(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 574 003**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/46 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.08.2004 E 04782780 (3)**

(97) Fecha y número de publicación de la concesión europea: **27.04.2016 EP 1678912**

(54) Título: **Procedimiento y aparato para proporcionar seguridad de red utilizando control de acceso basado en roles**

(30) Prioridad:

10.09.2003 US 659614

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.06.2016

(73) Titular/es:

CISCO TECHNOLOGY, INC. (100.0%)
170 WEST TASMAN DRIVE
SAN JOSE, CA 95134-1706, US

(72) Inventor/es:

SMITH, MICHAEL, R.

(74) Agente/Representante:

PONTI SALES, Adelaida

DESCRIPCIÓN

Procedimiento y aparato para proporcionar seguridad de red utilizando control de acceso basado en roles

ANTECEDENTES DE LA INVENCIÓN

Campo de la invención

[0001] Esta invención se refiere al campo de la seguridad de redes de información, y más en particular se refiere a un procedimiento y aparato para asegurar el acceso a una red por parte de un usuario basándose en el rol del usuario.

Descripción de la técnica relacionada

[0002] Las tecnologías de acceso a redes flexibles tales como inalámbricas, el protocolo dinámico de configuración de anfitrión, pasarelas de red privada virtual (VPN) y similares permiten a los usuarios acceder a una red protegida dada desde una diversidad de puntos de acceso o entrada. Esto es cierto para todo tipo de redes, incluyendo las redes empresariales, las redes de proveedores de servicios y similares. Al mismo tiempo, la seguridad brindada mientras se proporciona tal acceso es de una preocupación creciente. Las tecnologías basadas en el servicio de autenticación remota telefónica de usuario (RADIUS), el sistema de control de acceso de controlador de acceso terminal (TACACS), el protocolo DIAMETER y otros protocolos permiten que un usuario sea autenticado en el momento de la entrada en la red.

[0003] Como es sabido, los trayectos de comunicaciones a través de tales redes están separados conceptualmente (por ejemplo, pueden verse como trayectos virtuales separados), aunque pueden pasar por algunos o todos de los mismos dispositivos de red (es decir, segmentos físicos), y por eso son controlados por separado utilizando, por ejemplo, listas de control de acceso (ACL). Convencionalmente, las restricciones sobre el acceso del que disfrutan los usuarios de la red están impuestas por las ACL, que se utilizan para procesar paquetes y controlar así el tráfico de red de tales usuarios. Por escalabilidad y manejabilidad, las ACL convencionales requieren que la correspondencia de una dirección de anfitrión de usuario (como la fuente del (los) paquete(s) dado(s); por ejemplo, una dirección de protocolo Internet (IP)) sea relativamente estática, o que la política de seguridad sea suficientemente laxa para permitir todas las posibles direcciones posibles para el usuario.

[0004] Las ACL de seguridad de hoy en día adolecen de varias debilidades. Estas ACL se aplican convencionalmente a una interfaz dada y contienen direcciones IP que vinculan la política de seguridad directamente a la topología de red. Como resultado, un cambio en la red tal como la redistribución de subredes hace que la política de seguridad tenga que ser revisada. Por otra parte, parecería que las ACL en diversas partes de la red tendrían que ser actualizadas cada vez que un usuario es autenticado en la red, con el fin de añadir reglas asociadas con la dirección IP fuente asignada al anfitrión de este usuario, que serían específicas de ese usuario. Esto causaría un enorme incremento en el número de ACL únicas y aumentaría espectacularmente el ritmo al que tales reglas tendrían que ser actualizadas.

[0005] Dentro de una ACL dada, también existe el problema de incrementos drásticos de tamaño resultantes de la expresión de direcciones IP individuales, donde el número de entradas a menudo es el número de direcciones fuente multiplicado por el número de direcciones de destino, multiplicado por el número de permisos. De este modo, la adición de una sola dirección IP individual puede tener un impacto significativo sobre el tamaño de un número sustancial de ACL.

[0006] Cuando un cliente cambia la topología de red, las ACL deben ser reexaminadas. Puesto que tales ACL pueden alcanzar con bastante facilidad varios cientos o incluso varios miles de líneas de longitud, tal reexamen puede resultar no insignificante, cuando menos. Debido a la complejidad de tal ACL, la confianza en los cambios que se efectúan no es muy alta, típicamente, y las ACL a menudo requieren pruebas extensivas por parte del usuario antes de ser implantadas en un entorno de producción. Por otra parte, como las plataformas que utilizan memorias direccionables según el contenido (CAM) para implantar ACL requieren la recompilación de algunas o todas las ACL cuando se efectúa algún cambio, los incrementos en el coste de procesamiento puede ser bastante graves, aproximándose a una ecuación de segundo grado en el número de usuarios. Estos incrementos de complejidad aumentan la posibilidad de una interrupción de la red, un agujero de seguridad, o ambos. Una sola ACL pone a prueba la capacidad de un usuario de gestionar su política de seguridad. Implantar tales ACL por toda la red empresarial tiene impacto, por lo tanto, sobre la manejabilidad de las redes de hoy en día. Dado lo anterior,

particularmente a la luz del acceso cada vez más flexible que se requiere ahora y que se requerirá en el futuro, es difícil confiar en las soluciones existentes basadas en ACL.

[0007] Lo que se requiere, entonces, es un mecanismo que permita la identificación eficiente del tráfico de red procedente de un anfitrión dado. Preferentemente, tal estrategia debería emplear la tecnología de ACL existente, en tanto que reduciendo o eliminando el problema del crecimiento multiplicativo de ACL que se encuentra actualmente cuando se añaden anfitriones. También preferentemente, tal estrategia debería permitir que la red sea reconfigurada y crecer fácilmente, sin incurrir en una carga administrativa desproporcionada o consumir cantidades excesivamente grandes de recursos de red.

[0008] El documento US2003/0110268 describe un servicio de red privada virtual (VPN) que se proporciona a través de una infraestructura de red compartida que comprende dispositivos de borde del proveedor (PE) interconectados que tienen interfaces de borde del cliente (CE). Algunas de las interfaces de CE están asignadas a una VPN que soporta LAN virtuales. Una correspondencia entre una interfaz de CE y una LAN virtual se aprende basándose en tramas marcadas recibidas en la interfaz de CE y que incluyen un identificador de la LAN virtual. El proceso de aprendizaje permite la detección de pares de interfaces de CE que corresponden a una LAN virtual común. Tras la detección, se establece una detección virtual en la infraestructura de red compartida entre los dispositivos de PE que tienen estas interfaces de CE, y posteriormente se utiliza para reenviar tramas que incluyen el identificador de la VLAN virtual.

[0009] Aspectos y ejemplos de la invención se exponen en las reivindicaciones.

[0010] Se desvela un dispositivo de red. El dispositivo de red incluye una lista de control de acceso. La lista de control de acceso incluye una entrada de lista de control de acceso, la cual, a su vez, incluye un campo de grupo de usuarios. En otra realización, el dispositivo de red incluye una tabla de reenvío. La tabla de reenvío incluye una pluralidad de entradas de tabla de reenvío. En tal realización, al menos una de las entradas de tabla de reenvío incluye un campo de grupo de usuarios.

[0011] En una realización, una lista de control de acceso es poblada con un identificador de grupo de usuarios de destino. El identificador de grupo de usuarios de destino identifica un grupo de usuarios de destino de un destino. En otra realización, se desvela un procedimiento en el cual una tabla de reenvío es poblada con un identificador de grupo de usuarios.

[0012] Lo precedente es un resumen y por lo tanto contiene, por necesidad, simplificaciones, generalizaciones y omisiones de detalle; en consecuencia, los expertos en la materia apreciarán que el resumen es sólo ilustrativo y no pretende ser limitativo de ningún modo. Otros aspectos, características inventivas y ventajas de la presente invención, tal como se define únicamente por las reivindicaciones, resultarán evidentes en la descripción detallada no limitativa expuesta más adelante.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0013] La presente invención puede comprenderse mejor, y numerosos objetos, características y ventajas hacerse evidentes para los expertos en la materia por referencia a los dibujos adjuntos.

La fig. 1A es un diagrama que ilustra un grupo jerárquico de usuarios según realizaciones de la presente invención.
La fig. 1B es un diagrama que ilustra un conjunto disjunto de grupos de usuarios según realizaciones de la presente invención.
La fig. 2 es un diagrama de bloques que ilustra una arquitectura para autenticación de usuario.
La fig. 3 es un diagrama de bloques que ilustra una tabla de reenvío según realizaciones de la presente invención.
La fig. 4 es un diagrama que ilustra un procedimiento de determinación de permisos aplicables para un paquete.
La fig. 5 es un diagrama de bloques que ilustra una matriz de permisos según realizaciones de la presente invención.
La fig. 6A es un diagrama de bloques que ilustra un ejemplo de encadenamiento de la matriz de permisos según realizaciones de la presente invención.
La fig. 6B es un diagrama de bloques que ilustra otro ejemplo de encadenamiento de la matriz de permisos según realizaciones de la presente invención.
La fig. 6C es un diagrama de bloques que ilustra una vista lógica de los ejemplos de encadenamiento de la matriz de permisos representados en las figs. 6A y 6B según realizaciones de la presente invención.
La fig. 7 es un diagrama de bloques que ilustra un ejemplo de una lista de control de acceso (ACL) según

realizaciones de la presente invención.
La fig. 8A es un diagrama de bloques que ilustra un ejemplo de subred del lado del anfitrión según realizaciones de la presente invención.
La fig. 8B es un diagrama de flujo que ilustra un ejemplo del funcionamiento de la subred del lado del anfitrión mostrada en la fig. 8A, de una manera según realizaciones de la presente invención.
La fig. 9A es un diagrama de bloques que ilustra un ejemplo de una subred del lado del servidor según realizaciones de la presente invención.
La fig. 9B es un diagrama de flujo que ilustra un ejemplo del funcionamiento de la subred del lado del servidor mostrada en la fig. 9A, de una manera según realizaciones de la presente invención.
La fig. 10 es un diagrama de bloques que ilustra un ejemplo de una arquitectura de red que incluye un anfitrión y un servidor, según realizaciones de la presente invención.
La fig. 11 es un diagrama de flujo que ilustra un ejemplo de un recorrido de paquetes a través de la arquitectura de red mostrada en la fig. 10 y el procesamiento realizado sobre los mismos según realizaciones de la presente invención.
La fig. 12 es un diagrama de flujo que ilustra un ejemplo del procesamiento realizado sobre un paquete sometido a procesamiento de control de acceso basado en roles (RBAC) según realizaciones de la presente invención, donde el paquete es primer paquete recibido de tales paquetes.
La fig. 13 es un diagrama de flujo que ilustra un ejemplo del procesamiento realizado sobre un paquete recibido posteriormente sometido a procesamiento de control de acceso basado en roles (RBAC) según realizaciones de la presente invención.
La fig. 14 es un diagrama de flujo que ilustra un ejemplo del procesamiento de un paquete a medida que el paquete circula a través de trayecto de datos de un dispositivo de red según realizaciones de la presente invención.

[0014] El uso de los mismos símbolos de referencia en diferentes dibujos indica elementos similares o idénticos.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

[0015] Lo siguiente pretende proporcionar una descripción detallada de un ejemplo de la invención y no debería considerarse como limitativo de la propia invención. Más bien, cualquier número de variaciones puede entrar dentro del alcance de la invención, el cual está definido en las reivindicaciones a continuación de la descripción.

Introducción

[0016] La presente invención proporciona un procedimiento y aparato que aborda las limitaciones resumidas anteriormente mediante el uso de listas de control de acceso basado en roles (RBACL), que están diseñadas para abordar directamente tales problemas. El acceso a la red permitido a un usuario (por ejemplo, una persona que tiene un identificador de usuario, un servidor, un teléfono de protocolo Internet (IP), y otros de tales dispositivos de red) está basado convencionalmente en el (los) grupo(s) al cual (los cuales) pertenece el usuario, el (los) rol(es) asignado(s) al usuario por la empresa, el (los) privilegio(s) que tiene el usuario como cliente ISP o criterios similares. Se apreciará que tal usuario puede, de hecho, ser una persona que tenga un identificador de usuario, un dispositivo de red, un dispositivo de telecomunicaciones o algún otro dispositivo o entidad identificable con una necesidad de acceso a una red de comunicaciones. Las RBACL controlan el tráfico de red imponiendo los permisos que han de aplicarse a ese tráfico de red, basándose en el (los) rol(es) del usuario que genera el tráfico de red.

[0017] Un procedimiento y aparato según la presente invención representan los roles del usuario utilizando grupos. A un usuario se le confiere la pertenencia a uno o más grupos basándose en los roles de ese usuario. Cada grupo puede representar uno o más roles. A su vez, se aplican listas de permisos al decidir si permitir la comunicación entre grupos. El grupo de un usuario, por ejemplo, cuando la entidad de red (por ejemplo, un usuario) es autenticado (por ejemplo, como parte de la autenticación de usuario por medio del protocolo 802.1X, u otro de tales mecanismos). Así, cuando la entidad se autentifica, la entidad es ubicada dentro de un “grupo de usuario” (UG). La autenticación puede estar basada en la identificación del usuario, la función del servidor en la red, u otra de tales características.

[0018] Esta información puede utilizarse entonces para efectuar una determinación en cuanto al tratamiento de un paquete originado por la entidad. Por ejemplo, cuando un paquete es originado sobre la red, la información respecto al grupo fuente se inserta dentro del paquete. La comunicación de esta información (también denominada indicador en este documento) puede implementarse de varias maneras. Por ejemplo, la información puede implementarse como un indicador de grupo fuente (un indicador que indica el grupo al cual pertenece la fuente), aunque pueden emplearse otros procedimientos.

[0019] A medida que el paquete recorre la red, la información del grupo fuente es transportada junto con otra información en el paquete. En el borde de egreso de la red, puede obtenerse el grupo de destino. Por ejemplo, en el borde “L3” (el dispositivo de red en el borde de la red de capa 3), el grupo de destino puede obtenerse de la base de información de reenvío (FIB) del dispositivo de red por medio del prefijo de anfitrión totalmente resuelto. El prefijo de anfitrión se resuelve mediante el protocolo de resolución de direcciones (ARP). La respuesta del ARP es marcada con el grupo de destino cuando el paquete es originado sobre la red. El resultado de la FIB es poblado con el grupo de destino además de la información de reescritura. Una vez que se han determinado los grupos fuente y de destino, pueden aplicarse los permisos (ACL) utilizando esta información.

[0020] Las ventajas clave de la presente invención incluyen la reducción multiplicativa del tamaño de las ACL, el incremento multiplicativo en el rendimiento de las ACL por software, el desacoplamiento de la topología de la red y las políticas de seguridad (u otras características) (que permiten a la ACL seguir al usuario a medida que el usuario se desplaza por la empresa), y una gestión de red simplificada.

La implementación de roles en una arquitectura de autenticación

[0021] La fig. 1A es un diagrama que ilustra un grupo jerárquico de usuarios según realizaciones de la presente invención. Los grupos jerárquicos de usuarios (UG) son similares a las jerarquías de clases encontradas en la programación orientada a objetos. Cada grupo vástago hereda los permisos de su grupo progenitor y amplía esos permisos con los suyos. Se representa una jerarquía de grupos de usuarios 100 que incluye varios grupos de usuarios, cada uno de los cuales tiene dependencias sobre otros grupos de usuarios. La jerarquía de grupos de usuarios 100 incluye un grupo de todos los usuarios 110, un grupo de empleados 120, un grupo de consultores 130, un grupo de directores 140 y un grupo de ejecutivos 150. Como puede verse en la fig. 1A, estos grupos están relacionados jerárquicamente entre sí, con el grupo de ejecutivos 150 siendo un subconjunto del grupo de directores 140, el grupo de directores 140 siendo subconjunto del grupo de empleados 120, y el grupo de empleados 120 y el grupo de consultores 130 siendo subconjuntos del grupo de todos los usuarios 110. De esta manera, el acceso a diversos recursos puede limitarse basándose en el (los) grupo(s) al cual (los cuales) pertenece el usuario. Por ejemplo, un usuario puede pertenecer al grupo de directores 140. Típicamente, un usuario del grupo de directores 140 tendrá acceso a más recursos informáticos y de información de la organización que lo tendrá un usuario del grupo de empleados 120, y menos de tal acceso que un usuario del grupo de ejecutivos 150. Como resultará evidente, cuanto más se recorra hacia abajo en la jerarquía de grupos de usuarios 100, mayor es el nivel de responsabilidad, y por eso, mayor es la cantidad de acceso.

[0022] La fig. 1B es un diagrama que ilustra un conjunto disjunto de grupos de usuarios según realizaciones de la presente invención. Los grupos de usuarios disjuntos se utilizan donde existen funciones no superpuestas, iguales y no relacionadas. En la implementación real de RBACL, los UG jerárquicos pueden implementarse utilizando UG disjuntos y la gestión de jerarquía (de haberla) puede hacerse la responsabilidad de la entidad de gestión de red responsable de configurar las RBACL. Estos grupos incluyen un grupo de ingeniería 160, un grupo de ventas 170 y un grupo de marketing 180. Tales grupos de usuarios disjuntos se utilizan donde existen funciones no superpuestas, iguales y no relacionadas realizadas por los grupos en cuestión. Como las responsabilidades de cada uno de estos grupos son tan diferentes y distintas de las de los otros grupos, se esperaría que cada uno de estos grupos tuviera su propio conjunto de recursos, accesible por los miembros del grupo dado. Así, se esperaría que los usuarios de un grupo dado mantendrían el mismo conjunto de permisos, permitiéndoles acceder al mismo conjunto de recursos, aunque esto no tiene que ser estrictamente el caso.

[0023] Se apreciará que los grupos de usuarios se meten en el mismo grupo porque comparten los mismos permisos. Esta creación de grupos no implica que no se produzcan comunicaciones entre o a través de grupos de usuarios. Ni esto implica que no existe imposición de permisos dentro de un grupo dado. Simplemente implica que como grupo, los usuarios tendrán los mismos privilegios dentro de la red.

[0024] Cabe destacar que la implementación de control de acceso basado en roles presenta problemas especiales en un entorno de red. Debido a la naturaleza bidireccional de las comunicaciones de red, el control de acceso tiene que aplicarse tanto entre el usuario (anfitrión) y el objeto (servidor), como entre el objeto (servidor) y el usuario (anfitrión). Esto requiere que los usuarios estén agrupados entre sí dentro de un rol y, igualmente, los objetos también estén agrupados entre sí en un rol. En este punto, el control de acceso se aplica estrictamente entre los grupos. Con tal desacoplamiento, los dispositivos de red son libres de desplazarse a través de la red, y cambiar las direcciones IP. Todas las topologías de red pueden cambiar sin perturbar las políticas de seguridad implementadas por las RBACL existentes. Siempre que los roles y los permisos sigan siendo los mismos, tales cambios pueden

producirse sin afectar a la política de seguridad implantada. Desde el punto de vista de cualquier paquete dado, el paquete simplemente es originado desde un grupo, destinado para otro grupo, donde los dos grupos pueden o pueden no ser diferentes. La cuestión respondida mediante el uso de RBACL es si, basándose en el grupo fuente y de destino, es admisible el transporte del paquete.

[0025] La implementación de RBACL incluye típicamente varias operaciones. Estas operaciones incluyen

1. La determinación del grupo de usuarios fuente (SUG; o usuario)
2. La determinación del grupo de usuarios de destino (DUG; u objeto)
3. La determinación de permisos
4. La imposición de permisos

[0026] La fig. 2 es un diagrama de bloques que ilustra una arquitectura para autenticación de usuario. La determinación de SUG puede efectuarse, por ejemplo, cuando el usuario es autentificado en la red. Los siguientes ejemplos pueden utilizar, por ejemplo, el protocolo de servidor de autenticación remota telefónica de usuario (RADIUS), que proporciona autenticación, autorización y contabilidad centralizadas para diversos tipos de acceso. La autenticación de usuario es iniciada por un usuario, quien intenta iniciar sesión en un anfitrión 200. El usuario (no mostrado) hace que el anfitrión 200 actúe como suplicante, y por tanto, envíe un mensaje de inicio a un servidor 210 (también denominado autenticador). El servidor 210 responde al anfitrión 200 con un mensaje de petición/identificación, al cual el anfitrión 200 responde con un mensaje de respuesta/identidad, basándose en la respuesta del usuario. Este mensaje de respuesta/identidad puede ser, por ejemplo, la típica combinación de nombre de usuario y contraseña. El servidor 210 pasa esta información a un servidor de autenticación 220.

[0027] El servidor de autenticación 220 responde con una puesta a prueba de acceso. Se observará que se produce una diversidad de intercambios entre el servidor 210 y el servidor de autenticación 220 durante la autenticación, y que estos se supone que son meramente ejemplares. Tales intercambios variarán, dependiendo del protocolo de autenticación empleado. Una vez que el intercambio de puesta a prueba de acceso se ha completado, el servidor 210 interactúa con el anfitrión 200 reenviando la puesta a prueba desde el servidor de autenticación 220 al anfitrión 200. El anfitrión 200, en este ejemplo, responde con una contraseña de un solo uso (OTP), que el servidor 210 reenvía al servidor de autenticación 220. Suponiendo que la contraseña es aceptada por el servidor de autenticación 220, el servidor de autenticación 220 responde con un mensaje de aceptación de acceso que hace que el servidor 210 autorice una dirección de red para el anfitrión 200.

[0028] Las realizaciones de la presente invención confían en este procedimiento de autenticación para permitir la diseminación de información de grupo de usuarios. La presente invención puede emplear un procedimiento de autenticación tal que presentado en relación con la fig. 2 proporcione la capacidad de transportar la pertenencia de grupo del usuario desde el servidor de autenticación 220 a un dispositivo de acceso a red de ingreso. En el protocolo RADIUS, un atributo específico del proveedor que contiene el grupo de usuarios que ha de pasarse al servidor 210 (y, en última instancia, al conmutador de ingreso) usa la respuesta de aceptación de acceso RADIUS. Así, la determinación del grupo de usuarios fuente se efectúa cuando el usuario es autenticado en la red. Alternativamente, si el sistema operativo del anfitrión es de confianza, el grupo de usuarios puede proceder del propio anfitrión. Si tal es el caso, cada aplicación puede marcar un paquete dado de manera diferente, basándose en la aplicación que origina el paquete.

[0029] Se observará que, en la especificación IEEE 802.1X original, todo el puerto es autenticado cuando se efectúa una sola autenticación válida en el puerto. Después de ello, cualquier anfitrión unido a ese puerto se considera autenticado. De la misma manera, el procedimiento más simple de obtención del indicador de grupo fuente (SGT) es marcar todo el puerto como autentificado en el momento de la primera autenticación válida. El identificador de grupo proporcionado por la autenticación inicial entonces se utiliza e instala en el puerto de ingreso.

[0030] La fig. 3 es un diagrama de bloques que ilustra una tabla de reenvío 300 según la presente invención. La tabla de reenvío 300 incluye varias entradas de tabla de reenvío (representadas en la fig. 3 como las entradas de tabla de reenvío 310(1)-(N)). Cada una de las entradas de tabla de reenvío 310(1)-(N) incluye varios campos, de los cuales se representan ciertos en la fig. 3. Entre estos campos están un campo de dirección MAC (representado como los campos de dirección MAC 320(1)-(N)), un campo de identificador de red de área local virtual (VLAN) (representado como los campos de identificador VLAN 330(1)-(N)), un campo de identificador de puerto (representado como los campos de identificador de puerto 340(1)-(N)), y un campo de identificador de grupo de usuarios (indicador) (representado como los campos de identificador de grupo de usuarios 350(1)-(N)).

[0031] Cuando la dirección del control de acceso a los medios (MAC) y la VLAN han sido autentificadas en un puerto dado, el grupo de usuarios recuperado mediante la autenticación RADIUS es asignado a la combinación de dirección MAC/identificador VLAN. Esta información aparece en la tabla de reenvío 300 en los campos de dirección MAC 320(1)-(N) y los campos de identificador VLAN 330(1)-(N). La tabla de reenvío 300 contiene así las combinaciones de dirección MAC/identificador VLAN que pueden utilizarse como clave de búsqueda con el resultado de la búsqueda que proporciona el identificador de puerto (tal como está almacenado en el campo apropiado de los campos de identificador de puerto 340(1)-(N)) y el identificador de grupo de usuarios (tal como está almacenado en un campo correspondiente de los campos de identificador de grupo de usuarios (350(1)-(N)). La entrada particular de las entradas de tabla de reenvío 310(1)-(N) es preferentemente estática en el conmutador de ingreso, y en tal caso, la eliminación debería ser activada por el protocolo de autenticación empleado, y no los criterios de antigüedad que se emplean típicamente con las entradas de tabla de reenvío.

[0032] Se observará que, en una implementación, cuando un paquete es enviado por un anfitrión tal como el anfitrión 200, la búsqueda de aprendizaje de capa 2 (proporcionada como parte de la función de aparejo en el conmutador de red que mantiene la tabla de reenvío 300) también obtiene el identificador de grupo de usuarios para el paquete buscando el contenido del paquete en la tabla de reenvío. Alternativamente, la búsqueda de aprendizaje de capa 2 del conmutador puede estar diseñada para extraer el identificador de grupo de usuarios del propio paquete. Este identificador de grupo de usuarios se utiliza para marcar el paquete para su identificación como que ha sido generado por un usuario del grupo de usuarios dado. Tal indicador se denomina en este documento el indicador de grupo fuente (SGT). Este STG se inserta dentro del paquete para su uso en el procesamiento subsiguiente del paquete. Por ejemplo, el SGT puede ser insertado dentro del encabezamiento de la capa 2, haciendo que tal información esté disponible para encaminadores de capa 3, así como conmutadores de capa 2.

[0033] Se observará que el identificador de variable “N” se utiliza en varios ejemplos en las figuras descritas en este documento para designar de manera más simple el elemento final de una serie de elementos relacionados o similares. El uso repetido de tales identificadores de variable no significa que implica necesariamente una correlación entre los tamaños de tales series de elementos, aunque tal correlación puede existir. El uso de tales identificadores de variable no requiere que cada serie de elementos tenga el mismo número de elementos que otra serie delimitada por el mismo identificador de variable. En cambio, en cada ejemplo de uso, la variable identificada por “N” (o cualquier otro de tales identificadores) puede contener el mismo valor o un valor diferente de otros ejemplos del mismo identificador de variable.

[0034] Por otra parte, respecto a las señales descritas en este documento, los expertos en la materia reconocerán que una señal puede ser transmitida directamente desde un primer bloque hasta un segundo bloque, o una señal puede ser modificada (por ejemplo, amplificada, atenuada, retardada, enclavada, almacenada en memoria intermedia, invertida, filtrada o modificada de otro modo) entre los bloques. Aunque las señales de la realización descrita anteriormente están caracterizadas como transmitidas desde un bloque hasta el siguiente, otras realizaciones de la presente invención pueden incluir señales modificadas en lugar de tales señales transmitidas directamente siempre que el aspecto de información y/o funcional de la señal sea transmitido entre bloques. Hasta cierto punto, una entrada de señal en un segundo bloque puede ser conceptualizada como una segunda señal obtenida de una primera señal producida como salida de un primer bloque debido a las limitaciones físicas de los circuitos implicados (por ejemplo, inevitablemente existirá algo de atenuación y retardo). Por lo tanto, tal como se utiliza en este documento, una segunda señal obtenida de una primera señal incluye la primera señal o cualquier modificación en la primera señal, ya sea debido a las limitaciones del circuito o debido al paso a través de otros elementos del circuito que no cambian el aspecto de información y/o funcional final de la primera señal.

[0035] Antes de que pueda aplicarse la RBACL apropiada, también se efectúa una determinación en cuanto al grupo de usuarios de destino. Aunque pueden utilizarse varios mecanismos para efectuar tal determinación, ahora se analizan dos maneras de determinar el DUG del objeto (servidor). Tal como se apreciará, cada una tiene sus propias ventajas en ciertos escenarios.

[0036] El primer mecanismo para determinar el DUG emplea información en la base de información de reenvío (FIB) proporcionada durante la resolución de dirección por el protocolo de resolución de direcciones (ARP) (es decir, la IP FIB). Para la mayoría de los casos que implican tráfico de red utilizando IP, el grupo de usuarios de destino puede obtenerse de la FIB. En el borde de la capa 3 (L3) de la red de egreso de la red, la FIB estará poblada con el prefijo de red resuelto después de realizarse la resolución del ARP. Puesto que la respuesta del ARP es el activador para la actualización de entrada de FIB y tiene que ser recibida antes de que circule cualquier tráfico al anfitrión, la respuesta del ARP se utiliza como el activador para insertar el grupo de usuarios de destino dentro de la entrada de la FIB.

[0037] El procedimiento exacto de obtención del grupo de usuarios de destino depende de la plataforma y la conectividad de red al anfitrión. Lo siguiente son los tres escenarios posibles diferentes para obtener el grupo de usuarios de destino.

[0038] En el primer escenario, el anfitrión es autentificado directamente con el encaminador. En este caso, el anfitrión está conectado directamente a un encaminador tradicional (uno sin conmutación de capa 2 (L2) de red). Cuando se recibe la respuesta del ARP, se interrogará a la base de datos de autenticación local para recuperar el grupo de usuarios correspondiente para la dirección IP de destino. Si no se encuentra ninguna entrada en la base de datos de autenticación local, se asignará un grupo de usuarios de destino por defecto.

[0039] En el segundo escenario, el anfitrión es autentificado directamente con el conmutador de capa 2 (L2) de red conectado directamente. Cuando el anfitrión es autentificado con el conmutador de L2 conectado directamente, el encaminador puede estar a múltiples saltos dentro de la capa 2 de red. Cuando la respuesta del ARP es recibida por el conmutador de borde conectado directamente al anfitrión, el paquete es marcado con el SGT mediante uno de los mecanismos descritos previamente. Cuando la respuesta del ARP es recibida por el encaminador que activó la petición del ARP, el grupo de usuarios de destino se tomará del propio paquete.

[0040] En el tercer escenario, el anfitrión es autentificado directamente con el conmutador de capa 3 (L3) de red. En este caso, el anfitrión está conectado directamente al conmutador de L3 que proporciona la autenticación y la interfaz de L3 de borde para el anfitrión. Se observará que el término “conmutador de L3” se refiere a un encaminador con la funcionalidad adicional de un conmutador de L2. Cuando llega la respuesta del ARP procedente del anfitrión, el paquete es marcado con el SGT procedente de la capa de control de acceso a los medios (MAC), la búsqueda de aprendizaje de VLAN en la tabla de L2. De esta manera, el conmutador de L3 puede ver este caso como el mismo que el escenario previo.

[0041] Alternativamente, el grupo de usuarios de destino puede determinarse por medio de una ACL de ingreso estático. Tal como se apreciará, cuando se conecta una red habilitada para RBACL a una red no habilitada para RBACL, la infraestructura de autenticación no estará presente en la red no habilitada para RBACL. De manera similar a la asignación del grupo de usuarios fuente descrita previamente, el grupo de usuarios de destino tiene que clasificarse por medio del mismo mecanismo en tales situaciones. Utilizando la ACL de ingreso para proporcionar la clasificación del grupo de usuarios de destino, las direcciones IP/subredes de destino pueden indicar el grupo de usuarios de destino para determinar la RBACL correcta que se ha de aplicar. Se observará que también puede utilizarse la ACL de egreso, siempre que la determinación de DUG se produzca antes de la imposición de RBACL. Se apreciará que, no infrecuentemente, es mejor comprobar utilizando una ACL de egreso.

[0042] La fig. 4 es un diagrama que ilustra un procedimiento de determinación de permisos aplicables para un paquete dado, utilizando las operaciones analizadas anteriormente. El grupo de usuarios fuente del paquete (representado en la fig. 4 como un grupo de usuarios fuente (SUG) 400) y el grupo de usuarios de destino (representado como un grupo de usuarios de destino (DUG) 410) se toman como entradas a un procedimiento de determinación de permisos (representado como una determinación de permisos 420). Así, el SUG y el DUG son así entradas al procedimiento de determinación de qué permisos aplicar, tal como se ha descrito. La determinación de permisos 420 empleará típicamente una lista de permisos. La determinación de la lista de permisos se realiza mediante la utilización de una matriz de control de acceso que es, en ciertas realizaciones, una matriz indexada por los grupos fuente y de destino con el fin de proporcionar una lista de permisos permitidos. En el caso aquí planteado, el grupo de usuarios fuente y el grupo de usuarios de destino se emplean para efectuar esta determinación. Los resultados de la determinación de permisos 420 son comprobados luego en una comprobación de RBACL 430. Así, el SUG y el DUG se utilizan para determinar la RBACL (lista de permisos) que se aplica.

Un ejemplo de una arquitectura de permisos basada en software

[0043] La fig. 5 es un diagrama de bloques que ilustra una matriz de permisos 500 y una lista de permisos 510, según la presente invención. Cada una de las entradas en la matriz de permisos 500 (representadas como entradas de la matriz de permisos 520(1,1)-(N,N)) apunta a una de las entradas en la lista de permisos 510 (representadas como entradas de la lista de permisos 530 (1)-(N)). Cada una de las entradas de la matriz de permisos (PME) 520(1,1)-(N,N) es indexada por uno de un número de identificadores de grupo de usuarios fuente 540(1)-(N) y uno de un número de identificadores de grupo de usuarios de destino 550(1)-(N). Como resultará evidente, cada uno de los identificadores de grupo de usuarios fuente 540(1)-(N) corresponde a una fila en la matriz de permisos 500, mientras que cada uno de los identificadores de grupo de usuarios de destino 550(1)-(N) corresponde a una

columna en la matriz de permisos 500. Cada una de las entradas de la lista de permisos 530(1)-(N) proporciona una lista de permisos en cuanto a las clases de tráfico de red que están permitidas entre el grupo de usuarios fuente y el grupo de usuarios de destino. Por ejemplo, dado un identificador de grupo de usuarios fuente de cuatro (4) y un identificador de grupo de usuarios de destino de tres (3), se identifica la PME 520(4,3). La PME 520(4,3) incluye un puntero a la entrada de la lista de permisos 530(5). La entrada de la lista de permisos 530(5) podría contener una lista de permisos tal como la siguiente:

permit tcp www
permit tcp telnet
permit tcp ftp
permit tcp ftp-data
implicit deny

[0044] Tal como se apuntó, estos permisos son típicamente muy pocos en comparación con las ACL tradicionales. Esto es porque tales permisos no se aplican a todo el tráfico de red que pasa por una interfaz dada, sino sólo al tráfico entre dos grupos de usuarios específicos. Por ejemplo, la especificación de los tipos de tráfico de entrada permitidos desde Internet (la interfaz ACL) ya no es necesaria – sólo tienen que especificarse (en la lista de permisos RBACL) los tipos de tráfico permitidos que entran de Internet a ciertos servidores.

[0045] Típicamente, la matriz de permisos estará poblada muy escasamente. Sin embargo, existe un escenario en el que una columna o fila particular de la matriz puede estar totalmente poblada. Si vemos la política de seguridad como una lista de conjuntos de permisos entre grupos fuente y de destino, la política de seguridad puede definirse como:

Tabla 1. Ejemplo de matriz de permisos.

SUG1	DUG4	ListaDePermisosA
SUG2	DUG5	ListaDePermisosB
SUG3	DUG6	ListaDePermisosC

[0046] La fig. 6A es un diagrama de bloques que ilustra un ejemplo de encadenamiento de matrices de permisos según la presente invención. En este escenario, el puntero que se selecciona en la matriz de permisos 500 apunta a una de varias listas de permisos (representadas en la fig. 6A como una lista de permisos 600, una lista de permisos 610 y una lista de permisos 620), que, a su vez, apuntan unas a otras y se terminan por un permiso de denegación implícita (representado como la denegación implícita 630 en la fig. 6A). En la tabla 1 anterior se da un ejemplo de listas de permisos 600, 610 y 620.

[0047] Así, como puede verse, la lista de permisos 620 se construye sobre los permisos enumerados en la lista de permisos 610, que a su vez, se construye sobre la lista de permisos enumerada en la lista de permisos 600. Como con una lista de permisos típica, la lista se termina por una denegación implícita, que indica que, a menos que se permita específicamente de otro modo, no se conceden permisos.

[0048] De la manera representada en la fig. 6A, puede crearse una lista de permisos para cada una de las entradas en la matriz de permisos 500 simplemente combinando listas de permisos (por ejemplo las listas de permisos 600, 610 y 620, así como otras de tales listas de permisos) para llegar al conjunto deseado de permisos para la combinación de grupo de usuarios fuente y grupo de usuarios de destino representada por la entrada en la matriz de permisos 500 que apunta al grupo dado de listas de permisos.

[0049] Una característica deseable es permitir que un administrador de seguridad de la red especifique una lista de permisos para cualquier grupo fuente que se comunique con un grupo de destino específico o viceversa. Si un identificador de grupo es un único identificador ninguna semántica codificada en el valor, proporcionar enmascaramiento variable del identificador de grupo sirve de poco. Sin embargo, enmascarar el identificador de grupo entero aborda la necesidad anterior. Esto conduce a las 4 posibles formas de especificar una asignación de lista de permisos.

SUGx	DUGy	ListaDePermisos1
CUALQUIERA	DUGy	ListaDePermisos2
SUGx	CUALQUIERA	ListaDePermisos3
CUALQUIERA	CUALQUIERA	ListaDePermisos4

[0050] Se observará que la forma final (CUALQUIERA a CUALQUIERA) rellenará toda la matriz con la ACL

ListaDePermisos4. Tal configuración puede conducir a que un paquete dado necesite potencialmente que se apliquen múltiples listas de permisos. Conceptualmente, la matriz apunta a una cadena de listas de permisos (como en las figs. 6A y 6B), donde cada una es recorrida en orden. Tal como se representa, cada lista de permisos se termina con un continuar implícito, y la denegación implícita se aplica al final de la cadena.

[0051] De hecho, las estructuras de punteros que soportan tales combinaciones pueden estar separadas de las propias listas de permisos, simplificando las estructuras de punteros y reduciendo la duplicación de la información de permisos. Tal estrategia se analiza más adelante en relación con la fig. 6B.

[0052] La fig. 6B es un diagrama de bloques que ilustra un ejemplo de un conjunto de listas de permisos que emplean un conjunto separado de estructuras de punteros (denominado encadenamiento) con el fin de simplificar el conjunto de estructuras de listas de permisos necesarias para soportar la presente invención. Como antes, una entrada en la matriz de permisos 500 es un puntero al conjunto deseado de listas de permisos. Sin embargo, a diferencia de las estructuras mostradas en la fig. 6A, la entrada dada en la matriz de permisos 500 apunta a uno de varios bloques de punteros (representados en la fig. 6B como los bloques de punteros 650, 655 y 660). Como puede verse, el bloque de punteros 650 apunta tanto a una lista de permisos 665 como al bloque de punteros 655. De modo similar, el bloque de punteros 655 apunta a una lista de permisos 670, así como al bloque de punteros 660. Igualmente, el bloque de punteros 660 apunta a una lista de permisos 675, pero, en cambio, también apunta a una denegación implícita 680, que termina la cadena de punteros. Resultará evidente que pueden crearse estructuras complejas utilizando esta estrategia, permitiendo a un usuario hacer un uso diferente de las listas de permisos mediante el uso acertado de punteros.

[0053] En la arquitectura representada en la fig. 6B, cada una de las entradas de la matriz de permisos 500 apunta a un bloque de punteros, tal como el bloque de punteros 650. El bloque de punteros 650 apunta tanto a una lista de permisos (por ejemplo, la lista de permisos 665) como a otro bloque de punteros cualquiera (por ejemplo, el bloque de punteros 655) o una denegación implícita (por ejemplo, la denegación implícita 680). Así, cada lista de permisos (por ejemplo, las listas de permisos 665, 670 y 675) están disponibles para uno cualquiera de los bloques de punteros que constituye la lista de permisos global implementada en última instancia para una entrada dada en la matriz de permisos 500. Tal arquitectura permite el uso eficiente de listas de permisos requiriendo sólo una de tales listas de permisos para cualquier tipo de permiso que pudiera implementarse. Así, para cada conjunto de permisos, el sistema simplemente implementa un conjunto de bloques de punteros y hace que los punteros de la lista de permisos de esos bloques de punteros apunten a las listas de permisos necesarias para implementar el conjunto deseado de permisos. Puesto que cada uno de estos permisos puede reutilizarse cualquier número de veces, el espacio consumido por tal implementación es significativamente inferior al que pudiera ser si no.

[0054] La fig. 6C es un diagrama de bloques que ilustra una vista lógica de los ejemplos de encadenamiento de la matriz de permisos representada en la fig. 6A y la 6B según la presente invención. Tal como se apuntó en ambos ejemplos, la entrada dada de la matriz de permisos 500 apunta al primero de varias listas de permisos (representadas en la fig. 6C como las listas de permisos 690, 692 y 694), que se terminan por una denegación implícita 696, de la manera analizada anteriormente.

[0055] Así, en una implementación basada en software, puede emplearse una estructura basada en árbol, basada en troceo, u otra de tales estructuras de búsqueda, siendo la búsqueda una concordancia en la concatenación de los grupos de usuarios fuente y de destino. El resultado de la búsqueda es un puntero a una cadena de ACL. Estas ACL son recorridas en el orden en que están presentes en la cadena. Las ACL se ven lógicamente como una sola ACL encadenada.

[0056] En muchas implementaciones de ACL, típicamente se emplean dos estrategias. Una estrategia es el modelo basado en procesador de red (software). Este tipo de implementación es similar a la implementación por software y puede beneficiarse de esa estrategia. La otra estrategia es usar una solución basada en CAM. La siguiente sección se centra en la implementación basada en CAM.

<u>Un ejemplo de una arquitectura de permisos basada en hardware implementada usando listas de control de acceso basadas en roles</u>

[0057] Una implementación basada en CAM proporciona la ventaja de una búsqueda paralela y la capacidad de enmascarar campos. La búsqueda paralela proporciona un rendimiento elevado, predecible y consistente. Por desgracia, una sola búsqueda crea una enorme cantidad de complejidad para la programación del software del dispositivo, porque la implementación típica supone procesamiento secuencial.

[0058] Si el número de grupos soportados por una plataforma es pequeño (por ejemplo, inferior a 256), una implementación ASIC de la matriz de permisos puede ser viable usando la memoria en chip. En tal escenario, la salida de la matriz proporciona una etiqueta (por ejemplo, una etiqueta de flujo) que puede utilizarse entonces para realizar una búsqueda de CAM de manera similar a la de las implementaciones de ACL basadas en CAM tradicionales.

[0059] El caso probable, sin embargo, es que el número de grupos que han de ser soportados será mucho mayor, haciendo inviable una implementación en chip. La determinación de permisos y la imposición de permisos se implementan así típicamente junto con la propia búsqueda de CAM. Utilizando una sola etiqueta de flujo para la búsqueda de RBACL, los grupos fuente y destino pueden situarse en la especificación de flujo de CAM en el lugar de las direcciones de red fuente y destino (por ejemplo, direcciones IP).

[0060] La fig. 7 es un diagrama de bloques que ilustra un ejemplo de una lista de control de acceso (ACL) según la presente invención, y representada como la lista de control de acceso 700. La lista de control de acceso 700 incluye varias entradas (denominadas entradas de lista de control de acceso o ACE), que están representadas en la fig. 7 como las entradas de lista de control de acceso 710(1)-(N). Cada una de las ACE 710(1)-(N) incluye, por ejemplo, una etiqueta de flujo (representada en la fig. 7 como los campos de etiqueta de flujo 720(1)-(N)), un identificador de grupo de usuarios fuente (SUG) (representado en la fig. 7 como los campos de SUG 730(1)-(N)), un identificador de grupo de usuarios de destino (DUG) (representado en la fig. 7 como los campos de DUG 740(1)-(N)), y otras especificaciones de flujo (representadas en la fig. 7 como otros campos de especificación de flujo 750(A)-(N)). Como es sabido, una ACL tal como la ACL 700 puede implementarse utilizando una memoria direccionable según el contenido (CAM), y más específicamente, una CAM ternaria (TCAM), permitiendo de ese modo la búsqueda rápida y eficiente de información. Se proporciona una etiqueta de flujo opcional (también denominada etiqueta ACL, mantenida en un campo apropiado de los campos de etiqueta de flujo 720(1)-N)) para distinguir las RBACL de las ACL de interfaz tradicional en el mismo dispositivo. Un dispositivo que emplee sólo RBACL no necesitaría tal campo.

Una red de ejemplo que emplea RBACL y el funcionamiento de la misma

[0061] La fig. 8A es un diagrama de bloques que ilustra un ejemplo de una arquitectura de subred del lado del anfitrión y autenticación según la presente invención. En esta arquitectura, un anfitrión 800 se comunica con una subred 810 por medio de un conmutador 820. Un usuario que inicia sesión en el anfitrión 800 es autentificado por un servidor de autenticación 830 por medio del conmutador 820, de la manera representada y analizada en relación con la fig. 2. Así, por ejemplo, un usuario inicia sesión en el anfitrión 800 y es autentificado por el servidor de autenticación 830 por medio del conmutador 820. Durante esta autenticación, el grupo de usuarios del usuario es identificado y asignado al usuario como un indicador de grupo fuente (SGT), que corresponde al rol del usuario (por ejemplo, ingeniería, dirección, marketing, ventas o similares).

[0062] Más específicamente, un usuario podría estar en un rol de ingeniería. El anfitrión 800 inicia la autenticación (por ejemplo, por medio del protocolo IEEE 802.1X). Bajo el protocolo RADIUS, el servidor de autenticación 830 pone a prueba al usuario para una combinación de identificación de usuario y contraseña. En el momento de una autenticación exitosa, la aceptación de acceso RADIUS asigna al usuario un SGT de 5, que corresponde al rol de ingeniería.

[0063] La MAC, la VLAN del ordenador del usuario (anfitrión 800) se inserta en la tabla L2 y se marca como una dirección MAC segura. La tabla 2 ilustra la tabla de capa 2 después de ser poblada con esta información.

Tabla 2. Ejemplo de tabla de capa 2

MAC	Identificador de VLAN	Puerto	Grupo de usuarios
1234.ABCD.1234	4	PortAI	5

[0064] La fig. 8B es un diagrama de flujo que ilustra un ejemplo del funcionamiento de la subred del lado del anfitrión mostrada en la fig. 8A. El procedimiento comienza con el anfitrión 800 iniciando el procedimiento de autenticación (etapa 850). A continuación, se emite una puesta a prueba desde el servidor de autenticación 830, para poner a prueba al usuario respecto a su nombre de usuario y contraseña (de nuevo, de la manera descrita en relación con la fig. 2) (etapa 855). En respuesta a esta puesta a prueba, el usuario suministra su nombre de usuario y contraseña (etapa 860). Entonces se efectúa una determinación en cuanto a si el servidor de autenticación 830 puede autentificar al usuario (etapa 865). Si el usuario no puede ser autentificado, se efectúa una determinación en cuanto a si no permitir que el usuario reintroduzca su nombre de usuario y contraseña (etapa 870). Si la

reintroducción de esta información es aceptable, el procedimiento ejecuta un bucle hasta el servidor de autenticación 830 poniendo a prueba al usuario (etapa 855). Si no (por ejemplo, si esta reintroducción ha sido permitida un número máximo de veces o si no se permite en absoluto), el procedimiento finaliza.

[0065] Alternativamente, si el usuario es autentificado (etapa 865), se permite que el usuario inicie sesión, lo cual se consigue reenviando la aceptación de acceso al anfitrión 800 (etapa 875). Además, se asigna un SGT basándose en el (los) rol(es) del usuario (etapa 880). Este, junto con otra información, se utiliza para poblar la tabla de capa 2 (es decir, la tabla de reenvío, o una construcción comparable) mantenida por el conmutador 820 (etapa 885). Esto completa el procedimiento de inicio de sesión del usuario.

[0066] Tal como se apuntó, la fig. 8B representa un diagrama de flujo que ilustra un procedimiento según una realización de la presente invención, como otras de las figuras analizadas en este documento. Se aprecia que las operaciones analizadas en este documento pueden consistir en comandos introducidos directamente por un usuario del sistema informático o por etapas ejecutadas por módulos de hardware de aplicación específica, pero la realización preferente de la invención incluye etapas ejecutadas por módulos de software. La funcionalidad de las etapas a las que se hace referencia en este documento puede corresponder a la funcionalidad de módulos o porciones de módulos.

[0067] Las operaciones a las que se hace referencia en este documento pueden ser módulos o porciones de módulos (por ejemplo, módulos de software, firmware o hardware). Por ejemplo, aunque la realización descrita incluye módulos de software y/o incluye comandos de usuario introducidos manualmente, los diversos módulos de ejemplo pueden ser módulos de hardware de aplicación específica. Los módulos de software analizados en este documento pueden incluir archivos de guión, por lotes u otros archivos ejecutables, o combinaciones y/o porciones de tales archivos. Los módulos de software pueden incluir un programa informático o subrutinas del mismo codificados en medios legibles por ordenador.

[0068] Además, los expertos en la materia reconocerán que los límites entre módulos son meramente ilustrativos y realizaciones alternativas pueden fusionar módulos o imponer una descomposición alternativa de la funcionalidad de los módulos. Por ejemplo, los módulos analizados en este documento pueden ser descompuestos en submódulos que han de ejecutarse como múltiples procesos informáticos, y, opcionalmente, en múltiples ordenadores. Por otra parte, realizaciones alternativas pueden combinar múltiples instancias de un módulo o submódulo particular. Además, los expertos en la materia reconocerán que las operaciones descritas en la realización de ejemplo son únicamente ilustrativas. Las operaciones pueden combinarse o la funcionalidad de las operaciones puede distribuirse en operaciones adicionales de acuerdo con la invención.

[0069] Alternativamente, tales acciones pueden incluirse en la estructura de circuitos que implementa tal funcionalidad, tal como el microcódigo de un ordenador con conjunto de instrucciones complejas (CISC), firmware programado dentro de dispositivos programables o borrables/programables, la configuración de una matriz de puertas programable in-situ (FPGA), el diseño de una matriz de puertas o un circuito integrado de aplicación específica (ASIC) totalmente personalizado, o similares.

[0070] Cada uno de los bloques del diagrama de flujo puede ser ejecutado por un módulo (por ejemplo, un módulo de software) o una porción de un módulo o un usuario de sistema informático. Así, el procedimiento descrito anteriormente, las operaciones del mismo y los módulos para el mismo pueden ser ejecutados en un sistema informático configurado para ejecutar las operaciones del procedimiento y/o pueden ser ejecutados desde medios legibles por ordenador. El procedimiento puede incluirse en un medio legible por una máquina y/o legible por ordenador para configurar un sistema informático para ejecutar el procedimiento. Así, los módulos de software pueden ser almacenados dentro de y/o transmitidos a una memoria de sistema informático para configurar el sistema informático para realizar las funciones del módulo.

[0071] Tal sistema informático normalmente procesa la información según un programa (una lista de instrucciones almacenadas internamente tal como un programa de aplicación particular y/o un sistema operativo) y produce información de salida resultante por medio de dispositivos de entrada/salida. Un proceso informático incluye típicamente un programa en ejecución (en funcionamiento) o una porción de un programa, valores de programa actuales e información de estado, y los recursos utilizados por el sistema operativo para gestionar la ejecución del proceso. Un proceso progenitor puede generar otros procesos vástagos para ayudar a realizar la funcionalidad global del proceso progenitor. Como el proceso progenitor genera específicamente los procesos vástagos para realizar una porción de la funcionalidad global del proceso progenitor, las funciones realizadas por los procesos vástagos (y los procesos nietos, etc.) a veces puede describirse que son realizadas por el proceso progenitor.

[0072] Tal sistema informático incluye típicamente múltiples procesos informáticos que se ejecutan "simultáneamente". A menudo, un sistema informático incluye una unidad de procesamiento individual que es capaz de soportar muchos procesos activos alternativamente. Aunque puede parece que se ejecutan múltiples procesos simultáneamente, en cualquier momento dado sólo es ejecutado realmente un proceso por la unidad de procesamiento individual. Cambiando rápidamente la ejecución del proceso, un sistema informático ofrece la apariencia de ejecución simultánea de procesos. La capacidad de un sistema informático de multiplexar los recursos del sistema informático entre múltiples procesos en varias fases de ejecución se denomina multitarea. Los sistemas con unidades de procesamiento múltiples, que por definición pueden soportar un verdadero procesamiento simultáneo, se denominan sistemas multiprocesamiento. Los procesos activos a menudo se denominan de ejecución simultánea cuando tales procesos se ejecutan en un entorno multitarea y/o multiprocesamiento.

[0073] Los módulos de software descritos en este documento pueden ser recibidos por tal sistema informático, por ejemplo, desde medios legibles por ordenador. Los medios legibles por ordenador pueden estar acoplados permanentemente, de manera desmontable o a distancia al sistema informático. Los medios legibles por ordenador pueden incluir de manera no exclusiva, por ejemplo, cualquier número de lo siguiente: medios de almacenamiento magnético incluyendo medios de almacenamiento en disco y en cinta, medios de almacenamiento óptico tales como medios de disco compacto (por ejemplo, CD-ROM, CD-R, etc.) y medios de almacenamiento en disco de vídeo digital, memoria de almacenamiento de memoria no volátil, incluyendo unidades de memoria basada en semiconductor tales como memoria FLASH, EEPROM, EPROM, ROM o circuitos integrados de aplicación específica. Medios de almacenamiento volátil incluyendo registros, memorias intermedias o cachés, memoria principal, RAM, y similares, y medios de transmisión de datos incluyendo una red informática, telecomunicación punto a punto, y medios de transmisión de ondas portadoras. En un entorno basado en UNIX, los módulos de software pueden incluirse en un archivo los cuales puede ser un dispositivo, un terminal, un archivo local o remoto, un zócalo, una conexión de red, una señal, u otro recurso de comunicación o cambio de estado. Pueden usarse otros tipos nuevos y diversos de medios legibles por ordenador para almacenar y/o transmitir los módulos de software analizados en este documento.

[0074] La fig. 9A es un diagrama de bloques que ilustra un ejemplo de una subred del lado del servidor según la presente invención. En este ejemplo, un servidor 900 está acoplado a una subred 910 mediante un conmutador 920. El conmutador 920 también acopla el servidor 900 a un servidor de autenticación 930, que proporciona la autenticación de entidades que intentan iniciar sesión y acceder a la subred 910. En este escenario, a diferencia de la autenticación de usuario representada en las figs. 8A y 8B, el procedimiento aquí es la autenticación del servidor 900 por el servidor de autenticación 930.

[0075] El servidor 900 es autentificado de manera similar a la utilizada para autentificar el ordenador anfitrión del usuario (anfitrión 800). El servidor 900 y el servidor de autenticación 930 emplean un protocolo de autenticación (por ejemplo, el IEEE 802.1X) que se utiliza para autentificar la identidad del servidor 900. La MAC, la VLAN del servidor (servidor 900) se inserta en la tabla de capa 2 y se marca como una dirección MAC segura. La tabla 3 ilustra la tabla de capa 2 después de ser poblada con esta información.

Tabla 3. Ejemplo de tabla de capa 2

MAC	Identificador de VLAN	Puerto	Grupo de usuarios
5678.1234.DCBA	100	PortB5	6

[0076] La fig. 9B es un diagrama de flujo que ilustra un ejemplo del funcionamiento de la subred del lado del servidor mostrada en la fig. 9A. El procedimiento comienza con el inicio del procedimiento de autenticación por el servidor 900 (etapa 950). Una vez que se inicia la autenticación, el servidor de autenticación 930 pone a prueba al servidor 900 por medio del conmutador 920 (etapa 955). En respuesta, el servidor 900 suministra información de autenticación al servidor de autenticación 930 por medio del conmutador 920 (etapa 960). Entonces se efectúa una determinación por el servidor 930 en cuanto a si el servidor 900 ha sido autentificado correctamente (etapa 965). Si el servidor 900 ha fallado este procedimiento de autenticación, el procedimiento termina y al servidor 900 no se le permite acceder, o que otros nodos de red accedan al mismo, a través de la red.

[0077] Sin embargo, si el servidor 900 es autentificado (etapa 965), se permite que el servidor 900 acceda a la red mediante el reenvío por el servidor de autenticación 930 de la aceptación de acceso al conmutador 920 y el servidor 900 (etapa 970). Además, se asigna un indicador de grupo (más específicamente, un DGT (aunque, desde la perspectiva del servidor 900, un SGT)) al servidor 900 en el conmutador 920 basándose en el (los) rol(es) del servidor (etapa 975). Se apreciará que, de hecho, la cuestión en cuanto a si un grupo de usuarios es un grupo de

usuarios fuente o de destino se toma desde el punto de vista de la dirección del paquete en cuestión. Esto, junto con otra información, se utiliza para poblar la tabla de capa 2 del conmutador 920 (etapa 980).

[0078] La fig. 10 es un diagrama de bloques que ilustra un ejemplo de una arquitectura de red 1000 que incluye un anfitrión (1005) y un servidor 1010. De la manera representada en las figs. 8A y 8B, el anfitrión 1005 es autentificado por un servidor de autenticación 1015 por medio de un conmutador 1020. El conmutador 1020 también proporciona al anfitrión 1005 acceso a una subred 1025. De la manera representada en las figs. 9A y 9B, el servidor 1010 es autentificado por un servidor de autenticación 1030 por medio de un conmutador 1035. El conmutador 1035 también proporciona al servidor 1010 acceso a (y desde) una subred 1040. Las subredes 1025 y 1040 están acopladas comunicativamente entre sí a través de un núcleo empresarial 1050. La subred 1025 accede al núcleo empresarial 1050 por medio de un encaminador 1055, e igualmente, la subred 1040 accede al núcleo empresarial 1050 por medio de un encaminador 1060.

[0079] En la fig. 10 también se muestra un paquete 1070, que tiene contenido 1075. El paquete 1070 es transmitido por el anfitrión 1005 al conmutador 1020. La información de grupo de usuarios fuente es añadida al paquete 1070 por el conmutador 1020 en forma de un indicador de grupo fuente 1080, basándose en la información proporcionada por el servidor de autenticación 1015 durante el procedimiento de autenticación, con el fin de crear un paquete 1085. Tal como se representa en la fig. 10, el paquete 1085 incluye tanto el contenido 1075 como el SGT 1080. El paquete 1085 recorre la subred 1025 y llega al encaminador 1055. El encaminador 1055 encamina el paquete 1085 a través del núcleo empresarial 1050 hasta el encaminador 1060. El encaminador 1060 presenta el paquete 1085 al conmutador 1035 (y de este modo, al servidor 1010) por medio de la subred 1040. El encaminado 1035 efectúa una determinación en cuanto a si pasar el paquete 1085 al servidor 1010, basándose, al menos en parte, en la información de DUG proporcionada al servidor 1010 por el servidor de autenticación 1030. Se apreciará que, alternativamente, el encaminador 1060 también podría encargarse de esta tarea y efectuar esta determinación.

[0080] A continuación se ofrece un ejemplo específico del recorrido de la arquitectura de red 1000 por el paquete 1075/el paquete 1085. Después de la autenticación, el anfitrión 1005 puede enviar paquetes (por ejemplo, el paquete 1075) en la red. Puesto que se están aplicando RBACL en la capa 3 de red en el presente ejemplo, cualquier paquete que el usuario intente enviar más allá de su subred local (por ejemplo, la subred 1025) será sometido a inspección de RBACL. Como se apreciará, los conmutadores 1020 y 1035 también pueden emplear RBACL en el dominio de la capa 2 (por ejemplo, dentro de las subredes 1025 y 1040, respectivamente). Sin embargo, en tal caso, probablemente se necesitarían ajustes, tales como basar las RBACL en el direccionamiento de capa 3 de los paquetes, de manera similar a las VLAN ACL (VACL).

[0081] Si el paquete 1085 es el primer paquete que ha de enviarse desde el anfitrión 1005 al servidor 1010, se activará un procedimiento de ARP para el destino. El envío del paquete 1085 comienza tomándose el SUG (en este caso, con un valor de 5) del SGT 1080. Una búsqueda de FIB en el encaminador 1055 para un paquete que tenga el destino del paquete 1085 indica el siguiente encaminador de salto al cual debería ser reenviado el paquete. Esta información de siguiente salto podría ser, por ejemplo, la información de reescritura de MAC para el encaminador 1060, o para un encaminador entre el encaminador 1055 y el encaminador 1060. Esto puede verse en la tabla 4, que ilustra una FIB con tal contenido.

Tabla 4. FIB de ejemplo (encaminador 1055).

CAM	**Memoria**	
Prefijo	**Grupo de usuarios**	**Información de siguiente salto**
3.4.X.X	---	Reescritura
23.X.X	---	
X.X.X.X	---	

[0082] Se observará que, en este ejemplo, la información de prefijo está contenida en una CAM, mientras que el grupo de usuarios y la información de siguiente salto están contenidos en una memora estándar (por ejemplo, SRAM). La búsqueda se realiza utilizando el prefijo para determinar qué entrada en la memoria inspeccionar.

[0083] Cuando el paquete 1075 (paquete posterior 1085) es enviado desde el anfitrión 1005, se quita el indicador al paquete 1075, tal como se apuntó. En este ejemplo, en el momento de entrar en el conmutador 1020, el paquete 1075 es marcado con el SGT 1080 (lo cual indica un grupo de usuarios de 5). Este grupo de usuarios es recuperado de la tabla de capa 2 en el conmutador de ingreso (conmutador 1020) de la manera analizada previamente. Este paquete (que ahora, incluyendo el SGT 1080, se denomina paquete 1085) es enviado luego a través de la arquitectura de red 1000 por medio del encaminamiento y la conmutación proporcionados de ese modo.

[0084] En el encaminador de egreso (encaminador 1060), se realiza la búsqueda de FIB). Si la búsqueda de FIB alcanza una subred unida localmente, la adyacencia de recolección hace que se genere una petición de ARP para el servidor deseado (por ejemplo, el servidor 1010). La petición de ARP es enviada desde el encaminador 1060 al servidor 1010. La respuesta de ARP es enviada luego desde el servidor 1010. El conmutador de L2 de ingreso (conmutador 1040) inserta el SUG para el servidor 1010 (o, tal como se utiliza por los conmutadores/encaminadores de la arquitectura de red 1000 (por ejemplo, el anfitrión 1005) como el DUG para los paquetes enviados al servidor 1010; lo cual se establece para un grupo de usuarios de 6) dentro de la respuesta de ARP (en el encabezamiento de L2). El encaminador 1060 recibe la respuesta de ARP y puebla la FIB con el prefijo de anfitrión resuelto, la información de reescritura que contiene la dirección MAC del anfitrión, y el grupo de usuarios de destino (6) a partir de la respuesta de ARP. Un ejemplo de la FIB que resulta se muestra en la tabla.

Tabla 5. Contenido de FIB de ejemplo después de la respuesta de ARP y la población.

CAM	**Memoria**	
Prefijo	**Grupo de usuarios**	**Información de siguiente salto**
3.4.1.1	6	Reescritura
3.4.X.X	---	Recolección
X.X.X.X	---	

[0085] En el caso en el que el paquete 1085 es un paquete subsiguiente desde el anfitrión 1005 al servidor 1010, las tablas en cuestión ya deberían estar pobladas. Una vez que la FIB del encaminador 1060 contiene el prefijo de anfitrión totalmente resuelto, el siguiente paquete al servidor 1010 estará sometido a control de acceso. (En una realización de la presente invención en este ejemplo, el primer paquete que activó la resolución de ARP se omite). Cuando el paquete subsiguiente llega desde el anfitrión 1005 llega al encaminador 1060, el encaminador 1060 ya posee la información relacionada con los grupos fuente y destino pertinentes. El SUG (5) es extraído del SGT del paquete subsiguiente y el DUG (6) es descubierto por la búsqueda de FIB.

[0086] En este punto, se realiza una búsqueda de ACL. Suponiendo que se emplea una implementación basada en CAM, la clave de búsqueda en la CAM contiene la información del paquete así como los grupos de usuarios fuente y destino (5 y 6). En este ejemplo, el único permiso admitido entre los 2 grupos es el tráfico web (puerto tcp 80). Las entradas de la RBACL de ejemplo se muestran en la tabla 6.

Tabla 6. Contenido de RBACL de ejemplo.

SUG	**DUG**	**Especificación de flujo**	**Resultado**
5	6	Puerto RCP 80	Permitir
7	8	Puerto TCP 23	Denegar
CUALQUIERA	CUALQUIERA	CUALQUIERA	CUALQUIERA

[0087] Puesto que, en este ejemplo, el paquete subsiguiente es en efecto tráfico web (destinado al puerto TCP 80), se alcanza la entrada de CAM apropiada y se permite la transmisión del paquete a la subred 1040 (y de ese modo, en el servidor 1010 por medio del conmutador 1035). Sin embargo, para ilustrarlo mejor, si el paquete subsiguiente ha sido un paquete Telnet (destinado al puerto TCP 23), el paquete alcanzará la entrada CUALQUIERA-CUALQUIERA en la CAM, lo cual no permitiría tal transmisión (implementando eficientemente la denegación implícita presente en las ACL por software). A continuación se presenta una discusión más generalizada de las operaciones descritas en los pasajes anteriores en relación con las figs. 11, 12, 13 y 14.

[0088] La fig. 11 es un diagrama de flujo que ilustra un ejemplo generalizado del proceso del recorrido de un paquete a través de una red tal como la representada como la arquitectura de red 1000. En tal escenario, el proceso comienza con el anfitrión 1005 enviando un paquete (por ejemplo, el paquete 1070) (etapa 1100). El paquete así transmitido pasa por el conmutador local (por ejemplo, el conmutador 1020), el cual marca el paquete con información de grupo de usuarios fuente (por ejemplo, un SGT) (etapa 1105). El paquete de destino (por ejemplo, el paquete 1085) pasa entonces por la subred local (por ejemplo, la subred 1025) (etapa 1110). Después de pasar por la subred local, el paquete pasa por el dispositivo de red próximo (por ejemplo, el encaminador 1055) (etapa 1115), En este punto, tal como se apuntó, el encaminador 1055 encamina el paquete a través de la interred dada (por ejemplo, el núcleo empresarial 1050) (etapa 1120). Después de pasar por la interred, el paquete es recibido por el dispositivo de red lejano (por ejemplo, el encamiandor 1055) (etapa 1125). En el dispositivo de red lejano, se realiza el procesamiento de control de acceso basado en roles (etapa 1130). Tal procesamiento se describe en detalle en relación con las figs. 12, 13 y 14.

[0089] Después se efectúa una determinación en cuanto a si el paquete dado ha pasado el procesamiento de RBAC que se realiza (etapa 1135). Si el paquete no pasa la inspección de RBAC (es decir, el procesamiento de RBAC que se realizó), el paquete se omite (etapa 1140). Como resultará evidente para los expertos en la materia, pueden realizarse otras acciones en respuesta a tal resultado. Alternativamente, si el paquete dado pasa la inspección de RBAC (etapa 1135), se permite que el paquete pase por el dispositivo de red lejano (etapa 1150), y luego pasa por la subred lejana (por ejemplo, la subred 1040) (etapa 1160). El paquete pasa entonces por al conmutador lejano (por ejemplo, el conmutador 1035) (etapa 1170). Por último, el paquete llega al servidor de destino (por ejemplo, el servidor 1010) (etapa 1180).

[0090] La fig. 12 es un diagrama de flujo que ilustra un ejemplo del procesamiento de RBAC realizado en el paquete por un dispositivo de red tal como el encaminador 1060, en el caso en el que el paquete es el primero de tales paquetes recibidos. El procedimiento comienza con la recepción de un paquete que ha de ser procesado utilizando la presente invención (etapa 1200). En primer lugar, se extrae el SGT del paquete (etapa 1210). A continuación, se realiza una búsqueda para determinar cómo debería ser tratado el paquete (etapa 1220). Después se efectúa una determinación en cuanto a si la dirección de destino del paquete dado indica que se requiere procesamiento de RBAC (etapa 1230). Si la dirección de destino indica que no se requiere procesamiento de RBAC, el encaminador lejano realiza otro procesamiento en el paquete, según se requiera, y encamina el paquete según corresponda (etapa 1235).

[0091] Sin embargo, si la dirección de destino del paquete indica que ha de realizarse el procesamiento de RBAC, el encaminador lejano envía una petición de protocolo de resolución de dirección (ARP) al servidor de destino (por ejemplo, el servidor 1010) (etapa 1240). El servidor responde con una respuesta de ARP (etapa 1250). A continuación, el conmutador lejano inserta el DGT (o el SGT, desde la perspectiva del servidor 1010) que corresponde al grupo del servidor, dentro de la respuesta de ARP (etapa 1260). El encaminador lejano recibe esta respuesta de ARP (incluyendo el DGT (o el SGT, desde la perspectiva del servidor 1010) que indica el DUG del servidor 1010) (etapa 1270)), y puebla si base de información de reenvío (FIB) con esta información (etapa 1280). Como antes, el encaminador lejano realiza entonces cualquier otro procesamiento requerido, y encamina el paquete según corresponda (etapa 1235). Se observará que, de hecho, este encaminamiento puede incluir omitir el paquete dado si la RBACL indica que el dispositivo de red ha de denegar el acceso al paquete.

[0092] La fig. 13 es un diagrama de flujo que ilustra un ejemplo del procesamiento realizado sobre un paquete recibido posteriormente al de la fig. 12, aunque aún sometido al procesamiento de RBAC según la presente invención. El procedimiento comienza, como antes, con la recepción del paquete dado (etapa 1300). También como antes, se extrae el SGT del paquete (etapa 1310). Se realiza una búsqueda mediante el dispositivo de red (por ejemplo, el encaminador 1060), con el fin de determinar cómo ha de ser tratado el paquete dado (etapa 1320). Después se efectúa una determinación en cuanto a si la dirección de destino del paquete indica que se requiere procesamiento de RBAC (etapa 1330). Si la dirección de destino del paquete no indica que se requiere procesamiento de RBAC, el dispositivo de red lejano realiza otro procesamiento según sea necesario, y encamina el paquete apropiadamente (etapa 1340).

[0093] Sin embargo, si el dispositivo de red lejano determina que la dirección de destino del paquete indica que se requiere procesamiento de RBAC, el dispositivo de red lejano realiza una búsqueda en la base de información de reenvío (FIB) para determinar el DUG (etapa 1350). El dispositivo de red lejano, durante el procesamiento de ACL de egreso, efectúa entonces una determinación en cuanto a si la entrada de la RBACL indica que el paquete dado debería ser denegado (etapa 1360). Si la entrada de la RBACL indica que el paquete debería ser denegado, el paquete se omite (etapa 1370). Alternativamente, si la entrada de RBACL indica que el paquete debería ser reenviado, el dispositivo de red lejano realiza otro procesamiento según sea necesario y encamina el paquete dado según corresponda (etapa 1340).

[0094] La fig. 14 es un diagrama de flujo que ilustra un ejemplo del procesamiento de un paquete dado a medida que el paquete circula a través del trayecto de datos de un dispositivo de red que implementa la presente invención (por ejemplo, el encaminador 1060). El procesamiento comienza con el paquete pasando a través de una ACL de seguridad de entrada (etapa 1400). Típicamente, los usuarios crean tales ACL con el fin de impedir que los paquetes que representen una amenaza conocida entren en el dispositivo de red dado. A continuación, las características de entrada del dispositivo de red responden al paquete dado (etapa 1410). Las características de entrada del dispositivo de red pueden incluir, por ejemplo, la intercepción del protocolo de control de transmisión (TCP), el equilibrio de carga del servidor, la detección de intrusión, funciones de cortafuego, redirección de la caché web, cifrado/descifrado, marcación/vigilancia de QOS (calidad de servicio) de entrada, encaminamiento basado en

políticas y similares. Tal como se apreciará, la mayoría de estas características son específicas de la interfaz de ingreso o anulan las decisiones de encaminamiento que pudieran efectuarse dentro del dispositivo de red.

[0095] A continuación, se realiza una comprobación de reenvío de trayecto inverso (RPF) (etapa 1420). Al realizar la comprobación de RPF, el dispositivo de red (por ejemplo, el encaminador 1060) determina si el paquete dado es recibido en la interfaz que se esperaría que el dispositivo de red utilizase para reenviar un paquete unidifusión de vuelta a la fuente del paquete entrante. Típicamente, si la comprobación de RPF tiene éxito, el encaminador reenvía el paquete a su destino previsto, por medio de las acciones restantes representadas en la fig. 14. Alternativamente, si la comprobación de RPF falla, se desecha el paquete.

[0096] Así, habiendo pasado la comprobación de RPF, el encaminador realiza entonces la búsqueda de encaminamiento (etapa 1430). A continuación, se realiza una búsqueda de ACL basada en roles (etapa 1440). En este punto se utilizan una búsqueda basada en el SUG del usuario (tal como se indica por el SGT del paquete, o asignación estática por medio de ACL) y el DUG del servidor (tal como se obtiene mediante la búsqueda de FIB (que se obtiene del SGT del paquete previo) o asignación estática) para determinar si ha de concederse acceso al paquete.

[0097] Una vez que se concede acceso al paquete basándose en la combinación de SUG/DUG, entonces se aplican al paquete las características de salida (etapa 1450). Ejemplos de características de salida que pueden implementarse incluyen, por ejemplo, detección de intrusión, conformación de tráfico, cifrado y descifrado criptográfico, contabilidad de protocolo internet (IP) y similares. Después se aplican las restricciones gobernadas por una ACL de seguridad de salida (etapa 1460). La ACL de seguridad de salida controla el reenvío de paquetes para asegurar que, después del procesamiento por el dispositivo de red, los paquetes potencialmente alterados no representen una amenaza para la seguridad de la(s) subred(es) en el lado de salida del dispositivo de red. De modo similar, pueden aplicarse características de salida adicionales (etapa 1470).

Ejemplos de ventajas de la presente invención

[0098] En su forma más simple, las RBACL proporcionan control de acceso entre grupos de dispositivos de red. La asignación de grupo está basada en el rol del individuo o dispositivo dentro de la empresa en cuestión. Mediante la aplicación de conceptos de RBAC a la red, el usuario se beneficia de varias maneras significativas. Las ventajas de una estrategia según la presente invención incluyen la escalabilidad mejorada de la red, la flexibilidad mejorada en la configuración de red y la manejabilidad mejorada de la red.

[0099] La primera, la escalabilidad, aborda el problema de incrementos multiplicativos en el consumo de recursos a medida que se añaden usuarios a la red. Por ejemplo, la presente invención aborda el problema de la “explosión” de la ACL reduciendo multiplicativamente el tamaño de la ACL. En general, el tamaño de la ACL (en cuanto al número de entradas de la ACL (ACE)) se ha reducido de:

$$NUM_{ACEs} = NUM_{DIRECCIONES\_FUENTE} * NUM_{DIRECCIONES\_DESTINO} * NUM_{PERMISOS}$$

a:

$$NUM_{ACEs} = NUM_{GRUPOS\_FUENTE} * NUM_{GRUPOS\_DESTINO} * NUM_{PERMISOS}$$

[0100] De los tres elementos (orígenes, destinos, permisos), el número de permisos a menudo es el menor de los tres elementos. Como puede verse, resulta razonable esperar que:

$$NUM_{DIRECCIONES\_FUENTE} >> NUM_{GRUPOS\_FUENTE}$$

y:

$$NUM_{DIRECCIONES\_DESTINO} >> NUM_{GRUPOS\_DESTINO}$$

[0101] Siendo ese el caso, uno de los términos multiplicativos es un número relativamente pequeño, con los otros dos términos multiplicativos habiéndose reducido sustancialmente, reduciendo el número de ACE multiplicativamente. Por ejemplo, en una ACL, si suponemos 20 orígenes diferentes (PC clientes o subredes), 5 destinos diferentes (servidores), y 4 permisos (permitir correo web, FTP y SMTP) entre ellos, esto crearía una ACL con 400 ACE. Si suponemos que los orígenes son todos del mismo grupo (razonable, ya que una fuente es un

miembro de grupo, o está sometido a una denegación implícita), y que los destinos son todos del mismo grupo (bajo el mismo razonamiento), el mismo ejemplo utilizando RBACL utilizaría sólo 4 ACE, una reducción de tamaño de dos órdenes de magnitud.

[0102] Una mejora adicional de los aspectos de escalabilidad de implementaciones de la presente invención es el hecho de que el conjunto de permisos de RBACL puede reutilizarse de una manera mucho más eficaz que las ACL existentes. Por ejemplo, supongamos que al grupo de Ingeniería se le permite acceder por el puerto TCP 80 (www) al grupo de Servidor Web de Ingeniería. La lista de permisos consiste en 1 ACE (permitir www) y deniega el resto del tráfico. Esta misma lista de permisos puede reutilizarse para que el grupo de Marketing se comunique con el grupo de servidor Web de Marketing. Tal reutilización no es posible con las ACL tradicionales.

[0103] Un beneficio secundario de la presente invención es que, dado el tamaño sustancialmente reducido de las RBACL cuando se compara con las ACL existentes, la disminución de tamaño tiene como resultado un incremento significativo en el rendimiento del software, el cual está en proporción directa a la reducción del tamaño de las ACL. En otras palabras, puede esperarse un incremento (potencialmente, un incremento multiplicativo) en el rendimiento de las RBACL por software comparado con las ACL tradicionales.

[0104] Otro beneficio fundamental de las RBACL es el desacoplamiento de la topología de red de la política de seguridad, proporcionando una estrategia mucho más flexible para el control del tráfico de red. Aunque las ACL han estado presentes en la tecnología de las operaciones en red durante muchísimo tiempo, las ACL no han podido introducirse en la empresa. La principal ubicación de las ACL hasta la fecha ha sido en el perímetro de la red, típicamente entre la empresa e Internet. El cambio constante experimentado dentro de la mayoría de las empresas ha hecho de tal implementación y uso de ACL una propuesta inmanejable. Algunos ejemplos de tal cambio constante incluyen:

1. Usuarios actualizando continuamente las direcciones de red (por ejemplo, actualización de direcciones IP por medio de DHCP)
2. Movilidad física de los usuarios
3. División en subredes
4. Cambios constantes que se efectúan en la topología general de la red empresarial
5. Adición constante de nuevos dispositivos/usuarios a la red

[0105] La flexibilidad proporcionada por las RBACL permite a los usuarios desplazarse a cualquier parte de la red sin causar efectos adversos en la política de seguridad. Una vez autentificado y asignado a un grupo de usuarios, los permisos pueden aplicarse independientemente de la posición del usuario en la red. La propia RBACL no cambia, porque los grupos relevantes y la política de seguridad permanecen sin cambiar. En un sentido, la política de seguridad de los usuarios les sigue alrededor de la red. No importa dónde inicia sesión el usuario o el conmutador/encaminador físico al que el usuario esté conectado, la política de seguridad aplicada sigue siendo la misma.

[0106] La manejabilidad proporcionada por las RBACL es quizá su mejor ventaja. Esto está estrechamente relacionado con las ventajas que las RBACL proporcionan con respecto a la escalabilidad y la flexibilidad. La escalabilidad que las RBACL proporcionan mejor la gestión de la red permitiendo que un administrador de red revise la RBACL y comprenda sus efectos (es decir, los objetivos que la RBACL pretende lograr). Con una ACL tradicional que puede tener cientos o incluso miles de líneas de longitud, comprender exactamente qué se hará para un flujo dado es casi imposible.

[0107] La disminución de tamaño de la RBACL también permite que la RBACL sea instalada en encaminadores/conmutadores por toda la red de la empresa. El desacoplamiento de la topología de red de la política de seguridad que está implementada hace posible mover la misma RBACL a cualquier parte de la red, ya que las RBACL no se ven afectadas por la topología de la red. Las direcciones de red y las interfaces de ingreso/egreso no afectan a la definición de la RBACL. Esto permite el movimiento del usuario por toda la red (y por tanto, la empresa), ya que sus permisos serán impuestos en todos los dispositivos de red.

[0108] A medida que se añaden usuarios a la red o se instalan nuevos servidores, las ACL tradicionales deben ser actualizadas para que incluyan el nuevo usuario/dispositivo. Esto supone un gran coste, especialmente a medida que las ACL se vuelven cada vez más grandes. Con cada cambio, existe un riesgo de interrupción de la red o un agujero de seguridad. El riesgo aumenta en proporción directa al tamaño de la ACL. Además, a medida que el tamaño de la ACL aumenta, el rendimiento del software disminuye en proporción directa. En una organización

grande, cuando una ACL necesita ser actualizada, el equipo de seguridad de la organización debe evaluar e introducir las entradas apropiadas. Después, esta ACL modificada es comprobada por la organización. Finalmente, la ACL revisada y comprobada se instalará mediante la coordinación con el equipo de gestión de red de la organización. El coste de tal procedimiento puede ser sustancial. En un escenario similar, utilizando RBACL, el nuevo servidor simplemente se añade al grupo apropiado. No existe cambio en la ACL y los permisos apropiados para el grupo se aplicarán automáticamente.

[0109] Aunque se han mostrado y descrito realizaciones particulares de la presente invención, resultará obvio para los expertos en la materia que, basándose en las enseñanzas de este documento, pueden efectuarse cambios y modificaciones sin apartarse de esta invención y sus aspectos más generales, por lo tanto, las reivindicaciones adjuntas son para englobar dentro de su alcance todos esos cambios y modificaciones como dentro del verdadero alcance de esta invención. Por otra parte, aunque la invención se ha mostrado y descrito particularmente con referencia a estas realizaciones específicas, se comprenderá por los expertos en la materia que lo anterior y otros cambios en la forma y los detalles pueden efectuarse en las mismas sin apartarse del alcance de la invención.

REIVINDICACIONES

1. Un aparato para asegurar el acceso a una red, comprendiendo el aparato;

un medio de extracción (220) para extraer de un paquete un identificador de grupo de usuarios fuente (400) del paquete;

un medio de recuperación (220) para recuperar, de una base de información de reenvío, un identificador de grupo de usuarios de destino (410) del paquete; y

un medio de determinación de permiso (220) para determinar los permisos aplicables para el paquete utilizando el identificador de grupo de usuarios fuente y el identificador de grupo de usuarios de destino del paquete para determinar los permisos que se aplican al paquete, en el que la utilización del identificador de grupo de usuarios fuente y el identificador de grupo de usuarios de destino comprende indexar una matriz de control de acceso con el identificador de grupo de usuarios fuente y el identificador de grupo de usuarios de destino para proporcionar una lista de permisos permitidos; y

un medio para comprobar los permisos en una comprobación de control de acceso basado en roles.

2. El aparato de la reivindicación 1, que comprende además:

un medio para poblar una lista de control de acceso con el identificador de grupo de usuarios de destino en el que el grupo de usuarios de destino identifica un grupo de usuarios de destino de un destino.

3. El aparato de la reivindicación 1, que comprende además:

un medio para determinar el identificador de grupo de usuarios de destino buscando

el identificador de grupo de usuarios de destino en una lista de control de acceso.

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

un medio para poblar una lista de control de acceso con el identificador de grupo de usuarios de destino.

5. El aparato de la reivindicación 4, en el que:

el medio para comparar y el medio para poblar están incluidos en el dispositivo de red.

6. El aparato de la reivindicación 5, en el que el medio para poblar comprende además:

un medio para recibir de otro dispositivo de red un mensaje de autenticación que incluye el identificador de grupo de usuarios fuente.

7. Un dispositivo de red que comprende:

un aparato según cualquiera de las reivindicaciones 1 a 6 implementado utilizando una lista de control de acceso; y

una memoria

en el que:

la memoria está configurada para almacenar la lista de control de acceso y para recibir un identificador de grupo de usuarios recibido por la memoria;

la lista de control de acceso comprende una entrada de lista de control de acceso;

la entrada de lista de control de acceso comprende un campo de grupo de usuarios; y,

el medio para comparar comprende la memoria configurada para soportar una comparación de un identificador de

grupo de usuarios almacenado en el campo de grupo de usuarios y el identificador de grupo de usuarios recibido por la memoria.

8. El dispositivo de red de la reivindicación 7, en el que la lista de control de acceso comprende una o una pluralidad de entradas de lista de control de acceso.

9. El dispositivo de red de la reivindicación 8, en el que cada una de las entradas de lista de control de acceso comprende:

un campo de etiqueta de flujo;

en el que el campo de etiqueta de flujo permite a la entrada de lista de control de acceso ser identificada como una entrada de lista de control de acceso basado en roles.

10. El dispositivo de red de la reivindicación 9, en el que cada una de las entradas de lista de control de acceso comprende además:

un campo de grupo de usuarios;

en el que el campo de grupo de usuarios permite además a la entrada de lista de control de acceso ser identificada como una entrada de lista de control de acceso basado en roles.

11. El dispositivo de red de la reivindicación 10, en el que cada una de las entradas de lista de control de acceso comprende además:

un campo de grupo de usuarios fuente; y,
un campo de grupo de usuarios de destino.

12. El dispositivo de red de la reivindicación 11, en el que:

el campo de grupo de usuarios fuente almacena el identificador de grupo de usuarios fuente; y,
el identificador de grupo de usuarios fuente identifica un grupo de usuarios de una fuente de un paquete procesado utilizando la lista de control de acceso.

13. El dispositivo de red de la reivindicación 11 o 12, en el que:

el campo de grupo de usuarios de destino almacena un identificador de grupo de usuarios de destino;

y,

el identificador de grupo de usuarios de destino identifica un grupo de usuarios de destino de un destino de un paquete procesado utilizando la lista de control de acceso.

14. Un procedimiento de determinación de permisos aplicables para un paquete dado para asegurar el acceso a una red que comprende: tomar como entradas a un procedimiento de determinación de permiso un grupo de usuarios fuente (400) y un grupo de usuarios de destino (410) del paquete; determinar una lista de permisos (420) indexando una matriz de control de acceso con el grupo de usuarios fuente y el grupo de usuarios de destino para proporcionar una lista de permisos permitidos; y, comprobar los permisos en una comprobación de control de acceso basado roles (430).

15. El procedimiento de la reivindicación 14, en el que:

el identificador de grupo de usuarios de destino es almacenado en una entrada de lista de control de acceso basado en roles de la lista de control de acceso.

16. El procedimiento de la reivindicación 14 o 15, en el que:

el grupo de usuarios fuente es asignado a una fuente del paquete basándose en un rol de la fuente; y,
el grupo de usuarios de destino es asignado al destino basándose en un rol del destino.

17. El procedimiento de la reivindicación 16, que comprende además:

determinar el grupo de usuarios de destino buscando el grupo de usuarios de destino en una lista de control de acceso.

18. El procedimiento de la reivindicación 17, en el que:

el identificador de grupo de usuarios de destino es almacenado en una entrada de lista de control de acceso basado en roles de la lista de control de acceso.

19. El procedimiento de la reivindicación 17, que comprende además:

poblar la lista de control de acceso con un identificador de grupo de usuarios de destino, que identifica el grupo de usuarios de destino.

20. El procedimiento de cualquiera de las reivindicaciones 15 a 19, que comprende además:

poblar un tabla de reenvío con un identificador de grupo de usuarios fuente que identifica el grupo de usuarios del paquete.

21. Un medio legible por ordenador que lleva instrucciones para configurar un sistema informático para llevar a cabo un procedimiento de acuerdo con cualquiera de las reivindicaciones 14 a 20.

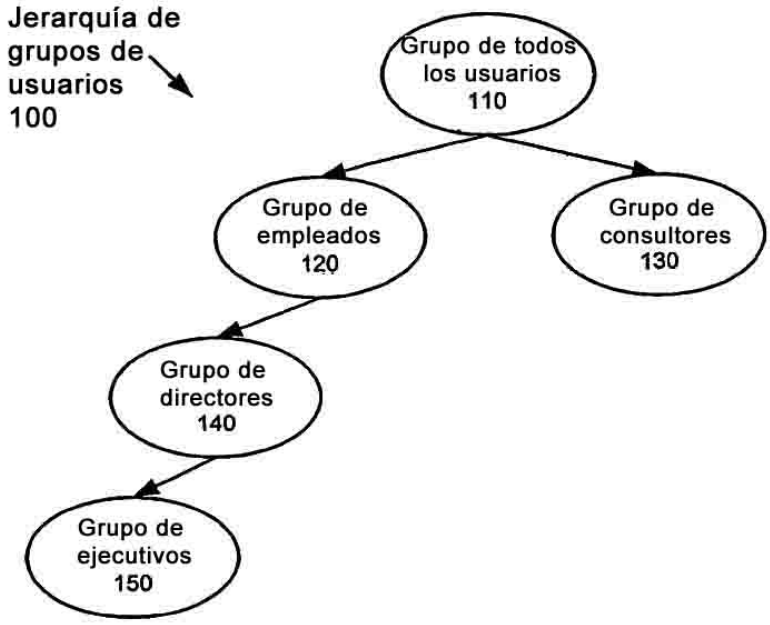
Jerarquía de grupos de usuarios 100
Grupo de todos los usuarios 110
Grupo de empleados 120
Grupo de consultores 130
Grupo de directores 140
Grupo de ejecutivos 150

Fig. 1A

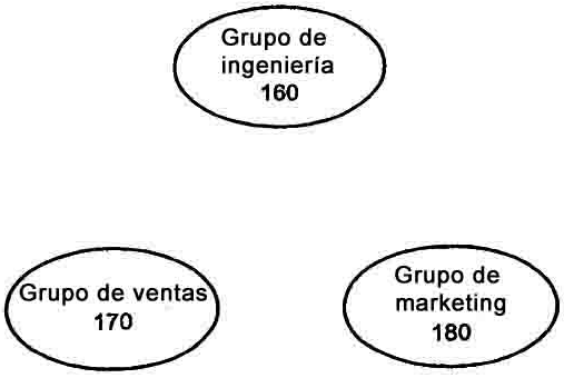
Grupo de ingeniería 160
Grupo de ventas 170
Grupo de marketing 180

Fig. 1B

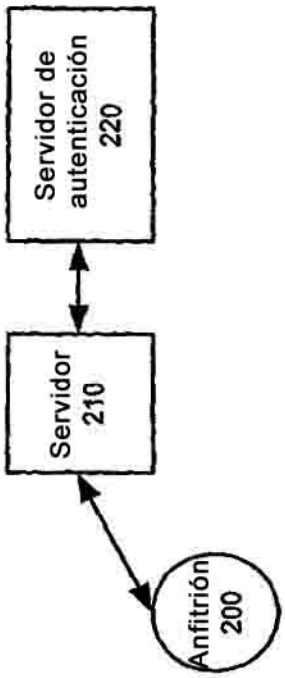
Servidor de autenticación 220
Servidor 210
Anfitrión 200

Fig. 2

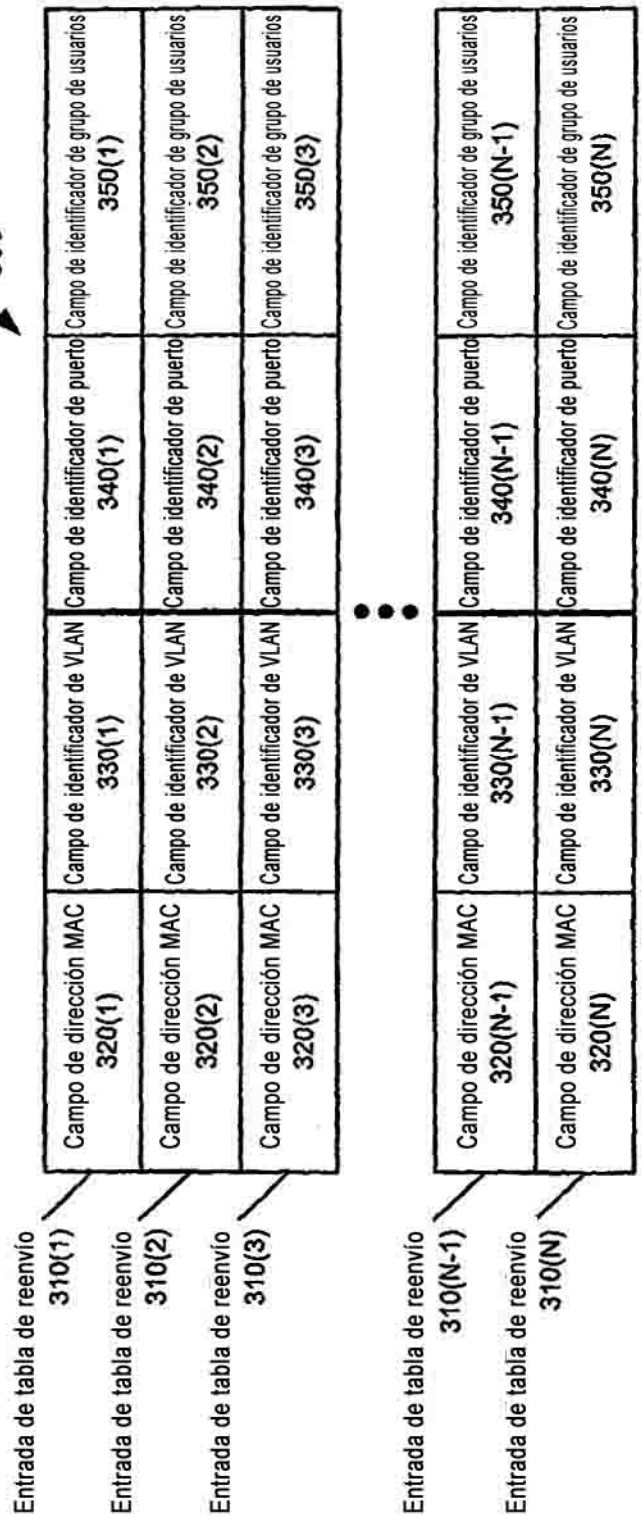
Tabla de reenvío
300
Entrada de tabla de reenvío 310(1)
Campo de dirección MAC 320(1)
Campo de identificador de VLAN 330(1)
Campo de identificador de puerto 340(1)
Campo de identificador de grupo de usuarios 350(1)
Entrada de tabla de reenvío 310(2)
Campo de dirección MAC 320(2)
Campo de identificador de VLAN 330(2)
Campo de identificador de puerto 340(2)
Campo de identificador de grupo de usuarios 350(2)
Entrada de tabla de reenvío 310(3)
Campo de dirección MAC 320(3)
Campo de identificador de VLAN 330(3)
Campo de identificador de puerto 340(3)
Campo de identificador de grupo de usuarios 350(3)
Entrada de tabla de reenvío 310(N-1)
Campo de dirección MAC 320(N-1)
Campo de identificador de VLAN 330(N-1)
Campo de identificador de puerto 340(N-1)
Campo de identificador de grupo de usuarios 350(N-1)
Entrada de tabla de reenvío 310(N)
Campo de dirección MAC 320(N)
Campo de identificador de VLAN 330(N)
Campo de identificador de puerto 340(N)
Campo de identificador de grupo de usuarios 350(N)

Fig. 3

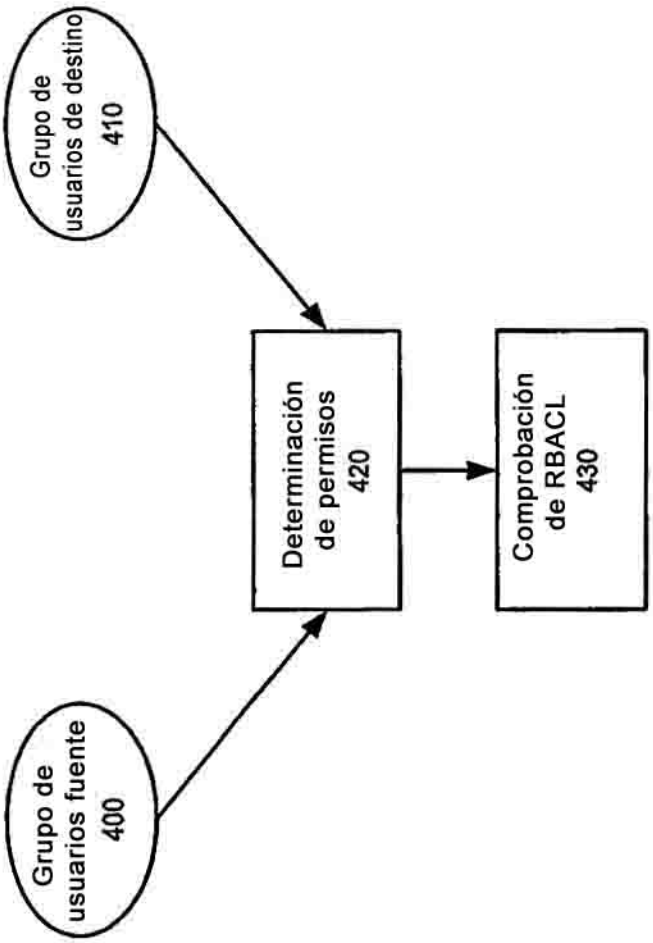
Grupo de usuarios de destino 410
Grupo de usuarios fuente 400
Determinación de permisos 420
Comprobación de RBACL 430

Fig. 4

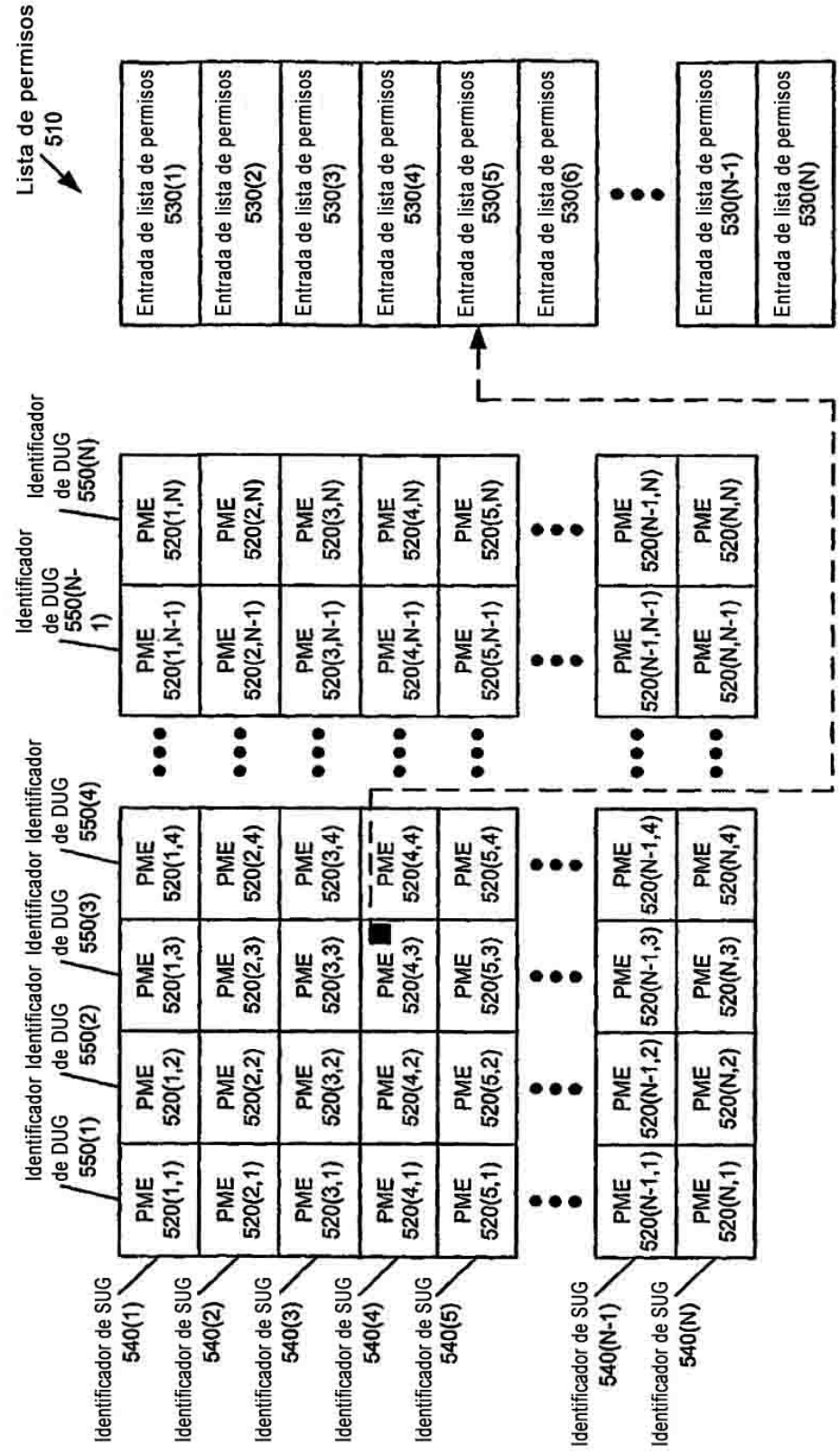
Lista de permisos
510
Entrada de lista de permisos 530(1)
Entrada de lista de permisos 530(2)
Entrada de lista de permisos 530(3)
Entrada de lista de permisos 530(4)
Entrada de lista de permisos 530(5)
Entrada de lista de permisos 530(6)
Entrada de lista de permisos 530(N-1)
Entrada de lista de permisos 530(N)
Identificador de DUG 550(1)
Identificador de DUG 550(2)
Identificador de DUG 550(3)
Identificador de DUG 550(4)
Identificador de DUG 550(N-1)
Identificador de DUG 550(N)
Identificador de SUG 540(1)
Identificador de SUG 540(2)
Identificador de SUG 540(3)
Identificador de SUG 540(4)
Identificador de SUG 540(5)
Identificador de SUG 540(N-1)
Identificador de SUG 540(N)
PME 520(1,1)
PME 520(1,2)
PME 520(1,3)
PME 520(1,4)
PME 520(1,N-1)
PME 520(1,N)
PME 520(2,1)
PME 520(2,2)
PME 520(2,3)
PME 520(2,4)
PME 520(2,N-1)
PME 520(2,N)
PME 520(3,1)
PME 520(3,2)
PME 520(3,3)
PME 520(3,4)
PME 520(3,N-1)
PME 520(3,N)
PME 520(4,1)
PME 520(4,2)
PME 520(4,3)
PME 520(4,4)
PME 520(4,N-1)
PME 520(4,N)
PME 520(5,1)
PME 520(5,2)
PME 520(5,3)
PME 520(5,4)
PME 520(5,N-1)
PME 520(5,N)
PME 520(N-1,1)
PME 520(N-1,2)
PME 520(N-1,3)
PME 520(N-1,4)
PME 520(N-1,N-1)
PME 520(N-1,N)
PME 520(N,1)
PME 520(N,2)
PME 520(N,3)
PME 520(N,4)
PME 520(N,N-1)
PME 520(N,N)

Fig. 5

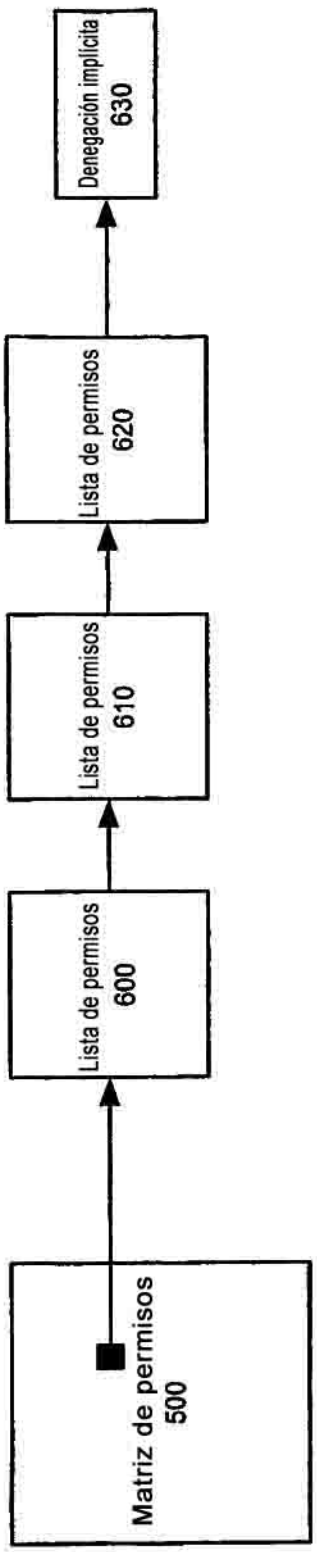
Matriz de permisos
500
Lista de permisos
600
Lista de permisos
610
Lista de permisos
620
Denegación implícita
630

Fig. 6A

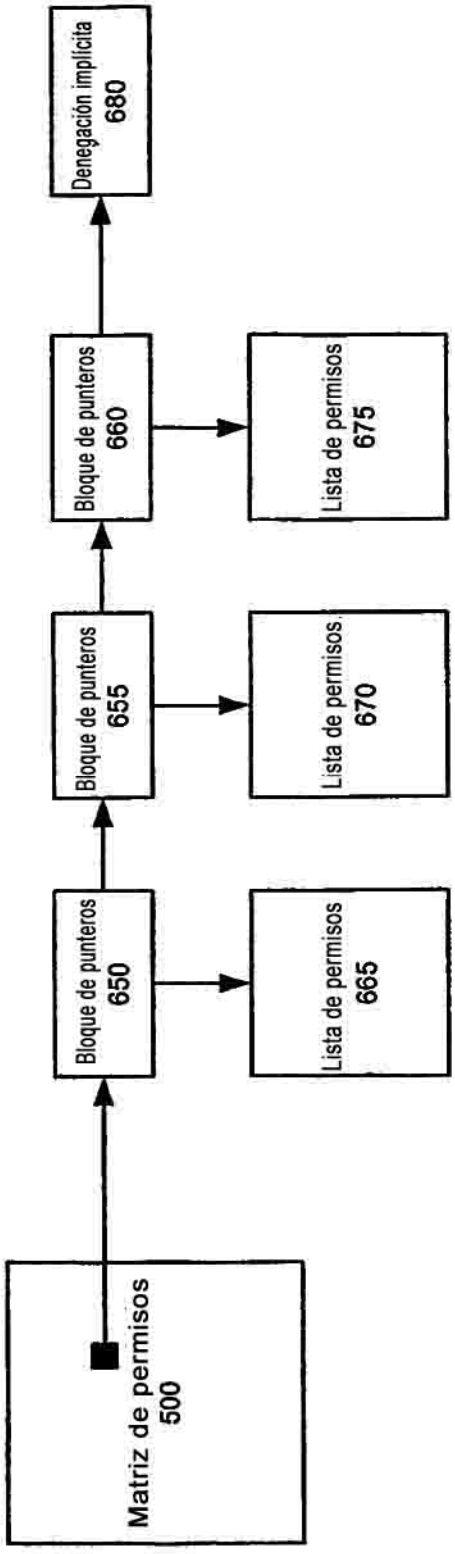
Matriz de permisos
500
Bloque de punteros
650
Lista de permisos
665
Bloque de punteros
655
Lista de permisos
670
Bloque de punteros
660
Lista de permisos
675
Denegación implícita
680

Fig. 6B

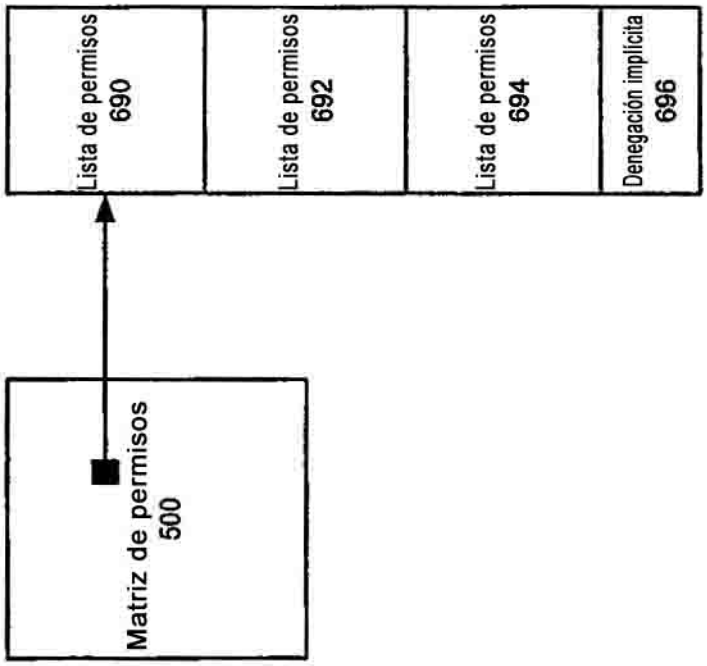
Lista de permisos
690
Lista de permisos
692
Lista de permisos
694
Denegación implícita
696
Matriz de permisos
500

Fig. 6C

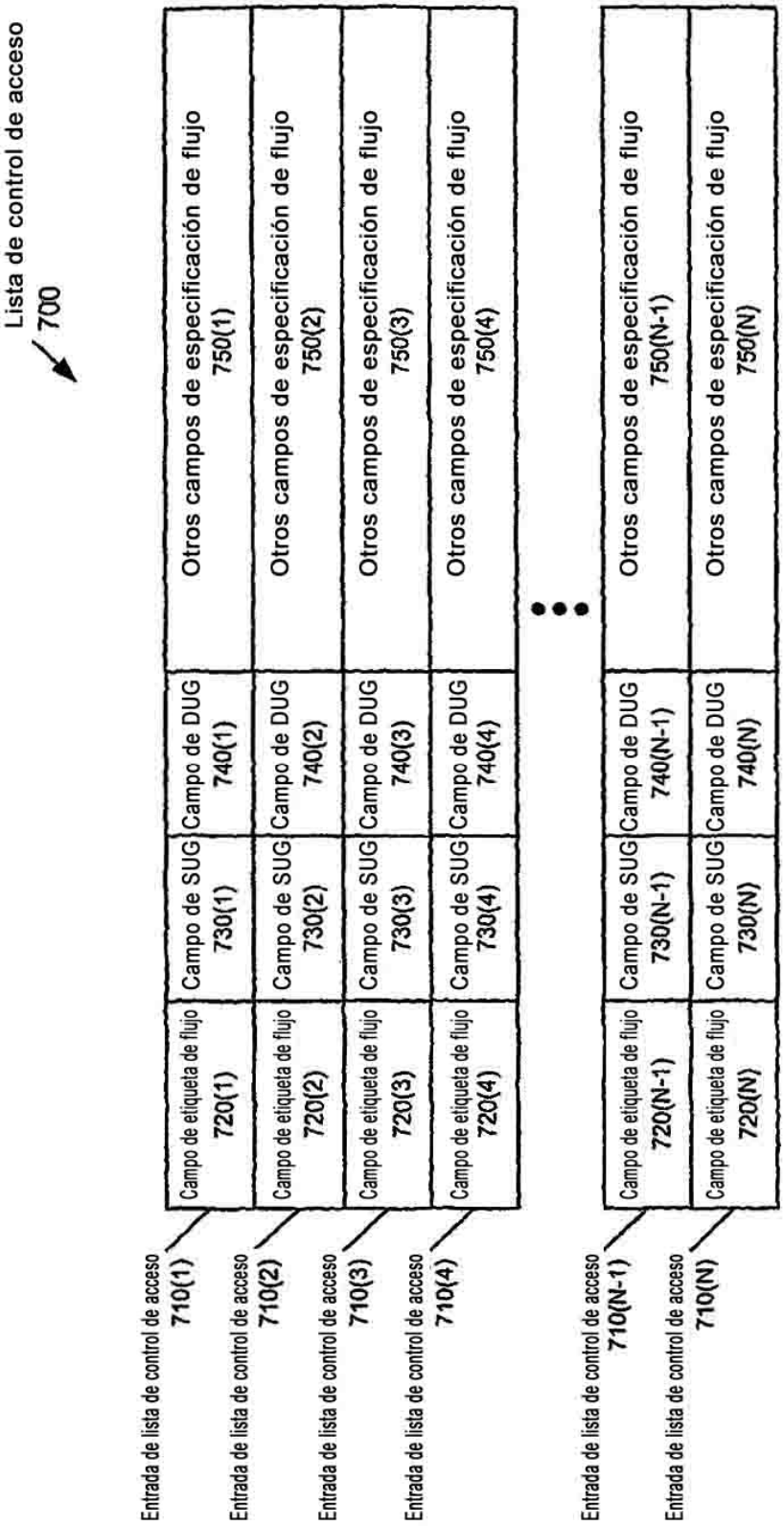
Lista de control de acceso
700
Entrada de lista de control de acceso
710(1)
Campo de etiqueta de flujo
720(1)
Campo de SUG
730(1)
Campo de DUG
740(1)
Otros campos de especificación de flujo
750(1)
Entrada de lista de control de acceso
710(2)
Campo de etiqueta de flujo
720(2)
Campo de SUG
730(2)
Campo de DUG
740(2)
Otros campos de especificación de flujo
750(2)
Entrada de lista de control de acceso
710(3)
Campo de etiqueta de flujo
720(3)
Campo de SUG
730(3)
Campo de DUG
740(3)
Otros campos de especificación de flujo
750(3)
Entrada de lista de control de acceso
710(4)
Campo de etiqueta de flujo
720(4)
Campo de SUG
730(4)
Campo de DUG
740(4)
Otros campos de especificación de flujo
750(4)
Entrada de lista de control de acceso
710(N-1)
Campo de etiqueta de flujo
720(N-1)
Campo de SUG
730(N-1)
Campo de DUG
740(N-1)
Otros campos de especificación de flujo
750(N-1)
Entrada de lista de control de acceso
710(N)
Campo de etiqueta de flujo
720(N)
Campo de SUG
730(N)
Campo de DUG
740(N)
Otros campos de especificación de flujo
750(N)

Fig. 7

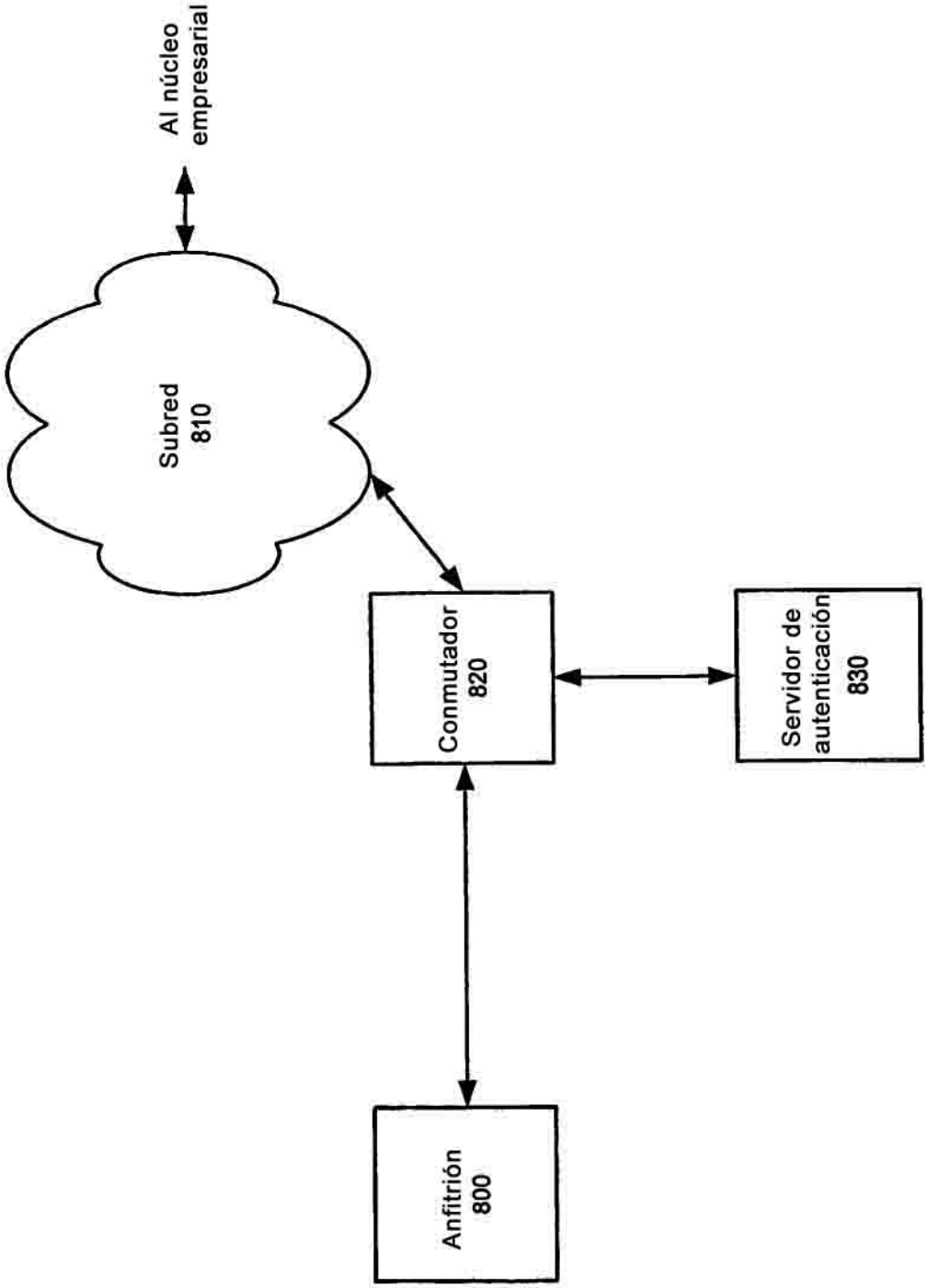
Al núcleo empresarial
Subred 810
Conmutador 820
Servidor de autenticación 830
Anfitrión 800

Fig. 8A

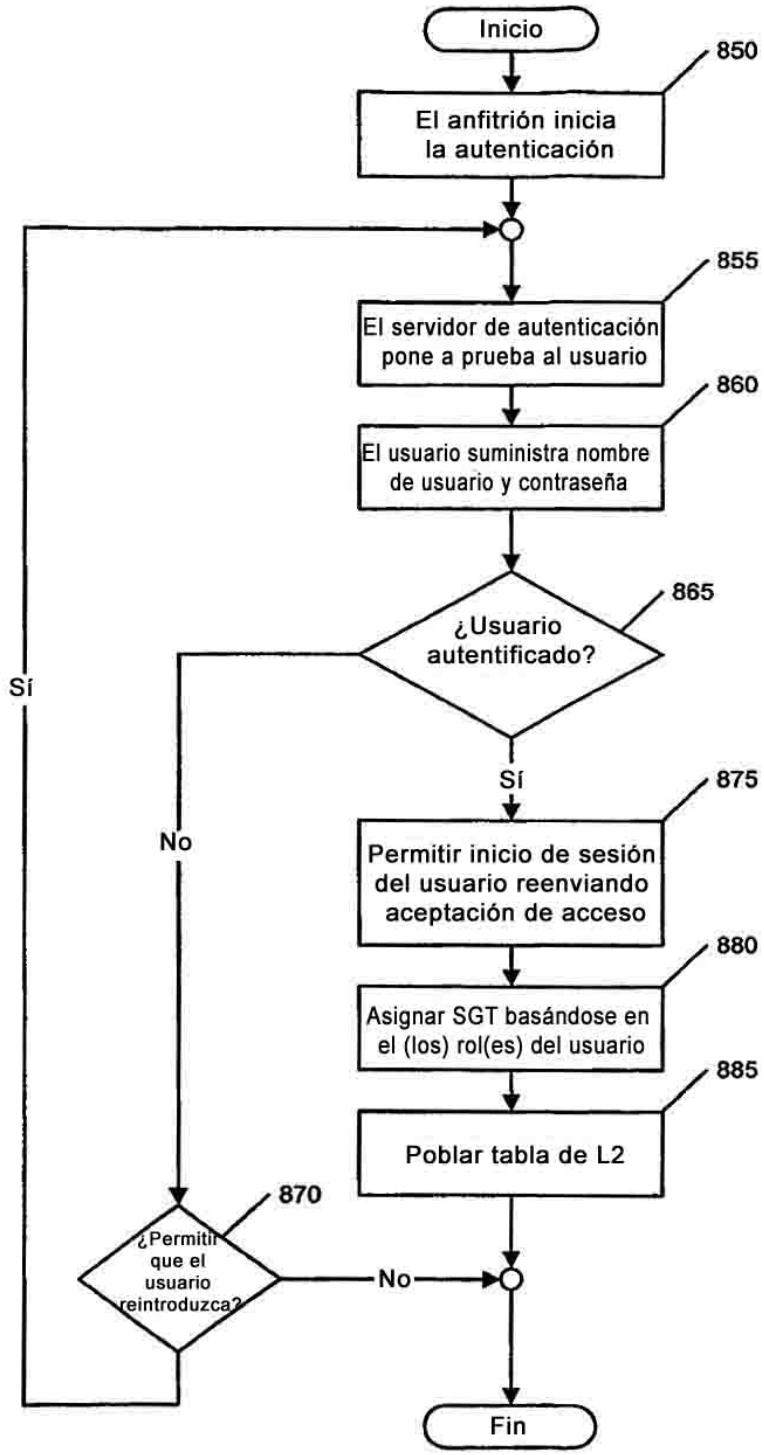
Inicio
850
El anfitrión inicia la autenticación
855
El servidor de autenticación pone a prueba al usuario
860
El usuario suministra nombre de usuario y contraseña
865
¿Usuario autentificado?
Sí
No
875
Permitir inicio de sesión del usuario reenviando aceptación de acceso
880
Asignar SGT basándose en el (los) rol(es) del usuario
885
Poblar tabla de L2
870
¿Permitir que el usuario reintroduzca?
No
Sí
Fin

Fig. 8B

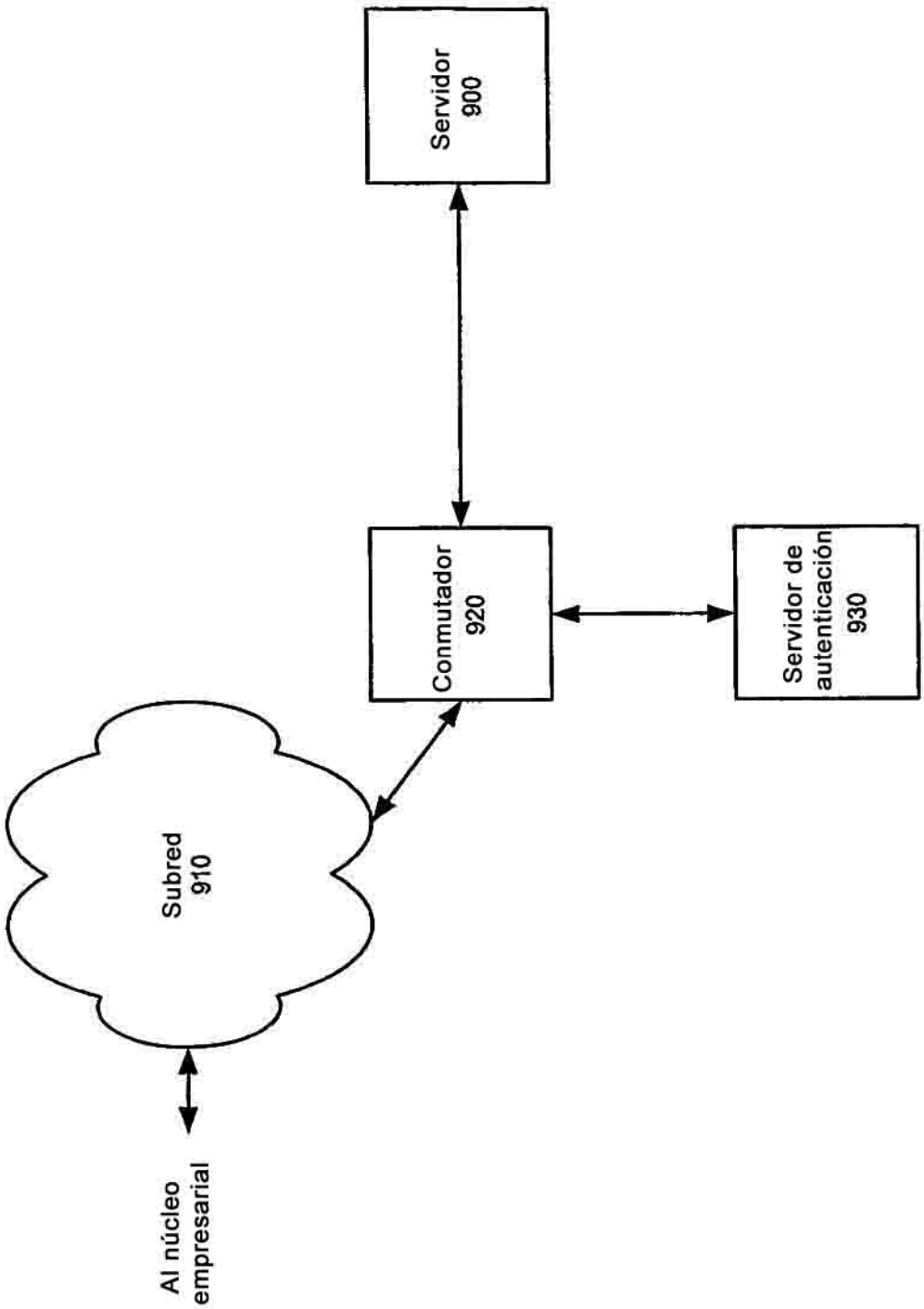
Servidor
900
Conmutador
920
Servidor de
autenticación
930
Subred
910
Al núcleo
empresarial

Fig. 9A

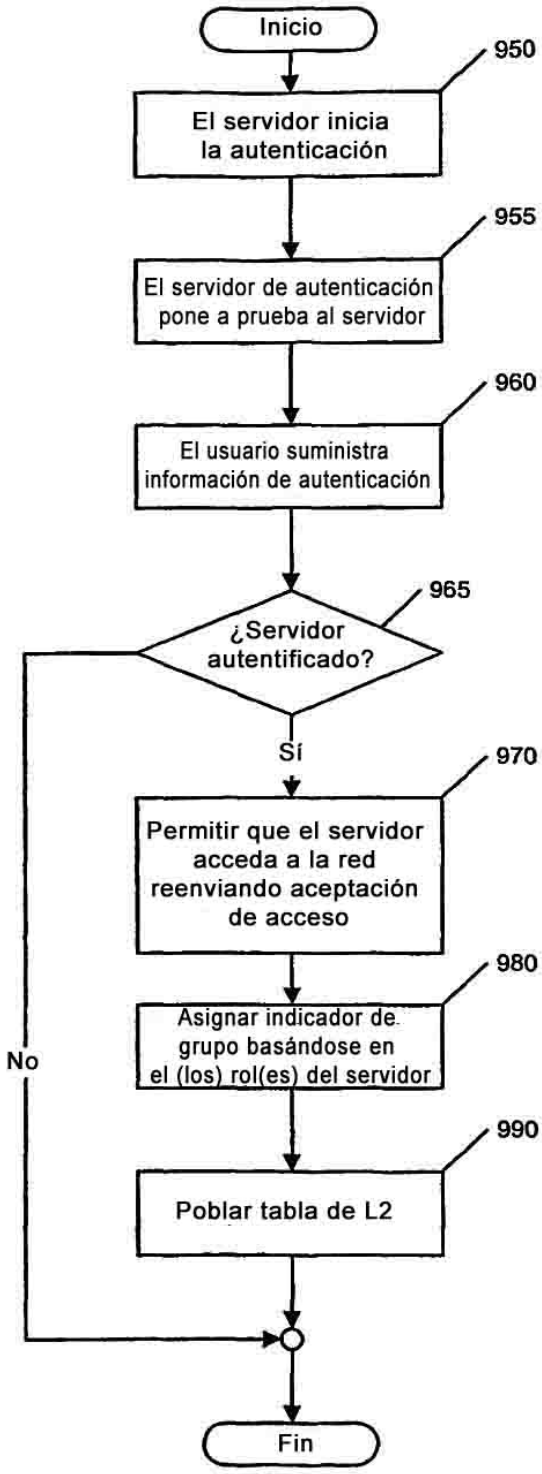
Inicio
950
El servidor inicia la autenticación
955
El servidor de autenticación pone a prueba al servidor
960
El usuario suministra información de autenticación
965
¿Servidor autentificado?
Sí
No
970
Permitir que el servidor acceda a la red reenviando aceptación de acceso
980
Asignar indicador de grupo basándose en el (los) rol(es) del servidor
990
Poblar tabla de L2
Fin

Fig. 9B

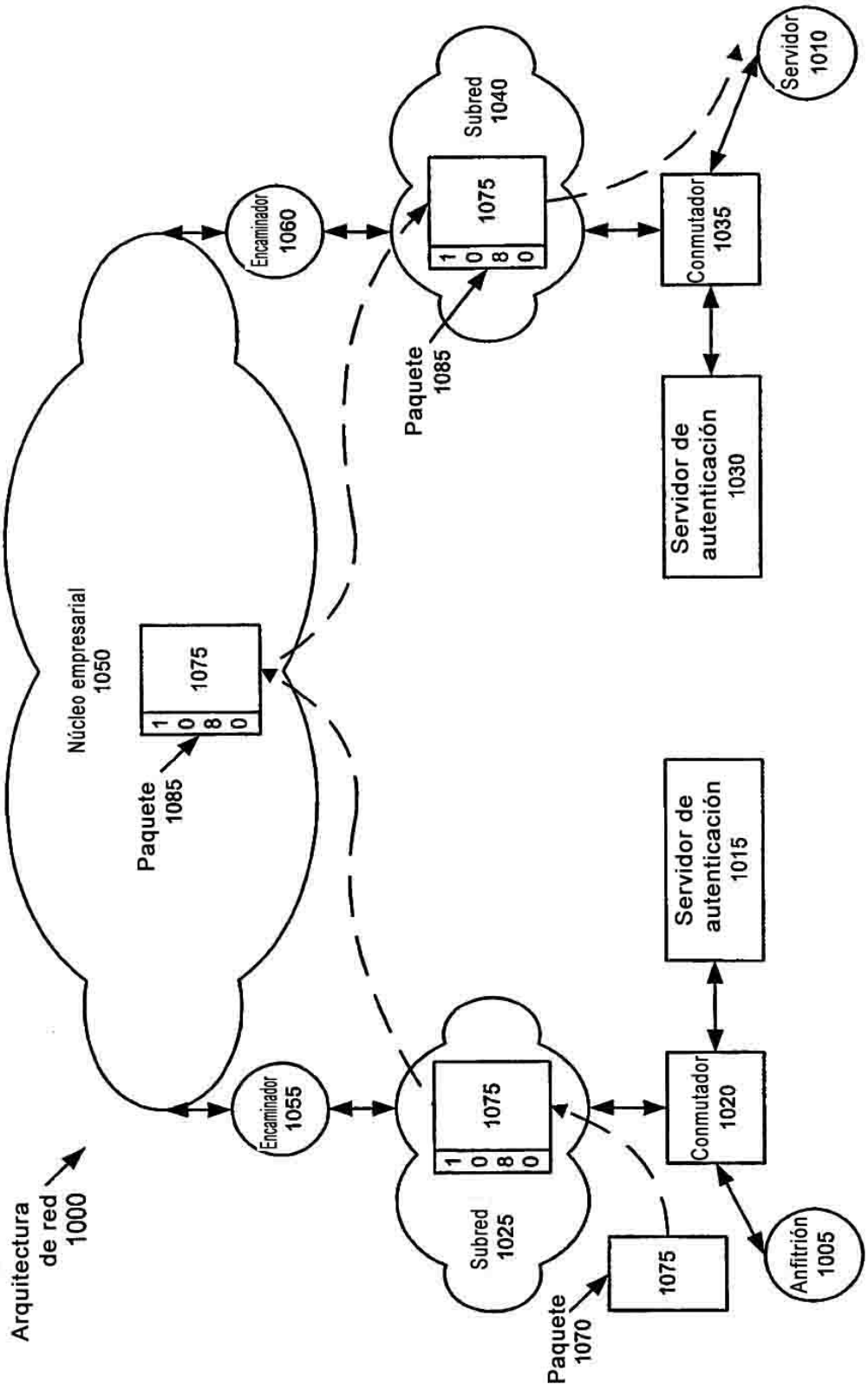
Arquitectura de red 1000
Núcleo empresarial 1050
Encaminador 1055
Encaminador 1060
Subred 1025
Subred 1040
1075
1080
Paquete 1085
Paquete 1070
Conmutador 1020
Conmutador 1035
Servidor de autenticación 1015
Servidor de autenticación 1030
Servidor 1010
Anfitrión 1005

Fig. 10

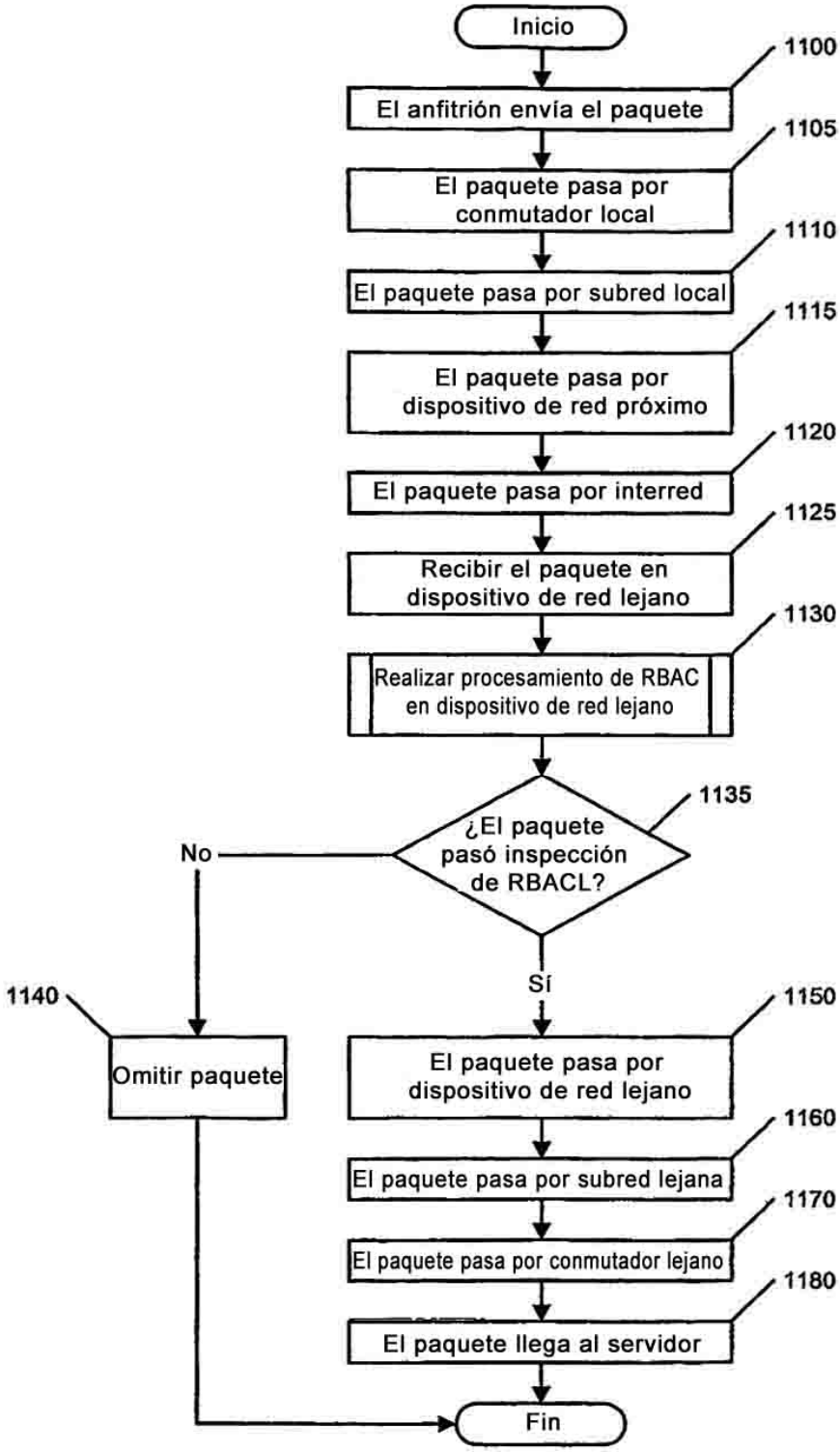
Inicio
1100
El anfitrión envía el paquete
1105
El paquete pasa por conmutador local
1110
El paquete pasa por subred local
1115
El paquete pasa por dispositivo de red próximo
1120
El paquete pasa por interred
1125
Recibir el paquete en dispositivo de red lejano
1130
Realizar procesamiento de RBAC en dispositivo de red lejano
1135
¿El paquete pasó inspección de RBACL?
No
Sí
1140
Omitir paquete
1150
El paquete pasa por dispositivo de red lejano
1160
El paquete pasa por subred lejana
1170
El paquete pasa por conmutador lejano
1180
El paquete llega al servidor
Fin

Fig. 11

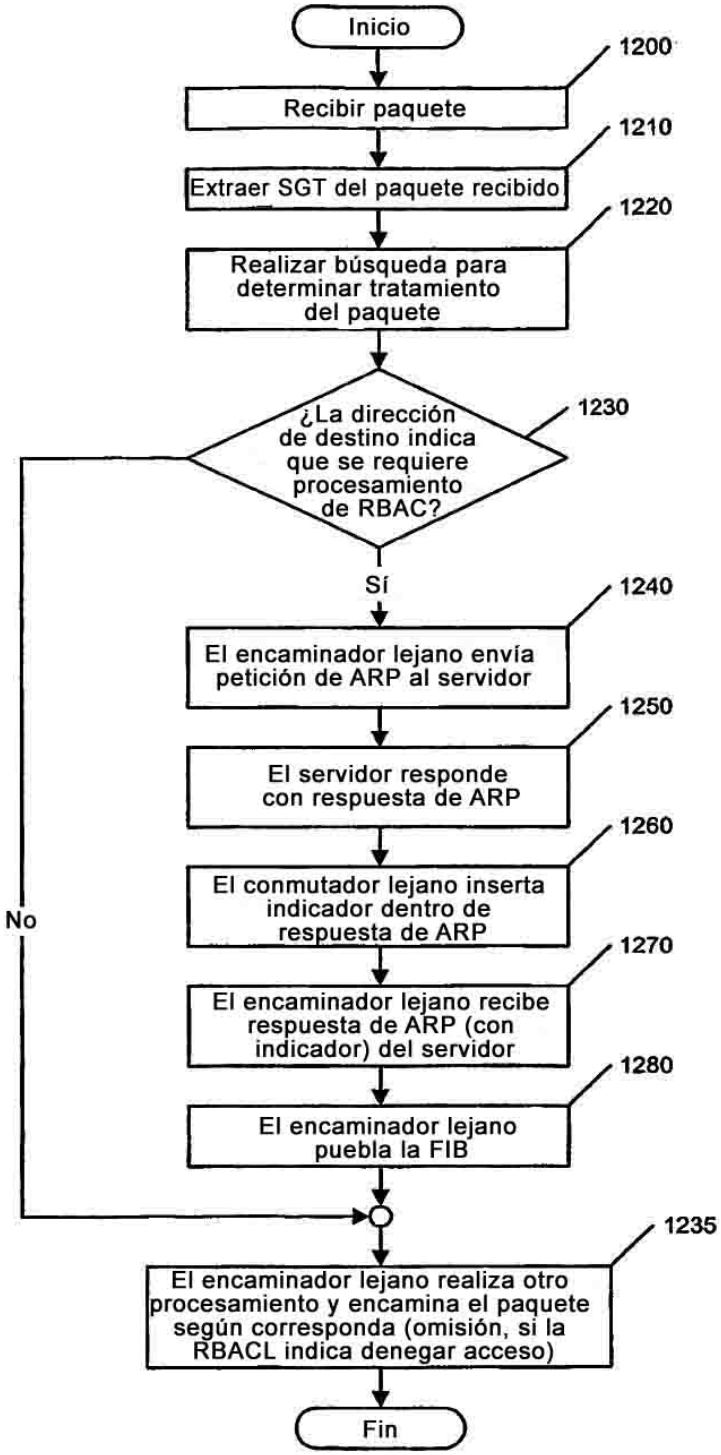
Inicio
1200
Recibir paquete
1210
Extraer SGT del paquete recibido
1220
Realizar búsqueda para determinar tratamiento del paquete
1230
¿La dirección de destino indica que se requiere procesamiento de RBAC?
Sí
No
1240
El encaminador lejano envía petición de ARP al servidor
1250
El servidor responde con respuesta de ARP
1260
El conmutador lejano inserta indicador dentro de respuesta de ARP
1270
El encaminador lejano recibe respuesta de ARP (con indicador) del servidor
1280
El encaminador lejano puebla la FIB
1235
El encaminador lejano realiza otro procesamiento y encamina el paquete según corresponda (omisión, si la RBACL indica denegar acceso)
Fin

Fig. 12

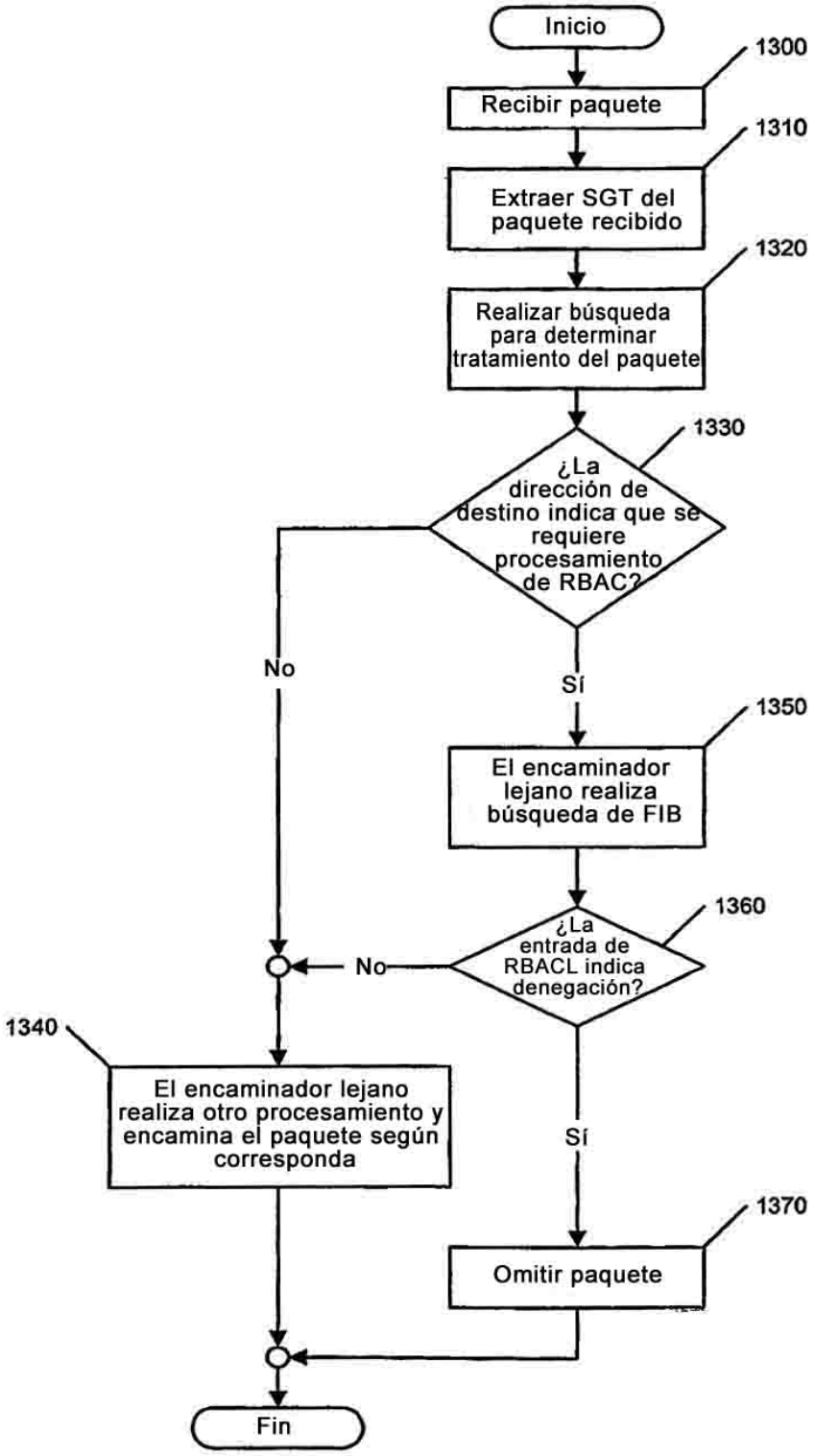
Inicio
1300
Recibir paquete
1310
Extraer SGT del paquete recibido
1320
Realizar búsqueda para determinar tratamiento del paquete
1330
¿La dirección de destino indica que se requiere procesamiento de RBAC?
No
Sí
1350
El encaminador lejano realiza búsqueda de FIB
1360
¿La entrada de RBACL indica denegación?
No
Sí
1340
El encaminador lejano realiza otro procesamiento y encamina el paquete según corresponda
1370
Omitir paquete
Fin

Fig. 13


Inicio
1400
Aplicar ACL de seguridad de entrada
1410
Aplicar características de entrada
1420
Realizar comprobación de RPF
1430
Realizar búsqueda de encaminamiento
1440
Realizar búsqueda de ACL basada en roles
1450
Aplicar características de salida
1460
Aplicar ACL de seguridad de salida
1470
Aplicar características de salida adicionales
Fin

Fig. 14