(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 574 788**

(51) Int. CI.:

H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.12.2008 E 08863780 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.04.2016 EP 2241058**

(54) Título: **Método para configurar ACL en dispositivo de red basándose en información de flujo**

(30) Prioridad:

18.12.2007 US 910

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.06.2016

(73) Titular/es:

SOLARWINDS WORLDWIDE, LLC (100.0%)
7171 Southwest Parkway, Building 400
Austin, TX 78735, US

(72) Inventor/es:

NEWMAN, GREG

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método para configurar ACL en dispositivo de red basándose en información de flujo

Campo de la invención

La presente invención se refiere al uso de datos de flujos de red exportados de encaminadores de red para proporcionar información sobre el tráfico entrante/saliente del dispositivo. Los encaminadores de red se pueden configurar para autorizar o denegar diversos tipos de tráfico de red entre dos dispositivos de red cuyo tráfico transita a través del encaminador. El método presentado describe la creación dinámica y la aplicación de listas de control de acceso en el encaminador de la información obtenida a partir de la información de flujo de red exportada por el encaminador de red.

Antecedentes de la invención

Los datos de uso de red son útiles para muchas funciones de negocio importantes, tales como facturación de abonados, mercadotecnia y atención al cliente, desarrollo de productos, gestión de operaciones de red, planificación de capacidad de la red y de sistemas y seguridad. Los datos de uso de red no incluyen la información real intercambiada en una sesión de comunicaciones entre las partes, sino que más bien incluye numerosos registros de detalle de uso, conocidos como “registros de flujo” que contienen uno o más tipos de metadatos (es decir, “datos sobre datos”). Los protocolos de registros de flujo de redes conocidos incluyen Netflow®, sFlow®, jFlow®, cFlow® o Netstream®. Tal como se usa en la presente descripción, un registro de flujo se define como una pequeña unidad de medida de uso unidireccional de red por una cadena de paquetes de IP que comparten parámetros comunes de origen y de destino durante un intervalo de tiempo.

Los tipos de metadatos incluidos dentro de cada registro de flujo varían basándose en el tipo de servicio y de red involucrado y, en algunos casos, basándose en el dispositivo de red particular que proporciona los registros de flujo, En general, un registro de flujo proporciona información de uso detallado sobre un evento particular o una conexión de comunicaciones entre las partes, tales como el tiempo de inicio y de fin de la conexión, la fuente (o el originador) de los datos que se están transportando, el destino o receptor de los datos y la cantidad de datos transferidos. Un registro de flujo resume información de uso para periodos muy cortos de tiempo (desde milisegundos hasta segundos, ocasionalmente minutos). Dependiendo del tipo de servicio y de red involucrado, un registro de flujo puede incluir también información sobre el protocolo de transferencia, el tipo de datos transferido, el tipo de servicio (ToS, *type of service*) proporcionado, etc. En las redes de telefonía, los registros de flujo que constituyen la información de uso se conocen como registros de detalle de llamada (CDR, *call detail record*).

En la supervisión de redes, los registros de flujo de red se recopilan, se almacenan y se analizan para producir un resultado significativo. Los sistemas de análisis de uso de red procesan estos registros de flujo y generan informes o archivos de datos resumidos que soportan diversas funciones de negocio. Los sistemas de análisis de uso de red proporcionan información sobre cómo se están usando, y por quién, los servicios de una red. Los sistemas de análisis de uso de red se pueden usar también para identificar (o predecir) cuestiones relacionadas con la satisfacción del cliente, tales como las causadas por la congestión de la red y por abusos en la seguridad de la red. En un ejemplo, el uso y el desempeño de la red, como una función del comportamiento de uso del abonado, se pueden supervisar para rastrear la experiencia de un usuario, para predecir la capacidad futura de la red o para identificar indicativos de comportamiento de uso de fraude, robo y abuso de red.

En la seguridad informática, una lista de control de acceso (ACL, *access control list*) es una lista de permisos adjunta a un objeto. De manera más específica, ACL en redes se refiere a una lista de reglas que detalla reglas de filtrado de tráfico. Las ACL pueden permitir o denegar el tráfico a través de un dispositivo de red. Solo los encaminadores y los servidores de seguridad pueden tener ACL de red. Las listas de control de acceso se pueden configurar en general para controlar tráfico tanto de entrada como de salida.

Las ACL son una manera para controlar el tráfico de red al limitar el acceso del usuario y del dispositivo hacia y desde direcciones y/o puertos no deseados. Las ACL filtran el tráfico de red al controlar si los paquetes encaminados se reenvían o se bloquean, por lo general en una interfaz de encaminador, a pesar de que otros dispositivos puedan filtrar paquetes. El encaminador examina cada paquete para determinar si reenviar o soltar el paquete, basándose en los criterios especificados dentro de las listas de acceso. Un criterio de una lista de control de acceso podría ser la dirección de origen del tráfico o la dirección de destino del tráfico, el puerto objetivo o el protocolo, o alguna combinación de los mismos. Por lo general las direcciones de Protocolo de Internet (IP, *Internet Protocol*) sirven como identificadores del dispositivo de origen en una red basada en IP. Las listas de control de acceso permiten accesos diferenciados basándose en este identificador de IP dentro de la red.

A pesar de que las ACL dan servicio a funciones útiles, establecer las ACL puede ser muy laborioso. En particular, comúnmente las ACL se programan manualmente. Además, la selección de direcciones de IP para colocar en las ACL puede ser arbitraria e impredecible.

En particular, muchas redes de IP autónomas o de empresa son grandes, complejas y dinámicas, lo que las hace difíciles de gestionar. Las tareas de gestión de redes tales como supervisar el tráfico en una red, analizar el desempeño de la red o reconfigurar la red para un mejor desempeño requieren información sobre la red. No obstante, debido a que las grandes redes de IP son altamente dinámicas, es difícil adquirir información útil para muchas tareas de gestión de redes. Considérese que una red de IP grande puede tener decenas de miles de nodos y centenares de encaminadores y pasarelas. Una red corporativa grande puede tener 300.000 nodos y 2.500 encaminadores. En ocasiones, los encaminadores, las pasarelas, los conmutadores y otros dispositivos de red fallan, se desconectan o retornan a servicio. Los enlaces a menudo fallan, retornan a servicio o se deteriora su desempeño. Por ejemplo, un enlace de microondas o de satélite puede experimentar interferencia que reduce su ancho de banda. Protocolos tales como OSPF y BGP que se usan para encaminar tráfico en grandes redes de IP son dinámicos y cambian las trayectorias de encaminamiento en una red grande a medida que cambian las condiciones en la red. Incluso a redes relativamente estables les puede llevar un tiempo prolongado alcanzar un estado de convergencia de encaminamiento. Por diseño, la trayectoria de comunicación entre dos ordenadores en una red de IP puede cambiar aun durante el periodo de una sola conexión entre ellas. A la vista de estos factores y de otros que se analizarán a continuación, ha sido difícil para las herramientas de gestión de redes obtener una información que, con el tiempo, esboce una imagen algo completa y precisa de una red.

La complejidad de las redes hace que la gestión de las redes sea costosa debido a que esta ha requerido de la intervención manual por parte de operadores humanos cualificados. La configuración y gestión de una red de IP grande ha sido difícil de automatizar. Esta necesidad de estrecha vigilancia humana ha llevado a muchos operadores a adoptar una política conservadora de preferir la estabilidad de red frente a la reconfiguración frecuente para optimizar el desempeño de la red. En consecuencia, otro problema en el campo de la gestión de redes ha sido que las redes de IP mantienen unas configuraciones de red subóptimas durante más tiempo del requerido, lo que conduce a un uso ineficiente de costosa capacidad de ancho de banda y a unas latencias de comunicación potencialmente más altas de lo que de lo contrario sería posible. No se han adoptado de forma generalizada unas herramientas para gestión y configuración automatizada.

A pesar de que existen, de hecho, herramientas para gestión de redes, incluyendo la supervisión y el mantenimiento de las ACL, las herramientas no son sofisticadas y tienen muchas deficiencias. La mayor parte de las herramientas de gestión de redes simplemente descubren y sondean dispositivos de red en vivo para generar informes que contienen mapas, valores de contadores, promedios, áreas de tráfico elevado, etcétera. Las herramientas comunes tienden a ignorar las dinámicas globales del comportamiento de redes, concentrándose en unificar centralmente datos potencialmente conflictivos tomados localmente de dispositivos de red individuales. Las herramientas comunes no facilitan a un operador ejecutar una variedad de tareas potencialmente útiles tales como descubrir la trayectoria que un conjunto particular de tráfico toma a través de la red, investigar el comportamiento de la red, investigar el comportamiento de la red en escenarios del tipo ¿qué pasaría si?, supervisar la evolución de la red a medida que tengan lugar fallos y recuperaciones o analizar el tráfico de la red según esté relacionado con aplicaciones o servicios particulares, etcétera.

Tal como se ha descrito en lo que antecede, ha habido intentos para medir el tráfico de red en ordenadores de usuario individuales, pero los datos de tráfico de ordenadores centrales ha sido de alcance limitado y en general no pueden revelar información relacionada con el flujo de tráfico a lo largo de trayectorias particulares en una red de IP. La medición de red de ordenador central o de sistema de extremo no proporciona información útil sobre la topología de la red. También hay herramientas que agregan datos de tráfico de IP en dispositivos de red como encaminadores y conmutadores, por ejemplo, NetFlow® de Cisco Systems. No obstante, estas aproximaciones han probado ser inadecuadas por numerosas razones tales como tráfico opaco (por ejemplo, cifrado, tunelizado), patrones de comunicación de aplicación complejos, artefactos de muestreo, carga en encaminadores introducida por la supervisión, y otras.

Además, las técnicas conocidas para identificar virus son limitadas. Las técnicas conocidas en general buscan los efectos secundarios de los virus, tales como supervisar el uso de recursos de la red e identificar aplicaciones que solicitan una cantidad innaturalmente grande de recursos de la red. No obstante, puede ser difícil diferenciar entre los virus y aplicaciones legítimas que requieren una gran cantidad de recursos de red. Asimismo, los virus se están volviendo más inteligentes para evitar su detección. Por ejemplo, un virus puede permanecer latente en un sistema por algún tiempo, esperando por una señal para iniciar. Por ejemplo, un virus malicioso puede permanecer latente hasta que se adquieren datos confidenciales. Por lo tanto, mientras el virus está esperando para actuar, sería difícil de detectar debido a que este produce unos efectos secundarios mínimos.

El documento US 2006/0282895 A1 divulga una técnica a la que se hace referencia como Rastreo de Sistemas Infectados que proporciona un mecanismo automatizado para crear y desplegar dinámicamente unos controles que reducen la difusión de soporte lógico malicioso usando, por ejemplo, un análisis heurístico.

El documento US 2005/0259654 A1 divulga un método que controla el acceso de un usuario a una red que incluye una pluralidad de ordenadores centrales acoplados entre sí a través de un conmutador de red. El método incluye almacenar en el conmutador de red una lista de control de acceso potenciada que contiene datos en relación con al menos uno de nombres de usuario, nombres de DNS, nombres de dominio y direcciones físicas. Se genera una lista

de control de acceso dinámica a partir de la lista de control de acceso potenciada, con la lista de control de acceso dinámica conteniendo una pluralidad de direcciones de IP que restringen el acceso del usuario a la red.

El documento US 2007/0192862 A1 divulga un sistema y método para segregar de forma automática tráfico perjudicial de otro tráfico en una pluralidad de nodos de red que incluyen conmutadores y encaminadores. El sistema comprende un sistema de detección de intrusiones para determinar la identidad de un intruso y un servidor adaptado para instalar de forma automática una regla de aislamiento sobre los uno o más nodos de red para poner en cuarentena paquetes procedentes del intruso.

Sumario de la invención

En respuesta a estas y otras necesidades, las realizaciones de la presente invención proporcionan un sistema y método para usar registros de flujo de red exportados de encaminadores de red para proporcionar información acerca del tráfico entrante/saliente del dispositivo. Los encaminadores de red se pueden configurar para autorizar o denegar diversos tipos de tráfico de red entre dos dispositivos de red cuyo tráfico transite a través del encaminador. El método presentado describe la creación y aplicación de listas de control de acceso en el encaminador de información obtenida a partir de la información de flujo de red exportada por el encaminador de la red.

De acuerdo con un aspecto de la invención, se proporciona un sistema tal como se define en la reivindicación 1.

De acuerdo con otro aspecto de la invención, se proporciona un método tal como se define en la reivindicación 6.

En las reivindicaciones dependientes se exponen aspectos y características adicionales de la invención.

Un sistema proporciona controlar dinámicamente una red, incluyendo el sistema: un almacenamiento de registros de flujo configurado para recibir registros de flujo de la red y para agregar los registros de flujo; una herramienta de análisis de datos configurada para recibir los registros de flujo agregados y para analizar los registros de flujo agregados de acuerdo con criterios predefinidos para identificar uno o más direcciones y puertos de red, y un dispositivo de red configurado para recibir las direcciones de red identificadas y para añadir las direcciones y puertos de red identificados a una lista de control de acceso. Opcionalmente, el sistema incluye adicionalmente un almacenamiento de lista de control de acceso opcionalmente configurado para almacenar las direcciones y puertos de red identificados y para proporcionar las direcciones de red identificadas al dispositivo de red. Opcionalmente, cada uno de los registros de flujo incluye una dirección de origen y los registros de flujo se agregan de acuerdo con las direcciones de origen. De lo contrario, los registros de flujo incluyen un tamaño de byte transmitido en cada uno de los flujos asociados, y en donde los criterios predefinidos incluyen el número total de bytes transmitidos en el flujo asociado para cada una de las direcciones de origen. Opcionalmente, un dispositivo de entrada de datos recibe una entrada de un usuario para definir los criterios predefinidos.

Los componentes en la red se pueden supervisar recibiendo registros de flujo de los componentes sobre el tráfico en una red. Los datos que definen criterios para el control de acceso se reciben opcionalmente, y los registros de flujo se analizan usando los criterios de control de acceso. Unas direcciones o rangos de red objetivo y de origen y/o puerto objetivo y de origen que cumplen con los criterios de control de acceso se identifican y presentan al usuario. El usuario puede revisar las direcciones o rangos identificados, y/o los puertos y optar por reenviar estos a uno de los componentes de red. Si se envían, el componente añade la dirección de red y/o el puerto de red identificado a una lista de control de acceso asociada, previniendo la lista de control de acceso que el tráfico alcance la dirección de red y/o puerto identificado. Opcionalmente, los periodos de tiempo para cada lista de control de acceso pueden establecerse para permitir retirar las entradas de la ACL que entraron de forma automática.

De esta manera, la ACL son reglas de filtrado de tráfico aplicadas en un encaminador o en un servidor de seguridad. Existen dos clases de ACL, ACL Estándar que bloquean o permiten el tráfico solo por direcciones de IP de origen y ACL Extendidas que bloquean por dirección de IP de origen y de destino y por puerto de origen y de destino. En consecuencia, las realizaciones de la presente solicitud incluyen almacenar las direcciones y puertos identificados.

En un sistema para controlar dinámicamente el tráfico de red, el sistema incluye un dispositivo generador de flujo configurado para acceder a un sistema de almacenamiento para proveer registros de flujo; un sistema de almacenamiento de registros de flujo configurado para recibir y almacenar los registros de flujo; y un dispositivo de análisis de datos configurado para acceder al sistema de almacenamiento y para evaluar los registros de flujo almacenados de acuerdo con criterios predefinidos. Si esos registros de flujo satisfacen los criterios predefinidos, esa dirección/puerto puede reenviarse a un usuario para que revise y apruebe que sea añadido en la ACL. Para ayudar al usuario, también se pueden presentar visualmente al usuario los datos del registro de flujo asociado con la dirección/puerto identificado.

En otra realización, las técnicas descritas en la presente invención describen un método para evaluar dirección/puertos en una ACL. En particular, registros de flujo asociados con una dirección/puertos en la ACL pueden ser evaluados de acuerdo con criterios predefinidos. Si esos registros de flujo satisfacen los criterios predefinidos, esa dirección/puerto puede reenviarse a un usuario para revisión y aprobación para ser renovado en la

ACL. De otro modo, si esos registros de flujo no satisfacen los criterios predefinidos y la dirección/puerto puede reenviarse a un usuario para revisar y aprobar que se retire de la ACL.

Breve descripción de los dibujos

Los anteriores y otros objetos, características y ventajas de ciertas realizaciones a modo de ejemplo de la presente invención serán más evidentes a partir de la siguiente descripción tomada junto con los dibujos que la acompañan en los que:

La figura 1A muestra una red a modo de ejemplo de acuerdo con realizaciones de la red de la presente invención;
La figura 1B (técnica anterior) muestra un sistema de análisis de registros de flujo conocido;
La figura 2 (técnica anterior) muestra un registro de flujo a modo de ejemplo conocido;
La figura 3 muestra una tabla a modo de ejemplo conocida para almacenar los registros de flujo de acuerdo con realizaciones de la presente invención;
La figura 4 muestra una tabla a modo de ejemplo para almacenar registros de flujo agregados de acuerdo con realizaciones de la presente invención;
La figura 5 muestra un sistema para crear ACL usando los datos de flujo de acuerdo con realizaciones de la presente invención;
La figura 6 es un diagrama de flujo de servicio que explica las comunicaciones entre un nodo de red, un sistema de control de acceso, y un sistema de almacenamiento de registros de flujo de acuerdo con realizaciones de la presente invención; y
La figura 7 es un diagrama de flujo que muestra las etapas en un método para crear ACL usando registros de flujo de acuerdo con realizaciones de la presente invención.

Descripción detallada de las realizaciones preferidas

Una red 100 de acuerdo con realizaciones de la presente invención se muestra en la figura 1A, en la que se muestra un diagrama de bloques que ilustra una vista de red de la presente invención, de acuerdo con una realización. Tal como se ilustra, los dispositivos cliente 108a - 108n se acoplan a servidores 110a - 110n a través del tejido de redes 112, el cual incluye un número de dispositivos de encaminamiento 106a - 106n acoplados entre sí formando una pluralidad de enlaces de red. Dispositivos cliente 108a - 108n, a través de los dispositivos de encaminamiento 106a - 106n, o más específicamente, sobre enlaces de red formados por dispositivos de encaminamiento 106a - 106n, accede a servidores selectivamente 110a - 110n para servicios. Desafortunadamente, como apreciarían los expertos en la materia, los mismos enlaces de red que hacen a los servidores 110a - 110n fácilmente accesibles a dispositivos de cliente 108a - 108n también los hace vulnerables al abuso o mal uso por uno o más de los dispositivos de cliente 108a- 108n. Por ejemplo, uno o más dispositivos de cliente 108a - 108n pueden comenzar, de forma individual o en combinación, un ataque, tal como un ataque de denegación de servicio, o abusar de otra manera de uno o más servidores 110a - 110n, dispositivos de encaminamiento 106a - 106b y/o los enlaces interconectando los elementos. De acuerdo con la presente invención, director 102, complementado por un número de sensores 104a - 104n, son empleados para detectar y prevenir dicho abuso o mal uso de los enlaces de red que serán descritos más extensamente a continuación. Para la realización ilustrada, los sensores 104a - 104n están dispuestos en ubicaciones distribuidas. En realizaciones alternas, algunos o todos los sensores 104a - 104n pueden ser dispuestos integralmente con dispositivos de encaminamiento 106a - 106b.

La red 112 representa un extenso rango de redes tanto privadas como públicas o redes interconectadas, tales como una red de empresa o de una corporación multinacional, o Internet. Los nodos de redes, tales como los clientes 108a- 108n y servidores 110a - 110n representan un amplio rango de estos elementos conocidos en la técnica, incluyendo máquinas de usuario individual, sitios de comercio electrónico, y similares. Tal como se aludió antes, los dispositivos de encaminamiento 106a - 106n representan un amplio rango de equipo de trafico de red, que incluye pero no se limita a encaminadores convencionales, conmutadores, pasarelas, concentrador y similares.

Mientras que para facilitar la comprensión, solo un director 102, y un puñado, cada uno de nodos de red, clientes 108a - 108n y servidores 110a - 110n, dispositivos de encaminamiento 106a - 106n y sensores 104a - 104n se incluyen en la ilustración, de la descripción a seguir, los expertos en la técnica apreciarán que la presente invención puede ponerse en práctica con más de un director 102 así como más o menos nodos de red, dispositivos de encaminamiento 106a - 106ny sensores 104a - 104n. En particular, la presente invención también se puede poner en práctica con uno o más directores 102. Cuando se emplea más de un director 102, a cada director 102 puede asignarse responsabilidad de un subconjunto de sensores 104a - 104n, y los directores 102 pueden relacionarse entre sí en una relación maestro/esclavo, con uno de los directores 102 sirviendo como el “maestro” (y los otros como “esclavo”), o como iguales uno del otro u organizados dentro de una jerarquía, para descarga colectiva de las responsabilidades descritas a continuación.

La operación del director 102 es descrito en mayor detalle a continuación y el director 102 incluye un sistema de conexión de datos de flujo y un dispositivo de control de acceso, tal como se describe más detalladamente a continuación.

Tal como se muestra en la figura 1B, un sistema de análisis de uso de red 111 incluye un servidor de sistema de recolección de datos 130 y un sistema de almacenamiento de datos 140, en una realización. El servidor de sistema de recolección de datos 130, también llamado oyente, es un servidor central que recopila los datagramas de flujo 190 de todos los diferentes agentes de red 120 para almacenaje y análisis. El servidor de sistema de recolección de datos 130 recibe registros de flujo 190 del dispositivo generador de registros de flujo 120, el cual es un dispositivo de red que es parte de una red de IP 114. En una realización, la red 114 incluye Internet 115.

En general, los dispositivos generadores de registros de flujo 120 pueden incluir sustancialmente cualquier dispositivo de red capaz de manejar tráfico en bruto de red en “líneas de velocidad” y generar registros de flujo de ese tráfico. Dispositivos de generación de registros de flujo 120 a modo de ejemplo incluyen encaminadores, conmutadores y pasarelas, y en algunos casos, puede incluir servidores de aplicaciones, sistemas, y sondas de red. En muchos casos, los registros de pequeños registros de flujo generados por dispositivos generadores de registros de flujo 120 se exportan como una cadena de registros de flujo 190 al servidor de sistema de recolección de datos 130.

Diversos protocolos de red corren en equipos de red para recopilar información del tráfico de red y del protocolo de Internet. Por lo general, diversos agentes de red 120, tales como encaminadores, tiene características de flujo habilitadas para generar registros de flujo. Los registros de flujo 190 se exportan por lo general del agente de red 120 en Protocolo de Datagramas de Usuario (UDP, *User Datagram Protocol*) o de paquetes de Protocolo de Transmisión de control de cadena (SCTP, *Stream Control Transmission Protocol*) y se recopilan usando un recopilador de flujo. Para mayor información, favor de referirse remitirse al estándar de Fuerza de Tarea de Ingeniería de Internet (IETF, *Internet Engineering Task Force*) para la exportación de información de flujo del Protocolo de Internet (IPFIX, *Internet Protocol Flow Information eXport*) en http://www.ietf.org/html.charters/ipfix-charter.html.

Tal como se ha descrito en lo que antecede, los registros de flujo 190 se envían usualmente por los agentes de red 120 a través de un UDP o SCTP, y por razones de eficiencia, los agentes de red 120 no almacenan registros de flujo una vez que ellos son exportados. Con un flujo UDP, si el registro de flujo 190 se cae debido a congestión de la red, entre el agente de red 120 y el servidor de recolección de datos 130, puede perderse para siempre debido a que no hay forma en que el agente de red 120 reenvíe el registro de flujo 190. El flujo puede ser habilitado también de una forma en función de la interfaz para evitar sobrecargar innecesariamente el procesador del encaminador. Por lo tanto, los registros de flujo 190 se basan en general en la entrada de paquetes a interfaces en las que está habilitado para evitar el doble conteo y para ahorrar trabajo para el agente de red 120. Asimismo, el agente de red 120 puede exportar un registro de flujo para paquetes caídos.

Los flujos de red han sido definidos de muchas maneras. En una implementación, un flujo incluye una tupla de 5: una secuencia unidireccional de paquetes para definir dirección de IP de origen, dirección de IP de destino, puerto de TCP de origen, puerto de TCP de destino y protocolo IP. Por lo general, el agente de red 120 arrojará un registro de flujo cuando determine que el flujo ha terminado. El agente de red 120 hace esto mediante “envejecimiento de flujo” reinicializando el agente de red 120 un contador de envejecimiento en el que el agente de red 120 observa nuevo tráfico para un flujo existente. Asimismo, la terminación de una sesión TCP en un flujo TCP causa que el agente de red 120 expire el flujo. EL agente de red 120 puede también ser configurado para arrojar un registro de flujo en un intervalo fijo aun si el flujo está todavía en marcha. Como alternativa, un administrador puede definir las propiedades del flujo en un agente de red 120.

Un registro de flujo 190 puede contener una amplia variedad de información sobre el tráfico en un flujo dado. Un registro de flujo a modo de ejemplo 200 contiene los siguientes valores, tal como se define en la figura 2. En particular, registros de flujo típicos 200 pueden incluir un número de versión 210 para identificar el tipo de flujo usado. Un número de secuencia 220 identifica el registro de flujo.

Continuando con la figura 2, se pueden usar índices 230 de protocolo de gestión de redes simple (SNMP, *simple network management protocol*) de interfaz de entrada y salida para identificar dinámicamente dispositivos de red a través del SNMP. El SNMP se usa por los sistemas de gestión de redes para supervisar dispositivos ligados a la red para condiciones que garanticen atención administrativa, y consiste en un conjunto de estándares para gestión de redes, incluyendo un protocolo de capa de aplicaciones, un esquema de base de datos y un conjunto de objetos de datos. El SNMP expone los datos de gestión en la forma de variables en los sistemas gestionados, los cuales describen la configuración del sistema. Por lo tanto, estas variables pueden consultarse (y en ocasiones ajustarse o establecerse) por aplicaciones de gestión. Los dispositivos modulares pueden reenumerar sus índices de SNMP siempre que se añade o se retira soporte físico ranurado. Los valores de los índices son asignados por lo general en el tiempo de inicio y permanecen fijos hasta el siguiente reinicio.

Continuando con la figura 2, cada uno de los registros de flujo 200 incluye adicionalmente por lo general información sobre la transmisión de datos, incluyendo una marca de tiempo de los tiempos de inicio y de fin 240. Otra información en los datos de transmisión incluye información sobre el número de bytes y/o paquetes en un flujo 250. Los condicionales de la transferencia de datos pueden incluirse también en el registro de flujo 200, tales como datos del encabezado 260 que describen las direcciones de origen y de destino, los números de puerto de las direcciones

de origen y de destino, el protocolo de transmisión, y el tipo de servicio (ToS). Para el Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*), el registro de flujo 200 puede indicar adicionalmente la unión de todos los indicadores de TCP durante el flujo. Como bien se conoce del TCP, una transmisión de datos involucra una serie de confirmaciones de comunicaciones, por ejemplo, por pares de indicadores de reconocimientos (ACK). Un desequilibrio de indicadores de TCP sugiere un fallo de mensaje, mediante lo cual un mensaje fue enviado y nunca recibido.

La falta de fiabilidad en el mecanismo de transporte UDP no afecta significativamente la precisión de las mediciones obtenidas de un flujo incluido en la muestra. Por ejemplo, si las muestras de flujo se pierden, entonces se enviarán nuevos valores cuando el siguiente intervalo de sondeo haya pasado. De esta forma, la pérdida de muestras de flujo de paquete es una ligera reducción en la tasa de muestreo efectivo. Cuando se emplea el muestreo, la carga útil de UDP contiene el datagrama de flujo muestreado. Por lo tanto, en lugar de incluir un registro de flujo entero 190 cada datagrama en su lugar proporciona información tal como la versión del flujo, su dirección de IP del agente originador, un número de secuencia, cuántas muestras contiene y las muestras de flujo.

Continuando con la figura 1B, el servidor de sistema de recolección de datos 130 recibe los registros de flujo encadenados 190 del dispositivo de generación de registros de flujo 120 a través de un enlace de comunicación 170. En una realización, el dispositivo de generación de registros de flujo 120 puede incluirse dentro de la red 114. En otra realización, el dispositivo de generación de registros de flujo 120 puede implementarse en una ubicación físicamente apartada, aunque funcionalmente acoplado a, la red 114. A pesar de que se muestra en la figura 1 como separado del servidor de sistema de recolección de datos 130, el dispositivo de generación de registros de flujo 120 puede ser una parte del servidor de sistema de análisis de datos 130, en otra realización.

Un servidor de sistema de análisis de datos 150 accede a, y usa, los registros de flujo 190 para realizar un análisis estadístico del uso de red predeterminado. En general, el servidor de sistema de análisis de datos 150 implementa diversos modelos estadísticos que están definidos para resolver uno o más problemas relacionados con el uso de red, tales como congestión de la red, abuso de la seguridad de la red, fraude y robo, entre otros. El servidor de sistema de análisis de datos 150 usa registros de flujo 190 y los modelos estadísticos para generar un resultado estadístico, el cual también se puede almacenar subsecuentemente dentro de un sistema de almacenamiento de datos 140. Realizaciones a modo de ejemplo para almacenar el resultado estadístico serán descritas en más detalle a continuación. Analizando datos de flujo, el servidor de sistema de análisis de datos 150 puede construir una imagen del flujo del tráfico y del volumen de tráfico en una red. El solicitante del sistema de análisis de datos 150 es descrito en mayor detalle a continuación.

En un aspecto, el servidor de sistema de análisis de datos 150 puede ser sensible a una interfaz de usuario 160 para análisis interactivo de los registros de flujo 190. La interfaz de usuario 160 puede comprender sustancialmente cualquier dispositivo de entrada/salida conocido en la técnica, tales como un teclado, un ratón, un almohadilla táctil, una pantalla de presentación visual, etcétera. En un ejemplo, una pantalla o visualizador gráfico de los resultados estadísticos puede ser arrojado a una pantalla de presentación visual en una interfaz de usuario 160.

En una realización, el servidor de sistema de análisis de datos 150 comprende un programa de soporte lógico informático, el cual es ejecutable en uno o más ordenadores o servidores para analizar los datos de uso de la red de acuerdo con diversas realizaciones de la invención. A pesar de que el sistema de almacenamiento de datos 140 se muestra como externo al servidor de sistema de recolección de datos 130 y/o el servidor de sistema de análisis de datos 150, el sistema de almacenamiento de datos 140 podría arreglarse, como alternativa, dentro de cualquiera de los servidores 130 y 150. El sistema de almacenamiento de datos 140 puede comprender sustancialmente cualquier memoria volátil (por ejemplo, RAM) o memoria no volátil (por ejemplo, una unidad de disco duro u otro dispositivo de almacenaje persistente) conocido en la técnica.

Refiriéndose ahora a la figura 3, se presenta una tabla a modo de ejemplo 300 para almacenar múltiples registros de flujo 200 en un dispositivo de almacenamiento 140. En particular, la tabla mostrada 300 incluye una columna que asigna un identificador de registro de flujo 310 para cada uno de los n registros de flujo recibidos 200. La tabla 300 también incluye una columna que contiene una dirección de IP de origen 320 para cada uno de los registros de flujo recibidos 200, una columna que contiene una marca de tiempo 330 para cada uno de los registros de flujo recibidos 200, y una columna que contiene un tamaño de byte 340 en los flujos asociados con los registros de flujo recibidos 200.

En el ejemplo de la figura 3, la tabla de flujo a modo de ejemplo 300 incluye siete registros de flujo que describen siete flujos, como se indica por el identificador de registro de flujo 310. En este particular ejemplo, los siete flujos fueron originados en tres únicas direcciones de origen 320. Por ejemplo, los registros de flujo 1, 2, 3, y 7 fueron todos originados de las mismas fuentes. A pesar de que no se muestran, la tabla de flujo a modo de ejemplo 300 podría similarmente incluir otros aspectos del registro de flujo 200, tal como se ha descrito en lo que antecede en la figura 2, tales como la ubicación de destino, QoS, protocolo de transmisión, etc. Continuando con la tabla de flujo a modo de ejemplo 300 en la figura 3, un valor de marca de tiempo 330 indica un tiempo asociado con cada uno de los flujos y valor de tamaño de bytes 340 para indicar el tamaño de cada uno de los flujos asociados con los registros de flujo listados 1 - 7 identificados en la columna 310.

Refiriéndose ahora a la figura 4, los datos en la tabla de datos de flujo a modo de ejemplo 300 se agregan en la tabla de flujo agregada 400 de acuerdo con la dirección de IP de origen 4240. Por lo general, la agregación es hecha sobre uno o más periodos de tiempo predefinidos. Por ejemplo, la tabla de flujo agregada 400 a modo de ejemplo incluye una columna que con el número agregado de registros de flujo 410 asociada con cada una de las direcciones de IP de origen 420 en la tabla 300. La tabla de flujo agregada 400 indica adicionalmente el total de tamaño de byte de los flujos para cada una de las direcciones de IP de origen 420 en la tabla 300. Aplicaciones de la tabla de flujo agregada 400 son descritas a continuación. Como con la tabla de registro de flujo 300, debería de apreciarse que los registros de flujo 190 se pueden agregar según se desee, por ejemplo de acuerdo con una o más de las categorías de registros de flujo descritas en el registro de flujo a modo de ejemplo 200 en la figura 2.

Refiriéndose ahora a la figura 7, se describe ahora un método de control de acceso 700 de acuerdo con realizaciones de la presente invención. En la etapa 710, el tráfico en los componentes de red son supervisores de acuerdo con técnicas conocidas, tal como se ha descrito en lo que antecede, y registros de flujo se recopilan en la etapa 720. Por lo general, las etapas 710 y 720 se pueden ejecutar usando las funcionalidades ya incluidas en muchos componentes de red, tales como encaminadores, concentrador, servidores, etc. y se pueden usar para recopilar y almacenar un registro de flujo, tal como la tabla de registro de flujo a modo de ejemplo 300. Los registros de flujo recopilados de la etapa 720 son analizados en la etapa 730. Por ejemplo, los registros de flujo se pueden agregar, tal como la formación de una tabla de registros de flujo agregados 400 descrita en lo que antecede.

Continuando con el método de control de acceso 700, las condiciones de control de acceso se definen en la etapa 740. Las condiciones de control de acceso previamente definidas por omisión se pueden usar para evaluar a los registros de flujo. Por ejemplo, direcciones o puertos asociados con un cierto porcentaje o cantidad de tráfico pueden identificarse. Por ejemplo, el acceso se puede limitar para las direcciones de IP de origen 420 basándose en el mayor número de transacciones 410, tiempos de los 330, o la mayor cantidad de datos transferidos 430. Estos criterios pueden ser objetivos tales como establecer un máximo umbral para ciertos criterios, o subjetivo basándose en clasificaciones de los criterios por la dirección de IP o puerto de origen o de destino con los mayores o más frecuentes consumidores de recursos de red (u otros criterios). Opcionalmente, los criterios pueden ser proporcionados por un usuario.

La dirección de IP de origen u objetivo y/o el puerto que cumple con estos criterios puede ser identificada en la etapa 750 usando simple lógica. En la etapa 760, la dirección de IP de origen o de destino identificada y/o identificadores de puerto pueden presentarse a un usuario. Estas direcciones de IP de origen (u otros identificadores de dispositivos) para los dispositivos de red identificados pueden entonces colocarse en una ACL en la etapa 770 para solicitar dispositivos de red para ignorar o de otra manera denegar el transmitir tráfico asociado con puertos/direcciones identificados, si son aprobados por un usuario.

Refiriéndose ahora a la figura 5, un sistema de control de acceso 500 de acuerdo con realizaciones de la presente invención es ahora descrita. Tal como se ha descrito en lo que antecede, un sistema de almacenamiento de datos de flujo 140 puede recibir los registros de flujo en bruto 190. El sistema de almacenamiento de datos de flujo 140 puede agregar los registros de flujo 190, tal como se ha descrito en lo que antecede, en diversas maneras conocidas para alcanzar las metas de sistema o los registros de flujo se pueden almacenar en una forma en bruto. La herramienta de análisis de datos 150 puede acceder a, y evaluar, los registros de flujo de acuerdo con criterios recibidos y/o definidos a través de la interfaz de usuario 160 para definir direcciones/puertos de red para añadirse a las ACL. De manera similar, debería apreciarse que los puertos/direcciones que no cumplen con los criterios predefinidos sobre un periodo de tiempo pueden ser también identificados de forma automática y sugerir al usuario retirarlos de las ACL. Por lo general, cualquier dirección en los registros de flujo o direcciones en la ACL identificados dinámicamente de acuerdo con criterios predefinidos se reenvía a la interfaz de usuario para ser revisado por un administrador. El administrador puede entonces aprobar la adición/remoción del puerto/dirección identificado de la ACL.

Las ACL 590 en un dispositivo de red 520 u, opcionalmente, se pueden almacenar en un sistema de almacenamiento de ACL 530 y reenviar a cualquier dispositivo de red 520 que recibe tráfico a través de las LAN 510 o Internet 115. El dispositivo de red 520 por lo general deniega reenviar cualquier tráfico asociado con un dispositivo identificado en la ACL o bien en el dispositivo 520 o bien en el almacenamiento de ACL opcional 530. Es decir, el tráfico destinado a y/u originándose de una dirección en la ACL llega al dispositivo 520 y no se reenvía a través de las redes 510, 115. Cuando las comunicaciones del tráfico caducan, la comunicación se retira del almacenamiento y nunca alcanza un destino indicado.

Refiriéndose ahora al diagrama de flujo de servicio 600 en la figura 6, un nodo de red 610 puede reenviar informes de flujo 650 que describen el tráfico de red a un sistema de supervisión de red 620. Tal como se ha descrito en lo que antecede, el sistema de supervisión de red 620 puede recopilar y almacenar los registros de flujo 650. Puede accederse a los registros de flujo almacenados 660 por un sistema de control de acceso 630 que evalúa los registros de flujo almacenados 660 de acuerdo con criterios predefinidos para identificar de forma automática direcciones/puertos de red. Las direcciones identificadas se reenvían a una interfaz de usuario 640 para ser revisados. Si la dirección/puerto identificado es aceptado por el usuario, la dirección/puerto puede ser enviado al nodo de red 610 como datos de actualización de ACL 680 para implementación del ACL.

Aunque la invención ha sido descrita con referencia a unas realizaciones a modo de ejemplo, diversas adiciones, supresiones, sustituciones u otras modificaciones pueden hacerse sin apartarse del alcance de la invención. En consecuencia, no debe considerarse que la invención se limita por la descripción anterior, sino que solo está limitada por el alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema (500) para controlar dinámicamente comunicaciones de redes, comprendiendo el sistema:

un dispositivo de red (520) configurado para recibir tráfico de red y para producir una pluralidad de registros de flujo que describen dicho tráfico de red; y
un almacenamiento de registro de flujo (140) configurado para recibir dichos registros de flujo de dicho dispositivo de red (520) y para almacenar dichos registros de flujo; caracterizado por
una herramienta de análisis de datos (150) configurada para acceder al almacenamiento de registro de flujo (140) para recuperar dichos registros de flujo almacenados y para evaluar cada uno de dichos registros de flujo de acuerdo con criterios predefinidos para identificar dinámicamente una dirección, en el que la herramienta de análisis de datos está configurada adicionalmente para implementar modelos estadísticos configurados para resolver problemas relacionados con el uso de red, y en el que la herramienta de análisis de datos usa los registros de flujo y modelos estadísticos para generar un resultado estadístico que se almacena entonces en el almacenamiento de registros de flujo;
en el que cada uno de dicha pluralidad de registros de flujo comprende al menos uno de una dirección de nodo de origen, una dirección de nodo de destino, una dirección de puerto de origen y una dirección de puerto de destino,
en el que dichos registros de flujo comprenden un tamaño de byte transmitido en cada flujo asociado, y en el que los criterios predefinidos comprenden el número total de bytes transmitidos en el flujo asociado para cada una de las direcciones de nodo o de puerto,
en el que el dispositivo de red (520) está configurado para recibir dicha dirección identificada y para añadir dicha dirección identificada a una lista de control de acceso.

2. El sistema de la reivindicación 1, que comprende adicionalmente un almacenamiento de lista de control de acceso (530) configurado para almacenar dicha dirección identificada y para proporcionar dicha dirección identificada al dispositivo de red (520).

3. El sistema de la reivindicación 1, en el que dichos registros de flujo se agregan de acuerdo con dichas direcciones de nodo y/o de puerto.

4. El sistema de la reivindicación 1, que comprende adicionalmente un dispositivo de entrada/salida (160) configurado para presentar visualmente a un usuario dicha dirección identificada recibida de la herramienta de análisis de datos (150), y en el que la herramienta de análisis de datos está configurada para reenviar la dirección identificada al dispositivo de red (520) para que se añada a la lista de control de acceso solo si el usuario proporciona una entrada para aceptar la dirección identificada.

5. El sistema de la reivindicación 1, en el que el dispositivo de entrada/salida (160) adicionalmente adquiere y presenta visualmente datos de registros de flujo asociados con dicha dirección identificada.

6. Un método para gestionar redes que comprende:

supervisar (710) tráfico a través de componentes en la red;
recibir (720) registros de flujo de dichos componentes que describen dicho tráfico; caracterizado por
analizar (730) los registros de flujo e identificar una dirección que cumple con un criterio previamente definido, en el que el criterio previamente definido comprende un número total máximo de bytes asociados con una dirección; y
reenviar la dirección identificada a uno de los componentes de red, en el que dicho componente añade la dirección de red identificada a una lista de control de acceso asociada, en el que dicha lista de control de acceso dirige el componente para evitar el reenvío de tráfico asociado con dicha dirección identificada.

7. El método de la reivindicación 6, en el que dicha dirección identificada se retira de forma automática de la lista de control de acceso después de un periodo de tiempo previamente definido.

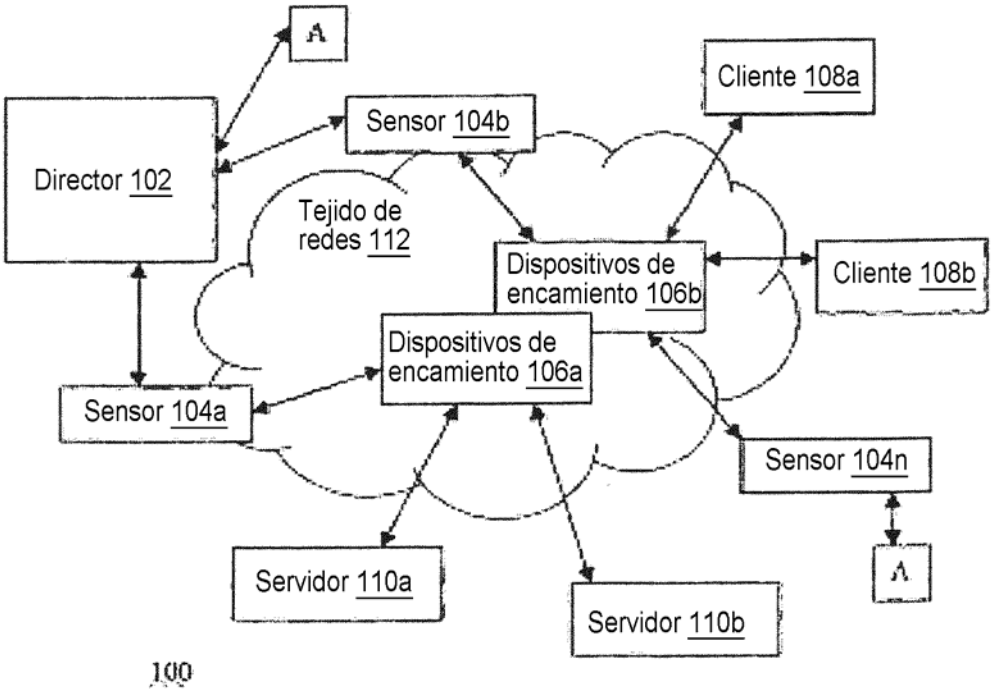
8. El método de la reivindicación 6, en el que dicha dirección identifica al menos uno de un nodo de origen, un nodo de destino, un puerto de origen y un puerto de destino.

9. El método de la reivindicación 8, en el que dicha dirección identifica un nodo de origen.

10. El método de la reivindicación 6, que comprende adicionalmente presentar visualmente (760) a un usuario dicha dirección identificada, y mediante lo cual el reenvío de la dirección identificada tiene lugar después de que el usuario apruebe la dirección identificada.

11. El método de la reivindicación 10, que comprende adicionalmente presentar visualmente al usuario datos de registros de flujo asociados con dicha dirección identificada.

Figura 1A


A
Director 102
Sensor 104b
Cliente 108a
Tejido de redes 112
Dispositivos de encamiento 106b
Cliente 108b
Dispositivos de encamiento 106a
Sensor 104a
Sensor 104n
A
Servidor 110a
Servidor 110b
100

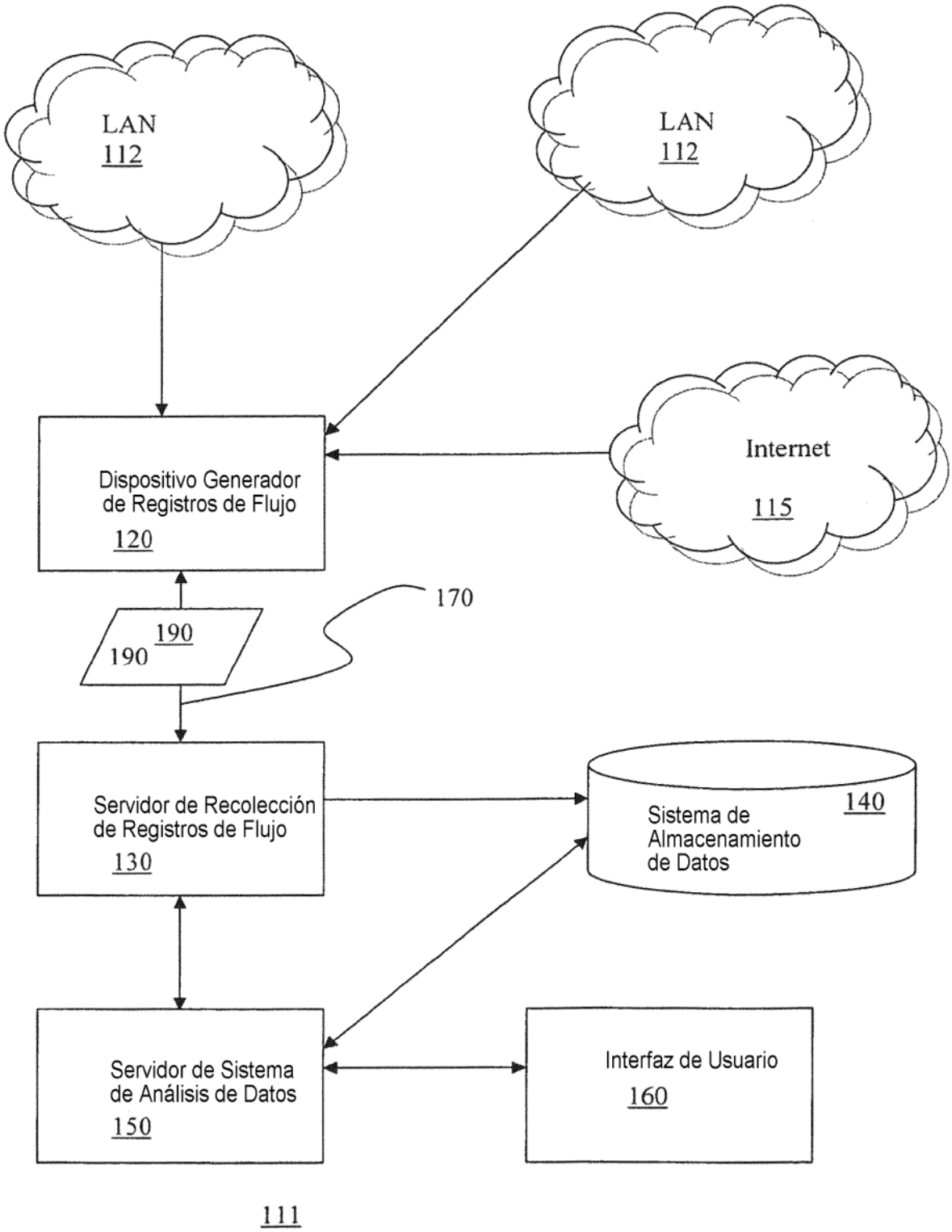


Figura 1B
(Técnica Anterior)

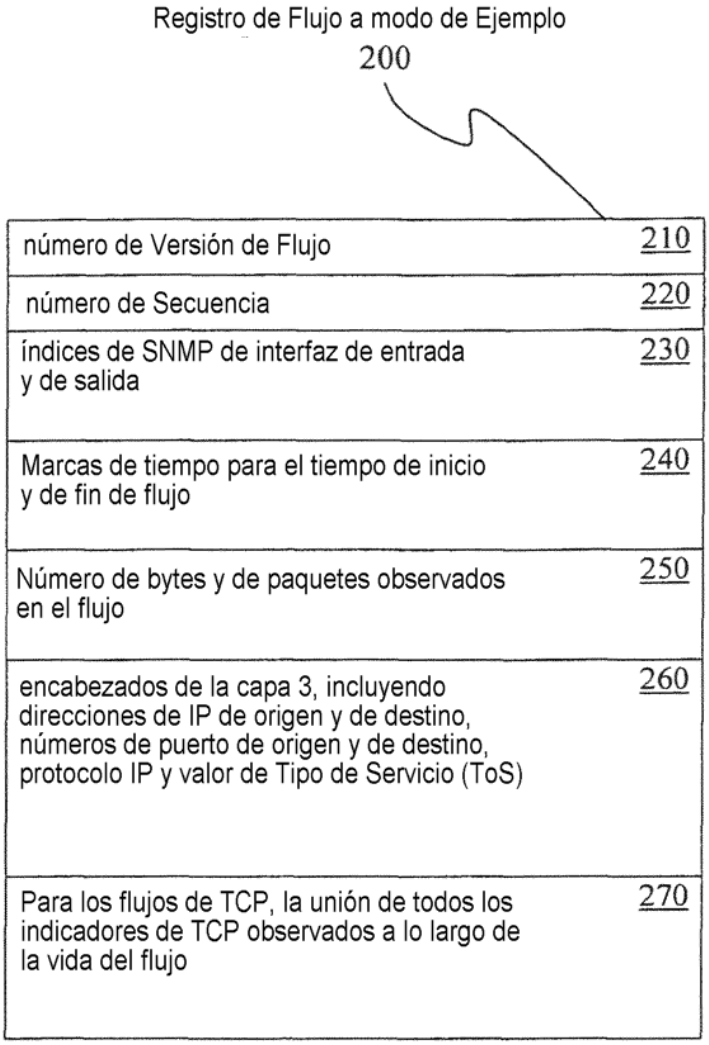


Figura 2
(TÉCNICA ANTERIOR)

Número de Registro de Flujo 310	Dirección de IP de Origen 320	Marca de Tiempo 330	Tamaño en Bytes 340
1	xxx.xxx.x.1	t_1	10
2	xxx.xxx.x.1	t_2	20
3	xxx.xxx.x.2	t_3	1000
4	xxx.xxx.x.2	t_4	2000
5	xxx.xxx.x.1	t_5	30
6	xxx.xxx.x.3	t_6	10
7	xxx.xxx.x.1	t_7	40

Tabla de Flujo a Modo de Ejemplo 300

Figura 3

Número de Números de Registro de Flujo 310	Dirección de IP de Origen 420	Tamaño en Bytes Total 430
4	xxx.xxx.x.1	100
2	xxx.xxx.x.2	3000
1	xxx.xxx.x.3	10

Tabla de Flujo Agregada 400

Figura 4

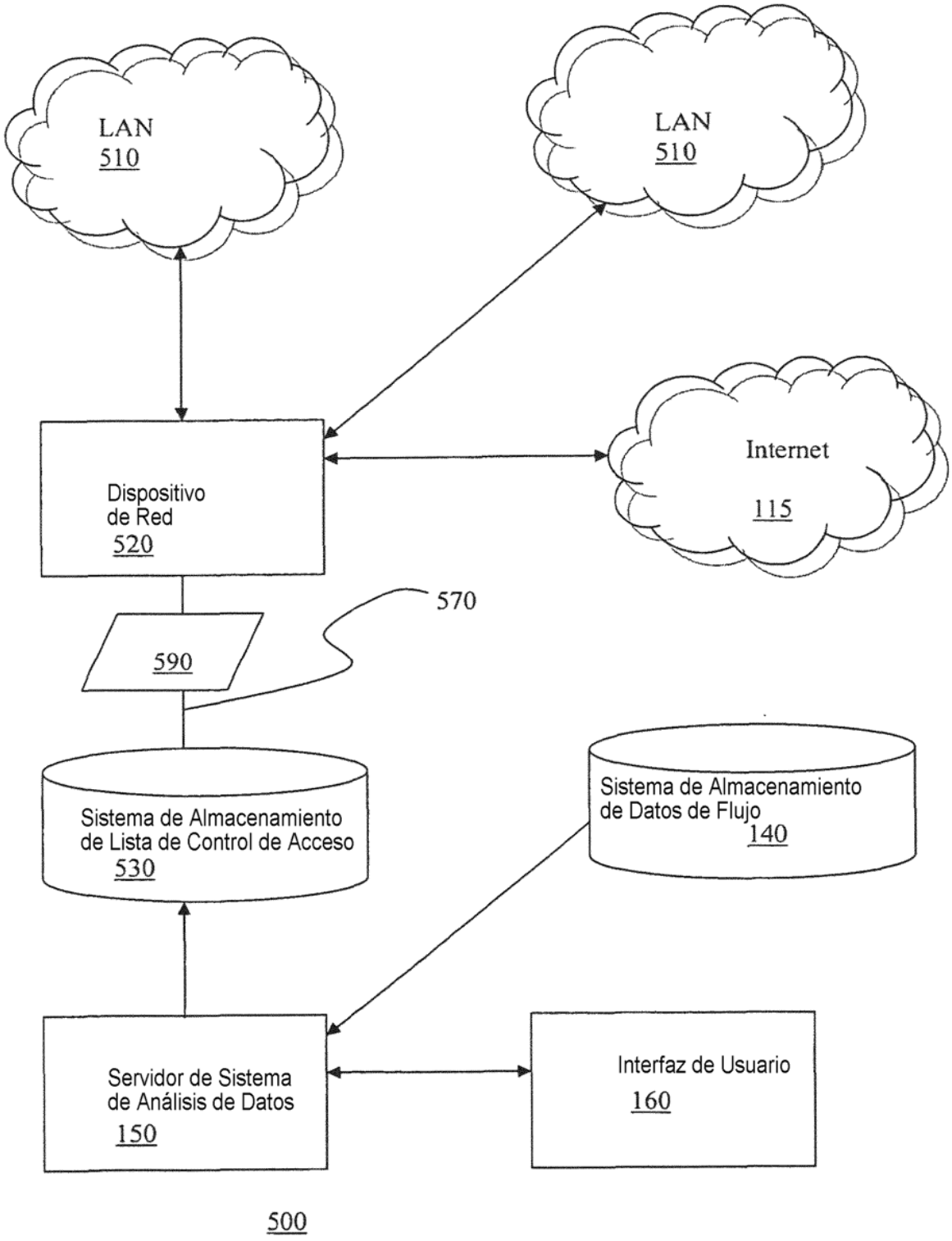

LAN
510
LAN
510
Internet
115
Dispositivo
de Red
520
570
590
Sistema de Almacenamiento
de Lista de Control de Acceso
530
Sistema de Almacenamiento
de Datos de Flujo
140
Servidor de Sistema
de Análisis de Datos
150
Interfaz de Usuario
160
500

Figura 5

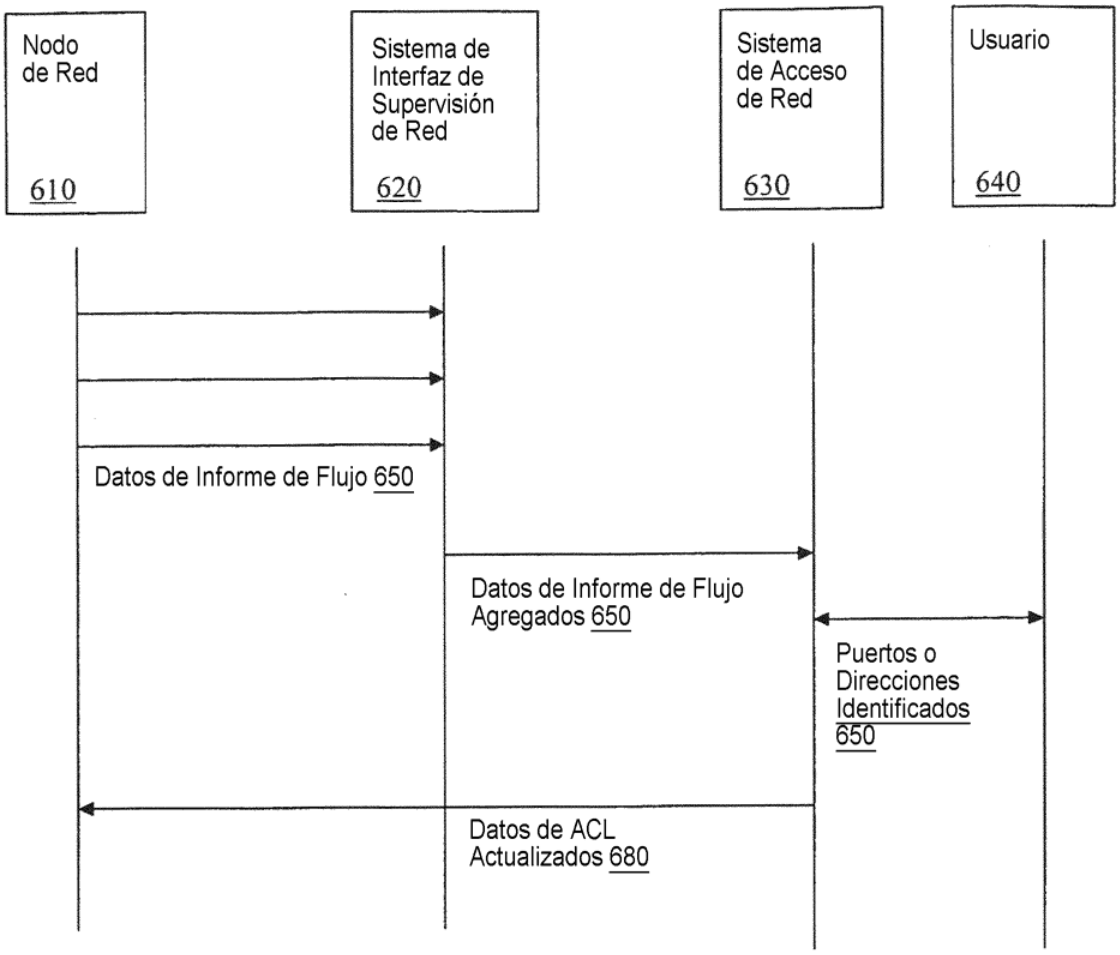

Nodo de Red
610
Sistema de Interfaz de Supervisión de Red
620
Sistema de Acceso de Red
630
Usuario
640
Datos de Informe de Flujo 650
Datos de Informe de Flujo Agregados 650
Puertos o Direcciones Identificados 650
Datos de ACL Actualizados 680
600

Figura 6

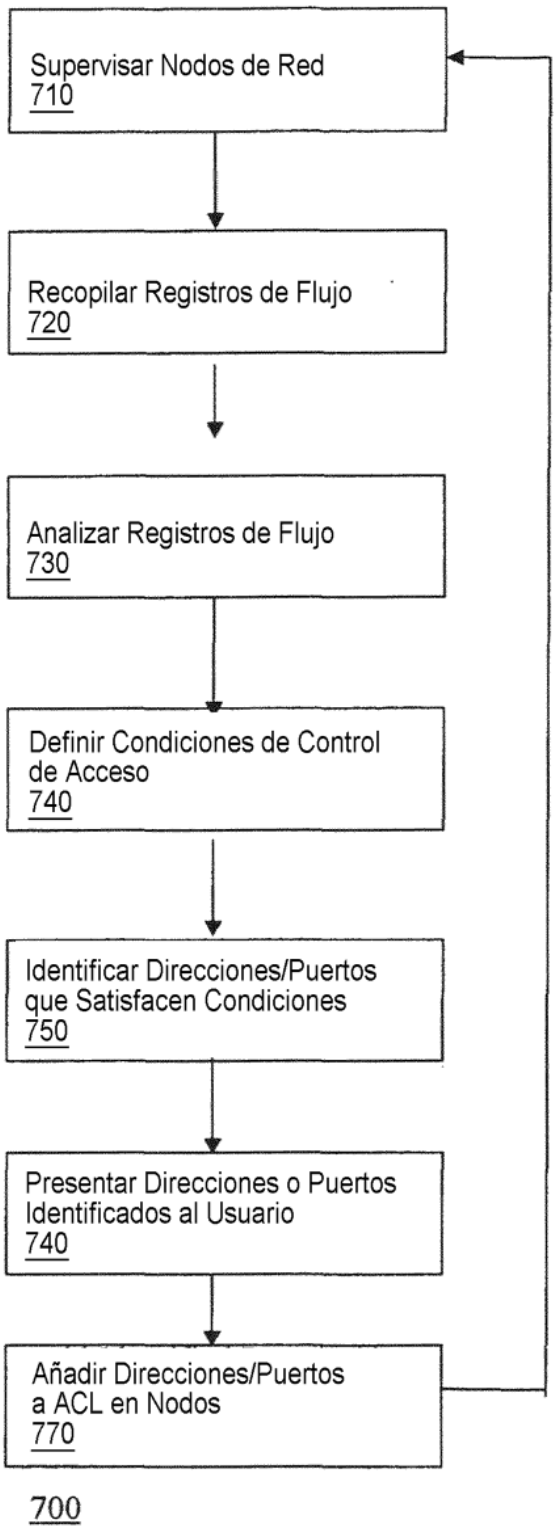

Supervisar Nodos de Red
710
Recopilar Registros de Flujo
720
Analizar Registros de Flujo
730
Definir Condiciones de Control de Acceso
740
Identificar Direcciones/Puertos que Satisfacen Condiciones
750
Presentar Direcciones o Puertos Identificados al Usuario
740
Añadir Direcciones/Puertos a ACL en Nodos
770
700

Figura 7