pase el tráfico procedente de una dirección de fuente específica, una dirección de destino específica o ambas, a través del primer cortafuego 30.

La interconexión secundaria 62 permite que el tráfico de HTP cifrado o el tráfico de Capa de Conexión entre Programas Segura (SSL -"Secure Socket Layer") pase a través del primer cortafuego 30, pero bloquea prácticamente todos los demás tipos de tráfico. El tráfico de HTTP seguro o cifrado puede considerarse como de HTTPS. El HTTPS es una variante o extensión del HTTP a la que se proporciona soporte por ciertos servidores de web y ojeadores. El SSL da soporte al establecimiento de una conexión segura entre dispositivos de red que se comunican a través de la red de comunicaciones externa 22, en tanto que el HTTP da soporte a la transmisión de mensajes seguros. Los documentos en XML y los documentos en HTML pueden ser transmitidos como tráfico de HTTPS. En una realización, la interconexión secundaria 62 tan solo permite que el tráfico procedente de una dirección de fuente específica, de una dirección de destino específica o de ambas, pase a través del primer cortafuego 30.

La interconexión terciaria 63 proporciona soporte a la supervisión de un servidor (por ejemplo, el servidor webMethods B2B, donde webMethods y webMethods B2B son marcas comerciales de webMethods, Inc.) y de sus componentes constitutivos. La interconexión cuaternaria 64 puede dar soporte al seguimiento del sistema y a operaciones de mantenimiento de un recurso interno 27 por medio de un software de aplicación para el seguimiento de componentes de sistema.

La disposición de seguridad 34 puede mejorar adicionalmente la seguridad proporcionada por el primer cortafuego 30 y por el segundo cortafuego 32 al hacer funcionar el servidor (por ejemplo, el servidor 29) en un modo de comisión o delegación, o como un modo de computadora central desprotegida. El modo de delegación y el modo de computadora central desprotegida pueden complementar cualquiera de las técnicas anteriormente mencionadas, incluyendo las técnicas a las que se hace referencia como primera técnica a cuarta técnica, ambas inclusive. Al tiempo que permite a un segundo sistema de comunicaciones 112 cambiar datos con el servidor 29, el servidor 29 puede actuar como un servidor subordinado o delegado para un recurso interno 27 (por ejemplo, el primer sistema 12 de tratamiento de datos), de tal manera que el sistema 112 de procesamiento a distancia nunca tenga que acceder directamente al recurso interno 27 del primer sistema de comunicaciones 40. De acuerdo con un modo de comisión o delegación, el servidor 29 puede conceder sencillamente el acceso del segundo sistema 112 de procesamiento de datos al servidor 29, el cual actúa como un intermediario entre el segundo sistema 112 de tratamiento de datos y el primer sistema 12 de tratamiento de datos. Por ejemplo, el segundo sistema 112 de tratamiento de datos puede comunicarse con el servidor 29, que remite información al primer sistema 12 de procesamiento de datos (por ejemplo, el sistema ERP) a través de la red de comunicaciones interna 14. De acuerdo con ello, el segundo sistema 112 de procesamiento de datos no necesita conocer y no recibe las configuraciones de red de la red de comunicaciones interna 14 para comunicarse con el primer sistema 12 de tratamiento de datos. Se preserva, por lo tanto, la integridad de la red de comunicaciones interna 14 y de los recursos internos 27, al menos en cierta medida, al no compartir información acerca de la configuración de la red de comunicaciones interna 14 con el segundo sistema 112 de tratamiento de datos, con el terminal externo autorizado 26 ó con el terminal de usuario no autorizado 24.

En una realización, el servidor 29 puede realizarse en la práctica como una computadora principal desprotegida o expuesta a los ataques, en la que la seguridad se proporciona en un nivel de aplicación, en contraposición al nivel de seguridad de las capas de red del filtrado por paquetes de los primer y segundo cortafuegos (30, 32). El servidor de bastión tan solo puede dar soporte a aplicaciones limitadas o enumeradas, o a funciones de las mismas, en tanto que otros servicios a los que, de otro modo, se podría dar soporte por parte del servidor 29, son denegados con el fin de promover adicionalmente la seguridad. Si bien podría instalarse un programa de comunicaciones delegado adicional en el servidor 29 con el fin de dar soporte al correo electrónico, e incluso otro programa de comunicaciones delegado podría proporcionar soporte a un acceso de web en todo el mundo, el servidor 29 puede estar limitado a contener un programa de comunicaciones delegado para servicios de empresa a empresa entre diferentes socios comerciales, tales como la primera entidad y la segunda entidad en una realización.

El servidor 29 puede hacer funcionar un sistema de funcionamiento cifrado y puede tener un programa delegado para proporcionar un servicio basado en una delegación a los terminales internos 10 ó a los terminales externos 26. Por otra parte, el servidor 29 puede haberse restringido intencionalmente en su capacidad para comunicarse con elementos de red de la red de comunicaciones interna 14.

En una realización alternativa, la red de comunicaciones externa 22 incluye una red de comunicaciones privada o un enlace de comunicaciones privado y virtual a través de la Internet. Una red de comunicaciones privada puede ser menos susceptible de uso indebido y de escuchas ocultas que las redes de comunicaciones internas 14 de las diferentes entidades comerciales que se comunican a través de la Internet. De acuerdo con ello, el primer sistema de comunicaciones y el segundo sistema de comunicaciones pueden intercambiar mensajes de datos o involucrarse en transacciones electrónicas a través de un canal de comunicaciones privado, un canal de comunicaciones cifrado, o bien un enlace de comunicaciones privado virtual, o similar.

La Figura 2 es un diagrama de flujo de un método para proporcionar seguridad para las comunicaciones entre un primer sistema de comunicaciones 40 de la primera entidad y un segundo sistema de comunicaciones 140 de la segunda entidad, a través de una red

de comunicaciones externa 22. El método de la Figura 2 comienza en la etapa S10.

En la etapa S10, un segundo sistema de comunicaciones 140 prepara un mensaje de datos asociado con (1) una dirección de fuente del segundo sistema 112 de tratamiento de datos o de un servidor de la segunda entidad, y (2) una dirección de destino del primer sistema 12 de tratamiento de datos o de un servidor 29 de la primera entidad. La dirección de fuente de un servidor (por ejemplo, el servidor 29) puede ser utilizada en el caso de que el servidor opere en un modo de delegación o como intermediario en representación del primer sistema 12 de tratamiento de datos y del segundo sistema 112 de tratamiento de datos.

En la etapa S12, el segundo sistema de comunicaciones 140 añade como anotación o anexa al mensaje de datos un primer identificador de puerta asociado con un primer cortafuego 30, y un segundo identificador de puerta asociado con un segundo cortafuego 32. El primer identificador de puerta es distinto del segundo identificador de puerta. El primer identificador de puerta y el segundo identificador de puerta pueden ser establecidos o actualizados por acuerdo mutuo de las primera y segunda entidades.

En la etapa S14, el segundo sistema de comunicaciones 140 envía el mensaje de datos, así como el primer identificador de puerta y el segundo identificador de puerta asociados, la dirección de destino y la dirección de fuente, desde el segundo sistema de comunicaciones 140 al primer sistema de comunicaciones 40 a través de la red de comunicaciones externa 22.

En la etapa S16, el primer cortafuego 30 determina lo siguiente: (1) si la dirección de destino enviada coincide con una dirección de destino de referencia, y (2) si el primer identificador de puerta enviado coincide con un primer identificador de puerta de referencia, el cual es residente en, y está asociado con, una interconexión o abertura activa existente en el primer cortafuego 30. Una interconexión asociada con el primer identificador de puerta puede estar abierta o activa para un propósito general (por ejemplo, para cualquier tráfico) o un propósito limitado (por ejemplo, para un tráfico relacionado con una transacción individual de empresa a empresa o con un grupo de transacciones de empresa a empresa). En el caso de que la dirección de destino enviada coincida con la dirección de destino de referencia, y si el identificador de puerta enviado coincide con el identificador de puerta de referencia, entonces el método prosigue con la etapa S18. En caso contrario, el método continúa en la etapa S20.

En la etapa S18, el primer cortafuego 30 hace pasar el mensaje de datos a través de una interconexión del primer cortafuego 30. En una realización alternativa, el primer cortafuego 30 puede aplicar otras medidas de seguridad antes de hacer pasar el mensaje de datos a través del primer cortafuego 30. Por ejemplo, en la realización alternativa, el primer cortafuego 30 puede determinar que un indicador de capacidad funcional definido y contenido en un mensaje de datos, coincide con un indicador de capacidad funcional de referencia, residente en el primer cortafuego, como condición necesaria para hacer pasar el mensaje de datos a través del primer cortafuego 30.

Por el contrario, en la etapa S20, el primer cortafuego 30 bloquea el mensaje de datos impidiendo que atraviese el primer cortafuego 30. El primer cortafuego 30 introduce los datos en un registro de entrada de actividades sospechosas. Un usuario u operador puede observar e investigar el registro de entrada de actividades sospechosas con el fin de frustrar o identificar a un usuario no autorizado que ha intentado el acceso ilícito al primer sistema de comunicaciones 40.

En la etapa S22, que va detrás de la etapa S18, el segundo cortafuego enviado 32 determina si el segundo identificador de puerta enviado coincide con una segundo identificador de puerta de referencia, el cual es residente en, y está asociado con, una interconexión o abertura activa existente en el segundo cortafuego 32. El segundo identificador de puerta de referencia es, preferiblemente, diferente del primer identificador de puerta de referencia, de tal manera que el acceso a través del primer cortafuego 30 no proporciona automáticamente acceso a través del segundo cortafuego 32. Una interconexión asociada con el segundo identificador de puerta puede estar abierta o activa para un propósito general (por ejemplo, un tráfico cualquiera) o para un propósito limitado (por ejemplo, tráfico relacionado con una única transacción de empresa a empresa o con un grupo de transacciones de empresa a empresa). Si el segundo identificador de puerta enviado coincide con un segundo identificador de puerta de referencia, entonces el método continúa con la etapa S24. Sin embargo, si el segundo identificador de puerta enviado no coincide con el segundo identificador de puerta de referencia, el método prosigue con la etapa S26.

En la etapa S24, el segundo cortafuego 32 hace pasar el mensaje de datos a través del segundo cortafuego 32. En una realización alternativa, el primer cortafuego 30 puede aplicar otras medidas de seguridad antes de hacer pasar el mensaje de datos a través del segundo cortafuego 32.

En la etapa S26, el segundo cortafuego 32 bloquea el mensaje de datos de manera que no atraviese el segundo cortafuego 32. El segundo cortafuego 32 introduce datos del mensaje de datos en un registro de entrada de actividades sospechosas, de tal manera que el usuario u operador puede frustrar la actividad fraudulenta o ilícita de un terminal de usuario no autorizado.

En la etapa S28, que sigue a la etapa S24, el primer sistema 12 de procesamiento de datos recibe el mensaje de datos en el servidor para cualquier acción subsiguiente que sea necesaria o apropiada. Otras medidas de seguridad que se describen en combinación con la Figura 1 pueden complementar el método de la Figura 2 para fomentar la protección de las transacciones electrónicas entre las primera y segunda entidades.

El método de la Figura 3 es similar al método de la Figura 2. Los mismos números de referencia en la Figura 2 y en la Figura 3 indican etapas similares. Sin embargo, la Figura 3 difiere de la Figura 2 en que la etapa S30 reemplaza a la etapa S12, la etapa S32 reemplaza a la etapa S14 y la etapa S34 reemplaza a la etapa S22.

La etapa S30 va a continuación de la etapa S10. En la etapa S30, el segundo sistema de comunicaciones 140 añade como anexo al mensaje de datos un primer identificador de puerta asociado con un cortafuego 30. Es decir, el segundo sistema de comunicación 140 puede no añadir como anexo al mensaje de datos el segundo identificador de puerta asociado con un segundo cortafuego 32, a fin de conservar la anchura de banda espectral o debido a que se reduce el riesgo de

seguridad con respecto a otras medidas de seguridad desplegadas activamente.

En la etapa S32, que sigue a la etapa S30, el segundo sistema de comunicaciones 140 envía el mensaje de datos y el primer identificador de puerta asociado, así como la dirección de destino y la dirección de fuente, desde el segundo sistema de comunicaciones 140 al primer sistema de comunicaciones 40 a través de la red de comunicaciones externa. La dirección de fuente puede consistir en una dirección del segundo sistema 112 de tratamiento de datos o de un servidor afiliado.

Saltando a la etapa S34, que sigue a la etapa S18, el segundo cortafuego 32 determina si la dirección de fuente enviada coincide con una dirección de fuente de referencia que reside en el segundo cortafuego 32. De esta forma, la etapa S34 se sirve de la dirección de fuente enviada a modo de un identificador que es distinto del primer identificador de puerta del primer cortafuego 30, al objeto de evitar que un usuario no autorizado obtenga acceso al primer sistema 12 de tratamiento de datos. Si el segundo cortafuego 32 determina que la dirección de fuente enviada coincide con la dirección de fuente de referencia, el método prosigue con la etapa S24. Si el segundo cortafuego 32 determina que la dirección de fuente enviada no coincide con la dirección de fuente de referencia, el método continúa con la etapa S26. De acuerdo con el método de la Figura 3, la segunda dirección de fuente puede utilizarse con independencia de cualquier segundo identificador de puerta o primer identificador de puerta asociado con el mensaje de datos.

Las Figuras 4 a 7 muestran que el sistema de seguridad (incluyendo la disposición de seguridad 34) de la presente solicitud puede ser configurado independientemente de la configuración asociada con la configuración ya existente del sistema de comunicaciones interno y de cualquier disposición de seguridad ya existente. Los mismos números de referencia indican, en la Figura 1 y en las Figuras 4 a 7, elementos similares. El sistema de comunicaciones a distancia 240 puede incluir una disposición de seguridad y un segundo sistema de tratamiento de datos, similares o idénticos a los de la Figura 1. En las Figuras 4 a 7, el establecimiento de la disposición de seguridad de empresa a empresa (por ejemplo, la disposición de seguridad 34) es generalmente el mismo, con independencia del sistema de seguridad existente. El sistema de seguridad 34 se añade a una configuración de servidor ya existente de una forma modular. De este modo, el sistema de seguridad de la presente invención es susceptible de someterse a estandarización o normalización, lo que facilita un tiempo de configuración reducido y un coste de establecimiento reducido.

La disposición de seguridad 34 puede ser producida de acuerdo con una única especificación o un grupo de especificaciones, en lugar de una solución personalizada para el cliente, a fin de ajustarse a la mayor parte de los requisitos de los clientes. El servicio y mantenimiento de la disposición de seguridad 34 puede seguir pautas de guía universales con independencia de la topología del servidor existente. En consecuencia, la implementación de los sistemas se planifica o ensaya fácilmente por adelantado con respecto al verdadero despliegue sobre el terreno, a fin de mejorar la calidad global. Puede dotarse al personal de ventas y de marketing, así como al marketing, de configuraciones de servidor estándares o normalizadas que tienen costes conocidos, en lugar de un sistema personalizado para el cliente, que podría requerir la intervención especializada de profesionales de ingeniería o de tecnologías de la información, siguiendo un criterio dependiente de cada caso particular.

La Figura 4 muestra una disposición de seguridad 34 instalada en una entidad comercial con un servidor ya existente 46, de tal modo que se proporcionan dos conexiones principales 52 a la red de comunicaciones externa 22. Por ejemplo, cada conexión principal 52 puede consistir en una línea T1 (o línea E1) hacia la red de comunicaciones externa 22 a través de un proveedor de servicios de Internet (no mostrado).

El servidor ya existente 46 que se muestra en la Figura 4 no está conectado, preferiblemente, a la red de comunicaciones interna 14 de la entidad. Como resultado de ello, un usuario no autorizado no plantea prácticamente ninguna amenaza a la seguridad de la red de comunicaciones interna 14 (o de los recursos internos afiliados 27) a través del servidor ya existente 46. La integridad del servidor existente 46 en sí mismo se mantiene y preserva por medio de un cortafuego exterior 44 que puede consistir en un dispositivo de encaminamiento de filtrado por paquetes, un servidor subordinado o delegado y una pasarela de aplicación, o similar.

Incluso si se comprometiese la integridad del servidor 46 existente y un terminal de usuario no autorizado 24 obtuviese el acceso al servidor existente 46, el usuario no autorizado no conseguiría obtener ninguna información acerca de la configuración de red de la red de comunicación interna 14, como tampoco sería capaz el terminal de usuario no autorizado 24 de utilizar indebidamente, interrumpir o incapacitar el servidor 29 de ninguna manera en absoluto. En el caso de que el usuario no autorizado consiga el control del servidor existente 46, tal control es irrelevante para el servidor 29 (por ejemplo, un servidor de empresa a empresa) debido a que el servidor 29 no trata, preferiblemente, al servidor existente 46 como un servidor de confianza sino como cualquier otro servidor o externo o extraño que está conectado a la red de comunicación externa 22.

La Figura 5 muestra un ejemplo en el que el servidor existente 46 no está protegido por un cortafuego. En lugar de ello, el servidor existente 46 puede confiar en otras medidas de seguridad. Por ejemplo, el servidor existente 46 puede confiar en una palabra de paso y en un identificador de registro de entrada para autentificar a los usuarios e impedir el acceso no autorizado en el ejemplo de la Figura 5. Por otra parte, el programa operativo y el programa de aplicación del servidor existente 46 puede estar cifrado a fin de impedir o disuadir de la alteración de cualquiera de los programas. Incluso si se ven comprometidas las medidas de seguridad del servidor existente 46 de la Figura 5, semejante fallo de la seguridad es irrelevante para el servidor 29 con la configuración de seguridad 34 por las razones que se han explicado en lo anterior en combinación con la Figura 4.

La Figura 6 muestra una instalación de la disposición de seguridad 34 en combinación con un servidor existente 46, en la que puede utilizarse, en tándem con la disposición de seguridad 34, un cortafuego interior adicional 48. El cortafuego interior adicional 48 proporciona, preferiblemente, una técnica complementaria o técnica de cortafuego diferente a la del primer cortafuego 30 ó la del segundo cortafuego 32 de la

disposición de seguridad 34. De acuerdo con ello, si el primer cortafuego 30 y el segundo cortafuego 32 consisten en dispositivos de encaminamiento de filtrado por paquetes, entonces el cortafuego interior adicional 48 comprende una pasarela de aplicación, una pasarela en el nivel de los circuitos o un servidor subordinado o delegado con el fin de mejorar adicionalmente la seguridad de todo el sistema.

La Figura 7 es similar a la Figura 6, a excepción de que la Figura 7 contiene un cortafuego exterior adicional 44 que protege el servidor existente 46. El cortafuego exterior adicional 44 tiene cualquier configuración de cortafuego, incluyendo un dispositivo de encaminamiento de filtrado por paquetes. El cortafuego exterior 44 se ha descrito anteriormente en combinación con la Figura 4.

Las Figuras 4 a 7 ilustran el hecho de que la configuración doble de cortafuego 34 y servidor 29 puede llevarse a la práctica fácilmente como un paquete modular estándar en una configuración estándar que se planifica, instala y mantiene de una manera consistente y repetitiva. La estandarización de la configuración favorece las logísticas comerciales de gestión y minimiza el coste de la fabricación, la instalación, el mantenimiento y el funcionamiento del sistema de seguridad de la invención.

En general, la disposición de seguridad 34 de la invención resulta muy adecuada a la hora de facilitar las transacciones de empresa a empresa entre la primera entidad y la segunda entidad, que están a salvo de interrupciones o lapsos en la seguridad que de otro modo podrían ser provocados por un terminal de usuario no autorizado 24. La disposición de seguridad 34 proporciona seguridad electrónica con respecto al tráfico en una red de comunicaciones externa 22 (por ejemplo, la Internet), a fin de impedir que un terminal de usuario no autorizado 24 consiga acceder a un recurso interno 27 del primer sistema de comunicaciones 40 ó del segundo sistema de comunicaciones 140.

Diversas modificaciones del sistema de seguridad y del esquema de seguridad pueden caer dentro del ámbito de la invención que aquí se ha descrito. Por ejemplo, en una realización alternativa, el servidor 29 puede proporcionar un servidor delegado que incluye un filtro en el nivel de aplicación, para el tráfico entrante desde la red de comunicación externa, al tiempo que proporciona una pasarela en el nivel de los circuitos, destinada a la comunicación saliente que procede de la red de comunicaciones interna 14 ó del terminal conectado a la misma. Si bien, en una realización preferida, el servidor 29 no da soporte al acceso por parte del terminal interno 10 a los servicios de web mundiales o de correo electrónico a través del servidor 29, en una realización alternativa, una pasarela en el nivel de los circuitos puede proporcionar acceso a los servicios de web mundiales, de correo electrónico u otros relacionados con Internet. La pasarela en el nivel de los circuitos puede estar asociada con una ligera degradación potencial de la seguridad ofrecida a la entidad comercial con respecto a ataques por parte de un usuario no autorizado.

Una pasarela en el nivel de los circuitos proporciona unos mecanismos de comunicación para una conexión de TCP o de UDP. La puerta de protocolo IP identifica el formato de los paquetes de datos, en tanto que el TCP permite a una computadora principal establecer una conexión para intercambiar una corriente de datos de tal manera que el suministro de los datos se lleva a cabo en el mismo orden en el que se enviaron desde la computadora principal transmisora. El UDP o Protocolo de Diagrama de Datos de Usuario (“User Datagram Protocol”) hace referencia a un protocolo de paquetes de datos para redes conmutadas en paquetes, el cual proporciona un soporte de recuperación de mínimo error y puede ser utilizado para emitir o difundir mensajes a través de una red de comunicación externa o interna.

La anterior descripción del sistema de seguridad y del esquema de seguridad describe diversos ejemplos ilustrativos de la invención. Son posibles modificaciones, disposiciones alternativas y variaciones de estos ejemplos ilustrativos, y pueden caer dentro del ámbito de la invención. De acuerdo con ello, las siguientes reivindicaciones han de considerarse en su interpretación más amplia razonable que sea consistente con la memoria aquí expuesta y no esté excesivamente limitada por aspectos de las realizaciones preferidas que aquí se han descrito.

REIVINDICACIONES

1. Un sistema (34) para proporcionar seguridad electrónica para un recurso interno (27) que es capaz de comunicarse a través de una red de comunicaciones externa (22), de tal modo que el sistema comprende:

un servidor (29), que tiene un primer conjunto de accesos o puertas (36) para la comunicación entre la red de comunicaciones externa (22) y el servidor (29), de manera que el servidor (29) tiene un segundo conjunto de puertas (38) para la comunicación entre una red de comunicaciones interna (14) y el servidor (29);

un primer cortafuego (30), en comunicación con el primer conjunto de puertas (36) e interpuesto entre el primer conjunto de puertas (36) y la red de comunicaciones externa (22) con el fin de proporcionar al menos una interconexión entre el primer conjunto de puertas (36) y la red de comunicaciones externa (22); y

un segundo cortafuego (32), en comunicación con el segundo conjunto de puertas (38) e interpuesto entre el servidor (29) y la red de comunicaciones interna (14) con el fin de proporcionar un número entero no negativo de interconexiones entre el segundo conjunto de puertas (38) y la red de comunicaciones interna (14), **caracterizado** porque el número de interconexiones depende de un modo de seguridad.

2. El sistema de acuerdo con la reivindicación 1, en el cual una interconexión es un recorrido o camino de comunicaciones a través de uno de dichos cortafuegos, y en el cual una ausencia de una interconexión consiste en un estado bloqueado en el que se bloquean las comunicaciones de modo que no pasen a través de uno de dichos cortafuegos.

3. El sistema de acuerdo con la reivindicación 1, en el cual el número de interconexiones del primer cortafuego (30) es menor o igual que el número entero no negativo de interconexiones del segundo cortafuego (32) durante un modo de seguridad normal.

4. El sistema de acuerdo con la reivindicación 1, en el cual el número entero no negativo de interconexiones es cero para un modo de seguridad elevada.

5. El sistema de acuerdo con la reivindicación 1, en el cual el primer cortafuego (30) incluye una interconexión primaria para proporcionar soporte al tráfico de Protocolo de Transferencia de Hipertexto, una interconexión secundaria, dedicada al tráfico de Protocolo de Transferencia de Hipertexto cifrado, una interconexión terciara, dedicada al seguimiento de un servidor, y una interconexión cuaternaria, destinada al seguimiento de las operaciones y el mantenimiento del recurso interno (27) afiliado con la red de comunicaciones interna (14).

6. El sistema de acuerdo con la reivindicación 1, en el cual, para el segundo cortafuego (32), el número entero no negativo de interconexiones se establece únicamente por una duración limitada y basándose en un criterio según se necesite, para las comunicaciones entre un recurso interno (27) de una entidad comercial (40) y el de otra entidad comercial (140).

7. El sistema de acuerdo con la reivindicación 1, en el cual la al menos una interconexión del primer cortafuego (30) está asociada con un primer identificador de puerta, de tal modo que el número entero no negativo de interconexiones del segundo cortafuego (32) está asociado con uno o más segundos identificadores de puerta, siendo el primer identificador de puerta diferente de los uno o más segundos identificadores de puerta para cada interconexión activa.

8. El sistema de acuerdo con la reivindicación 5, 6 ó 7, en el cual el primer cortafuego (30) tiene unos accesos o puertas exteriores (15) y el segundo cortafuego (32) tiene unos accesos o puertas interiores (17), de tal manera que las puertas exteriores (15) del primer cortafuego (30) tienen identificadores de puerta diferentes a los de las puertas interiores (17) del segundo cortafuego (32), de modo que una progresión de un mensaje de datos entrante no autorizado que atraviesa una interconexión a través de una de las puertas exteriores (15) del primer cortafuego (30), es bloqueada en las puertas interiores (17) del segundo cortafuego (32).

9. El sistema de acuerdo con la reivindicación 5, 6 ó 7, en el cual el segundo cortafuego (32) bloquea un mensaje de comunicaciones en el que un usuario de la red de comunicaciones externa (22) trata de utilizar un primer identificador de puerta asociado con una interconexión del primer cortafuego (30) para penetrar en el segundo cortafuego (32), que tiene un segundo identificador de puerta, distinto del primer identificador de puerta.

10. El sistema de acuerdo con la reivindicación 7 ó la reivindicación 9, en el cual el segundo cortafuego (32) tiene identificadores de puerta diferentes de los del primer cortafuego (30).

11. El sistema de acuerdo con la reivindicación 10, en el cual el segundo cortafuego (32) bloquea el paso a través de un segundo cortafuego (32) de un mensaje de datos en el que un usuario de la red de comunicaciones externa (22) trata de utilizar un primer identificador de puerta asociado a una interconexión del primer cortafuego (30), con el fin de penetrar en el segundo cortafuego (32), que tiene un segundo identificador de puerta distinto del primer identificador de puerta.

12. El sistema de acuerdo con cualquiera de las reivindicaciones precedentes, en el cual el primer cortafuego (30) y el segundo cortafuego (32) comprenden instrucciones de software o programación para su ejecución por parte del servidor (29).

13. El sistema de acuerdo con cualquiera de las reivindicaciones precedentes, en el cual la red de comunicaciones externa comprende la Internet (22).

14. Un método para proporcionar seguridad electrónica para un recurso interno (27), capaz de comunicarse a través de una red de comunicaciones externa (22), de tal modo que el método comprende:

proporcionar al menos una interconexión en un primer cortafuego (30), entre la red de comunicaciones externa (22) y un primer conjunto de puertas (36) de un servidor (29); y

proporcionar un número entero no negativo de interconexiones en un segundo cortafuego (32), entre un segundo conjunto de puertas (38) del servidor (29) y el recurso interno (27), **caracterizado** porque el número de interconexiones depende de un modo de seguridad.

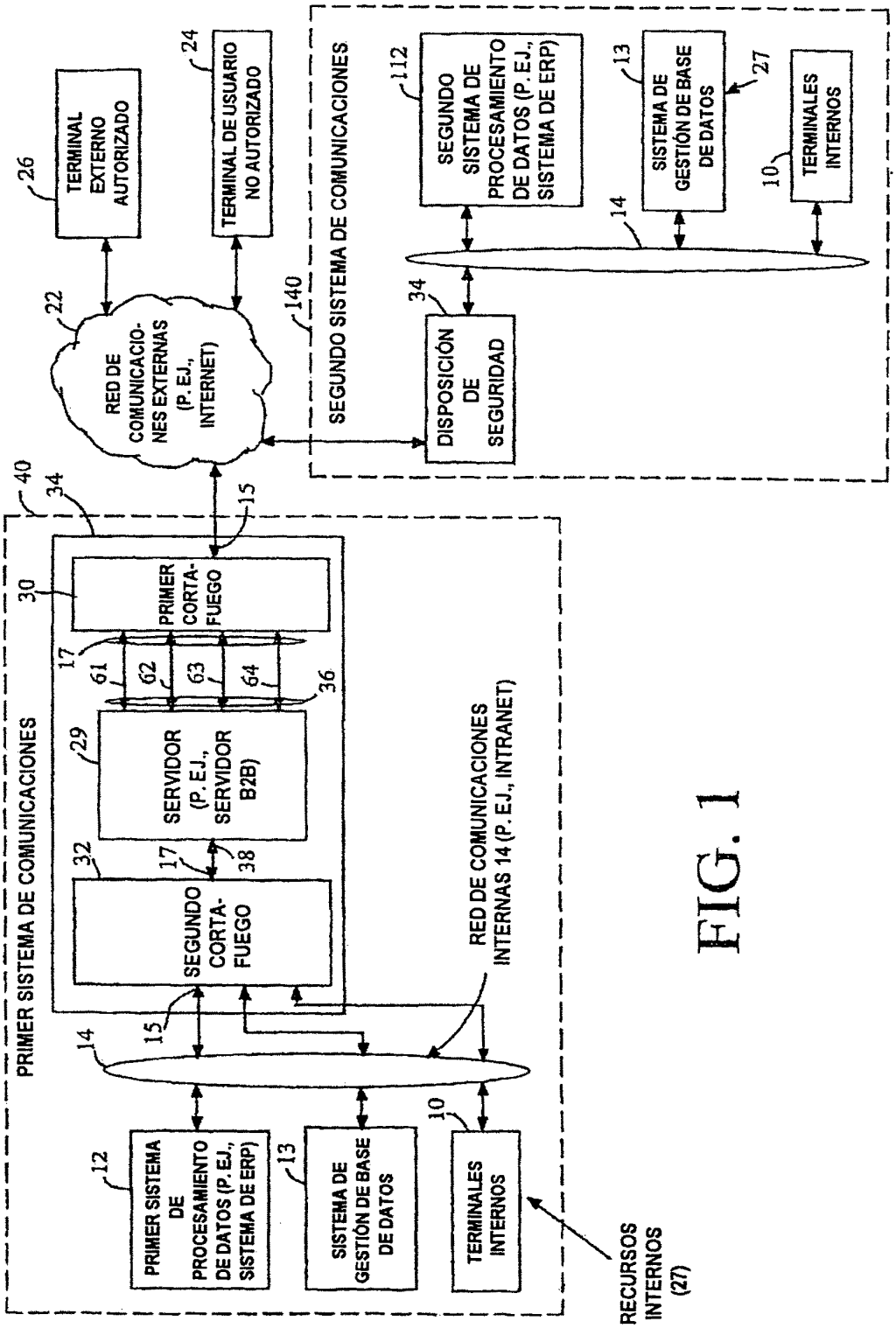

PRIMER SISTEMA DE COMUNICACIONES
40
34
30
PRIMER CORTA-FUEGO
17
61
62
63
64
36
29
SERVIDOR (P. EJ., SERVIDOR B2B)
32
17
38
SEGUNDO CORTA-FUEGO
15
14
RED DE COMUNICACIONES INTERNAS 14 (P. EJ., INTRANET)
12
PRIMER SISTEMA DE PROCESAMIENTO DE DATOS (P. EJ., SISTEMA DE ERP)
13
SISTEMA DE GESTIÓN DE BASE DE DATOS
10
TERMINALES INTERNOS
RECURSOS INTERNOS (27)
15
22
RED DE COMUNICACIO-NES EXTERNAS (P. EJ., INTERNET)
140
SEGUNDO SISTEMA DE COMUNICACIONES
34
DISPOSICIÓN DE SEGURIDAD
14
112
SEGUNDO SISTEMA DE PROCESAMIENTO DE DATOS (P. EJ., SISTEMA DE ERP)
13
SISTEMA DE GESTIÓN DE BASE DE DATOS
27
10
TERMINALES INTERNOS
26
TERMINAL EXTERNO AUTORIZADO
24
TERMINAL DE USUARIO NO AUTORIZADO

FIG. 1

FIG. 2

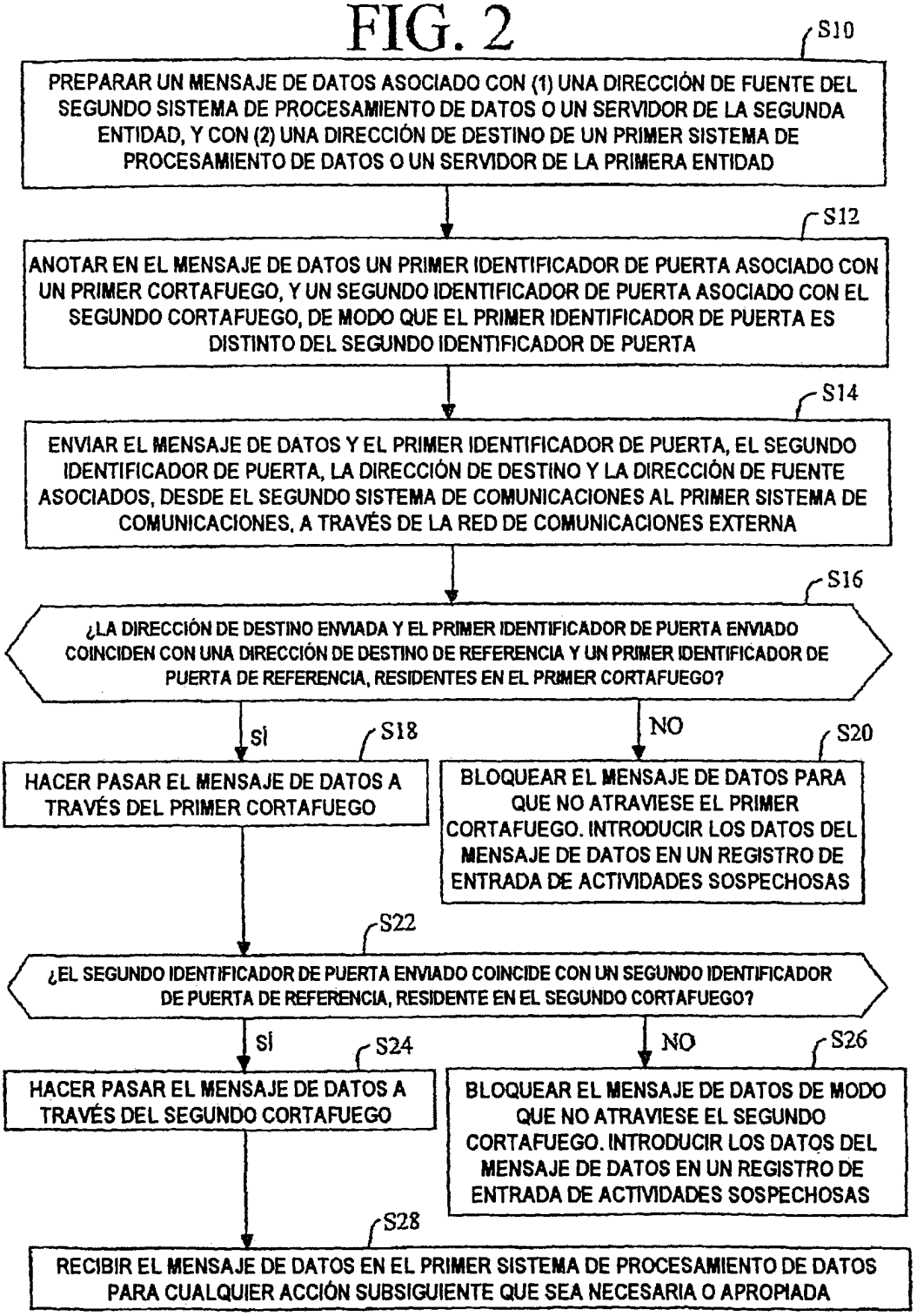
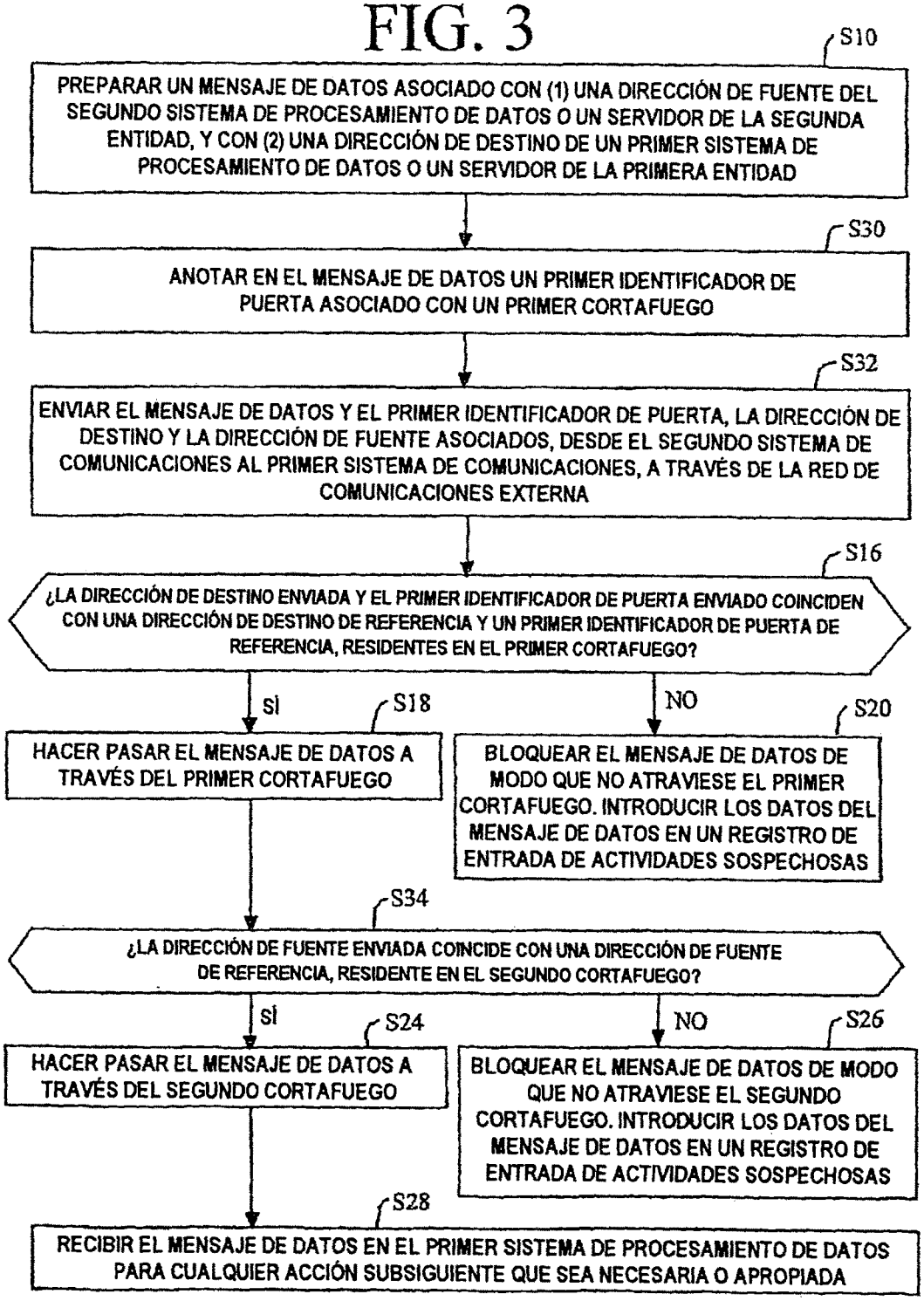

S10
PREPARAR UN MENSAJE DE DATOS ASOCIADO CON (1) UNA DIRECCIÓN DE FUENTE DEL SEGUNDO SISTEMA DE PROCESAMIENTO DE DATOS O UN SERVIDOR DE LA SEGUNDA ENTIDAD, Y CON (2) UNA DIRECCIÓN DE DESTINO DE UN PRIMER SISTEMA DE PROCESAMIENTO DE DATOS O UN SERVIDOR DE LA PRIMERA ENTIDAD
S12
ANOTAR EN EL MENSAJE DE DATOS UN PRIMER IDENTIFICADOR DE PUERTA ASOCIADO CON UN PRIMER CORTAFUEGO, Y UN SEGUNDO IDENTIFICADOR DE PUERTA ASOCIADO CON EL SEGUNDO CORTAFUEGO, DE MODO QUE EL PRIMER IDENTIFICADOR DE PUERTA ES DISTINTO DEL SEGUNDO IDENTIFICADOR DE PUERTA
S14
ENVIAR EL MENSAJE DE DATOS Y EL PRIMER IDENTIFICADOR DE PUERTA, EL SEGUNDO IDENTIFICADOR DE PUERTA, LA DIRECCIÓN DE DESTINO Y LA DIRECCIÓN DE FUENTE ASOCIADOS, DESDE EL SEGUNDO SISTEMA DE COMUNICACIONES AL PRIMER SISTEMA DE COMUNICACIONES, A TRAVÉS DE LA RED DE COMUNICACIONES EXTERNA
S16
¿LA DIRECCIÓN DE DESTINO ENVIADA Y EL PRIMER IDENTIFICADOR DE PUERTA ENVIADO COINCIDEN CON UNA DIRECCIÓN DE DESTINO DE REFERENCIA Y UN PRIMER IDENTIFICADOR DE PUERTA DE REFERENCIA, RESIDENTES EN EL PRIMER CORTAFUEGO?
SÍ
S18
HACER PASAR EL MENSAJE DE DATOS A TRAVÉS DEL PRIMER CORTAFUEGO
NO
S20
BLOQUEAR EL MENSAJE DE DATOS PARA QUE NO ATRAVIESE EL PRIMER CORTAFUEGO. INTRODUCIR LOS DATOS DEL MENSAJE DE DATOS EN UN REGISTRO DE ENTRADA DE ACTIVIDADES SOSPECHOSAS
S22
¿EL SEGUNDO IDENTIFICADOR DE PUERTA ENVIADO COINCIDE CON UN SEGUNDO IDENTIFICADOR DE PUERTA DE REFERENCIA, RESIDENTE EN EL SEGUNDO CORTAFUEGO?
SÍ
S24
HACER PASAR EL MENSAJE DE DATOS A TRAVÉS DEL SEGUNDO CORTAFUEGO
NO
S26
BLOQUEAR EL MENSAJE DE DATOS DE MODO QUE NO ATRAVIESE EL SEGUNDO CORTAFUEGO. INTRODUCIR LOS DATOS DEL MENSAJE DE DATOS EN UN REGISTRO DE ENTRADA DE ACTIVIDADES SOSPECHOSAS
S28
RECIBIR EL MENSAJE DE DATOS EN EL PRIMER SISTEMA DE PROCESAMIENTO DE DATOS PARA CUALQUIER ACCIÓN SUBSIGUIENTE QUE SEA NECESARIA O APROPIADA

FIG. 3


S10
PREPARAR UN MENSAJE DE DATOS ASOCIADO CON (1) UNA DIRECCIÓN DE FUENTE DEL SEGUNDO SISTEMA DE PROCESAMIENTO DE DATOS O UN SERVIDOR DE LA SEGUNDA ENTIDAD, Y CON (2) UNA DIRECCIÓN DE DESTINO DE UN PRIMER SISTEMA DE PROCESAMIENTO DE DATOS O UN SERVIDOR DE LA PRIMERA ENTIDAD
S30
ANOTAR EN EL MENSAJE DE DATOS UN PRIMER IDENTIFICADOR DE PUERTA ASOCIADO CON UN PRIMER CORTAFUEGO
S32
ENVIAR EL MENSAJE DE DATOS Y EL PRIMER IDENTIFICADOR DE PUERTA, LA DIRECCIÓN DE DESTINO Y LA DIRECCIÓN DE FUENTE ASOCIADOS, DESDE EL SEGUNDO SISTEMA DE COMUNICACIONES AL PRIMER SISTEMA DE COMUNICACIONES, A TRAVÉS DE LA RED DE COMUNICACIONES EXTERNA
S16
¿LA DIRECCIÓN DE DESTINO ENVIADA Y EL PRIMER IDENTIFICADOR DE PUERTA ENVIADO COINCIDEN CON UNA DIRECCIÓN DE DESTINO DE REFERENCIA Y UN PRIMER IDENTIFICADOR DE PUERTA DE REFERENCIA, RESIDENTES EN EL PRIMER CORTAFUEGO?
SÍ
S18
HACER PASAR EL MENSAJE DE DATOS A TRAVÉS DEL PRIMER CORTAFUEGO
NO
S20
BLOQUEAR EL MENSAJE DE DATOS DE MODO QUE NO ATRAVIESE EL PRIMER CORTAFUEGO. INTRODUCIR LOS DATOS DEL MENSAJE DE DATOS EN UN REGISTRO DE ENTRADA DE ACTIVIDADES SOSPECHOSAS
S34
¿LA DIRECCIÓN DE FUENTE ENVIADA COINCIDE CON UNA DIRECCIÓN DE FUENTE DE REFERENCIA, RESIDENTE EN EL SEGUNDO CORTAFUEGO?
SÍ
S24
HACER PASAR EL MENSAJE DE DATOS A TRAVÉS DEL SEGUNDO CORTAFUEGO
NO
S26
BLOQUEAR EL MENSAJE DE DATOS DE MODO QUE NO ATRAVIESE EL SEGUNDO CORTAFUEGO. INTRODUCIR LOS DATOS DEL MENSAJE DE DATOS EN UN REGISTRO DE ENTRADA DE ACTIVIDADES SOSPECHOSAS
S28
RECIBIR EL MENSAJE DE DATOS EN EL PRIMER SISTEMA DE PROCESAMIENTO DE DATOS PARA CUALQUIER ACCIÓN SUBSIGUIENTE QUE SEA NECESARIA O APROPIADA

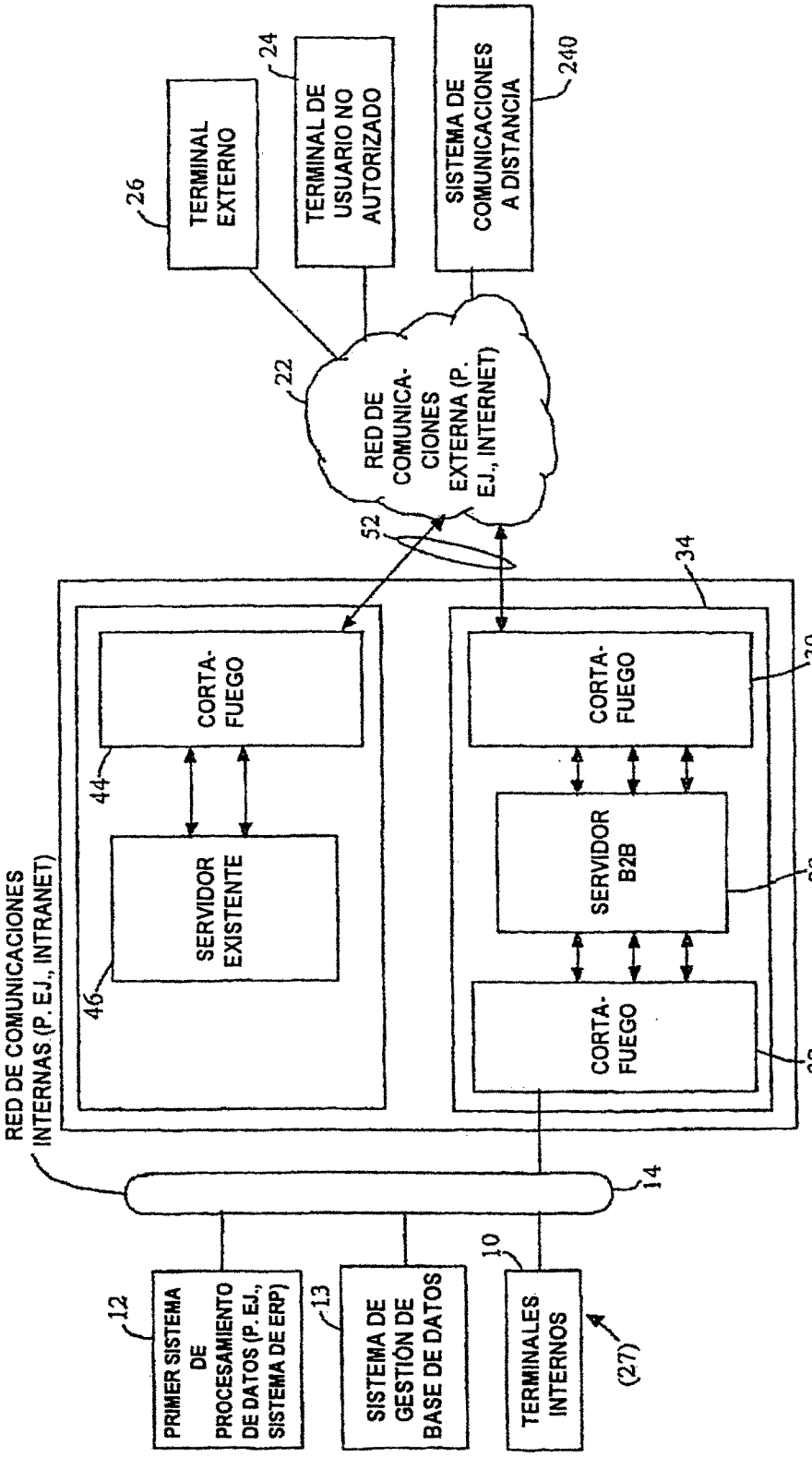

TERMINAL EXTERNO
26
TERMINAL DE USUARIO NO AUTORIZADO
24
SISTEMA DE COMUNICACIONES A DISTANCIA
240
RED DE COMUNICA-CIONES EXTERNA (P. EJ., INTERNET)
22
52
34
CORTA-FUEGO
44
SERVIDOR EXISTENTE
46
CORTA-FUEGO
30
SERVIDOR B2B
29
CORTA-FUEGO
32
RED DE COMUNICACIONES INTERNAS (P. EJ., INTRANET)
14
10
PRIMER SISTEMA DE PROCESAMIENTO DE DATOS (P. EJ., SISTEMA DE ERP)
12
SISTEMA DE GESTIÓN DE BASE DE DATOS
13
TERMINALES INTERNOS
(27)

FIG. 4

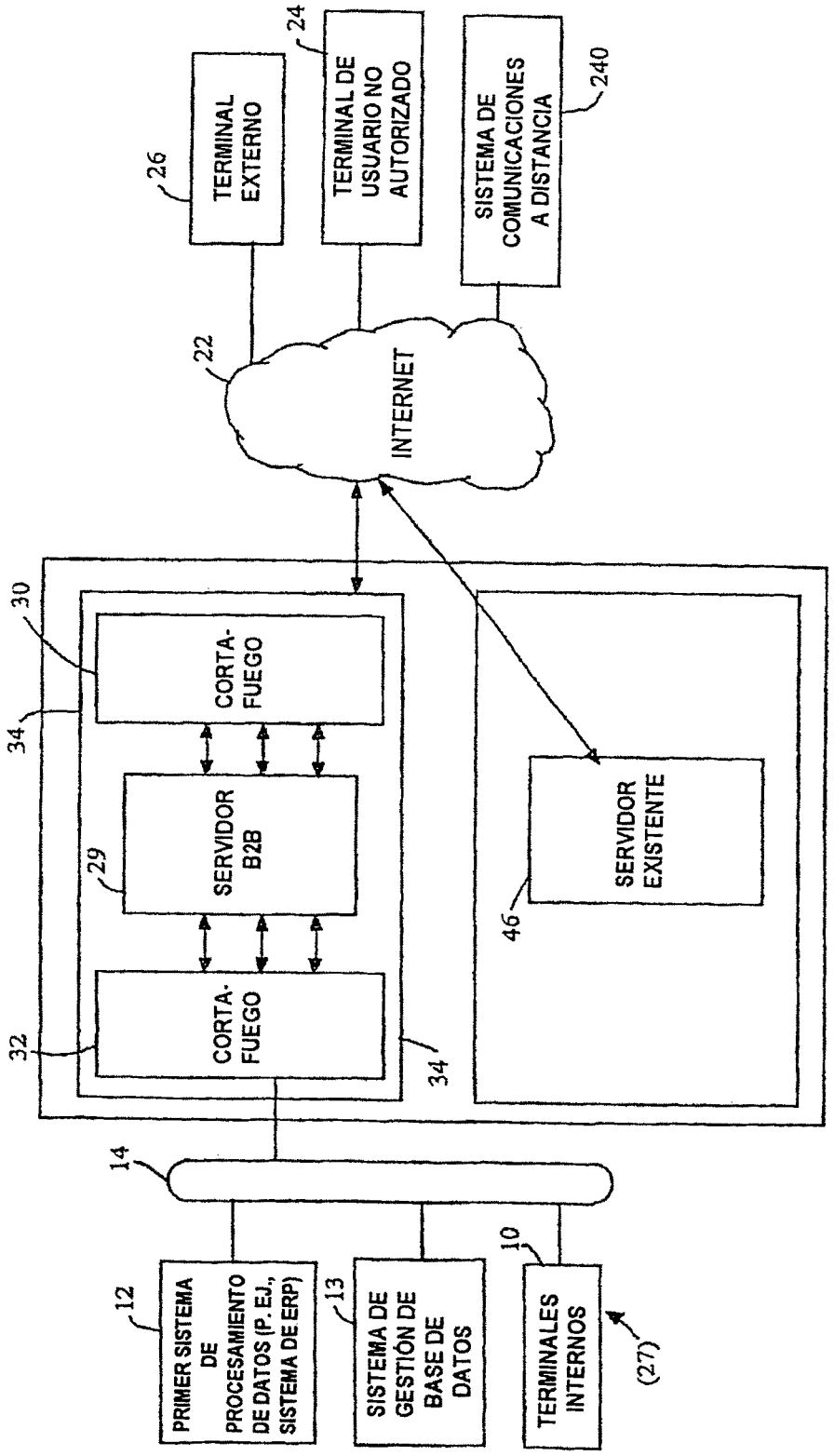

TERMINAL EXTERNO
26
TERMINAL DE USUARIO NO AUTORIZADO
24
SISTEMA DE COMUNICACIONES A DISTANCIA
240
INTERNET
22
30
CORTA-FUEGO
34
SERVIDOR B2B
29
CORTA-FUEGO
32
34
SERVIDOR EXISTENTE
46
14
PRIMER SISTEMA DE PROCESAMIENTO DE DATOS (P. EJ., SISTEMA DE ERP)
12
SISTEMA DE GESTIÓN DE BASE DE DATOS
13
TERMINALES INTERNOS
10
(27)

FIG. 5

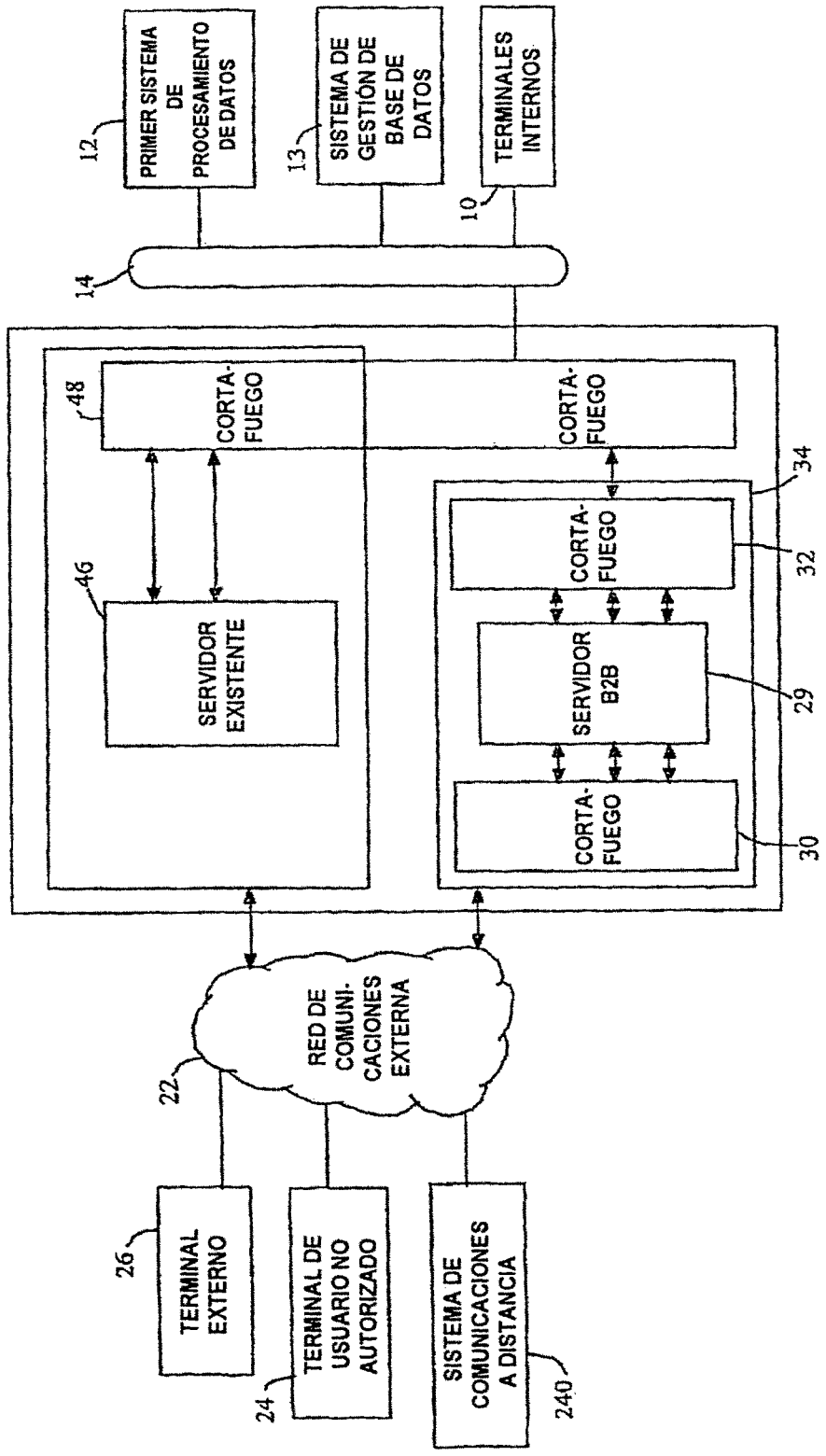

12
PRIMER SISTEMA DE PROCESAMIENTO DE DATOS
13
SISTEMA DE GESTIÓN DE BASE DE DATOS
10
TERMINALES INTERNOS
14
48
CORTA-FUEGO
CORTA-FUEGO
46
SERVIDOR EXISTENTE
34
CORTA-FUEGO
32
SERVIDOR B2B
29
CORTA-FUEGO
30
RED DE COMUNI-CACIONES EXTERNA
22
26
TERMINAL EXTERNO
TERMINAL DE USUARIO NO AUTORIZADO
24
SISTEMA DE COMUNICACIONES A DISTANCIA
240

FIG. 6

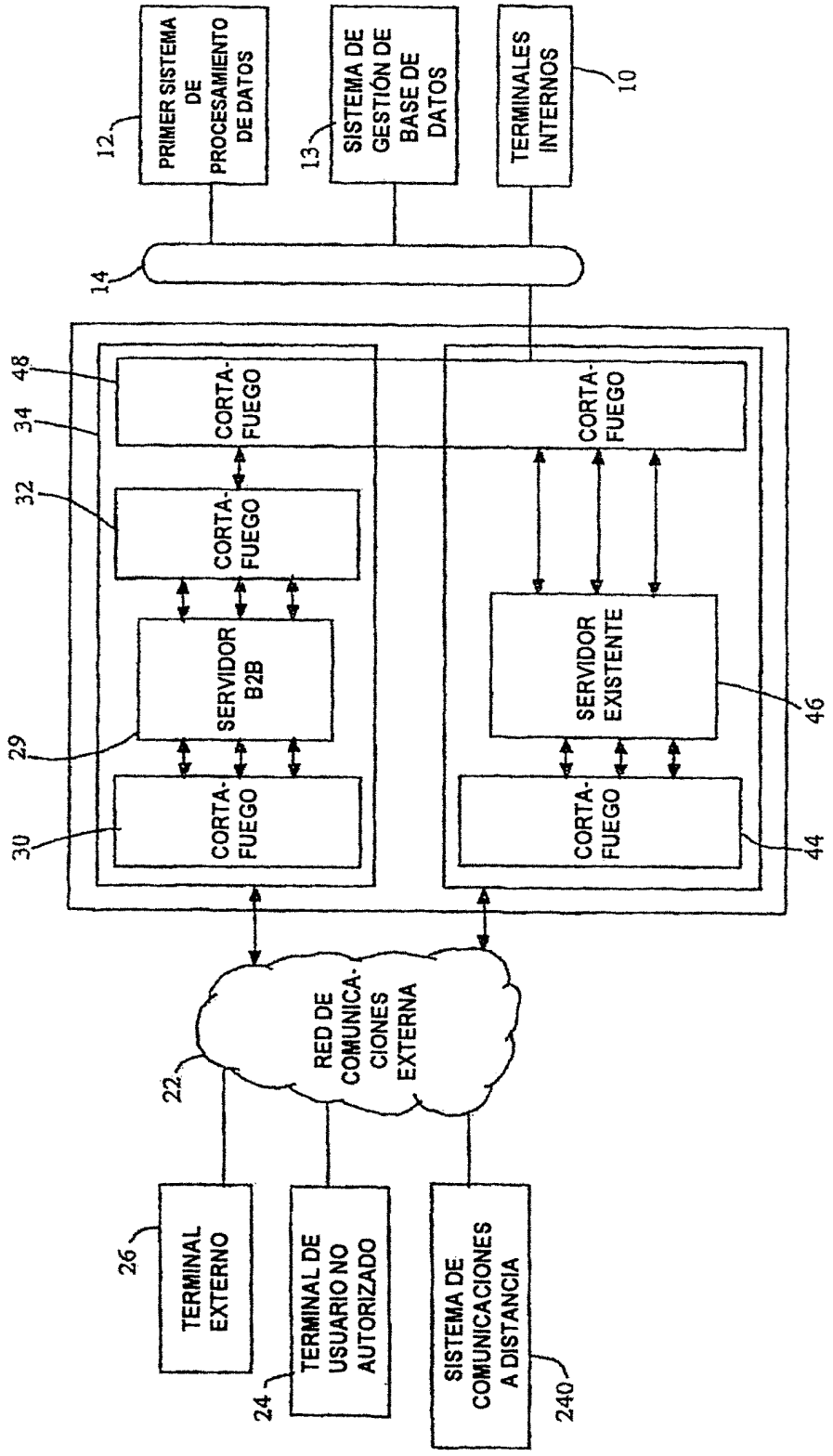

PRIMER SISTEMA DE PROCESAMIENTO DE DATOS
12
SISTEMA DE GESTIÓN DE BASE DE DATOS
13
TERMINALES INTERNOS
10
14
48
34
32
29
30
CORTA-FUEGO
CORTA-FUEGO
CORTA-FUEGO
SERVIDOR B2B
CORTA-FUEGO
CORTA-FUEGO
SERVIDOR EXISTENTE
46
44
RED DE COMUNICA-CIONES EXTERNA
22
TERMINAL EXTERNO
26
TERMINAL DE USUARIO NO AUTORIZADO
24
SISTEMA DE COMUNICACIONES A DISTANCIA
240

FIG. 7